Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

ЗАЩИТА ОБЪЕКТОВ СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Рекомендовано УМО вузов Республики Беларусь по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для студентов учреждений, обеспечивающих получение высшего образования по специальности «Защита информации в телекоммуникациях»

Минск БГУИР 2010

УДК 004.056(076)
ББК 32.973.202я7
З-40

А в т о р ы:
Л. М. Лыньков, Т. В. Борботько, Б. И. Беляев, Л. В. Катковский

Р е ц е н з е н т ы:
заместитель заведующего лабораторией оптической диагностики
Института физики НАН Беларуси,
доктор физико-математических наук В. Н. Белый;

заведующий кафедрой управления информационными ресурсами Учреждения образования «Академия управления при Президенте Республики Беларусь»,
кандидат технических наук, доцент В. И. Новиков

Защита объектов связи от несанкционированного доступа . Лабо-
З-40 раторный практикум : учеб.-метод. пособие / Л. М. Лыньков [и др.]. – Минск. : БГУИР, 2010. – 79 с.
ISBN 978-985-488-491-2

Практикум состоит из пяти лабораторных работ, каждая из которых содержит краткие теоретические сведения к темам курса, ход выполнения лабораторного задания, требования к оформлению отчета и вопросы для самоконтроля, ответы на которые контролируются программной экспертной системой. При выполнении работ реализована возможность автоматизации контроля знаний студентов.

УДК 004.056(076)
ББК 32.973.202я7

ISBN 978-985-488-491-2

СОДЕРЖАНИЕ

ЛАБОРАТОРНАЯ РАБОТА №1
ОБНАРУЖЕНИЕ СРЕДСТВ ТЕХНИЧЕСКОЙ РАЗВЕДКИ С ПОМОЩЬЮ НЕЛИНЕЙНОГО ЛОКАТОРА

Цель: изучить демаскирующие признаки закладных устройств, методику поиска средств технической разведки с помощью нелинейного локатора, получить практические навыки по поиску средств технической разведки с использованием модели нелинейного локатора, реализованной программным методом.

1.1. Теоретическая часть

1.1.1. Обнаружение закладных устройств

Закладное устройство – автономное устройство, конструктивно объединяющее в себе приемный и передающий модули с источником питания и предназначенное для перехвата речевой информации.

Наиболее информативные прямые и косвенные демаскирующие признаки закладных устройств приведены в табл. 1.1.

Таблица 1.1

Демаскирующие признаки закладных устройств

Вид признака	Наименование признака
1	2
Видовой	Тонкий провод от миниатюрного микрофона, уходящий в соседнее помещение; малогабаритный предмет в виде параллелепипеда, цилиндра или иной формы с проводом (антенной); одно или несколько отверстий малого диаметра в корпусе; свежие царапины на элементах крепления технических средств; несоответствие топологии схемы радиоэлектронного устройства документации или топологии других однотипных образцов; несоответствие рентгеновского изображения конструкции ее назначению

Окончание табл. 1.1

1	2
Сигнальный	Наличие радио- и ИК-излучений; электрический сигнал в проводе частотой десятки-сотни кГц и более; АМ и ЧМ несущего колебания с речевым сигналом, ширина полосы сигнала-десятки, реже сотни кГц; случайные изменения напряжения в телефонной линии; емкости, индуктивности, дополнительные неоднородности в телефонной линии
Вещественный	Нелинейность элементов и металлические детали в малогабаритной конструкции; непрозрачность рентгеновским лучам, пустота в твердой среде с неизвестным вложением

1.1.2. Способы обнаружения закладных устройств

В зависимости от демаскирующих признаков закладных устройств методы их поиска можно разделить на 3 группы (рис. 1.1).

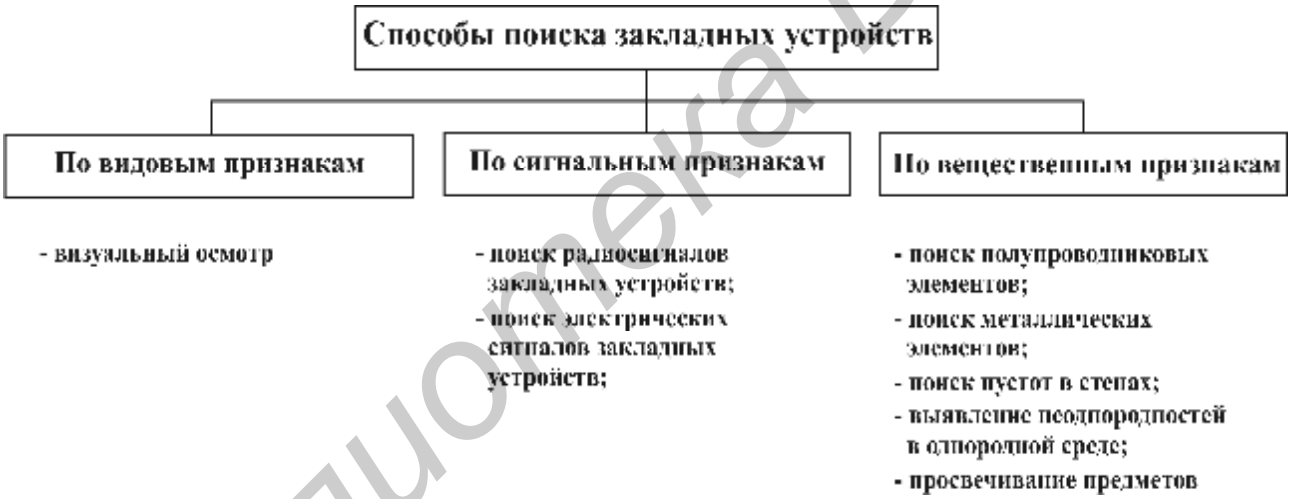


Рис. 1.1. Способы поиска закладных устройств

Поиск закладных устройств по видовым признакам осуществляется путем визуального осмотра помещения сотрудниками службы безопасности или иными сотрудниками. Визуальный осмотр требует минимальных затрат по сравнению с другими и может производиться периодически как силами службы безопасности, так и секретарем руководителя организации или иного должностного лица.

Сущность поиска закладки путем визуального осмотра состоит в тщательном осмотре помещения, предметов мебели, компьютера, радио- и электробытовых устройств, телефонных аппаратов, устройств громкоговорящей и

диспетчерской связи, картин на стенах, портьер и жалюзи, других предметов в помещении на предмет наличия в них закладных устройств. Осмотр проводится без разборки рассматриваемого предмета.

В целях обеспечения полноты визуального контроля целесообразно проводить его по определенной схеме, аналогичной схеме осмотра места происшествия криминалистами: от двери по или против часовой стрелки от периферии к центру помещения. Во время смотра обращается внимание на свежие царапины на обоях, возле сетевых и телефонных розеток и выключателей освещения, на стенах, винтах корпуса телефонного аппарата, на пылевые следы смещения картины или других предметов, на отрезки проводов и на другие следы или непонятные на первый взгляд предметы.

Для визуального осмотра при поиске закладных устройств применяют различное вспомогательное оборудование. Это оборудование, имея невысокую стоимость, позволяет повысить вероятность обнаружения закладки в ходе визуального осмотра помещения. К такому оборудованию относятся фонари, досмотровые зеркала и технические эндоскопы.

Поиск закладных устройств, вмонтированных в технические средства, производят в ходе специальных исследований путем сравнения топологии схемы исследуемого образца с эталонной, зафиксированной в документации или в топологии образца, в котором заведомо отсутствует закладное устройство. Для обеспечения неразрушающего контроля применяются специальные рентгеновские установки, позволяющие наблюдать изображения отдельных слоев микросхем и многослойных печатных плат.

Остальные методы предусматривают поиск закладных устройств дистанционно с использованием различных технических средств, способных обнаруживать сигнальные и вещественные демаскирующие признаки таких устройств. Так как наиболее распространены радиоизлучающие закладные устройства, то их поиск производится путем обнаружения сигнальных демаскирующих признаков радиоизлучающих закладных устройств.

Наиболее широко применяются следующие методы поиска закладных устройств по их прямым и косвенным сигнальным демаскирующим признакам:

– поиск источников радиоизлучений, мощность которых превышает мощность электромагнитного фона;

– поиск и селекция радиосигналов по частоте с последующей идентификацией их текущей признаковой структуры с эталонной признаковой структурой закладного устройства;

– поиск проводных закладных подслушивающих устройств по косвенным признакам изменений электрических характеристик линий, к которым подключены эти устройства.

Учитывая повсеместное распространение телефонов как средств коммуникаций и особый интерес злоумышленников к подслушиванию телефонных разговоров, при обеспечении защиты информации большое внимание уделяется способам и средствам контроля телефонных линий.

После обнаружения закладного устройства его необходимо изъять, разрушить или использовать для дезинформирования. Для изъятия закладного устройства из стены ее приходится вскрывать. Так как достоверность идентификации закладного устройства в железобетонной стене мала, то разрушения стены во время его поиска могут быть весьма существенны. Для повышения достоверности обнаружения закладных устройств в железобетонных стенах применяют также обнаружители естественных и искусственных пустот, в которых могут быть размещены закладные устройства, а также рентгеновские установки (интерсепторы).

Для обнаружения пустот применяются средства – обнаружители пустот, которые реагируют на отличия диэлектрической проницаемости или теплопроводности воздуха (пустоты) и бетона. Измерительная катушка генератора обнаружителя пустоты локализует место в однородной среде (стене) – пустоту, диэлектрическая проницаемость которого отличается от диэлектрической проницаемости вещества среды. Также будут отличаться температура внутри пустоты

и бетона в нагретом солнечными лучами или обогревателем помещении. Границы пустот будут видны на экране тепловизора.

1.1.3. Обнаружение закладных устройств с помощью нелинейного локатора

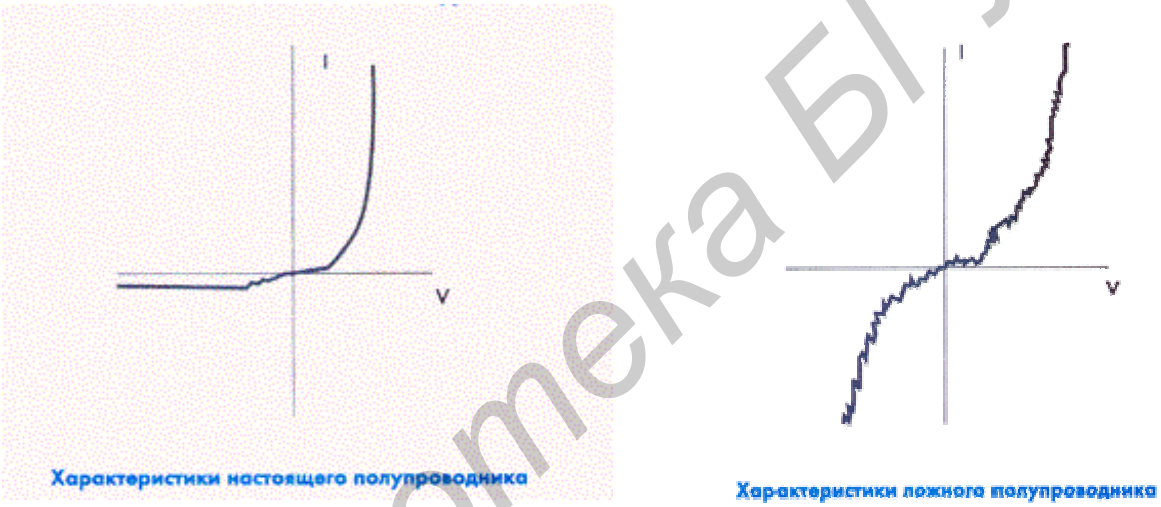
Поиск и обнаружение дистанционно управляемых и пассивных (параметрических) закладных устройств производятся по прямым и косвенным признакам входящих в их состав веществ. Прямыми признаками закладных устройств является наличие в них полупроводниковых и металлических элементов. Косвенный признак установки закладного устройства в стене или иной твердой среде – наличие в них пустоты.

Так как любое радиоэлектронное закладное устройство содержит полупроводниковый элемент (транзистор, диод), то наиболее информативным признаком не излучающего во время поиска закладного устройства является наличие полупроводниковых элементов в местах, в которых не должно быть радиоэлектронных устройств. Такими местами являются стены, мебель, картины, подвесные потолки и др. Для обнаружения полупроводникового элемента используются нелинейные свойства его вольт-амперной характеристики – зависимость тока, протекающего по p-n-переходу полупроводника, от величины подводимого к нему напряжения (рис. 1.2, а, б). Вихревые электрические токи через p-n-переходы полупроводников возникают при облучении проводника электромагнитным полем. Поле создает антенна передатчика нелинейного локатора, излучающего непрерывные гармонические или импульсные сигналы на частоте f, составляющие для разных локаторов доли и единицы ГГц (400–1000 МГц). В силу нелинейности полупроводника токи в нем имеют форму, отличную от гармонического колебания, и могут быть разложены в ряд Фурье. Вихревые токи создают вторичное электромагнитное поле, содержащее кроме электромагнитной волны на основной частоте f также волны с частотой $2f$, $3f$ и других частотах спектра вторичного сигнала. В отличие от классического радиолокатора нелинейный локатор имеет приемник, настроенный на частоту $2f$, а в некоторых

типах – дополнительный приемник на частоте 3*f*. Появление в отраженном сигнале колебаний с частотами 2*f* и 3*f* позволяет сделать вывод о наличии в области облучения зондирующей электромагнитной волны элементов с нелинейной вольт-амперной характеристикой. Мощность сигнала на второй гармонике в приемной антенне нелинейного локатора определяется по формуле

$$P_2 = \frac{\left(P_з G_п\right)^2 S_{эф}}{\left(4\pi R^2\right)^3}, \quad (1.1)$$

где $P_з$ – мощность зондирующего импульса; $G_п$ – коэффициент усиления передающей антенны; $S_{эф}$ – эффективная площадь приемной антенны нелинейного локатора; R – расстояние от локатора до обследуемой поверхности.



а б

Рис. 1.2. Характеристики нелинейных соединений

На практике достоверность обнаружения полупроводникового элемента снижается в связи с тем, что нелинейными свойствами обладают не только полупроводниковые элементы, но и места контактов металлических предметов и конструкций помещения и здания: ржавой арматуры железобетонных стен, гвоздей и болтов мебели, даже скрепок для бумаги.

Поэтому для обнаружения полупроводников приходится учитывать различия в мощности сигналов на частотах 2*f* и 3*f*, отраженных от полупроводников и окисленных металлических конструкций и предметов. Эти различия обусловлены разной формой нелинейных вольт-амперных характеристик полупро-

водниковых и других элементов, что приводит к различиям амплитуд гармоник спектров отраженных сигналов. Для настоящих полупроводников уровень второй гармоники в среднем на 20 дБ превышает уровень 3-й гармоники, для ложных – соотношения противоположны. Но эти отличия не столь существенны для формального однозначного принятия решения о наличии в рассматриваемой области полупроводника, а не иного элемента с нелинейной вольт-амперной характеристикой. Поэтому вероятность идентификации полупроводника тем выше, чем более опытным является оператор, проводящий поиск закладного устройства.

Для повышения достоверности обнаружения полупроводниковых элементов используется нестабильность вольт-амперных характеристик «ложных» полупроводников при механическом воздействии (ударе) по ним. Это связано с тем, что при ударе нарушается контакт между металлическими поверхностями или разрушается пленка оксида, кроме того, при облучении работающего закладного устройства переотраженный им сигнал модулируется по амплитуде первичным информационным сигналом. Предусмотренный в современных нелинейных локаторах режим выделения огибающей переотраженного сигнала и его индикации позволяет обнаруживать и идентифицировать работающие закладные устройства с высокой достоверностью.

Проникающая глубина зондирующей волны нелинейного локатора зависит от мощности и частоты излучения. В силу увеличения затухания электромагнитной волны в среде распространения с повышением частоты колебаний уровень мощности переизлученного (отраженного) сигнала тем выше, чем ниже частота локатора. Но для излучений с более низкой частотой ухудшаются возможности локатора по локализации места нахождения нелинейности, так как при приемлемых размерах его антенны расширяется диаграмма направленности антенны локатора.

Очевидно, что чем выше мощность излучения локатора, тем глубже проникает электромагнитная волна и тем больше вероятность обнаружения помещенной в стену закладки. Но большая мощность излучения оказывает вредное воздействие на оператора. Для обеспечения его безопасности максимальная

мощность излучения локатора в непрерывном режиме не превышает 3–5 Вт. При импульсном режиме работы локатора мощность в импульсе достигает 300 Вт при меньшей средней мощности, не превышающей 1,5 Вт.

