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

Факультет инфокоммуникаций

Кафедра защиты информации

ЗАЩИТА ОБЪЕКТОВ СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальности 1-98 01 02 «Защита информации в телекоммуникациях»

Минск БГУИР 2017

УДК 004.056(076.5)
ББК 32.972.5я73
З-40

Авторы:

Л. М. Лыньков, О. В. Бойправ, Я. В. Рощупкин, Т. В. Борботько

Рецензенты:

кафедра автоматизированных систем управления войсками
учреждения образования «Военная академия Республики Беларусь»
(протокол №7 от 02.06.2016);

доцент кафедры управления информационными ресурсами
Академии управления при Президенте Республики Беларусь,
кандидат технических наук, доцент Н. И. Белодед

Защита объектов связи от несанкционированного доступа. Лабо-
З-40 раторный практикум : учеб.-метод. пособие / Л. М. Лыньков [и др.]. – Минск : БГУИР, 2017. – 112 с.
ISBN 978-985-543-327-0.

Состоит из двенадцати лабораторных работ, каждая из которых содержит краткие теоретические сведения, описание хода выполнения лабораторного задания, требования к оформлению отчета и вопросы для самоконтроля, ответы на которые оцениваются программной экспертной системой. При выполнении работ реализована возможность автоматизации контроля знаний студентов.

УДК 004.056(076.5)
ББК 32.972.5я73

ISBN 978-985-543-327-0

СОДЕРЖАНИЕ

ЛАБОРАТОРНАЯ РАБОТА №1
ИЗУЧЕНИЕ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Цель: изучить принципы построения систем контроля и управления доступом, получить практические навыки по программной настройке средств таких систем.

1.1. Теоретическая часть

Классификация, принципы функционирования и использования систем контроля и управления доступом

Система контроля и управления доступом (СКУД) – совокупность средств контроля и управления, обладающих технической, программной и эксплуатационной совместимостью и реализующих контроль и управление доступом (рис. 1.1).

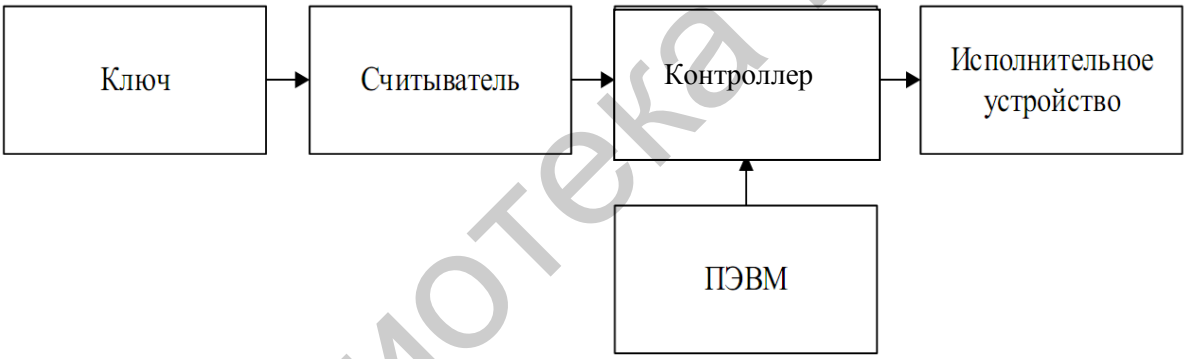


Рис. 1.1. Общая структурная схема СКУД

Основные элементы СКУД:

– автономный или сетевой контроллер;

– исполнительное устройство;

– устройства считывания ключей доступа, биометрических параметров.

Пропускная способность СКУД – количество штатных проходов в единицу времени.

Частота ошибок СКУД – количество ложных допусков и ложных отказов в единицу времени.

Причины ошибок СКУД:

– сбои в работе оборудования;

– неверная информация в базе данных;

– обман системы при входе или выходе.

Автономный или сетевой контроллер – устройство, управляющее имеющимися в системе исполнительными устройствами, в памяти которого хранятся коды ключей лиц, имеющих доступ прохода в соответствующие зоны.

Исполнительное устройство – электромеханический или электромагнитный замок, электромеханическая защелка, двери или ворота, оборудованные электроприводом, турникеты.

Устройство считывания – электронные ключи Touch Memory, бесконтактные карты, проксимити-карты.

Виды идентификаторов:

– пароль;

– устройство аутентификации;

– биометрия;

– многофакторная аутентификация.

Пароль – отличительная характеристика субъекта, представляющая собой секретную информацию, которая неизвестна непосвященным людям.

Формы представления:

– комбинация цифр для замка;

– информация, вводимая с клавиатуры.

Устройство аутентификации – некоторый уникальный предмет, находящийся у субъекта и являющийся его отличительной характеристикой.

Типы устройств аутентификации:

– smart-карта;

– USB-брелок;

– OTP-токен (One time Password);

– бесконтактные радиочастотные проксимити-карты;

– магнитные карты;

– штрих-кодовые карты;

– ключ-брелок (Touch Memory);

– карты Виганда.

Smart-карта – пластиковая карта со встроенной микросхемой.

Бесконтактные радиочастотные проксимити-карты – наиболее перспективный в настоящее время тип карт. Бесконтактные карты срабатывают на расстоянии и не требуют четкого позиционирования, что обеспечивает их устойчивую работу и удобство использования, высокую пропускную способность.

Магнитные карты – наиболее широко распространенный вариант. Существуют карты с низкокоэрцитивной и высококоэрцитивной магнитной полосой и с записью на разные дорожки.

Штрих-кодовые карты – карты, на которые наносится штриховой код. Существует более сложный вариант: штрих-код закрывается материалом, прозрачным только в инфракрасной свете, считывание происходит в ИК-области.

Ключ-брелок – металлическая «таблетка», внутри которой расположен чип ПЗУ.

Карты Виганда – карты, названные по имени ученого, открывшего магнитный сплав, обладающий прямоугольной петлей гистерезиса.

Биометрическая характеристика – измеримая физиологическая или поведенческая черта живого человека.

Группы биометрических характеристик:

– поведенческая;

– физиологическая.

Поведенческая характеристика основана на данных, полученных путем измерения действий человека.

Физиологическая характеристика основана на данных, полученных путем измерения анатомических характеристик человека.

Многофакторная аутентификация – аутентификация, в процессе которой используются аутентификационные факторы нескольких типов:

1. Халатность пользователя типа 1: устройства аутентификации могут оставляться на рабочей станции.

Меры противодействия:

– заставить пользователя носить устройство с собой;

– блокировка устройства по поставленному тайм-ауту;

– разблокировка устройства при повторной аутентификации.

2. Халатность пользователя типа 2: устройства аутентификации могут быть утеряны.

Меры противодействия:

– многофакторная аутентификация;

– защита от подбора PIN-кода;

– задержка авторизации.

Устройство ввода идентификационных признаков (УВИП) – электронные устройства ввода идентификатора.

Устройство управления – устанавливает режим доступа и обеспечивает прием и обработку информации с УВИП, управление преграждающим устройством, отображение и регистрацию информации.

Управление преграждающим устройством (УПУ) – обеспечивает физическое препятствие доступа людей, транспорта и других объектов.

Идентификатор – уникальный признак субъекта доступа.

Способы ввода идентификатора:

– ручной;

– контактный;

– бесконтактный.

Способы управления преграждающими устройствами:

– автономные;

– централизованные;

– универсальные.

Структурная схема процесса авторизации представлена на рис. 1.2.

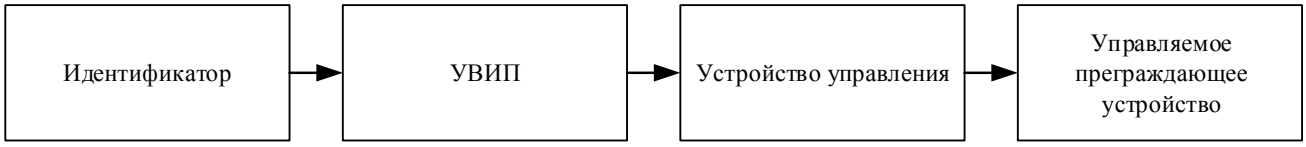


Рис. 1.2. Структурная схема процесса авторизации

Современные технические средства СКУД позволяют решать целый ряд задач. К числу наиболее важных можно отнести следующие:

– противодействие промышленному шпионажу;

– противодействие воровству;

– противодействие саботажу;

– противодействие умышленному повреждению материальных ценностей;

– учет рабочего времени;

– контроль своевременности прихода и ухода сотрудников;

– защита конфиденциальности информации;

– регулирование потока посетителей;

– контроль въезда и выезда транспорта.

Любая СКУД предназначена для того, чтобы автоматически пропускать тех, кому этот вход разрешен, и не пропускать тех, кому вход запрещен. Все ее остальные функции (сохранность материальных ценностей, контроль и учет рабочего времени и др.) вытекают из основного предназначения.

Структурная схема устройства управления СКУД представлена на рис. 1.3.

Модуль обработки предназначен для преобразования идентификатора субъекта доступа в электрический сигнал, удобный для функционирования СКУД.

Буфер событий предназначен для хранения протокола функционирования устройства управления.

Модуль принятий решений предназначен для сравнения текущего идентификатора с идентификаторами в базе данных. В случае положительной про-

цедуры аутентификации он выдает электрический сигнал на исполнительное устройство.

События:

– запрос на аутентификацию;

– результат аутентификации.

Этапы:

– предъявление идентификатора;

– аутентификация;

– сигнал на исполнительное устройство.

По способу управления можно выделить следующие виды СКУД:

– автономные;

– централизованные;

– распределенные.

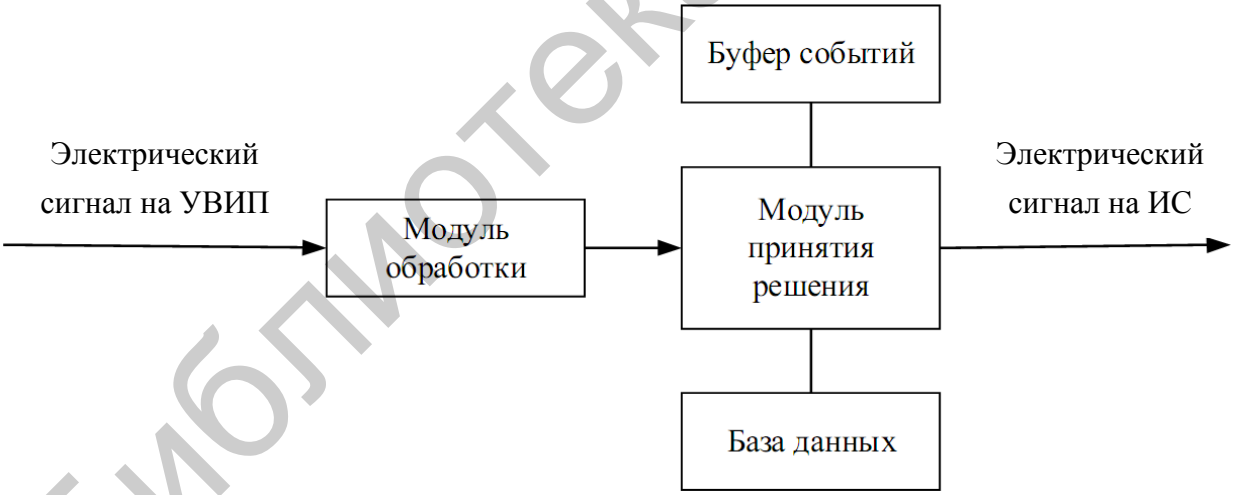


Рис. 1.3. Структурная схема устройства управления СКУД

Автономные СКУД предназначены для обслуживания одной точки доступа. Структурные схемы автономных СКУД представлены на рис. 1.4 и 1.5.