1.1.4. Технические характеристики нелинейного локатора, удовлетворяющие требованиям безопасности обслуживания

Вариант установки НЛ в системе «рамка» схематично показан на рис. 1.3. Для повышения вероятности обнаружения антенны располагаются с двух сторон. Примем средний рост человека 170 см, а условную «ширину» – 60 см. Тогда облучаемая поверхность составит (170 х 60) х 2 = 20400 см^2. В соответствии с регламентирующими документами допустимая плотность потока мощности, которой подвергается персонал непрерывно в течение рабочего дня, не должна превышать 10 мкВт/см^2. Зная величину облучаемой поверхности, находим, что максимальная мощность источника излучения не должна превышать 10^{-5} Вт/см^2 х 2,04 х 104см^2 = 0,212 Вт. Данная величина представляет собой среднюю мощность максимально допустимого излучения. Для локаторов с непрерывным режимом указанное значение мощности передатчика является ее средней мощностью.

Для локаторов с импульсным режимом излучения средняя мощность определяется как импульсная мощность, деленная на скважность:

$$P_{\text{ср}} = \frac{P_{\text{имп}}}{Q}, \qquad (1.2)$$

где $Q = 1/F_\tau$, F – частота следования импульсов, Гц; τ – длительность импульса, с.

С учетом потерь мощности при делении, потерь в кабелях СВЧ и за счет коэффициента стоячей волны антенн локатора допустимая средняя мощность передатчика может составлять 0,7 Вт. Необходимо помнить, что это значение равно сумме воздействующей мощности с двух сторон облучения. Таким образом, ни одна модель НЛ с непрерывным режимом излучения не удовлетворяет

требованиям по безопасной норме облучения обслуживающего персонала. Напротив, все импульсные локаторы, несмотря на их кажущиеся значительные величины излучаемой импульсной мощности, полностью удовлетворяют требованию безопасности при обслуживании.

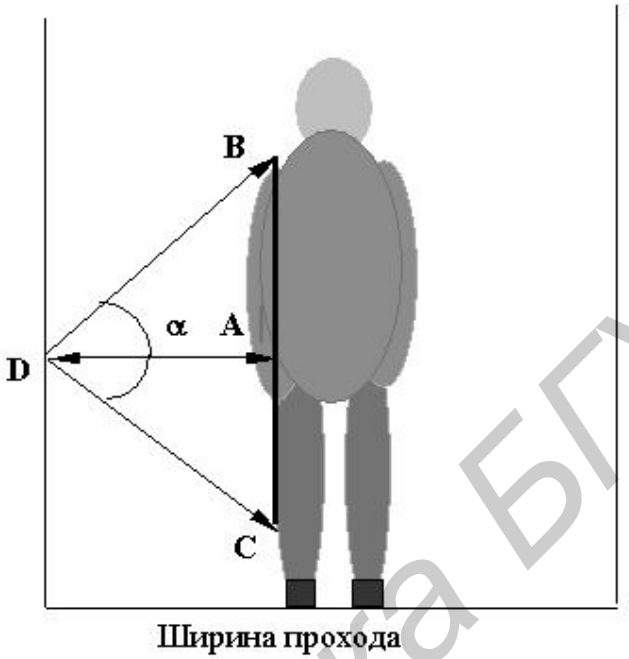


Рис. 1.3. Установка НЛ в системе «рамка» (вариант):
D – место расположения антенн; BC – зона обнаружения;
AD – расстояние до объекта звукозаписи; α – угол обзора

Отсюда также следует, что вопрос применения средств защиты от скрытой звукозаписи с помощью постановки помехи ВЧ и СВЧ генераторами не должен противоречить безопасности для самого руководителя, в кабинете которого находится и эксплуатируется данная аппаратура.

1.1.5. Частотные характеристики нелинейного локатора

Большинство нелинейных локаторов работают на одной фиксированной частоте, некоторые имеют несколько каналов. Из-за увеличения количества средств радиосвязи и правительственного регулирования радиодиапазона нелинейные локаторы с ограниченной частотой излучения часто конфликтуют с другими электронными устройствами. Если нелинейный локатор работает на

занятой частоте, его показания могут быть случайными и ненадежными. Здесь одной из необходимых опций НЛ выступает возможность его перестройки по частоте.

1.1.6. Уровень мощности и чувствительность нелинейного локатора

Многие оценивают НЛ по излучаемой мощности, так как эта характеристика сравнительно легка для восприятия. Чувствительность приемника также важна, как и мощность передатчика. Нелинейный локатор с низкой мощностью излучения и качественным приемником может иметь более высокие характеристики по обнаружению, чем мощный локатор с плохим приемником. Следует иметь в виду, что мощный локатор может вывести из строя электронные приборы и даже нанести ущерб здоровью людей.

Часто моделируют диод в качестве простого переключателя тока, позволяющего протекать току в направлении положительного смешения напряжения. Однако это чрезмерное упрощение, которое не следует использовать при анализе теории нелинейной локации. Полупроводниковое соединение – это определенная показательная постоянная функция, показанная на рис. 1.2 и представленная формулой

$$I = I_0\left(e^{\frac{qU}{kT}} - 1\right), \tag{1.3}$$

где I_0 – ток утечки, q – заряд электрона; k – постоянная Больцмана; T – температура; U – напряжение на концах диода.

Поэтому маломощные НЛ могут иметь лучшие характеристики, чем мощные, если первые имеют лучшие приемники.

1.1.7. Эргономические характеристики нелинейного локатора

Во время работы с НЛ очень важно иметь хороший обзор его дисплея для оценки показаний. На некоторых НЛ дисплей находится на блоке приемопередатчика, который переносится с помощью ремня на плече или шее оператора.

Некоторые НЛ имеют дисплей, размещенный на рукоятке. Наилучшим типом дисплея является дисплей высокой яркости, расположенный на корпусе антенны. Показания с такого дисплея легко считывать с разных углов. Дисплей,

встроенный в корпус антенны, позволяет пользователю одновременно считывать показания и перемещать антенну. Если у оператора нет возможности легко считывать дисплей, качество поисковых работ снижается из-за ухудшения интерпретации уровней гармоник.

Рис. 1.4. Внешний вид нелинейного локатора SP-61/M «Катран» (Россия)

Основные технические характеристики SP-61/M «Катран» (рис. 1.4)

Режим излучения	Непрерывный
Мощность излучения, Вт	2,5
Частота излучения, МГц	885–895, с шагом 1 МГц
Анализируемые гармоники	2-я, 3-я
Вид излучаемого сигнала	ЧМ
Девиация частоты, кГц	1,5
Полоса тракта ПЧ, кГц	10
Чувствительность, дБм	минус 127
Коэффициент усиления передающей и приемной антенн	6
Наличие АМ и ЧМ детекторов	АМ, ЧМ
Напряжение питания, В	12
Цена, тыс. дол. США	4

1.2. Лабораторное задание

Обнаружить места нахождения в помещении средств технической разведки с классификацией обнаруженного устройства по типу и материалу при помощи программной модели нелинейного локатора. Для этого необходимо:

1. Запустить файл Locator.exe на выполнение.

2. Установить желаемый размер окна программы. В процессе работы с программой изменение установленного размера окна программы не рекомендуется.

3. Включение локатора осуществляется нажатием кнопки **Вкл** (рис. 1.5), после чего все настройки прибора становятся активными. После включения локатора курсор мыши принимает вид антенны (в том случае, когда он находится в пределах изображенной на экране комнаты).

4. Для работы в импульсном режиме необходимо нажать кнопку **Импульсный,** затем – **Начать**. По истечении двух минут она автоматически деактивируется. Для возобновления работы в импульсном режиме требуется повторно нажать кнопку **Начать**.

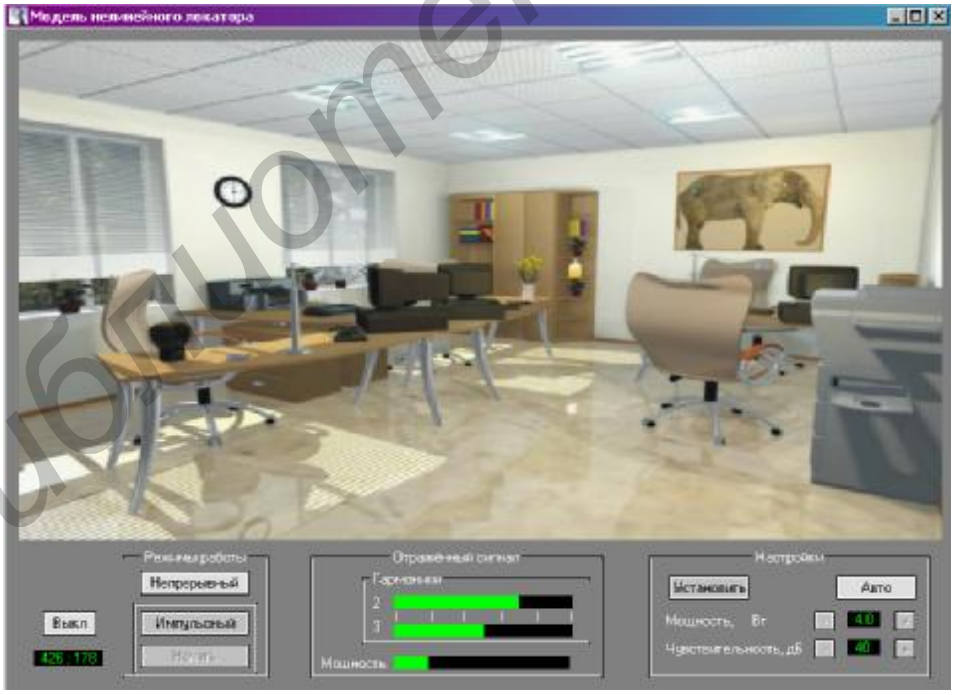


Рис. 1.5. Внешний вид главного окна программы

5. Установка мощности излучения локатора и чувствительности его приемников выполняется соответствующими органами управления и подтвержде-

ния выбранных параметров нажатием кнопки **Установить**. Для того чтобы установить данные параметры по умолчанию, необходимо нажать кнопку **Авто**.

6. Поиск устройств осуществляется путем передвижения приемо-передающей антенны при помощи мыши.

7. Идентификация обнаруженного устройства производится нажатием правой кнопки мыши в месте его нахождения. В выпадающем меню необходимо выбрать тип материала и тип устройства. В случае определения типа материала как МОМ-структуры тип устройства выбирать не требуется. Правильно идентифицированное устройство помечается красной точкой.

8. Точная идентификация нелинейных соединений выполняется с учетом показаний индикатора **Мощность**:

– минимальная мощность – **Радиомикрофон**;

– затем – **Закладка**;

– после – **Телефон**;

– максимальная мощность – **Бытовая техника**.

9. При попадании в радиус действия нелинейного локатора нескольких нелинейных соединений отраженный сигнал на 2-й и 3-й гармониках, отображаемый на соответствующих индикаторах, имеет одинаковый уровень. В данном случае требуется корректировка мощности и чувствительности нелинейного локатора для классификации каждого из соединений в отдельности.

10. После обнаружения последнего закладного устройства (в каждом помещении находится 20 закладных устройств) на экране появится таблица результатов выполнения работы.

11. Для завершения работы и просмотра таблицы результатов необходимо нажать кнопку **Выкл**. Отображение таблицы результатов также происходит по истечении 45 мин с момента начала работы программы.

12. Таблицу результатов выполнения работы показать преподавателю.

13. Оформить отчет.

1.3. Содержание отчета

1. Цель работы.

2. Таблица результатов выполнения работы.

3. Вывод по работе.

4. Ответы на контрольные вопросы.

1.4. Контрольные вопросы

1. Назначение нелинейного локатора.

2. Характерный признак обнаружения полупроводника.

3. Характерный признак обнаружения МОМ-структуры.

4. Назначение демодулятора аудиосигналов НЛ.

5. Какова способность НЛ обнаруживать закладные устройства при работе в импульсном и непрерывном режимах работы.

Приложение

Методика проведения работ по поиску средств технической разведки с помощью нелинейного локатора

1. Ознакомиться с планом обследуемого помещения.

2. Проанализировать наиболее вероятные места установки средств технической разведки в данном помещении, уделяя особое внимание ограждающим конструкциям.

3. Разделить помещение на зоны с высокой и малой вероятностью установки средств технической разведки.

4. Составить план поиска закладных устройств с учетом размещения бытовой техники для данного помещения.

5. Включить и настроить нелинейный локатор, выставить частоту излучения локатора таким образом, чтобы смежные частоты работы различных радиопередающих средств в пределах данного помещения не создавали помехи нелинейному локатору.

6. Осуществить проверку зон помещения с наиболее вероятной установкой средств технической разведки.

7. При поиске закладного устройства необходимо плавно перемещать антенну нелинейного локатора в обследуемой зоне с постоянным визуальным контролем индикатора уровня отраженного сигнала на второй и третьей гармониках.

8. Идентификация закладного устройства производится в соответствии с уровнем отраженного сигнала на 2-й и 3-й гармонике, решение об удалении найденного закладного устройства принимается начальником службы безопасности объекта исходя из соображений необходимости дезинформирования стороны, осуществляющей перехват.

9. Регламент и регулярность проверки помещений устанавливается в соответствии с назначением помещения. В случае появления в нем дополнительной мебели или его реконструкции проводится внеплановая проверка.

10. Проверка помещения должна проводиться скрытно сотрудниками службы безопасности данного объекта с соблюдением всех мер секретности проводимого мероприятия.

ЛАБОРАТОРНАЯ РАБОТА №2
ОБНАРУЖЕНИЕ И КЛАССИФИКАЦИЯ РАДИОЧАСТОТНЫХ ИЗЛУЧЕНИЙ С ПОМОЩЬЮ СКАНИРУЮЩЕГО ПРИЕМНИКА

Цель: изучить основы проведения радиомониторинга; получить практические навыки по классификации радиочастотных излучений с помощью модели сканирующего приемника, реализованного программным методом.

2.1. Теоретическая часть

2.1.1. Основные цели и условия проведения радиомониторинга

В процессе регулярного ведения радиомониторинга возможно решение следующих основных задач по обеспечению безопасности объекта:

– выявление излучений радиосредств несанкционированного перехвата информации, внедренных в помещения объекта, и их локализация;

– контроль соблюдения дисциплины связи при использовании сотрудниками открытых каналов радиосвязи;

– выявление информативных побочных излучений, возникающих при работе средств оргтехники, компьютеров и т.п.;

– оценка эффективности используемых на объекте технических средств защиты информации;

– контроль за местонахождением и состоянием транспортных средств фирмы в реальном масштабе времени с использованием спутниковых навигационных систем;

– накопление данных по радиоэлектронной обстановке в зоне расположения объекта и обнаружение новых сигналов.

При решении любой из указанных задач в процессе ведения радиомониторинга требуется учитывать совокупность ряда основных условий, без выполнения которых нельзя обеспечить эффективность проводимого мероприятия. К этим обязательным условиям следует отнести прежде всего:

1. Плановость и регулярность проведения радиомониторинга в зоне объекта.

2. Обязательное наличие специально подготовленных для этой работы операторов, так как от их профессиональной подготовки, умения правильно оценивать обстановку, способности воспринимать и выделять необходимую информацию во многом зависит точность и полнота добываемых с помощью радиомониторинга данных.

3. Знание операторами структур систем радиосвязи и методов передачи информации по их каналам, а также характерных признаков и основных диапазонов работы радиосредств негласного перехвата информации.

4. Обязательное составление и регулярное обновление специальных карты и таблицы занятости радиоэфира в зоне объекта. Знание частотных диапазонов, режимов работы и параметров сигналов «легальных» средств связи, радиовещания и телевидения, контролируемых в зоне объекта.

5. Тщательный анализ всех получаемых в процессе радиомониторинга данных, сопоставление их с режимом работы объекта и ранее накопленной информацией по радиообстановке в окружении объекта.

6. Оборудование на объекте специального помещения для ведения радиомониторинга, оптимальный подбор и размещение технических средств.

2.1.2. Методы и средства негласного перехвата информации

Наибольшее распространение в практике промышленного шпионажа в настоящее время нашли следующие способы негласного перехвата информации, циркулирующей на коммерческих объектах:

– подслушивание разговоров в помещении или автомашине с помощью радиотехнических средств перехвата информации (РСПИ);

– контроль проводных телефонных и факсимильных линий связи с использованием РСПИ;

– контроль радиотелефонов, систем персонального вызова (пейджеров) и радиостанций с использованием средств радиомониторинга;

– перехват информации с технических средств ее обработки и хранения с помощью РСПИ;

– дистанционный перехват с использованием средств РМ информативных побочных излучений технических средств, эксплуатируемых на объекте;

– перехват акустической информации за счет переизлучения (микрофонного эффекта) используемых на объекте основных или вторичных технических средств либо специально внедренных переизлучающих устройств.

Радиотехнические средства перехвата акустической информации, как правило, состоят из радиозакладки (радиомикрофона, радиостетоскопа и т. п.) и аппаратуры контрольного пункта (КП). Радиозакладка (РЗ) представляет собой миниатюрный радиопередатчик, который либо негласно устанавливается на контролируемом объекте, либо в закамуфлированном виде и под соответствующей легендой заносится в интересующее помещение на непродолжительное время. С помощью радиозакладки производится перехват информации, преобразование ее в радиосигнал и передача по радиоканалу на КП. Аппаратура контрольного пункта осуществляет прием сигнала от РЗ, его обратное преобразование в низкую частоту и регистрацию принятой информации с помощью магнитофона. В некоторых случаях в состав КП входит также аппаратура дистанционного управления (ДУ) работой радиозакладки.