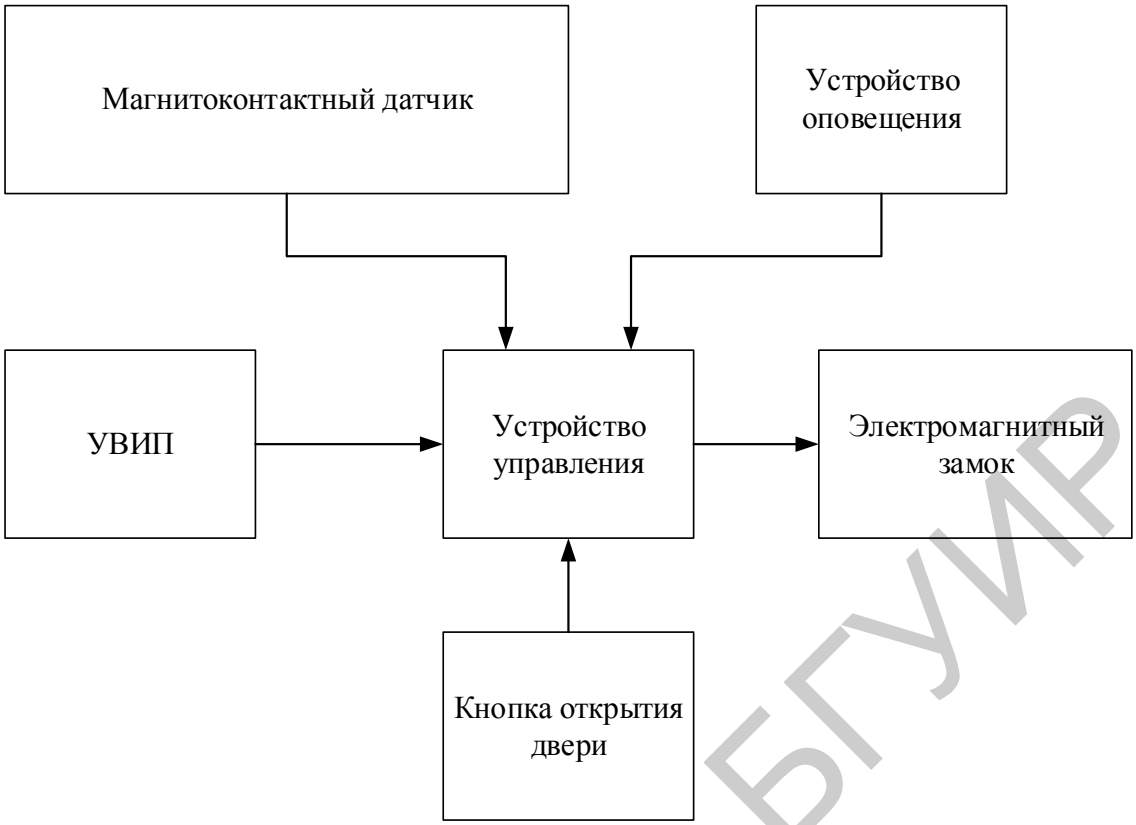


Рис. 1.4. Типовая схема автономного СКУД без накопителя памяти

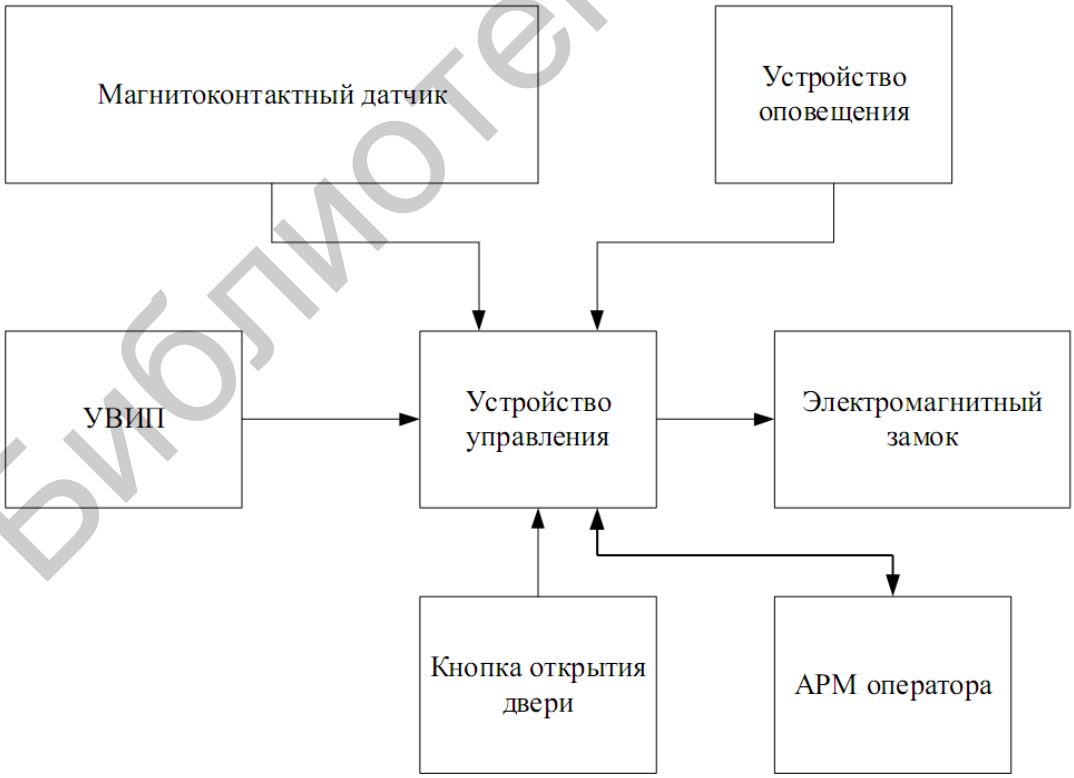


Рис. 1.5. Типовая схема автономного СКУД с накопителем памяти

Магнитоконтактный датчик на рис. 1.5 предназначен для оповещения устройства управления о положении двери. В случае если дверь открыта, устройство управления включает устройство оповещения, иначе – выключает устройство оповещения.

Кнопка открытия двери устанавливается в контролируемом помещении и позволяет без использования идентификатора открыть дверь.