Применяемые для негласного перехвата информации радиотехнические средства можно также классифицировать по целому ряду признаков:

– способу перехвата информации;

– частотному диапазону работы;

– дальности действия;

– виду модуляции сигнала и способу его маскировки (кодирования);

– виду питания;

– способу управления;

– типу используемого контрольного пункта;

– способу камуфлирования и др.

Акустический способ перехвата информации осуществляется с помощью микрофонов различных типов; виброакустический – с помощью специальных вибродатчиков (стетоскопов, акселерометров), укрепляемых на ограждающих поверхностях помещений. При гальваническом способе информация снимается путем непосредственного подключения к контролируемой линии (телефонной и т. п.), при индукционном или емкостном – с помощью соответствующих датчиков без прямого подключения к линии.

Выпускаемые в настоящее время коммерческими фирмами радиотехнические средства перехвата информации в основном работают в диапазонах ОВЧ (30–300 МГц) или УВЧ (300–3000 МГц). Исходя из особенностей распространения радиоволн в условиях городской застройки, наиболее предпочтительным с точки зрения обеспечения максимальной дальности работы РЗ считается диапазон 200–500 МГц.

Более подробные сведения о диапазонах частот и других важных с точки зрения радиомониторинга параметрах РСПИ, которые выпускаются некоторыми московскими коммерческими предприятиями, приведены в табл. 2.1.

Дальность действия – максимальное расстояние, на котором возможны устойчивый прием сигнала радиозакладки на контрольном пункте и уверенное дистанционное управление ее работой. Эта работа зависит от многих факторов, основными из которых являются:

– технические параметры аппаратуры РСПИ (мощность излучения, рабочая частота и эффективная длина антенны радиозакладки, чувствительность приемника КП и др.);

– условия прохождения радиоволн между РЗ и КП на конкретной трассе (наличие мешающих препятствий, источников радиопомех);

– взаимное расположение антенн РЗ и КП и т.д.

Таблица 2.1

Технические характеристики РСПИ

Тип РСПИ	Диапазоны рабочих частот (МГц)	Выходная мощность (мВт)	Макс. дальность действия (м)	Вид модуляции и способа маскировки сигнала	Ресурс непрерывной работы (ч)	Вид ДУ
Микрофонные долговременные с автономным или комбинированным питанием	106–115 130–205 320–327 330–450 470–480 870–1050 10500	1–500	50–1500	NFM,WFM FM с кодировкой FM с расширенным спектром, импульсная с цифровой кодировкой	100 1000	Р/канал
Микрофонные с питанием от электросети	110–115 130–150 470–475	5–20	100–500	NFM, WrM, FM с кодированием	Неогр.	Р/канал
Микрофонные камуфлированные малого ресурса с автономным питанием	88–105 135–220 320–330 390–460 470–480 630–640	1–20	50–500	NFM,WFM	5–30	Нет
Телефонные с питанием от ТЛФ линии	88–200, 320–325, 390–395 415–475	5–15	100–500	NFM. WFM, FM с кодированием	Неогр.	Автопуск
Радиостетоскопы	320–325 390–395 415–475	5–50	100–500	NFM,WFM	10–700	Р/канал

Приводимая в рекламных проспектах дальность действия РСПИ, как правило, измеряется в условиях открытого пространства, при прямой видимости между радиозакладкой и контрольным пунктом. В условиях города реальная дальность действия может уменьшиться в 2–3 раза. Так, при оптимальной выходной мощности радиозакладки 20 мВт и чувствительности приемника около 1 мкВ

реальная дальность в условиях неплотной городской застройки составляет приблизительно 300–400 м (в диапазоне частот 200–500 МГц).

При передаче акустической информации в РСПИ в основном используются узкополосная (NFM) и широкополосная (WFM) фазовая (частотная) модуляция несущей частоты радиопередатчиков. Кроме того, с целью затруднения выявления работающей радиозакладки путем радиомониторинга в последнее время довольно активно начали применяться аналоговые и цифровые способы электронного кодирования передаваемого речевого сигнала (скремблирование, дискретизация с последующим шифрованием и т. д.), прикрытие модулированного сигнала шумом, скачкообразное изменение по определенному закону несущей частоты (СИЧ, ППРЧ), расширенная (5 МГц и выше) частотная модуляция и др. Для этого передатчик РЗ оборудуется специальным блоком дополнительного преобразования передаваемого сигнала, а приемник КП – блоком обратного преобразования.

Аналоговые скремблеры преобразуют исходный речевой сигнал посредством изменения его амплитудных, частотных и временных параметров в различных комбинациях. Скремблированный сигнал может быть передан по каналу связи в той же полосе, что и открытый. В РСПИ могут использоваться следующие виды аналогового скремблирования:

1. Скремблирование в частотной области: частотная инверсия (преобразование спектра сигнала), частотная инверсия и скачкообразное смещение несущей частоты, разделение полосы частот речевого сигнала на ряд поддиапазонов с последующей их перестановкой и инверсией.

2. Скремблирование во временной области (разбиение блоков речи на слоговые сегменты с перемешиванием их во времени).

Преобразование речевых сигналов в цифровую форму обеспечивает более высокий уровень закрытия по сравнению с аналоговыми методами. В основе этого метода лежит представление речевого сигнала в виде цифровой последовательности, закрываемой по одному из криптографических алгоритмов.

Вместе с тем маскировка информации ведет к дополнительному расходу энергии источников питания радиозакладки и в конечном итоге либо к увеличению ее размеров, либо к уменьшению ресурса работы.

Наиболее широкое применение в радиотехнических системах негласного перехвата информации получили радиозакладки с автономным питанием от батарей или аккумуляторов. Основное преимущество РЗ с автономным питанием – возможность их быстрой установки на объект и последующего изъятия, главный недостаток – ограниченность энергоресурса.

Указанного недостатка лишены радиозакладки с питанием от электро- или телефонной сети. Но из-за необходимости скрытого подключения к сети подобные РЗ требуют существенно большего времени для их установки и определенной квалификации установщика.

Способы управления включением/выключением внедряемых на объекты радиозакладок зависят в основном от характера и длительности мероприятия, способа перехвата информации, режима обеспечения безопасности контролируемого объекта, максимально допустимых размеров радиозакладки, требований к ее камуфлированию и т. д. Так, например, если требуется проконтролировать только ход какого-то важного совещания, то обычно на объекте устанавливается миниатюрная камуфлированная радиозакладка с автономным питанием и ручным управлением при помощи механического выключателя или геркона. При осуществлении долговременного перехвата акустической информации на регулярной основе из соображений экономии ресурса радиозакладки и повышения конспиративности мероприятия используется дистанционное управление работой РЗ по радиоканалу. В случае проведения контроля телефонных разговоров в основном применяется управление работой РСПИ с использованием автопусков, включающих РЗ при поднятии телефонной трубки и отключающих при опускании ее на рычаг телефонного аппарата. Возможно управление работой радиозакладок и по определенной программе, зависящей от режима функционирования объекта контроля.

В зависимости от продолжительности мероприятия по перехвату информации, обстановки вокруг объекта проникновения, дальности работы и типа внедренных РСПИ используются либо стационарные контрольные пункты, приемная аппаратура которых размещается в помещении и питается от электросети, а в качестве антенн используются эффективные направленные антенны типа «диполь» или «волновой канал»; либо автомобильные, аппаратура которых располагается в салоне автомобиля и питается от его бортовой сети, а в качестве антенны применяется штатная автомобильная; либо носимые, размещаемые в сумках, атташе-кейсах или в одежде оператора. Стационарный КП обеспечивает большие конспиративность, удобства и дальность работы, поэтому на практике этому варианту размещения КП отдается предпочтение.

Радиозакладки с автономным питанием камуфлируются, как правило, под конструктивные элементы мебели (крепежные бруски, планки и т. п.), предметы интерьера помещения (мусорные корзины, пепельницы, картины и др.), предметы оргтехники (калькуляторы, авторучки, фломастеры). Радиозакладки с питанием от сети в большинстве случаев выполняются в виде некамуфлированных устройств, устанавливаемых внутри ограждающих конструкций помещения (например в нише для электророзеток) или камуфлируются в электроразветвители, распределительные коробки, телефонные аппараты и т. д.

Одним из демаскирующих признаков работающей радиозакладки является наличие в излучаемом ею радиоспектре большого количества высших гармоник несущей частоты, так как в отличие от связной и вещательной аппаратуры, в которой принимаются специальные конструктивные меры подавления внеполосных излучений (экранирование, фильтрация и др.), РСПИ генерируют радиосигнал не только на основной (несущей) частоте, но и на ее гармониках.

Радиотехнические средства негласного перехвата информации, методы их установки и использования постоянно совершенствуются. Основная тенденция состоит в их дальнейшей миниатюризации, повышении скрытности работы и увеличении дальности действия.

Одним из нетрадиционных способов получения акустической информации из помещений является использование переизлучающих пассивных радиозакладок (эндовибраторов), у которых отсутствуют источник питания, передатчик и микрофон. Основой эндовибратора является цилиндрический объемный резонатор, настроенный на внешнее излучение определенной частоты (чаще всего в диапазоне 300 МГц). При этом собственный четвертьволновый вибратор внутри резонатора создает свое поле переизлучения. При ведении разговоров в помещении меняется и собственная резонансная частота эндовибратора, влияющая в свою очередь на поле переизлучения, которое становится модулированным акустическими колебаниями. Работать эндовибратор может только при облучении мощным источником на частоте резонатора, поэтому его невозможно обнаружить такими средствами поиска радиозакладок, как нелинейный локатор, индикатор поля и др. Исключение составляет радиомониторинг.

2.1.3. Организация работ по радиомониторингу, регистрация результатов

Поиск и выявление различных радиоизлучений, определение их происхождения, степени информативности и угрозы для безопасности коммерческого объекта – достаточно сложная и трудоемкая задача. Успех этой работы зависит от опыта и квалификации оператора поста радиомониторинга, тактико-технических характеристик используемых средств, знания радиообстановки, частот, режимов работы, методов организации и ведомственной принадлежности сетей радиосвязи как в зоне расположения защищаемого объекта, так и в целом по городу и в его окрестностях.

Так, даже одновременный контроль нескольких каналов сотовых систем связи не в состоянии обеспечить возможность непрерывного контроля переговоров интересующего абонента. Для этой цели необходимо иметь автоматизированный компьютерный комплекс радиомониторинга, позволяющий по идентификационному номеру этого абонента определять предоставленный ему в данный момент канал связи и переключать приемный тракт комплекса на его контроль.

В процессе работы по радиомониторингу необходимо также учитывать, что из-за особенностей распространения радиоволн в диапазонах ОВЧ и УВЧ размеры зоны приема очень сильно зависят от характера городской застройки. Примерные дальности приема стационарного поста радиомониторинга в зависимости от типа застройки приведены в табл. 2.2. Вместе с тем из-за отражений и переотражений радиоволн от зданий возникает сложная картина пространственного распределения излучений радиопередатчиков, которая не поддается предварительному расчету. В результате в месте расположения стационарного поста радиомониторинга могут приниматься достаточные по уровню передачи удаленных радиостанций.

На начальном этапе радиомониторинга следует в режиме автоматического поиска сканера произвести 3–4 раза в разное время суток обзор всего частотного диапазона, в котором работает используемое на посту РМ радиоприемное устройство, выделить и зафиксировать частоты всех постоянно присутствующих в эфире радиовещательных и телевизионных станций, организационных каналов сетей радиосвязи общего пользования, несущих частот РРЛ и т.д. Последующее исследование радиоэфира следует производить в более узких частотных диапазонах (не более 10–20 МГц), причем в каждом из них контроль должен осуществляться в течение нескольких суток и в различное время. Обследование наиболее загруженных участков радиодиапазона, а также тех, где наиболее вероятна работа РСПИ (см. табл. 2.2) необходимо проводить еще в более узких пределах (2–3 МГц).

Главные задачи, решаемые на первом этапе радиомониторинга, в основном сводятся к следующему:

– оценка загрузки радиодиапазона, выявление и идентификация радиоизлучений в окружении коммерческого объекта;

– выявление подозрительных радиоизлучений, требующих дополнительного исследования;

– систематизация и документирование полученных данных. Помимо регулярного контроля эфира с позиций поста РМ на первом этапе должны проводиться также мероприятия по сбору сведений о ведомственном распределении частотных диапазонов в регионе с использованием различных справочников, данных местного радиоклуба, рекламных объявлений фирм, оказывающих услуги в области связи и др.

Таблица 2.2

Примерные дальности приема стационарного поста радиомониторинга в зависимости от типа застройки

Тип застройки, этажность	Стационарные радиостанции	Автомобильные радиостанции	Портативные радиостанции
1–3	70	15–20	10–15
До 9	50	10–15	5–10
Выше 9	30	5–10	3–5

Существенную помощь при выявлении каналов связи каких-либо близлежащих учреждений может оказать визуальное наблюдение, проводимое с целью обнаружения мест нахождения их пунктов связи. Характерным признаком действующей системы радиосвязи является наличие связных антенн на крыше здания учреждения и на принадлежащих ему автомобилях, портативных радиостанций у службы охраны. В этом случае важно не только обнаружить факт наличия антенны, но и установить длину ее вибраторов, положение в пространстве, что в свою очередь может дать представление о рабочей частоте и направлении излучения радиопередатчика.

С целью облегчения идентификации выявленных в процессе поиска неизвестных сигналов полезно с помощью магнитофона составить своего рода «библиотеку» акустических сигналов, характерных для работы в эфире различных средств связи, записав их на известных частотах, и затем сопоставлять обнаруженные радиоизлучения с этими образцами. Например, организационные каналы транкинговых и сотовых сетей звучат в эфире в виде специфического рокота,

характер которого изменяется в зависимости от степени загрузки каналов связи. Прикрытые с использованием инверсии или временного скремблирования речевые сигналы звучат в эфире в виде некой смеси звуков, но при этом иногда можно разобрать отдельные слоги. Несущую частоту РРЛ в момент передачи по ней информации можно идентифицировать по характерному «звону» и т. д.

Для хранения, учета и постоянного обновления полученных данных наиболее удобными являются две формы их систематизации, используемые во всем мире (на бумаге или в компьютере):

– диаграмма или карта занятости радиоэфира;

– таблицы занятости радиоэфира.

Знакомство с диаграммой занятости радиоэфира дает представление о том, какое количество радиопередатчиков работает как в окружении вашего объекта, так и вообще в городе. Назначение диаграммы в том и состоит, чтобы выбирать последовательно полосы частот и определять в них максимальное количество постоянно или периодически работающих радиопередатчиков, таких, как теле- и радиовещание, мобильные и стационарные радиостанции городских транспортных служб, сотовые радиотелефоны и т. д.

2.2. Лабораторное задание

Обнаружить и классифицировать радиочастотные излучения в полосе приема сканирующего приемника. Для этого необходимо:

1. Запустить программу, имитирующую сканирующий приемник. С этой целью в командной строке файлового менеджера (например Total Commander) указать имя запускаемой программы client.exe и через пробел – имя файла базы данных (например freq_db_1) соответствующего варианта.

2. Ввести пароль (соответствует номеру варианта).

3. В режиме **Панорама** (кнопка **Панорама** нажата) установить начальную частоту, с которой будет начато сканирование (рис. 2.1). Для этого в параметрах сканирования нажать кнопку **Начальная частота** и, используя цифро-

вую клавиатуру в главном окне программы, ввести значение частоты. Результат ввода отображается на индикаторе.

4. В режиме **Панорама** установить конечное значение диапазона частот, в котором будет происходить сканирование (кнопка **Конечная частота**).

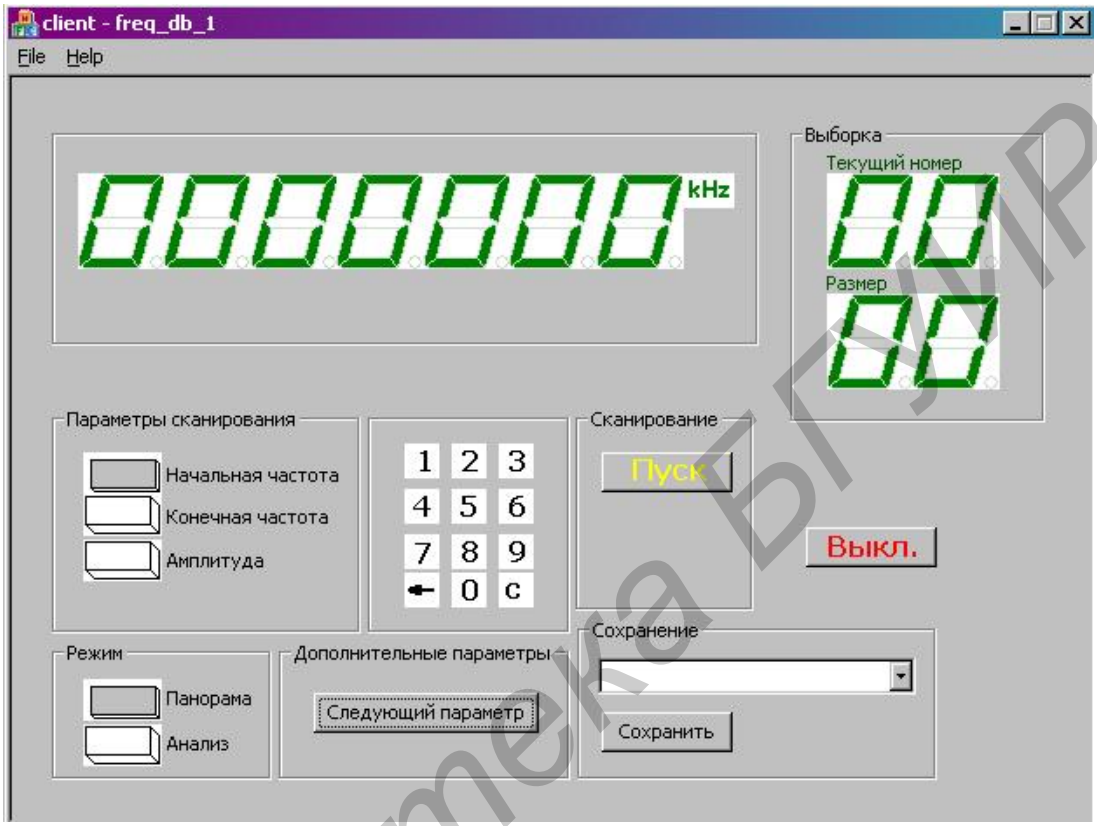


Рис. 2.1. Внешний вид главного окна программы

5. В режиме **Панорама** в параметрах сканирования указать максимальную амплитуду сканируемых сигналов. Для этого нажать кнопку **Амплитуда** и с помощью цифровой клавиатуры ввести необходимое значение.

6. Нажать кнопку **Пуск**.

7. Переключиться в режим **Анализ**.

8. В правом верхнем углу окна в пункте **Размер** опции **Выборка** будет указано количество источников излучения, обнаруженных приемником с заданными параметрами сканирования.

9. Выбор любого из обнаруженных источников излучения выполняется путем набора его номера (1–99) на цифровой клавиатуре. При этом на семизначном цифровом индикаторе в левом верхнем углу программы при нажатой

кнопке **Амплитуда** в параметрах сканирования отображается амплитуда обнаруженного сигнала. Если в параметрах сканирования нажать кнопку **Начальная частота** или **Конечная частота**, на индикаторе будет отображаться частота обнаруженного сигнала.

10. При нажатии кнопки **Следующий параметр** в опции **Дополнительные параметры** под семизначным цифровым индикатором будет указываться **Модуляция**. Повторное нажатие кнопки **Следующий параметр** приведет к отображению параметра **Время** по данному сигналу.

11. В соответствии с параметрами обнаруженного сигнала: частота, амплитуда, вид модуляции, временная характеристика – сделать вывод о принадлежности данного излучения к какому-либо техническому средству, выбрать которое можно в опции **Сохранение** (радиостанция, базовая станция CDMA, базовая станция GSM, радиомикрофон), после чего нажать кнопку **Сохранить**.

12. Результаты поиска и анализа излучений занести в таблицу.

Частота (МГц)	Ведомственная принадлежность радиоканала	Амплитуда сигнала	Вид модуляции	Время работы

13. Оформить отчет.

2.3. Содержание отчета

1. Цель работы.
2. Таблица результатов выполнения работы.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

2.4. Контрольные вопросы

1. Что такое закладное устройство.
2. Какие цели преследует проведение радиомониторинга.

3. Какие существуют методы и средства передачи информации по радиоканалу?

4. Какие существуют методы и средства перехвата информации по радиоканалу?

5. Каким образом организуется радиомониторинг?

Приложение

Сетка частот радиостанций FM диапазона, работающих в г. Минске

Частота, МГц	Название радиостанции
92,4	Минск
96,2	Мелодии века
97,4	Минская волна
98,4	Новое радио
98,9	Русское радио
99,5	Unistar
100,4	Хит FM
101,2	Пилот
101,7	ОНТ
102,1	Rocks
102,9	Культура
103,7	Радиус FM
104,6	Радио b.a.
105,1	Авторадио
106,2	Белорусское радио (1 канал)
107,1	Мир
107,9	Альфарадио

ЛАБОРАТОРНАЯ РАБОТА №3
ИЗУЧЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ

Цель: изучить основные физические принципы распространения акустических волн в твердых средах и проблему утечки речевой информации в виброакустических каналах; получить практические навыки по настройке и эксплуатации систем виброакустической защиты.

3.1. Теоретическая часть

3.1.1. Основные понятия, определения и единицы измерения в акустике

Звук – колебательное движение упругой среды. Процесс распространения колебательного движения в среде называется звуковой волной. За один полный период колебания T звуковой процесс распространяется в среде на расстояние, равное длине волны λ (рис. 3.1).

$$\lambda = \frac{1}{T}, \text{ Гц;} \tag{3.1}$$

$$\lambda = c \cdot T, \text{ м.} \tag{3.2}$$

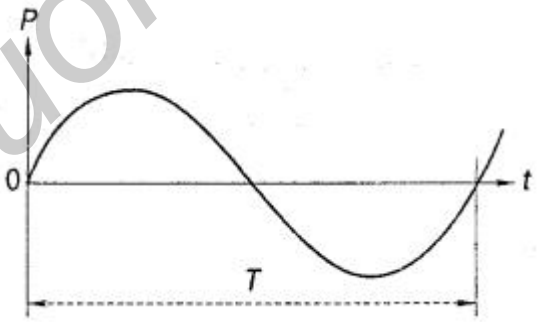


Рис. 3.1. Полный период колебания

Длина волны зависит от скорости распространения звука в среде.

$C_{воздух}$ – 340 м/с;
$C_{кирпич}$ – 2300 м/с;
$C_{сталь}$ – 5200 м/с;
$C_{вода}$ – 1490 м/с;
$C_{бетон}$ – 3700 м/с.

Изменения давления в звуковой волне относительно среднего значения называется **звуковым давлением (*P*)** и измеряется в паскалях. **Один паскаль** – давление, создаваемое силой в один ньютон, действующей на площадь один квадратный метр.

$$P = \frac{1\text{Н}}{1\text{м}^2} = 1\text{Па} = \frac{1}{100000}\text{атм}. \qquad (3.3)$$

В акустике принято использование относительных единиц измерения уровня звукового давления – **децибел.**

$$L_{\text{дБ}} = 20\lg\frac{P}{P_0}. \qquad (3.4)$$

В качестве P_0 выбрана величина $P = P_0 = 2\cdot10^{-5}$ Па, что соответствует минимальному звуковому давлению, воспринимаемому человеческим слухом. При этом изменение уровня звукового давления на 1 дБ является минимальной различаемой человеческим слухом величиной изменения громкости.

Следует отметить, что в акустике при частотном анализе сигналов используют стандартизированные частотные полосы шириной в 1 октаву, 1/3 октавы, 1/12 октавы. **Октава** – полоса частот, у которой верхняя граничная частота в два раза больше нижней граничной частоты.

$$\Delta f = (f_{\text{в}} - f_{\text{н}}) = 1 \text{ окт., если } f_{\text{в}} = 2 f_{\text{н}}. \qquad (3.5)$$

Центральные частоты стандартных октавных полос соответствуют следующему ряду: 2, 4, 8, 16, 31,5, 63, 125, 250, 500 (Гц), 1, 2, 4, 8, 16 (кГц).

3.2.1. Основные акустические параметры речевых сигналов

Основные звуки речи образуются следующим образом:

– гласные образуются при прохождении воздуха через голосовые связки. Акустические колебания гласных звуков носят периодический, близкий к гармоническому характер и могут изменяться в значительном частотном диапазоне;

– глухие согласные (сонорные, щелевые, взрывные) образуются за счет преодоления воздухом препятствий в носовой и ротовой полостях и носят характер как отдельных акустических импульсов, так и шумовых сигналов со сплошным спектром различной конфигурации;

– звонкие согласные образуются так же, как глухие, но при участии голосовых связок.

Таким образом, речевой сигнал представляет собой сложный частотно- и амплитудно-модулированный шумовой процесс, характеризующийся следующими основными статистическими параметрами: частотный диапазон; уровень речевых сигналов; динамический диапазон.

Частотный диапазон речи лежит в пределах 70 – 7000 Гц. Энергия акустических колебаний в пределах указанного диапазона распределена неравномерно. На рис. 3.2, кривая *1*, представлен вид среднестатистического спектра русской речи. Следует отметить, что порядка 95 % энергии речевого сигнала лежит в диапазоне 175 – 5600 Гц.

Важно отметить, что информативная насыщенность отдельных участков спектра речи неравномерна. Кривая *2* на рис 3.2 представляет вклад отдельных участков спектра речи в суммарную разборчивость.

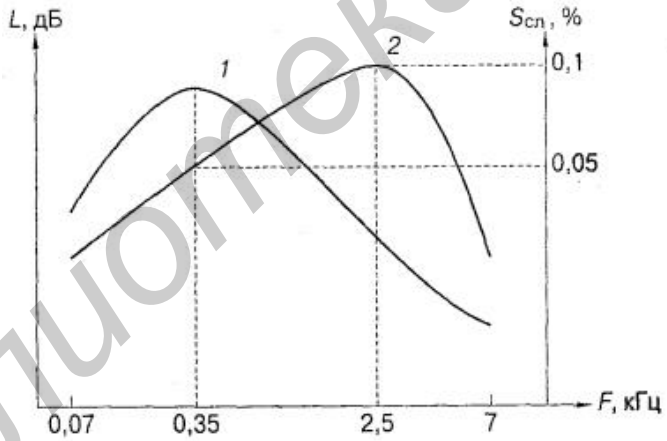


Рис. 3.2. Среднестатистический спектр русской речи

Уровни речевых сигналов. В различных условиях человек обменивается речевой информацией с различным уровнем громкости, при этом создаются следующие уровни звукового давления, в дБ:

тихий шепот	35–40;
спокойная беседа	55–60;
выступление в аудитории без средств звукоусиления	65–70.

Динамический диапазон. Уровень речи в процессе озвучивания одного сообщения может меняться в значительных пределах. Разность между квазимаксимальными и квазиминимальными уровнями для различных видов речи составляет в дБ:

дикторская речь	25–35;
телефонные переговоры	35–45;
драматическая речь	45–55.

3.2.3. Распространение акустических сигналов в помещениях и строительных конструкциях

При своем распространении звуковая волна, доходя до какой-либо преграды (границы двух сред) и взаимодействуя с ней, частично отражается от нее, а частично продолжает распространяться по преграде. Количество акустической энергии, прошедшей из одной среды в другую, зависит от соотношения их акустических сопротивлений (рис. 3.3).

$$\rho_1 C_1 = 41 \text{ (МПа·с)/м}; \ \rho_2 C_2 = 30–40 \text{ (МПа·с)/м}. \qquad (3.6)$$

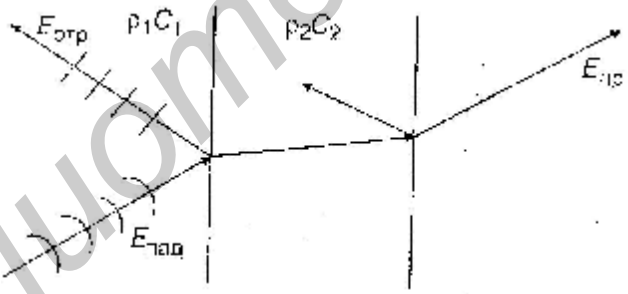


Рис. 3.3. Прохождение акустической волны из одной среды в другую

В строительной акустике используются следующие основные понятия:

– коэффициент поглощения $\alpha = \dfrac{\left(E_{пад} - E_{отр}\right)}{E_{пад}}$;

– коэффициент отражения $\beta = \dfrac{E_{отр}}{E_{пад}}$;

– коэффициент звукопроницаемости $\gamma = \frac{E_{\text{пр}}}{E_{\text{пад}}}$;

– звукоизоляция $Q = 10\lg\frac{E_{\text{пад}}}{E_{\text{пр}}}$.

3.2.4. Технические каналы утечки речевой информации

На рис. 3.4 представлены основные варианты возможной утечки речевой информации из объемов выделенных помещений. Все их можно объединить в две группы – это акустические каналы (обозначены буквами *а*, *б*, *в*), т. е. такие каналы, по которым информация может быть перехвачена с помощью микрофонов воздушной проводимости или прослушана непосредственно человеком, и виброакустические каналы (обозначены буквами *г*, *д*, *е*), т.е. каналы, по которым информация может быть зафиксирована с помощью микрофонов твердой среды (виброметров, велосиметров, акселерометров).

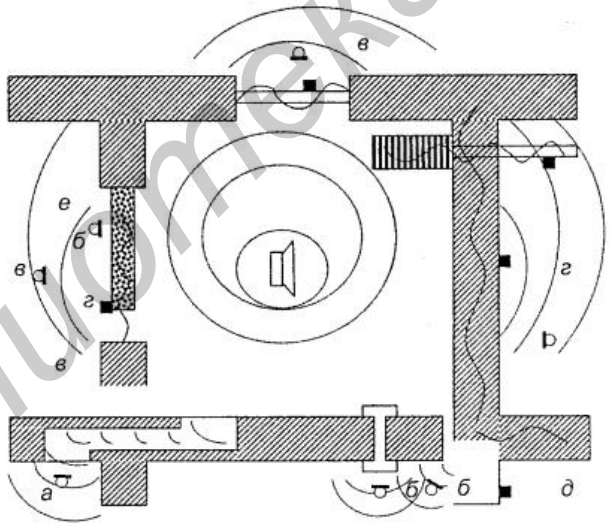


Рис. 3.4. Основные технические каналы утечки речевой информации

Наибольшую опасность представляют технологические окна и каналы с большой площадью поперечного сечения, такие как короба коммуникаций и воздуховоды вентиляции. Эти объекты являются по сути акустическими волноводами, и звуковые колебания могут распространяться по ним на значительные расстояния. Так, если поперечные размеры короба сравнимы с длиной звуковых волн L = λ,

затухание при распространении по нему звука составляет $\delta = 0{,}01 – 1$ дБ/м и зависит от размеров короба, материала стенок и пр.

Следующими по степени опасности являются звуководы с размерами, значительно меньшими длины звуковых волн $L << \lambda$. Таковыми могут быть отверстия электропроводки, щели и трещины в строительных конструкциях, неплотности дверных и оконных проемов. Затухание звука в таких каналах весьма значительно $\delta = 1–20$ дБ/м. Оно определяется вязкостью воздуха и зависит от поперечных размеров отверстий, шероховатости поверхности и продольной конфигурации отверстия.

Несмотря на заметную величину затухания, этого абсолютно недостаточно для обеспечения защиты информации. Так, если в стене толщиной 0,5 м имеется трещина с площадью поперечного сечения 5 мм^2 и длиной 0,75 м, звукоизоляция в области выхода этой трещины на поверхность будет составлять 18 дБ, в то время как при отсутствии трещины такая стена может обеспечить звукоизоляцию более 65 дБ.

Звуковые колебания могут распространяться за пределы выделенного помещения не только за счет тех или иных воздушных каналов, но и за счет переизлучения колебаний ограждающими строительными конструкциями.

Переизлучение звука за пределы выделенного помещения происходит за счет колебаний строительных конструкций, вызванных падающими на них звуковыми волнами. Так как толщина подавляющего большинства строительных конструкций (стены, полы, потолки, двери, окна) значительно меньше их поперечных размеров, процессы, происходящие в них, хорошо описываются теорией колебания мембран и пластин.

Таким образом:

– акустическое сопротивление ограждающих строительных конструкций в направлении, перпендикулярном их поверхности, невелико;

– строительные конструкции имеют большое количество собственных мод колебаний.

Последнее явление в строительной акустике носит название «волнового совпадения». Оно возникает, когда длина падающей звуковой волны совпадает с длиной изгибной волны в строительной конструкции, и приводит к значительному снижению звукоизоляции (рис. 3.5).