Электромагнитный замок – исполнительное устройство.

Конструкция электромагнитного замка:

– электромагнит;

– якорь.

Способ установки электромагнитного замка:

– электромагнит закрепляется на дверной коробке;

– якорь закрепляется на двери.

Автономное рабочее место (АРМ) оператора предназначено для чтения информации из буфера обмена управляющего устройства и корректировки базы данных идентификаторов.

Централизованная СКУД имеет единый центр управления и предназначена для обслуживания многих точек доступа. Структурные схемы централизованных СКУД представлены на рис. 1.6 и 1.7.

АРМ администратора используется для обеспечения технической эксплуатации СКУД и функция доступа к базе данных идентификаторов для него должна быть запрещена.

АРМ охраны используется:

– для контроля аутентификации субъекта;

– блокирования устройств управления;

– блокирования доступа.

АРМ бюро пропусков предназначено для корректировки базы данных идентификаторов.

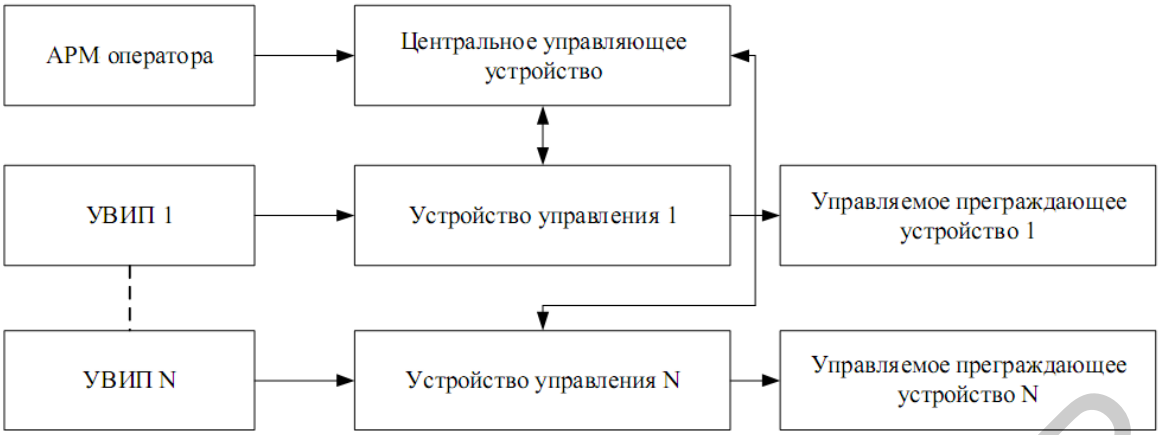


Рис. 1.6. Типовая схема централизованного СКУД

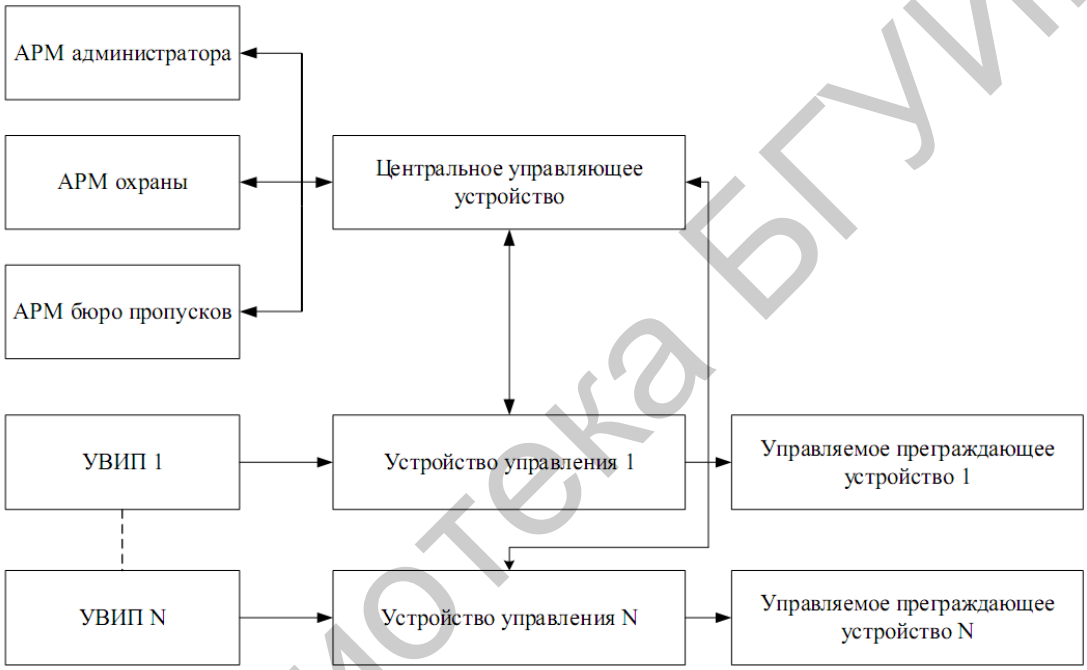


Рис. 1.7. Типовая схема централизованного СКУД крупного объекта

Состав и описание комплекса Ардуино, используемого для создания средств для организации систем контроля и управления доступом

Ардуино (Arduino) – комплекс аппаратно-программных средств для построения простых систем автоматики и робототехники, состоящий из двух частей:

– программной части (состоит из программной оболочки для написания программ (IDE – интегрированная среда разработки), их компиляции и программирования аппаратуры);

– аппаратной части (представляет собой набор смонтированных печатных плат).

Платы Ардуино спроектированы таким образом, чтобы их можно было расширять путем подключения к ним с помощью штыревых разъемов новых компонентов (рис. 1.8).

Рис. 1.8. Внешний вид платы Ардуино

На рис. 1.9 представлен внешний вид индикатора работы, клавиатура ввода – на рис. 1.10, сервопривод – на рис 1.11. Сервопривод (следящий привод) – привод с управлением через отрицательную обратную связь, позволяющую точно управлять параметрами движения. Сервоприводом является любой тип механического привода (устройства, рабочего органа), имеющий в составе датчик (положения, скорости, усилия и т. п.) и блок управления приводом (электронную схему или механическую систему тяг), автоматически поддерживающий необходимые параметры на датчике (и соответственно на устройстве) согласно заданному внешнему значению (положению ручки управления или численному значению от других систем).