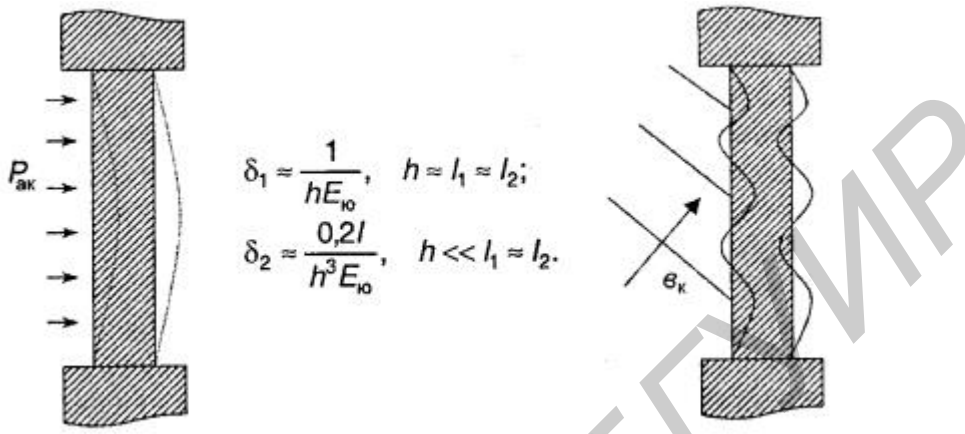


Рис. 3.5. Снижение звукоизоляции строительных конструкций

Так как за счет многократных переотражений звуковой волны в помещении равновероятны любые углы падений, возбуждаются все собственные моды колебаний строительных конструкций, что приводит к существенному снижению звукоизоляции.

3.2.5. Виброакустические каналы

Таким образом, строительные конструкции совершают значительные колебания под воздействием акустических волн. Чтобы перехватить информацию, переносимую этими колебаниями, необязательно регистрировать акустические колебания, переизлученные этими конструкциями, достаточно зафиксировать колебания собственно строительных конструкций. Так, например, под воздействием звука $P_{ак}$ = 70 дБ кирпичная стена толщиной 0,5 м совершает вибрационные колебания с ускорением $a = 3 \cdot 10^{-5} g$. При таких условиях современными средствами может быть прослушан даже шепот. При этом переизлученный акустический сигнал будет $P_{ак.пр}$ < 10 дБ, что практически исключает возможность перехвата информации. Таким образом, вибрационные колебания ограждающих конст-

рукций под воздействием звуковых волн образуют один из наиболее опасных виброакустических каналов утечки информации.

Современные строительные материалы и конструкции (монолитный железобетон, сборные железобетонные конструкции, кирпичная кладка) обладают весьма низкими показателями затухания механических колебаний в области звуковых частот. Это обеспечивает распространение колебаний на значительные расстояния и создает возможность перехвата информации, регистрируя вибрации не только ограждающих конструкций выделенного помещения, но и регистрируя колебания значительно удаленных (1 – 3 стыка) элементов здания. Например, существует реальная возможность перехвата информации по несущей стене из выделенного помещения, расположенного через 1, 2 этажа от места установки аппаратуры перехвата. В общем случае в зависимости от конструкции здания и качества выполнения стыков между его элементами затухание на стыках варьируется в пределах от 1 – 3 дБ до 10 – 15 дБ. Отсюда следуют важная тактическая особенность и повышенная опасность виброакустического канала утечки информации: перехват информации возможен не только из смежных помещений, но и из помещений, значительно удаленных от источника информации.

Некоторые элементы строительных конструкций, как и в случае рассмотрения акустического канала, представляют собой волноводы вибрационных колебаний. К ним относятся трубы различных коммуникаций (отопления, водоснабжения, электропитания и пр.). Как и в случае воздушных волноводов, значительная разница в величинах акустического сопротивления материала труб и окружающей среды составляет

$$\frac{(\rho C)_{ср}}{(\rho C)_{бет}} = 4 - 8, \qquad (3.7)$$

где $(\rho C)_{ср}$ – волновое сопротивление среды распространения акустической волны; $(\rho C)_{бет}$ – волновое сопротивление бетона.

Создаются условия волноводного распространения сигналов на значительные расстояния. Данный канал становится особенно опасным, если трубо-

провод соединен с какой-либо жесткой и развитой поверхностью, которая играет роль согласующего элемента при передаче энергии из воздуха в трубопровод. Таким согласующим элементом, например, являются современные легкие радиаторы отопления.

3.2.6. Аппаратный комплекс имитации утечки информации по виброакустическому каналу и ее защиты

Состав и назначение аппаратных средств. Структурная схема аппаратного комплекса представлена на рис. 3.6.

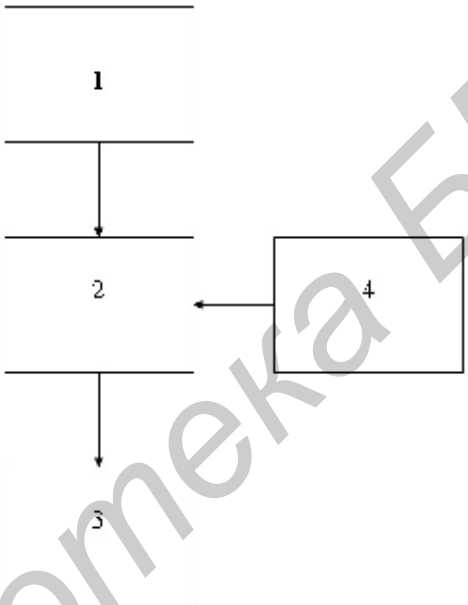


Рис. 3.6. Структурная схема аппаратного комплекса утечки информации:
1 – источник звука; 2 – среда распространения колебаний;
3 – приёмное устройство; 4 – устройство активного зашумления

Источник звука. В качестве источника звука используется низкочастотный генератор гармонических сигналов ГЗ-112 (рис. 3.7), нагруженный на динамическую головку прямого излучения (рис. 3.8).

Рис. 3.7. Внешний вид и назначение органов управления генератора Г3-112:

1 – тумблер сети питания; 2 – диск со шкалой частот; 3 – ручка плавной регулировки частоты; 4 – переключатель множителя частоты; 5 – тумблер выбора формы генерируемого сигнала; 6 – переключатель выходного аттенюатора; 7 – ручка плавной регулировки уровня выходного сигнала; 8 – разъем выхода генератора

Среда распространения сигнала. В качестве среды распространения может использоваться любой твёрдый материал: оргстекло, бетон и т.д. В данном комплексе используется модель ограждающей конструкции (см. рис. 3.8) из листа оргстекла размером 300х400 мм.

Рис. 3.8. Внешний вид модели ограждающей конструкции и размещение элементов комплекса на ней:

1 – разъем виброэлектрического датчика; 2 – виброэлектрический датчик; 3 – крепление виброэлектрического преобразователя; 4 – виброэлектрический преобразователь; 5 – динамическая головка прямого излучения

Приёмное устройство (электронный стетоскоп). Представляет собой электронное устройство, которое преобразует механические колебания в электрический сигнал (рис. 3.9) и состоит из виброэлектрического датчика, усилителя, источника питания и головных телефонов.

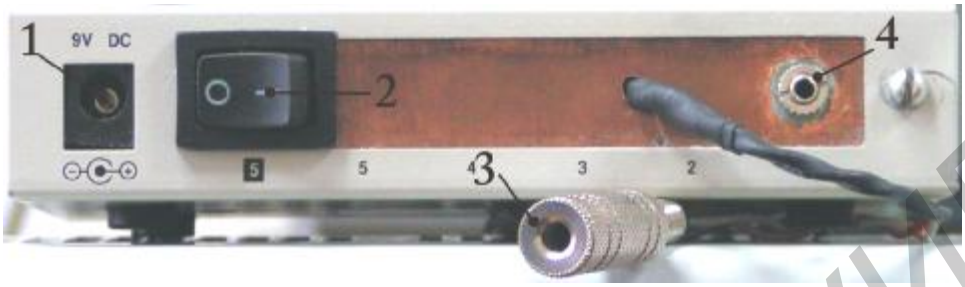


Рис. 3.9. Назначение органов управления приемного устройства:

1 – разъем для подключения источника питания; 2 – тумблер питания; 3 – разъем для подключения головных телефонов; 4 – разъем для подключения виброэлектрического датчика

Устройство активного зашумления. В качестве устройства активного зашумления используется устройство защиты речевой информации (УЗРИ) «Кабинет».

Устройство «Кабинет» предназначено для предотвращения несанкционированного перехвата речевой информации через ограждающие конструкции и инженерные коммуникации выделенных помещений.

«Кабинет» обеспечивает защиту от следующих технических средств перехвата информации:

– устройства, использующие контактные микрофоны (электронные, проводные и радиостетоскопы);

– устройства дистанционного перехвата информации (лазерные микрофоны, направленные микрофоны);

– закладные устройства, внедряемые в строительные элементы конструкций.

Технические характеристики устройства «Кабинет» приведены в табл. 3.1.

Устройство защиты речевой информации «Кабинет» состоит из акустического генератора шума (АГШ), подключенных к нему электроакустических преобразователей (подключаются к выходам Л1, Л2, Л3). Структурная схема устройства приведена на рис. 3.10.

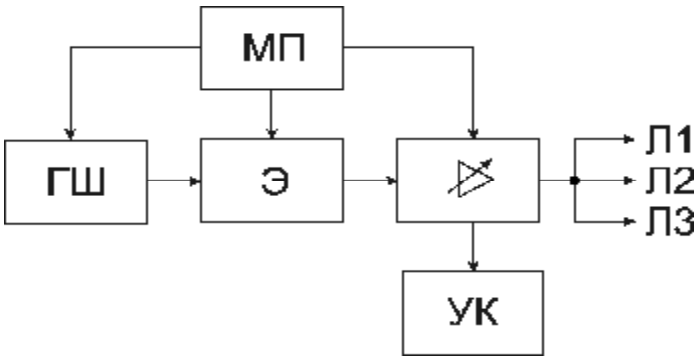


Рис. 3.10. Схема электрическая структурная устройства защиты речевой информации «Кабинет»

В состав АГШ входят (рис. 3.11):

– генератор шума (ГШ);

– усилитель мощности;

– модуль питания (МП);

– эквалайзер (Э);

– устройство контроля (УК).

Таблица 3.1

Технические характеристики УЗРИ «Кабинет»

Эффективная шумовая полоса	175–5600 Гц
Время готовности к работе, не более	3 мин
Питание (сеть переменного тока)	220 В +10%(-15%); 50 ± 1 Гц
Мощность, потребляемая от сети, не более	55 ВА
Габариты АГШ, не более	340×210×100 мм
Масса АГШ, не более	10 кг
Масса преобразователей акустических, не более	0,7 кг
Количество подключаемых преобразователей, не более	12

Основой акустического генератора шума является генератор «окрашенного» шума. Сигнал с генератора «окрашенного» шума после амплитудного ограничения поступает на полосовой фильтр с частотами среза 175 и 5600 Гц и затуханием сигнала 12 дБ на октаву вне полосы пропускания.

В АГШ предусмотрена возможность регулировки частотной характеристики формируемого сигнала помехи с помощью пятиполосного октавного эквалайзера (центральные октавные частоты 250, 500, 1000, 2000, 4000 Гц), после чего сигнал поступает на усилитель мощности с регулируемым коэффициентом усиления (рис. 3.11). Глубина регулировки усиления по полосам не менее ±20 дБ. Глубина регулировки общего уровня сигнала не менее 40 дБ.

Рис. 3.11. Назначение органов управления УЗРИ «Кабинет»:

1 – тумблер сети питания; 2 – сетевой предохранитель; 3 – регулятор усиления; 4, 5, 6, 7, 8 – регуляторы эквалайзера для соответствующих октавных частот; 9 – разъем подключения заземления; 10 – разъемы для подключения электромеханических преобразователей; 12 – ручка плавной регулировки уровня шума на встроенной динамической головке прямого излучения

К усилителю мощности подключено устройство контроля, предназначенное для индикации исправной работы АГШ. Оно позволяет проверить наличие шумового сигнала на выходе АГШ.

К выходам усилителя мощности подключаются электромеханические преобразователи. Общее количество одновременно подключаемых электромеханических преобразователей – до 12. Модуль питания служит для обеспечения устройства питающим напряжением постоянного тока.

3.2. Лабораторное задание

Обеспечить невозможность перехвата речевой информации в ограждающей конструкции в частотном диапазоне 175 – 5600 Гц средствами акустической разведки. Для этого необходимо:

1. К выходу генератора ГЗ-112 подключить динамическую головку прямого излучения, находящуюся на модели ограждающей конструкции.

2. Подключить виброэлектрический преобразователь к электронному стетоскопу.

3. Подключить головные телефоны к электронному стетоскопу.

4. Подключить источник питания к электронному стетоскопу.

5. Подключить электромеханический преобразователь, размещенный на модели ограждающей конструкции, к УЗРИ «Кабинет». УЗРИ «Кабинет» размещают на резиновых ножках таким образом, чтобы были легко доступны его регуляторы эквалайзера и усиления для дальнейшей работы.

6. Установить регуляторы уровня сигнала и эквалайзера на УЗРИ «Кабинет» в крайнее левое положение.

7. Повернуть ручку плавной регулировки уровня выходного сигнала генератора в крайнее левое положение.

8. Выставить на генераторе частоту 1 кГц.

9. Включить в электрическую сеть генератор ГЗ-112 и УЗРИ «Кабинет».

10. Перевести тумблеры питания генератора и электронного стетоскопа в положение «включено».

11. Плавно вращая вправо ручку регулировки уровня выходного сигнала генератора, добиться наличия звукового сигнала в головных телефонах, подключенных к электронному стетоскопу.

12. Настроить генератор на частоту 250 Гц и при отсутствии или слабом уровне сигнала в головных телефонах увеличить его путем плавного вращения вправо ручки регулятора уровня выходного сигнала генератора.

13. Перевести тумблер питания УЗРИ «Кабинет» в положение «включено».

14. В случае отчетливого прослушивания в наушниках сигнала генератора частотой 250 Гц необходимо, плавно вращая регулятор 250 Гц эквалайзера УЗРИ «Кабинет», добиться зашумления сигнала генератора до полной его неразборчивости.

15. В случае если регулятор 250 Гц эквалайзера УЗРИ «Кабинет» выведен в крайнее правое положение, а сигнал с генератора все равно прослушивается, необходимо, плавно вращая вправо регулятор «усиление», добиться зашумления сигнала генератора до полной его неразборчивости.

16. Повторить выполнение пп. 14 и 15 для октавных частот 500, 1000, 2000 и 4000 Гц.

17. После настройки УЗРИ «Кабинет» убедиться в гарантированном зашумлении диапазона частот 175–5600 Гц путем плавного вращения ручки регулировки частоты генератора и контроля звукового сигнала в головных телефонах на предмет отсутствия звукового сигнала с плавным изменением частоты от низких тонов до высоких.

18. Оформить отчет.

3.3. Содержание отчета

1. Цель работы.

2. Структурная схема аппаратного комплекса имитации утечки информации.

3. Вывод по работе.

4. Ответы на контрольные вопросы.

3.4. Контрольные вопросы

1. Что характеризует коэффициент звукоизоляции.

2. Чем объясняется повышенная опасность виброакустического канала утечки информации.

3. Какие виды шумовых сигналов используют в системах активной защиты.

4. Чем определяется звукоизоляция сложных стен.

5. Каковы особенности установки средств активной защиты на трубопроводах и в тамбурах.

ЛАБОРАТОРНАЯ РАБОТА №4

ИЗУЧЕНИЕ СИСТЕМЫ ОХРАННОГО ТЕЛЕВИДЕНИЯ

Цель: изучить принципы построения систем охранного телевидения; получить практические навыки по настройке и эксплуатации системы охранного телевидения.

4.1. Теоретическая часть

4.1.1. Состав и описание системы охранного телевидения

Состав системы охранного телевидения:

1. Персональный компьютер.
2. Цифровой видеорегистратор (DVR) NVB-025/4A (Novus, Польша).
3. Беспроводная система аудиовидеонаблюдения W413C.

Состав беспроводной системы аудиовидеонаблюдения W413C:

1. Видеокамеры с поворотными устройствами (4 шт.).
2. Трансивер с пультом дистанционного управления.
3. Адаптер для трансивера (12 В).
4. Адаптеры для видеокамер (8 В, 4 шт.).

Система охранного телевидения выполнена на базе персонального компьютера с платой цифрового видеорегистратора NVB-025/4A.

Таблица 4.1

Основные технические характеристики цифрового видеорегистратора NVB-025/4A

Характеристика	Описание
1	2
Максимальная скорость записи на канал, кадров/с	6,25
Вход видеокамеры	4 порта (NTSC/PAL)
Аудиовход	4 порта
Вход датчика	4 порта

Окончание табл. 4.1

1	2
Релейный выход	4 порта
Композитный выход	1 порт (NTSC/PAL, режим квадратора или режим переключения)
Формат изображений	S/W MPEG-4
Режим записи	Слежение, обычный, детектор движения, датчик, запись по расписанию
Удаленное управление	Полнофункциональное по PSTN, ISDN, DSL, Ethernet
Резервное копирование	DAT, CD, DVD
PAN(панорамирование)/TILT(наклон)/ ZOOM(масштабирование)/FOCUS(фокусировка)	Интерфейс RS-232/422/485
Проверка подлинности записанного изображения	Метод водяного знака

Рис. 4.1. Внешний вид платы цифрового видеорегистратора (DVR) NVB-025/4A

Основные функции цифрового видеорегистратора NVB-025/4A

1. **Входы видеокамер.** На экране могут отображаться до четырех каналов видеокамер с возможностью цифрового управления ими. Стандартные параметры входа: 75 Ом, размах видеосигнала 1 В.