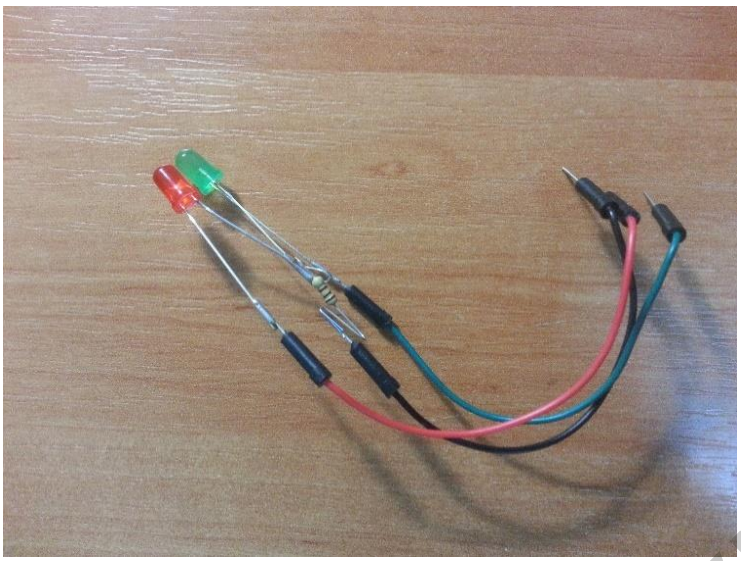


Рис. 1.9. Внешний вид индикатора работы

Рис. 1.10. Внешний вид клавиатуры ввода

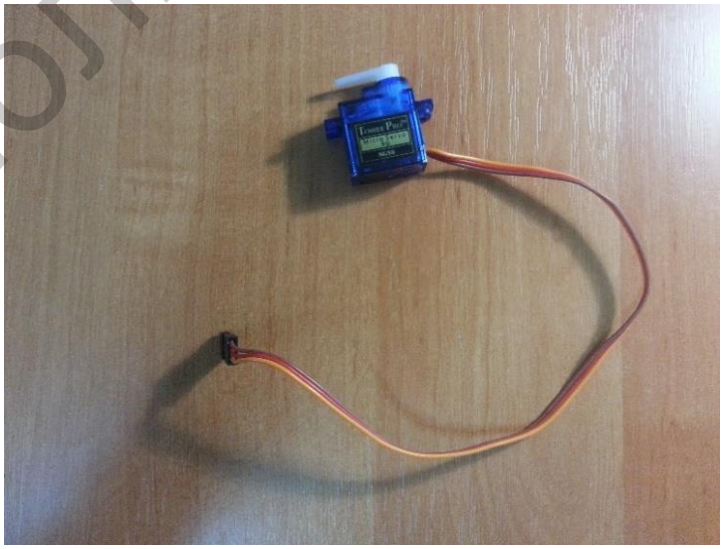


Рис. 1.11. Внешний вид сервопривода

Виды сервоприводов:

1. Сервопривод вращательного движения:

– синхронный;

– асинхронный.

2. Сервопривод линейного движения:

– плоский;

– круглый.

3. По принципу действия:

– электромеханический;

– электрогидромеханический.

У электромеханического сервопривода движение формируется электродвигателем и редуктором. У электрогидромеханического сервопривода движение формируется системой поршень – цилиндр. У данных сервоприводов быстродействие на порядок выше в сравнении с электромеханическими.

Синхронный сервопривод позволяет точно задавать угол поворота (с точностью до угловых минут), скорость вращения, ускорение. Разгоняется быстрее асинхронного, но его стоимость в разы дороже.

Асинхронный сервопривод позволяет точно задавать скорость даже на низких оборотах.

Линейные двигатели могут развивать огромные ускорения (до 70 м/с²).

Сервоприводы применяются для точного позиционирования приводимого элемента в автоматических системах.

Язык программирования Ардуино разработан на базе языка программирования C++. Самый простой программный код, созданный при помощи Ардуино, состоит из двух функций:

– setup() – вызывается один раз при старте микроконтроллера;

– loop() – вызывается после вызова функции setup() все время работы микроконтроллера.

Среда разработки Ардуино состоит из следующих элементов (рис. 1.12):

– встроенный текстовый редактор программного кода;

– область сообщений;

– окно вывода текста;

– панель инструментов.

Для загрузки программ и связи среда разработки подключается к аппаратной части Ардуино.

Интегрированная среда разработки (IDE) – комплекс программных средств, используемый программистами для разработки программного обеспечения.

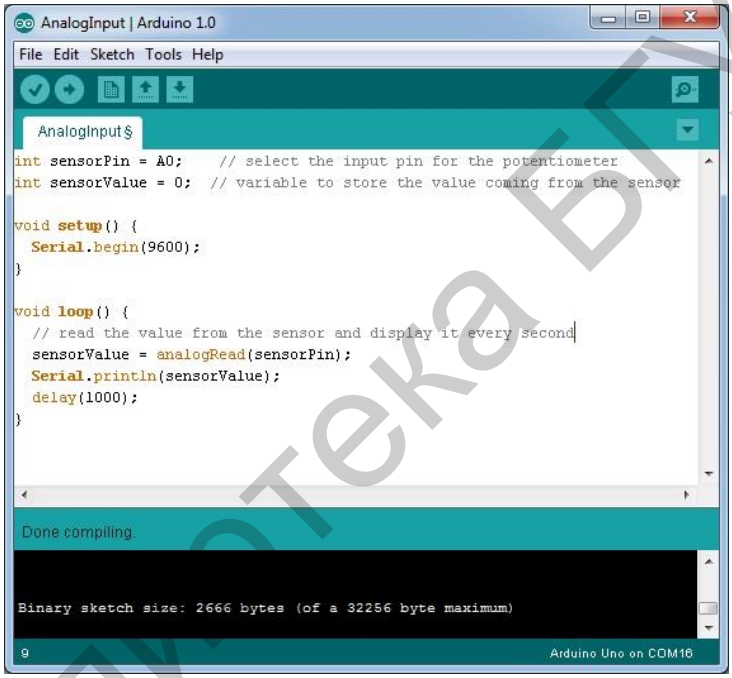


Рис. 1.12. Интерфейс программы среды Ардуино

Среда разработки включает в себя:

– текстовый редактор;

– компилятор и/или интерпретатор;

– средства автоматизации сборки;

– отладчик.