2. **Входы датчиков.** К DVR могут быть подключены до четырех датчиков. Требуется внешний источник питания 12 В.

3. **Цифровые (релейные) выходы.** Цифровые выходы DVR могут быть использованы, например, для управления электрозамками и сиренами, которые могут срабатывать по датчику или детектору движения.

4. **Запись звука и возможность двухсторонней связи.** Запись звука возможна вместе с записью видеоизображения. Возможен двухсторонний обмен данными между программами DVR-Main и DVR-Net.

5. **Параметры отображения (w/ Multi-Viewing – многоэкранный режим просмотра).** Многоэкранный режим позволяет одновременно отображать на экране 4 изображения видеокамер. Среди прочих характеристики экрана – увеличение всех изображений видеокамер или только одного из них до полноформатного.

6. **Функции PAN (панорамирование)/TILT (наклон) /ZOOM (масштабирование) /FOCUS (фокусировка).** Любая из подключенных видеокамер может управляться посредством программы DVR-Main, если это позволяют возможности видеокамеры.

7. **Система автоматической перезагрузки.** При обнаружении ошибки или сбоя в операционной системе DVR автоматически выполнит ее перезагрузку для устранения неполадок.

8. **Детектор движения и триггер датчика.** Функция детектора позволяет записывать изображения только при обнаружении движения, что экономит свободное место на диске и позволяет максимально эффективно использовать физический объем памяти.

9. **Запись по расписанию.** Функция расписания дает возможность администратору вести запись изображений только в заданные промежутки времени, если в этом есть необходимость. Программа DVR позволяет комбинировать любые режимы записи по расписанию.

10. **Ручное и автоматическое резервное копирование данных.** Данные могут сохраняться на различных носителях (DAT, CD, DVD), также возможно резервное копирование данных отдельных видеокамер и/или данных за определенные периоды времени. Так же как и для записи, для режима копирования предусмотрена функция расписания.

11. **Поиск цифровых видеозаписей.** Цифровое воспроизведение записей одновременно для всех или одной видеокамеры. Функция воспроизведения вклю-

чает возможности расширенного поиска и извлечения изображений, что позволяет извлекать фрагменты видеозаписей и сохранять их в виде отдельных файлов.

12. **Поддержка сети (PSTN, TCP/IP, LAN , поддержка модемного протокола).** DVR поддерживает доступ по сети, позволяющий администратору входить в программу DVR-Main для удаленного доступа ко всем локальным функциям.

13. **Поддержка POS (платежный терминал), Access Control (контроль доступа), ATM (кассовый терминал).** Запись данных с внешних устройств (POS, Access Control, ATM, и т. д.) вместе с видеозаписью DVR. Функция поиска текста «Text Search» позволяет искать данные с внешних устройств вместе с видеозаписями DVR при наступлении какого-либо события. Это повышает уровень достоверности и безопасности.

Беспроводная система аудиовидеонаблюдения W413C предназначена для эфирной передачи аудио- и видеосигналов на частоте 2,4 ГГц и имеет защиту от интерференции частотой 900 МГц.

Таблица 4.2

Основные технические характеристики беспроводной системы аудиовидеонаблюдения W413C

Характеристика	Описание
Разрешение видеокамер, пикселов	628x628 (PAL), 510x429 (NTSC)
Разрешение по горизонтали, ТВЛ	380
Рабочая частота, ГГц	2,4
Выходная мощность видеокамеры, мВт	10
Чувствительность приемника, дБ	Минус 85
Напряжение питания трансивера, В	12
Напряжение питания видеокамеры, В	8
Рабочий ток видеокамеры, мА	80
Рабочий ток трансивера, мА	250
Дальность приемопередачи в условиях отсутствия помех, м	200
Количество независимых радиоканалов	4
Настройка частоты	Автоматическая

4.1.2. Внешний вид аппаратуры беспроводной системы аудиовидеонаблюдения W413C и назначение органов ее управления

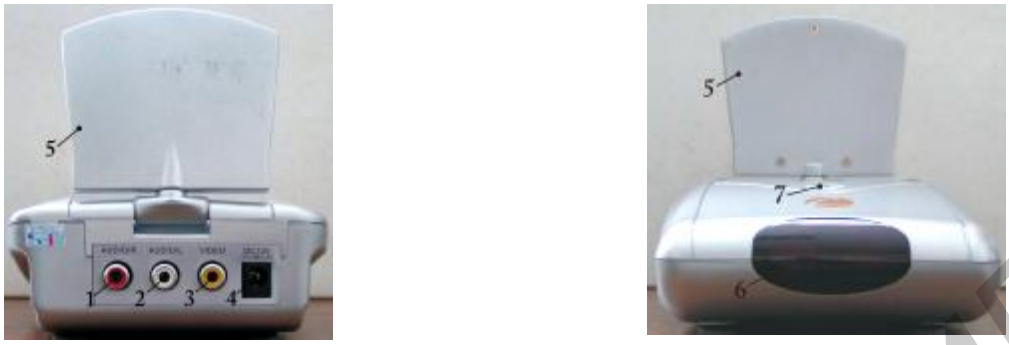


Рис. 4.2. Внешний вид и расположение органов управления трансивера:

1 – выход аудио правый канал; 2 – выход аудио левый канал; 3 – выход видео; разъем источника питания; 5 – антенна; 6 – ИК-приемник сигналов пульта ДУ; 7 – кнопка управления переключением видеокамер; 8 – пульт дистанционного управления

а *б*

Рис. 4.3. Внешний вид адаптеров для трансивера (*а*) и видеокамер (*б*)

(*а*) (*б*)

Рис. 4.4. Вариант вертикального размещения антенны трансивера (*а*) и вертикального с поворотом на 90° (*б*)

Рис. 4.5. Внешний вид видеокамеры:

1 – объектив; 2 – поворотное устройство; 3 – разъем блока питания; 4 – номер, указывающий номер канала, на котором работает видеокамера; 5 – антенна

4.1.3. Порядок работы с системой охранного телевидения

1. Если персональный компьютер не выключен, выключить его.

2. Установить трансивер на системном блоке персонального того компьютера, к которому он будет подключен.

3. Соединить кабелем выход «видео» трансивера (рис. 4.2) с одним из видео входом DVR (например первый канал) (см. рис. 4.1).

4. Антенну трансивера поднять в вертикальное положение.

5. Подключить блок питания (12 В) к трансиверу (см. рис. 4.3, а).

6. Позиционировать видеокамеры в помещении.

7. Подключить блок питания (8 В) к видеокамерам (рис. 4.3, б).

8. Включить блоки питания трансивера и видеокамер в сеть электропитания.

9. Включить персональный компьютер.

10. Выключение оборудования выполняется в обратной последовательности.

4.2 Лабораторное задание

Получить практические навыки по настройке и технической эксплуатации системы охранного телевидения. Для этого необходимо:

1. Собрать систему охранного телевидения.

2. Настроить фокусировку изображения видеокамер (дополнительное оборудование для настройки получить у преподавателя).

3. Запустить программу конфигурирования DVR – DVR Search.exe.

4. Ввести Login Name и Password.

5. Ознакомиться с закладками главного окна программы в соответствии с инструкцией (Integration. User manual.pdf).

6. Изучить назначение органов настройки, для программы настройки конфигурации DVR, переключаясь по закладкам Disk tool, System, Camera, Sensor, Backup, User admin в соответствии с инструкцией по работе с программой.

7. Настроить DVR следующим образом:

7.1. Создать 20 томов для записи видеоданных на диске E.

7.2. Включить следующие опции:

- ведение системного журнала;
- ведение журнала срабатывания детектора движения;
- ведение журнала, регистрирующего вход пользователей в систему;
- остальные журналы отключить.

7.3. Установить минимально возможное количество изображений видеокамер на экране при запуске системы.

7.4. Включить опцию предупреждения о заполнении диска и выполнить ее настройку по своему усмотрению.

7.5. Указать путь для программы записи CD.

7.6. Установить минимально возможное разрешение для видеокамер.

7.7. Настроить степень сжатия видеопотока по своему усмотрению.

7.8. Включить уведомление о потери видеосигнала.

7.9. Настроить детектор движения по своему усмотрению.

7.10. Проверить срабатывание детектора, при необходимости скорректировать его настройку.

7.11. Настроить яркость, контрастность и насыщенность изображения, получаемого с видеокамер по своему усмотрению.

7.12. Настроить автоматическое резервное копирование по расписанию (расписание составить по своему усмотрению). Директория для резервного копирования E:/номер группы, например E:/463003.

7.13. Включить подачу звукового сигнала динамиком ПК при наступлении различных событий.

8. Запустить программу DVR main.exe.

9. Ввести Login Name (user) и Password (reader).

10. Изучить назначение органов управления программой в соответствии с инструкцией (Integration. User manual.pdf).

11. Произвести запись видеопотока по срабатыванию детектора движения.

12. Просмотреть записанный видеопоток.

13. Сохранить файл в MP4 формате (директория для сохранения E:/номер группы, например E:/463003) и просмотреть его (DVR AVI Viewer.exe).

14. Сохранить отдельные 3 кадра записанного видеопотока (директория для сохранения E:/номер группы, например E:/463003) и просмотреть их (Auth Tool.exe). Удостовериться в том, что каждый кадр защищен водяным знаком.

15. Произвести запись видеопотока по расписанию и для полученных данных выполнить пп. 12, 13, 14.

16. Выполнить резервное копирование всех записанных данных, запустив программу Backup.exe.

17. Убедиться в том, что резервное копирование выполнено успешно (Backup Viewer.exe).

18. Записать сохраненные данные (видеофайлы с расширением MP4 и отдельные кадры с расширением JPG) на CD или DVD диск.

19. Просмотреть записи системного журнала с помощью программы Log Viewer.exe.

4.3. Содержание отчета

1. Цель работы.

2. Таблица результатов:

№	Название файла	Информация водяного знака
Время входа в систему		
Время срабатывания детектора движения		

3. Вывод по работе.

4. Ответы на контрольные вопросы.

4.4. Контрольные вопросы

1. Назначение цифрового видеорегистратора.

2. Что такое водяной знак для изображения?

3. Назначение детектора движения.

4. Назначение беспроводной системы аудиовидеонаблюдения W413C в составе системы охранного телевидения.

5. К чему приведет увеличение разрешения видеоизображения?

ЛАБОРАТОРНАЯ РАБОТА №5
ИЗУЧЕНИЕ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ ОБЪЕКТОВ РАЗЛИЧНЫХ КАТЕГОРИЙ

Цель: изучить принципы построения систем контроля и управления доступом, получить практические навыки по выбору и обоснованию методов и средств аутентификации пользователей в системах контроля и управления доступом для объектов различных категорий.

5.1. Теоретическая часть

5.1.1. Категории объектов

Категория охраняемого объекта – комплексная оценка состояния объекта, учитывающая его экономическую или иную значимость в зависимости от концентрации сосредоточенных ценностей, последствий от возможных преступных посягательств на них, сложности обеспечения требуемой надежности охраны. Результат оценки может быть выражен качественно или количественно. Примером качественных оценок служат перечневые классификаторы (список категорий объектов с краткими пояснениями). В табл. 7.1 приведена классификация, основанная на оценке ущерба от реализации угроз.

К категории А следует отнести особо важные объекты, на которых возможный ущерб в случае реализации основных угроз безопасности максимален по характеру и по масштабам. Его последствия выходят за пределы территории объектов и не могут быть локализованы в пространстве и во времени за счет принятия немедленных ликвидационных мер. Характер ущерба заключается в создании угрозы для жизни и здоровья персонала и населения, а также в негативном воздействии на природную среду.

К категории Б предлагается отнести важные объекты, на которых характер возможного ущерба заключается в угрозе для жизни и здоровья персонала объекта, а его последствия не выходят за пределы территории объекта и могут быть локализованы путем принятия ликвидационных мер. К этой же категории

предлагается отнести объекты, возможный ущерб на которых носит материальный характер, но его масштабы имеют региональное значение.

Таблица 5.1

Классификация объектов

Категория	Наименование категории	Ущерб или последствия от осуществления угроз	Назначение или принадлежность объектов
А	Особо важные	Особо крупный или невосполнимый материальный ущерб, экологическая катастрофа на объекте или в регионе, гибель большого числа людей на объекте или в регионе, политические последствия, утечка государственных секретов, другие особо тяжкие последствия	Хранилища и депозитарии банков, предприятия по производству или хранилища химически опасных, наркотических и взрывчатых веществ, боеприпасов, ядерных материалов; предприятия оборонного профиля; правительственные учреждения; энергетические комплексы
Б	Важные	Значительный материальный или финансовый ущерб, угроза здоровью или жизни людей, утечка государственных или коммерческих секретов	Кассовые залы банков, подъезды инкассаторских машин; помещения для хранения и работы с конфиденциальной информацией; крупные торговые центры; производственные помещения
В	Прочие	Материальный или финансовый ущерб; информационный ущерб; нарушение комфортности личной жизни или служебной деятельности	Магазины, служебные помещения, офисы, производственные помещения, жилые помещения

Прочие объекты (категория В) характеризуются тем, что возможный ущерб носит локальный и в основном материальный характер и по масштабу может иметь региональное значение.

В свою очередь каждую категорию объектов можно классифицировать по масштабу или размеру нанесенного ущерба в результате несанкционированного доступа (НСД) нарушителей.

Например, особо важные объекты предлагается дополнительно разделить на три группы безопасности (№1, 2, 3). Номер группы определяет масштаб возможного ущерба, который может иметь последствия соответственно трансграничного, государственного, регионального значений.

Для других категорий объектов можно использовать предложенную в таблице классификацию по группам значимости и уровням защищенности. При этом следует заметить, что при установлении уровня защищенности необходимо дополнительно учитывать возможные угрозы безопасности для конкретного объекта, которые определяются в основном сложившейся криминогенной обстановкой в данном регионе.

Принадлежность объекта к соответствующей категории и группе необходимо определять на начальной стадии проектирования системы информационной безопасности (СИБ), так как от этого зависит не только уровень его защищенности, но и планируемая тактика действий сил охраны по ликвидации последствий несанкционированного доступа на объект. От этой тактики зависят общие затраты на создание СИБ.

Различие в тактике действий сил охраны должно учитываться в процессе создания СИБ при определении структуры, количественного состава и оснащенности сил охраны, а также при выборе типов и взаимного расположения инженерных средств задержки нарушителя. Оптимизация структуры СИБ по критерию «эффективность – стоимость» позволяет обеспечить достаточно эффективную защиту объекта от НСД при минимальных затратах ресурсов.

5.1.2. Классификация помещений и территории объекта

К вопросу классификации служебных помещений с точки зрения их безопасности существует несколько подходов. Учитывая, что степень безопасности от перечисленных выше угроз тесно связана прежде всего с режимом пребывания в помещениях сотрудников и посетителей, целесообразно проводить классификацию по степени режимных ограничений и возможности доступа в них.

Предлагается все помещения и территорию разбить на шесть категорий, или зон, представленных в табл. 5.2.

Свободная зона – помещения и прилегающая территория, доступ в которые свободен для любой категории лиц. За этими территориями не ведется наблюдения и там не размещено никаких технических средств охраны и безопасности. Примером такой зоны может быть бюро пропусков, справочное бюро и др.

Наблюдаемая зона – помещения и территория, доступ в которые также не ограничен, но за ними ведется систематическое наблюдение силами службы безопасности или охраны. Наблюдение может вести лицо, находящееся в данном помещении или в других помещениях, с помощью оптических или телевизионных приборов. Типичным примером может служить вестибюль объекта, территория служебной автостоянки и др.

Регистрационная зона – зона, вход в которую свободен для любого желающего при условии, что он предъявит для регистрации документ, удостоверяющий его личность. Такая система часто используется в учреждениях, работающих с большим числом клиентов.

Режимная зона – зона, на входе в которую находится пост охраны. Проход допускается либо по пропускам установленной формы, либо по именным заявкам лиц, имеющих соответствующее право.

Зона усиленной защиты – это помещения, куда допускаются только сотрудники предприятия, а для посторонних лиц доступ туда возможен только по специальным пропускам или в сопровождении уполномоченных лиц. Такого рода помещения, как правило, оборудуются средствами контроля доступа и охранной сигнализацией. Вход в эту зону может также контролироваться постом охраны.