Программа, написанная в среде Ардуино, называется скетч. Скетч пишется в текстовом редакторе, имеющем инструменты вырезки/вставки, поиска/замены текста. Во время сохранения и экспорта проекта в области сообще-

ний появляются пояснения, также могут отображаться возникшие ошибки. Окно вывода текста показывает сообщения Ардуино, включающие полные отчеты об ошибках и другую информацию.

Кнопки панели инструментов позволяют проверить и записать программу, создать, открыть и сохранить скетч, открыть мониторинг последовательной шины:

–  Verify/Compile – проверка программного кода на ошибки, компиляция;

–  Stop – остановка мониторинга последовательной шины (Serial monitor) или затемнение других кнопок;

–  New – создание нового скетча;

–  Open – открытие меню доступа ко всем скетчам в блокноте. Открывается нажатием в текущем окне;

–  Save – сохранение скетча;

–  Upload to I/O Board – компиляция программного кода и загрузка его в устройство Ардуино;

–  Serial Monito – открытие мониторинга последовательной шины (Serial monitor).

Добавить библиотеку в текущий скетч можно путем вставки директивы #include в код скетча.

В панель меню входят:

– Show Sketch Folder – открытие папки, содержащей файл скетча, на рабочем столе;

– Add File... – добавление файла в скетч (файл будет скопирован из текущего места расположения). Новый файл появляется в новой закладке в окне скетча. Файл может быть удален из скетча при помощи меню закладок;

– Auto Format – оптимизация кода, например, выстраивание в одну линию по вертикали открывающей и закрывающей скобки и помещение между ними утверждения;

– Board – выбор используемой платформы. Список с описанием платформ приводится ниже.

Средой Ардуино используется принцип блокнота, который является стандартным местом для хранения программ (скетчей). Скетчи из блокнота открываются через меню **File > Sketchbook** или кнопкой **Open** на панели инструментов. При первом запуске программы Ардуино автоматически создается директория для блокнота. Расположение блокнота меняется через диалоговое окно Preferences.

Закладки, файлы и компиляция позволяют работать с несколькими файлами скетчей. Файлы кода могут быть стандартными Ардуино (без расширения), файлами C (расширение *.c), файлами C++ (*.cpp) или головными файлами (.h).

Загрузка скетча в Ардуино. Перед загрузкой скетча требуется задать необходимые параметры в меню **Tools > Board и Tools > Serial Port**. Платформы описываются далее по тексту. В ОС Windows порты могут обозначаться как COM1 или COM2 (для платы последовательной шины) или COM4, COM5, COM7 и выше (для платы USB). Определение порта USB производится в поле *Последовательной шины USB* Диспетчера устройств Windows.

При загрузке скетча используются загрузчики Ардуино – небольшая программа, загружаемая в микроконтроллер на плате. Она позволяет загружать программный код без использования дополнительных аппаратных средств. Загрузчик активен в течение нескольких секунд при перезагрузке платформы и при загрузке любого из скетчей в микроконтроллер. Работа загрузчика распознается по миганию светодиода (13 пин) (например, при перезагрузке платы).

1.2. Лабораторное задание

Получить практические навыки по сборке и настройке СКУД с использованием Ардуино. Для этого требуется выполнить следующее:

1. Собрать СКУД согласно схеме, представленной на рис. 1.13.

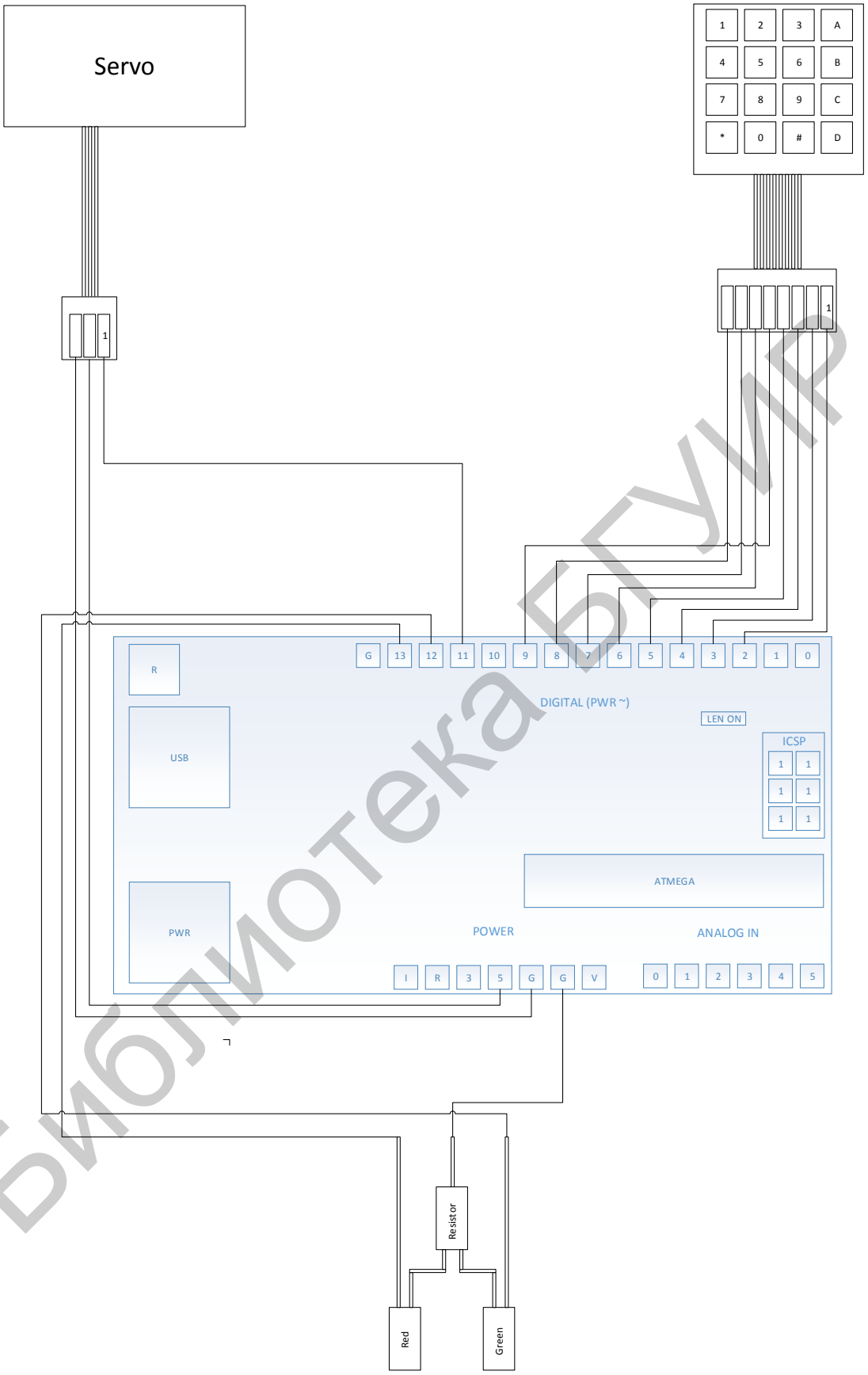


Рис. 1.13. Схема СКУД

2. Подключить USB к порту компьютера.

3. Запустить среду разработки Ардуино IDE.

4. Открыть тестовый пример программы.

5. Ознакомиться с примером.

6. Настроить СКУД следующим образом:

а) открыть заготовку программы;

б) скомпилировать заготовку и проверить работоспособность макета;

в) выявить уязвимость макета;

г) исправить в коде эту уязвимость.

Вначале подключаются библиотеки для работы с подключаемыми модулями. Определяются и инициализируются переменные. В функции setup устанавливаются начальные настройки Ардуино. В функции loop описывается логика обработки введенного кода и сравнение.

```
if(key != NO_KEY) {
        Serial.println("INFO :: Pressed key");
        if(key == '*' || key == '#') {
        position = 0;
        LockedPosition(true);
}
```

Key != NO_KEY проверяется, нажата ли клавиша. ‘*’ и ‘#’ сбрасывается ввод и закрывается замок.

```
if(key == password[position]) {
        position ++;
}
```

В этом фрагменте кода сравнивается нажатый символ с первым символом в массиве, если он совпадает, то переменная position увеличивается на один, тем самым двигаясь на один символ вперед. Следующее нажатие уже будет сравниваться со вторым символом в массиве.

Для проверки ввода/вывода в среде есть мониторинг порта (рис. 1.14).

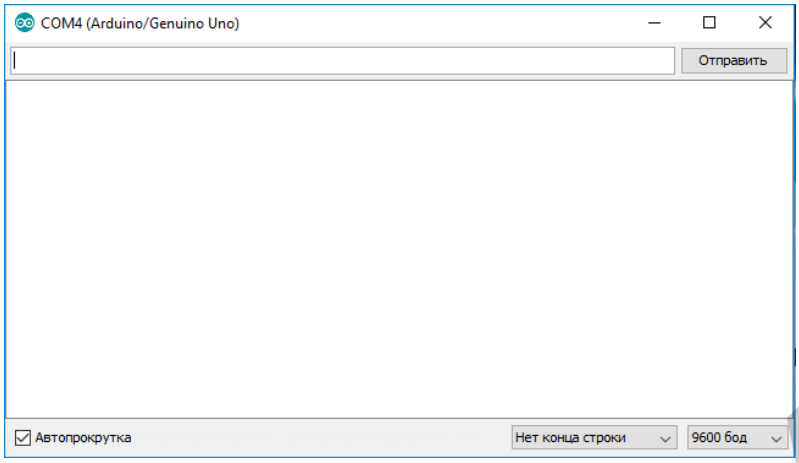


Рис. 1.14. Окно мониторинга порта

Для вывода любой информации в мониторинг порта существует функция Serial.println.

Функция LockedPosition управляет положением сервопривода и индикаторными диодами. В функции вызывается digitalWrite, принимающий два параметра: 1) порт; 2) потенциал HIGH – высокий, т. е. подается напряжение, LOW – низкий, напряжения нет. ServoMotor.write принимает угол поворота сервопривода.

Текст программного кода представлен ниже.

```
// Подключаются библиотеки для работы с клавиатурой и сервоприводом
#include <Servo.h>
#include <Keypad.h>
// Объект для управления сервоприводом
Servo ServoMotor;
// Задаем пароль
char* password = "123";
// Переменная для подсчета правильности введеного пароля
int position = 0;
// Определяется размер клавиатуры
const byte ROWS = 4;
```

```
const byte COLS = 4;
// Определяется клавиатура
char keys[ROWS][COLS] = {
  {'1','2','3','A'},
  {'4','5','6','B'},
  {'7','8','9','C'},
  {'*','0','#','D'}
};

byte rowPins[ROWS] = { 8, 7, 6, 9 };
byte colPins[COLS] = { 5, 4, 3, 2 };
// Объект для работы с клавиатурой
Keypad keypad = Keypad(makeKeymap(keys),
                  rowPins, colPins,
                  ROWS, COLS);
// Указываются порты для светодиодов
int RedpinLock     = 12;
int GreenpinUnlock = 13;

/*
 * Функция начальных настроек
 */
void setup()
{
// Устанавливается частота обновления порта
  Serial.begin(9600);
// Выводится вспомогательная информация в мониторинг порта
  Serial.println("--- Start Serial Monitor SEND_RCVE ---");
```

```
  Serial.println(position);
// Устанавливаются порты на светодиоды
  pinMode(RedpinLock, OUTPUT);
  pinMode(GreenpinUnlock, OUTPUT);
// Устанавливается положение сервопривода в закрытое положение
  ServoMotor.attach(11);
  LockedPosition(true);
}

void loop()
{
// Записывается нажатый символ с клавиатуры
  char key = keypad.getKey();

  if(key != NO_KEY) {
    Serial.println("INFO :: Pressed key");

    if(key == '*' || key == '#') {
      position = 0;
      LockedPosition(true);
    }

    if(key == password[position]) {
      position ++;
    }/*
    else {
      Serial.println("Input wrong key value");
      Serial.println(position);
      position = 0;
```

```
    }*/

    if(position == 3) {
      LockedPosition(false);
    }

    Serial.println(position);
  }
// Установка задержки
  delay(100);
}

/*
 * Функция открытия/закрытия замка
 * Параметры: locked - 1(Закрыто)/0(Открыто)
 */
void LockedPosition(int locked)
{
  if(locked) {
    Serial.println("Closed!!!!");
    digitalWrite(RedpinLock, HIGH);
    digitalWrite(GreenpinUnlock, LOW);
    ServoMotor.write(11);
  }
  else {
    Serial.println("Opened!!!");
    digitalWrite(RedpinLock, LOW);
    digitalWrite(GreenpinUnlock, HIGH);
    ServoMotor.write(180);
```