Таблица 5.2

Классификация территории и помещений объекта

Категория зоны	I	II	III	IV	V	VI
Наименование зоны	Свободная зона	Наблюдаемая зона	Регистрационная зона	Режимная зона	Зона усиленной защиты	Зона высшей защиты
Пример функционального назначения	Места свободного посещения	Комнаты приема посетителей	Кабинеты сотрудников	Секретариат, компьютерные залы, архивы	Материальные склады	Кабинеты руководителей, комнаты для ведения переговоров, спецхранилища
Условия доступа сотрудников	Свободный	Свободный	Свободный	По служебным удостоверениям, идентификационным картам	По спецдокументам	По спецдокументам
Условия доступа посетителей	Свободный	Свободный	Свободный с регистрацией по удостоверениям личности	По разовым пропускам	По спецпропускам	По спецпропускам
Наличие охраны	Есть	Есть	Есть	Усиленная охрана	Усиленная охрана	Усиленная охрана
Наличие технических средств охраны	Нет	Средства наблюдения	Охранная сигнализация	Охранная сигнализация, система контроля доступа (СКУД)	Охранная сигнализация (2 рубежа), СКУД, механическое усиление	Охранная сигнализация (2 рубежа), СКУД, защита от утечки информации, механическое усиление

Зона высшей защиты – зона, вход в которую ограничен не только для клиентов и посетителей, но и для собственных сотрудников, не имеющих прямого отношения к данным помещениям. Хорошим примером может служить помещения высшего руководства или помещения, связанные с хранением и обработкой особо ценной и конфиденциальной информации. Зона высшей защиты оборудует-

ся инженерно-техническими средствами, приборами контроля и наблюдения и дополнительными постами охраны.

Представленные шесть категорий режимности практически способны охватить все варианты функционального назначения служебных помещений. Задание помещению одной из приведенных категорий сразу регламентирует следующие факторы:

– условия доступа сотрудников предприятия;

– условия доступа клиентов и посторонних лиц;

– наличие и вид физической охраны;

– виды использования технических средств наблюдения и охраны.

Кроме этого, нанесение на план здания, например, категорий режимности всех помещений позволит наглядно увидеть все недостатки в распределении помещений по функциональному назначению. Наиболее оптимальным способом распределения помещений является компактное размещение в одном месте помещений одной и той же категории. При этом желательно, чтобы между собой соседствовали зоны одинаковых или не слишком различающихся категорий. Например, попасть в помещение IV зоны можно только из помещения III или V зоны. Это позволит наиболее экономным способом разместить средства инженерного усиления строительных конструкций и технические средства безопасности.

5.1.3. Принципы построения систем контроля доступа

Структура систем контроля доступа

Системой контроля и управления доступом (СКУД) называется совокупность программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также оперативного контроля за персоналом и временем его нахождения на территории объекта.

СКУД обеспечивает возможность доступа определенных лиц в определенные помещения и ограничивает доступ лиц, не имеющих права доступа в соответствующие зоны.

Общая структура систем контроля доступа представлена на рис. 5.1.

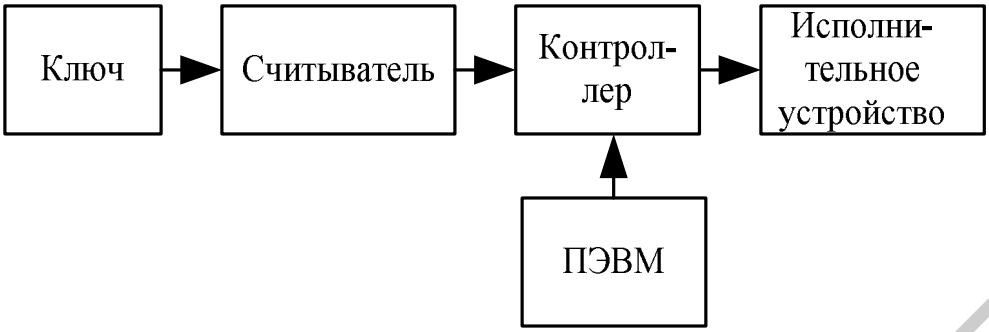


Рис. 5.1. Общая структура СКУД

Более детальная схема с перечислением разновидностей управляющих, исполнительных устройств и считывателей представлена на рис. 5.2.

Основными элементами типовой системы контроля доступа являются следующие устройства:

– автономный или сетевой контроллер – устройство, управляющее в свою очередь имеющимися в системе исполнительными устройствами, в памяти которого также хранятся коды ключей лиц, имеющих право прохода и настройки системы управления доступом;

– исполнительное устройство – электромеханический или электромагнитный замок, электромеханическая защёлка, двери или ворота, оборудованные электроприводом, шлагбаумы или турникеты;

– устройства считывания ключей доступа, биометрических параметров или непосредственно носителей цифрового кода, в качестве которых чаще всего применяются электронные ключи Touch Memory или пластиковые бесконтактные Proxy-карты, радиочастотные метки. В состав устройств считывания входит также один или несколько персональных компьютеров, необходимых для организации автоматизированного рабочего места охраны, бюро пропусков, руководителя.

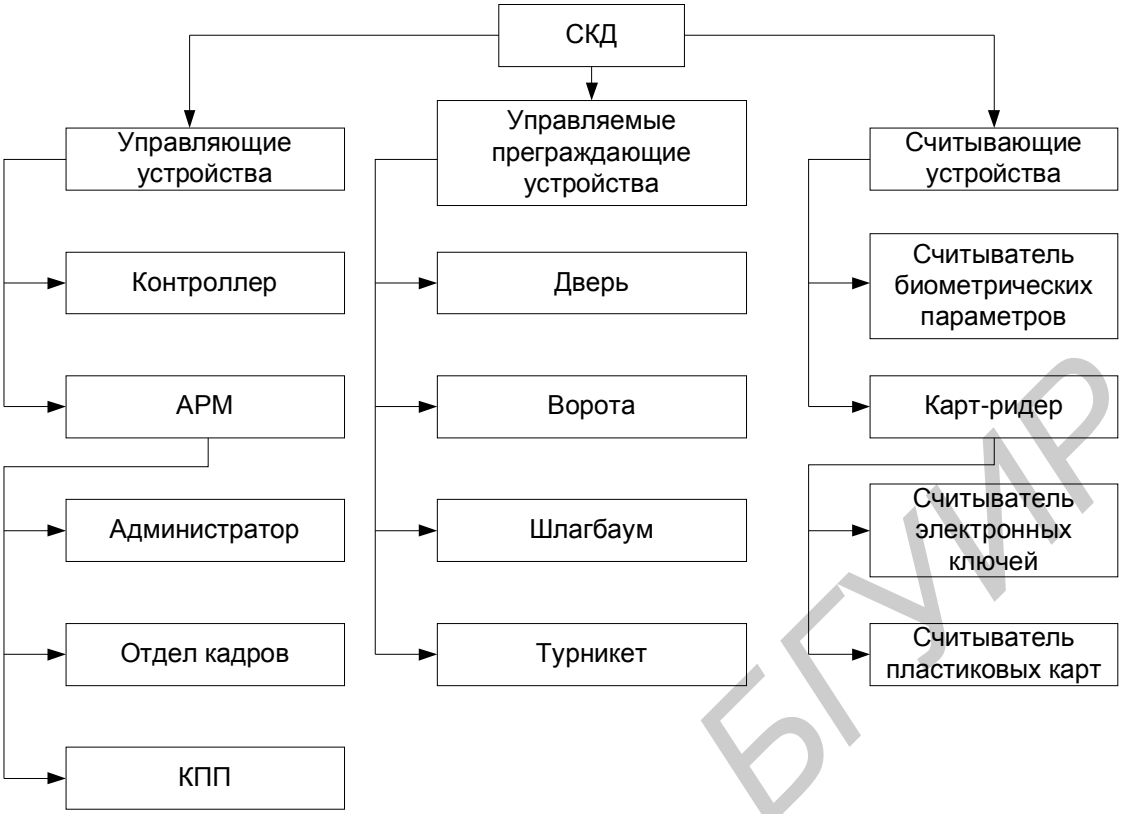


Рис. 5.2. Состав СКУД

Для получения информации с ключей использованы устройства идентификации. В зависимости от типа носителя изменяется и тип устройства идентификации. Передачу информации с различного вида карт осуществляют специальные считыватели, использующие те или иные физические принципы. Для получения информации о биометрических параметрах человека используют биометрические терминалы, а PIN-код вводится с клавиатур различных типов.

Информация, получаемая с ключей, поступает в процессорный блок – контроллер, который ее обрабатывает, анализирует, принимает решение об аутентификации. Любая система обязательно имеет плату, на которой размещаются микропроцессор и другие электронные элементы. Плата располагается в отдельном блоке-контроллере или в корпусе считывателя. Архитектура контроллера, совмещенного со считывателем, более устойчива к обрывам сети передачи данных, но и менее защищена от несанкционированного доступа, так как решающее устройство расположено вне охраняемого помещения.

СКУД имеет интерфейс с персональным компьютером. В системах достаточно большой емкости компьютер, используя специализированное программное обеспечение, полностью управляет контроллерами, принимает, обрабатывает и архивирует информацию, поступающую с защищаемого объекта, осуществляет взаимодействие с системой охраны его периметра.

Важнейшим элементом СКУД является периферийное оборудование, поскольку именно оно вступает в непосредственный «физический» контакт с пользователем в процессе идентификации и аутентификации его личности. **Идентификация** – процедура опознания объекта (пользователя) по предъявленному идентификатору (некоторой уникальной информации), установление тождества объекта или личности по совокупности общих и частных признаков. В отличие от идентификации **аутентификация** подразумевает установление подлинности личности на основе сообщаемых проверяемым субъектом сведений о себе. Такие сведения называют идентификационными признаками. При проверке на контрольно-пропускном пункте (КПП) они представляют собой, как правило, персональные установочные данные (фамилия, имя, отчество), личный идентификационный номер (код), биометрические характеристики, однозначно определяющие личность пользователя системой. Идентификационные признаки, или идентификаторы, могут быть зафиксированы на материальном носителе (пластикой карте, электронном ключе), который при проверке на КПП считывается аппаратурой или непосредственно в процессе проверки вводится пользователем в систему через терминал. Для ввода идентификаторов пользователя в СКУД применяются следующие основные виды периферийного оборудования:

– кодонаборные терминалы;

– считывающие устройства;

– биометрические терминалы.

Основу современных СКУД составляют автоматические и автоматизированные СКУД, в них процедура проверки может включать также сопоставление лица проверяемого с видеопортретом на мониторе контроллера. В таких систе-

мах в составе периферийного оборудования имеется видеокамера, вмонтированная в считывающий терминал.

Современные автоматические и автоматизированные СКУД в зависимости от способа управления подразделяются на автономные, централизованные и распределенные.

Автономные (локальные) СКУД, управляемые микрокомпьютером, как правило, обслуживают один КПП (возможно, с несколькими линейками прохода и соответственно с несколькими контрольными терминалами). Идентификационная информация о пользователях и их полномочиях хранится в локальной базе данных. СКУД такого типа наиболее просты по конфигурации, но и наименее надежны. Их можно применять в основном на тех объектах, где не требуется высокий уровень безопасности. Часто такие системы называются однодверными. На рис. 5.3 приведена типовая схема построения такой системы.

Чаще всего к контроллеру можно подключить до двух считывателей, которые устанавливают на две двери или на одну для контроля входа и выхода. Один из считывателей можно заменить на клавиатуру для набора кода. Кроме этого, система позволяет взаимодействовать с электрозамками, кнопками выхода, герконами, ИК-датчиками, сиренами и др.

Существуют однодверные системы, аналогичные описанной выше, но в них считыватель и контроллер объединены в один корпус, т. е. блок, принимающий решение об открытии замка, сосредоточен в считывающем модуле. Это, с одной стороны, удешевляет систему, но с другой, – уменьшает функциональные возможности, а главное увеличивает вероятность взлома путем вскрытия корпуса считывателя и замыкания контактов, к которым подключен замок.

Рис. 5.3. Схема автономной СКУД

В еще более дешевых системах совмещаются в одном корпусе принимающий решение блок, клавиатура для набора кода, считыватель и замок. Наибольшее распространение такие системы получили в гостиницах.

На объектах с требованиями повышенной безопасности применяются контроллеры с цифровым управлением реле замка. Выносной модуль реле замка монтируется непосредственно возле замка и управляется особым цифровым кодом.

Чаще всего в автономных системах используются считыватели магнитных карт Touch Memory и «проксимити», гораздо реже – биометрических параметров, карт Виганда. В большинстве автономных систем считыватели совмещены с клавиатурой для набора индивидуального кода.

Существуют также системы на основе одного или нескольких автономных контроллеров, которые осуществляют все необходимые действия, присущие СКУД, автономно (без использования управляющего компьютера). Контроллеры в таких системах обязаны иметь собственный буфер памяти номеров карт (идентификаторов) и происходящих в системе событий. Как правило, они имеют выход на локальный принтер для распечатки протокола событий. Программируются указанные контроллеры, как правило, с кнопочных панелей или с помощью «мастер-карт», позволяющих заносить в память контроллера новые карты и удалять старые.

Один контроллер в таких системах обычно управляет одной (максимум двумя) дверями. В качестве идентификаторов (электронных пропусков) в таких системах могут применяться магнитные карты, электронные ключи – «i-Button», радиочастотные PROX-карты и др. Все устройства управления дверями и охранными шлейфами (реле управления замком, входы для подключения датчика двери, кнопки выхода и охранных датчиков) располагаются в автономных системах, как правило, на плате самого контроллера. Часто сам контроллер конструктивно объединяется в одном корпусе со считывателем.

В целях повышения безопасности в наиболее совершенных автономных системах применяется вынесенное цифровое реле управления замком. Эта мера позволяет предотвратить попытки проникновения в помещение путем прямого подключения электрозамка к проводам питания.

В некоторых системах предусмотрена возможность их расширения. Достигается это различными способами:

– объединением отдельных контроллеров в сеть (использованием добавочного сетевого модуля в дополнение к контроллеру);

– увеличением мощности и усложнением самого контроллера, что позволяет подключать к нему более двух считывателей.

Централизованные СКУД находятся под непосредственным и постоянным управлением центрального компьютера системы охраны объекта, обслуживающего все периферийные звенья КПП. Схема централизованной СКУД приведена на рис. 5.4.

Применение таких систем экономически оправдано, если к центральному компьютеру подключено достаточно большое количество терминалов – несколько десятков и более. Преимущество таких систем в том, что они в отличие от автономных позволяют вести централизованную регистрацию времени прохода служащих и осуществлять статистическую машинную обработку этих сведений, а также оперативно вводить все необходимые изменения в режимы доступа тех или иных лиц или в целом на объект. Такие СКУД способны обеспе-

чить высокий уровень безопасности объекта. Для повышения надежности функционирования системы может быть применена параллельная обработка данных на двух ПЭВМ.

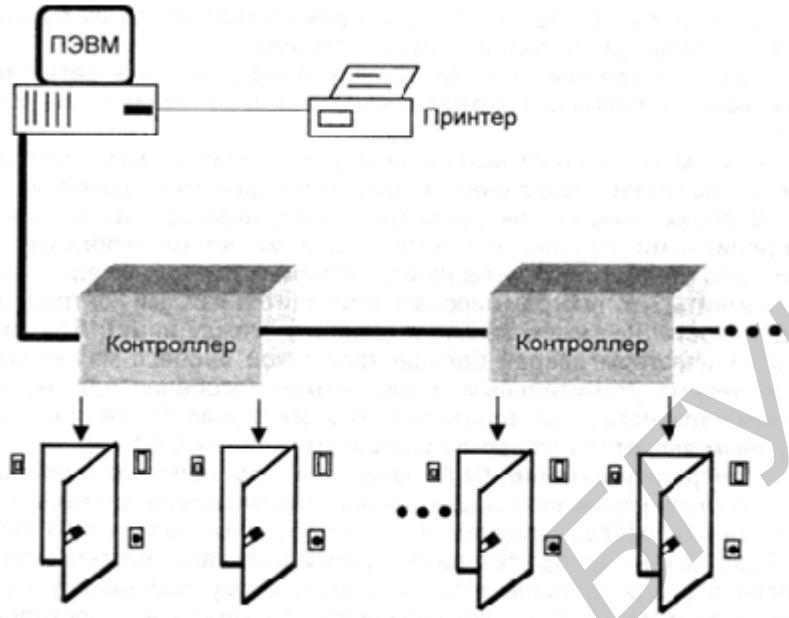


Рис. 5.4. Схема централизованной СКУД

Число контроллеров зависит от емкости системы и максимального количества считывателей, обслуживаемых одним контроллером.

Как правило, для увеличения эффективности работы и уменьшения стоимости всей системы безопасности объекта централизованные СКУД позволяют осуществлять интеграцию с датчиками сигнализации охраны периметра объекта.

Особенность систем средней емкости – существенное увеличение числа пользователей и количества обрабатываемой информации. В связи с этим использование персонального компьютера в таких системах обязательно. Компьютер и его специализированное программное обеспечение позволяют программировать каждый контроллер, собирать и анализировать информацию, составлять всевозможные отчеты и сводки, более эффективно отслеживать ситуацию на объекте.

Главная особенность таких СКУД – возможность конфигурирования аппаратуры и управления процессом доступа с компьютерных терминалов (терминала). Различные СКУД имеют свои индивидуальные особенности, которые определяются:

– архитектурой;

– возможностями;

– масштабом (предельным количеством считывателей/дверей);

– количеством управляющих компьютеров;

– типом применяемых считывателей;

– степенью устойчивости к взлому;

– степенью устойчивости к электромагнитным воздействиям.

Большинство сетевых СКУД сохраняют многие достоинства автономных систем, основное из которых – работа без использования управляющего компьютера. Это означает, что при выключении управляющего компьютера система фактически превращается в автономную. Контроллеры данных систем, так же, как и автономные контроллеры, имеют собственный буфер памяти номеров карт пользователей и событий, происходящих в системе. Наличие в системе компьютера позволяет службе безопасности оперативно вмешиваться в процесс доступа и управлять системой в режиме реального времени. Важнейший элемент сетевых СКУД – программное обеспечение. Оно отличается большим разнообразием по возможностям – от относительно простых программ для одного управляющего терминала, позволяющих добавлять в базу данных новых пользователей и убирать выбывших, – до сложнейших программ с архитектурой клиент-сервер.

В сетевых системах используются мощные центральные контроллеры, осуществляющие процесс управления большим количеством периферийных исполнительных устройств. Как правило, контроллеры в таких системах являются электронными устройствами и не содержат релейных выходов. В таких системах функции управления внешними устройствами и охранными шлейфами обычно выполняют внешние интерфейсные модули и релейные блоки, устанавливаемые в свою очередь недалеко от объектов управления (двери, охранные шлейфы и др.). Для обмена информацией между контроллером и интерфейсными модулями наиболее часто используется интерфейс RS-485.

Контроллер в системах с централизованной архитектурой хранит всю базу данных идентификаторов и событий, произошедших в системе. Разделение функции принятия решений и непосредственно управления позволяет повысить степень безопасности СКУД.

Распределенные СКУД наиболее совершенны с точки зрения организации процесса обработки информации в системе, так как наилучшим образом противостоят сбойным и аварийным ситуациям, в частности, при сбоях в работе центральной ПЭВМ, нарушении целостности проводной линии, связывающей его с периферией и т. п. Периферийные пункты оснащены локальными сетями на базе микрокомпьютеров (контроллеров), выполняющих процедуру проверки самостоятельно, а центральный компьютер включается в работу лишь для актуализации локальных баз данных и статистической и логической обработки информации. На рис. 5.5 изображена схема распределенной СКУД.

Отличительная особенность СКУД с распределенной архитектурой состоит в том, что база данных идентификаторов (и событий в системе) содержится не в одном, а в нескольких контроллерах, которые, как правило, сами выполняют функции управления внешними устройствами и охранными шлейфами через реле и входы охранной сигнализации, расположенные непосредственно на плате самого контроллера.

Еще одна отличительная особенность системы такого класса – возможность связи входных и выходных устройств разных контроллеров системы. Например, можно запрограммировать систему так, чтобы срабатывание датчика сигнализации у входа в офис вызывало блокирование электрозамков, подключенных к нескольким контроллерам, контролирующим близлежащие помещения.

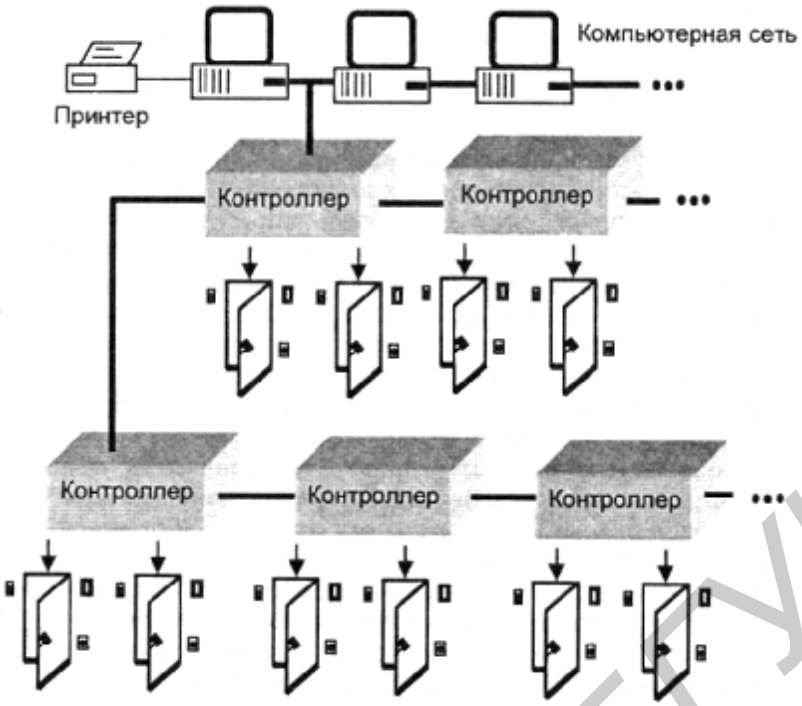


Рис. 5.5. Схема распределенной СКУД

Кроме того, программное обеспечение больших систем позволяет использовать для управления сразу несколько компьютеров и распределять исполнительные функции между ними. Например, можно на компьютер администратора возложить обязанности отслеживать местонахождение сотрудников и использование ими рабочего времени, оператору компьютера отдела кадров вменить в обязанность пополнять базу данных и печатать пропуска, на проходную установить компьютер с программами, помогающими идентифицировать личность, а на пост охраны – выводить тревожную информацию и т.д.

Большие СКУД, как правило, работают в самом тесном взаимодействии с другими инженерными системами объекта: охранной сигнализацией, системами телевизионного наблюдения и контроля, системами жизнеобеспечения, оперативной связи и др.

Ввиду невозможности удаленной установки от объекта управления эти контроллеры устанавливаются непосредственно внутри защищаемых ими помещений. Это не способствует снижению вероятности несанкционированного манипулирования контроллером, но имеет свои плюсы: при обрыве линии свя-

зи между контроллерами и компьютером система продолжает выполнять основные функции по управлению процессом доступа в автономном режиме. Наиболее часто в системах с распределенной архитектурой контроллер может управлять проходом в 1–2 двери.

Распределенные системы обладают также теми преимуществами, что благодаря своей модульной конструкции позволяют наращивать мощность СКД постепенно, переходя от локальных пунктов к распределенной сети; проще выполняется и модернизация оборудования; авария на отдельном КПП не влияет на работу всей сети; для обработки проверяемых лиц требуется меньше времени.

Средства контроля доступа позволяют обеспечить решение необходимых задач по физической защите объектов. В зависимости от конкретных условий могут применяться комбинации различных систем контроля доступа, например, бесконтактные устройства считывания карточек при входе и выходе из здания в сочетании с системой контроля доступа по голосу в зоне обработки секретной информации. Наилучший выбор системы или сочетания систем может быть сделан только на основе четкого определения текущих и перспективных потребностей организации.

5.2. Лабораторное задание

Обеспечить контроль доступа на объект и его отдельные категорированные помещения, используя методы и средства аутентификации в соответствии с вариантами приложения. Для этого необходимо:

1. Запустить файл RFID.exe на выполнение.

2. Выполнить переход к изучению теоретического материала путем нажатия на кнопку **Теория**, расположенную в верхнем левом углу окна (рис. 5.6). Просмотр теоретического материала обеспечивается нажатием на кнопки двойных стрелок, указывающих влево или вправо, расположенных в нижней части окна программы (рис. 5.7).

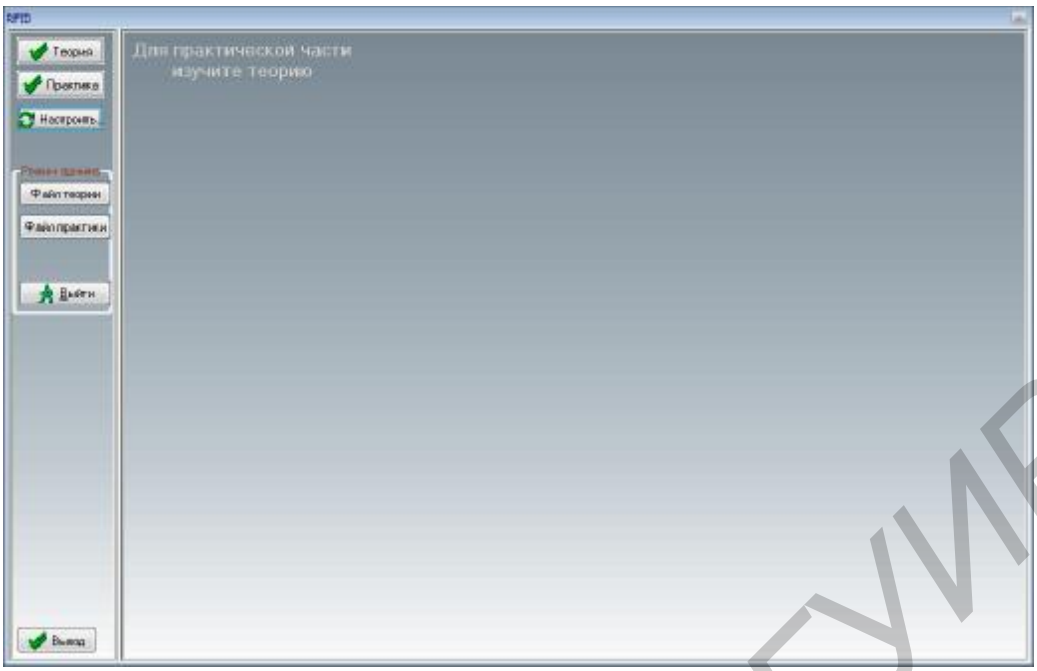


Рис. 5.6. Внешний вид главного окна программы

2. Выполнение практической части работы начинается при нажатии на кнопку **Практика**, расположенную в верхнем левом углу окна.

3. В соответствие с вариантом (см. приложение) выбрать тип объекта. Для выбора объекта подвести мышь к белому кругу около соответствующего названия категории объекта и выбрать его, нажимая левую кнопку мыши. При этом в белом круге выбранного объекта появится черная точка и возле нее – название выбранной категории, а названия остальных (невыбранных) объектов исчезнут.

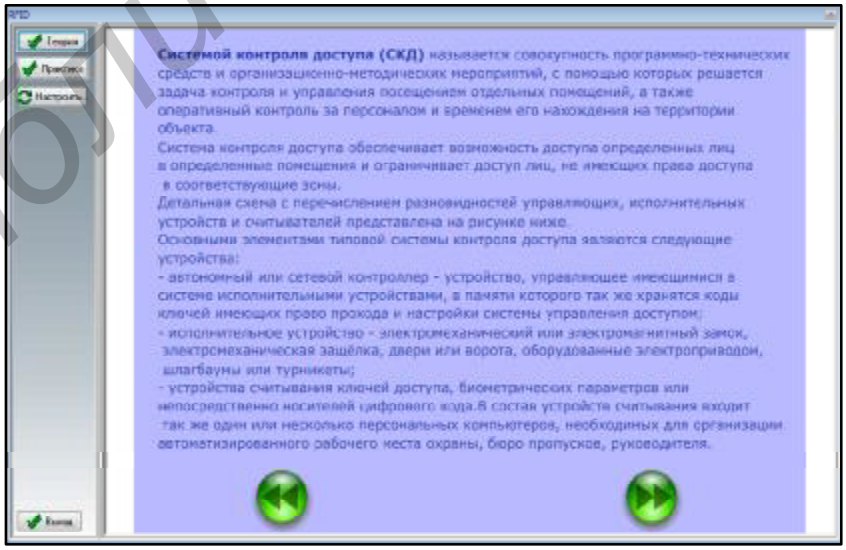


Рис. 5.7. Внешний вид окна программы с теоретическим материалом

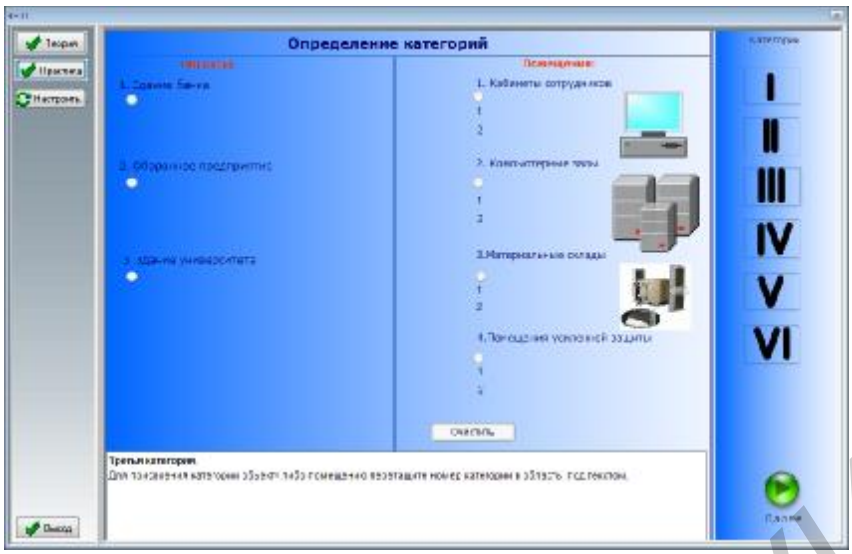


Рис. 5.8. Внешний вид окна программы с лабораторным заданием

4. Присвоить объекту с учетом его назначения категорию (рис. 5.8). Присвоение категории обеспечивается путем перемещения манипулятора мышь на номер соответствующей категории в поле **Категории**. После чего необходимо нажать левую кнопку мыши и, удерживая ее, перетащить номер выбранной категории в область под названием объекта и отпустить левую кнопку мыши. При этом в белом круге категорированного помещения появится черная точка и возле нее – название выбранной категории.

5. Провести категорирование помещений выбранного объекта, учитывая его собственную категорию и назначение. Перечень помещений находится в правой части окна. Присвоение категории помещению выполняется аналогично присвоению категории объекту (см. п. 4). В случае ошибочного присвоения категории помещению коррекция данных выполняется нажатием кнопки **Очистить**. Переход к следующему шагу работы выполняется нажатием кнопки **Далее**, позиционируемой в правом нижнем углу окна программы.

6. Определить средства аутентификации, используемые для доступа в категорированные помещения. Для чего необходимо переместить мышь на изображение соответствующего средства аутентификации. После чего необходимо нажать левую кнопку мыши и, удерживая ее, перетащить изображение выбранного средства аутентификации в область под названием категории помещения и отпустить левую кнопку мыши. При этом в белом круге категорированного помещения появится черная точка и возле нее название выбранного средства ау-

тентификации. Необходимо учитывать, что в СКД допускается многофакторная аутентификация. Переход к следующему шагу работы выполняется нажатием кнопки **Далее**, позиционируемой в правом нижнем углу окна программы.

7. Проверка правильности выполнения работы обеспечивается нажатием кнопки **Проверить**, после нажатия которой в нижней центральной части окна отображаются ошибки выполнения работы. Лабораторная работа считается выполненной при отсутствии ошибок.

8. Результаты выполнения работы показать преподавателю.

9. Оформить отчет.

5.3. Содержание отчета

1. Цель работы.

2. Таблица результатов выполнения работы.

Объект	Помещение	Категории помещений	Средства аутентификации

3. Вывод по работе.

4. Ответы на контрольные вопросы.

5.4. Контрольные вопросы

1. Назначение систем контроля и управления доступом.

2. Каковы достоинства и недостатки автономных систем контроля и управления доступом?

3. Каковы достоинства и недостатки сетевых систем контроля и управления доступом?

4. Каковы достоинства и недостатки распределенных систем контроля и управления доступом?

5. С какими техническими средствами сопрягаются системы контроля и управления доступом?

Приложение

Вариант	Объект
1	Здание банка
2	Оборонное предприятие
3	Здание университета

Литература

1. Вернигоров, Н. С. Нелинейный локатор в системах ограничения доступа и контроля / Н. С. Вернигоров // Частный сыск. Охрана. Безопасность. – 1998. – №8. – С. 36.

2. Топоровский, П. Средства нелинейной радиолокации: реальный взгляд / П. Топоровский // Системы безопасности. – 1998. – №6. – С. 94.

3. Бузов, Г. А. Защита от утечки информации по техническим каналам : учеб. пособие для подготовки экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005. – 416 с.

4. Энциклопедия промышленного шпионажа / Ю. Ф. Каторин [и др.] / под общ. ред. Е. В. Куренкова. – СПб. : ООО «Издательство Полигон», 2000. – 512 с.

5. Технические методы и средства защиты информации / Ю. Н. Максимов [и др.]. – СПб. : ООО «Издательство Полигон», 2000. – 224 с.

6. Меньшаков, Ю. К. Защита объектов и информации от технических средств разведки / Ю. К. Меньшаков. – М. : Российский гуманитарный университет, 2002. – 399 с.

Учебное издание

Лыньков Леонид Михайлович
Борботько Тимофей Валентинович
Беляев Борис Илларионович
Катковский Леонид Владимирович

ЗАЩИТА ОБЪЕКТОВ СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Редактор *Т. П. Андрейченко*
Корректор *Е. Н. Батурчик*
Компьютерная верстка и дизайн обложки *Е. С. Чайковская*

Подписано в печать 04.01.2010. Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».
Печать ризографическая. Усл. печ. л. 4,77. Уч.-изд. л. 4,4. Тираж 150 экз. Заказ 396.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6