1.3. Содержание отчета

Отчет по лабораторной работе №1 должен содержать:

1. Цель работы.
2. Описание основных полученных результатов.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

1.4. Контрольные вопросы

1. Что такое Ардуино?
2. Что включает в себя набор внешней периферии?
3. Каковы основные функции Ардуино и их назначение?
4. Что включает в себя интегрированная среда разработки?
5. Каково назначение языка программирования Ардуино?

ЛАБОРАТОРНАЯ РАБОТА №2
АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

Цель: изучить основные принципы аутентификации пользователей информационных систем по клавиатурному почерку. Получить практические навыки по анализу таких систем.

2.1. Теоретическая часть

Клавиатурный почерк относится к динамическим (поведенческим) биометрическим характеристикам. Он характеризует динамику ввода парольной фразы с помощью клавиатуры. К свойствам клавиатурного почерка относятся:

– длительность удержания клавиши;

– интервал времени между нажатиями клавиш;

– общее время набора парольной фразы;

– частота возникновения ошибок при наборе;

– использование при наборе числовой клавиатуры, клавиш Shift, Caps Lock и т. д.

Для применения клавиатурного почерка в целях аутентификации пользователей информационных систем не требуется установки специальных аппаратных средств.

Основные сложности использования клавиатурного почерка для аутентификации пользователей информационных систем связаны с зависимостью его свойств:

– от физиологических состояний человека: усталость, травма кисти или пальцев руки;

– от эргономических свойств клавиатуры, которые зависят от их типа, размеров, расположения и материала клавиш и т. п.

При использовании рассматриваемого способа аутентификации могут применяться как кнопочные, так и виртуальные клавиатуры.

Выделяют следующие виды кнопочных клавиатур:

– мембранные;

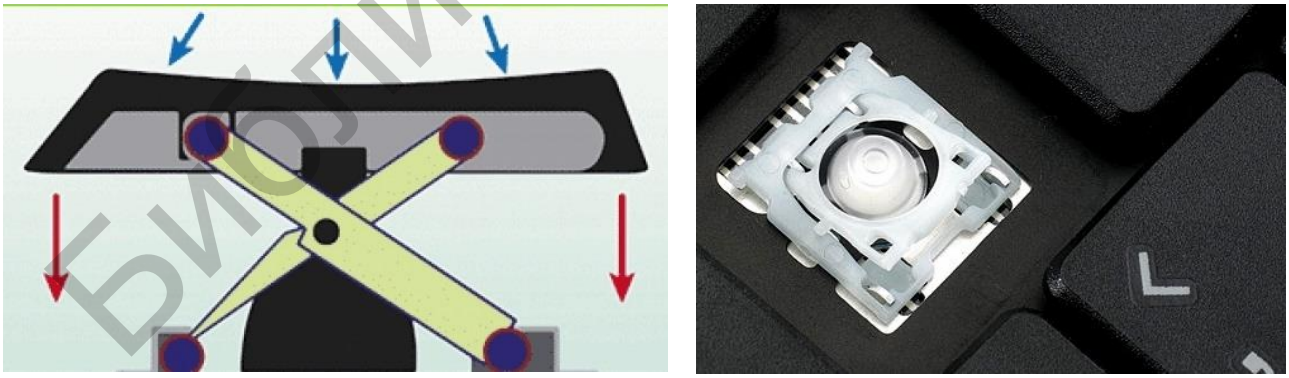
– ножничные;

– механические.

В мембранных клавиатурах под каждой клавишей находится мембрана, которая при нажатии клавишы продавливается и замыкает контакты на печатной плате (рис. 2.1).

Рис. 2.1. Внешний вид фрагмента мембранной клавиатуры

Ножничная клавиатура является модификацией мембранной. В ней для соединения крышек клавиш и мембран используется так называемый ножничный механизм, изготовленный из пластика (рис. 2.2). Такие клавиатуры используются в абсолютном большинстве случаев в ноутбуках.



а *б*

Рис. 2.2. Конструкция клавиши ножничной клавиатуры:

а – схематическое изображение сбоку; *б* – внешний вид сверху

В механической клавиатуре каждая клавиша содержит переключатель с металлическими пружиной и контактами, которые замыкаются при ее нажатии (рис. 2.3).

Рис. 2.3. Внешний вид клавиши механической клавиатуры в разобранном виде

В зависимости от принципа действия системы аутентификации пользователей информационных систем по клавиатурному почерку условно делятся на две группы:

– системы, основанные на вводе фиксированного слова (как правило, парольного);

– системы, основанные на оценке свойств клавиатурного почерка пользователя во время выполнения им набора текста в редакторе, браузере и т. п. (как правило, используются в системах многофакторной аутентификации).

Если для реализации рассматриваемого способа аутентификации используются виртуальные клавиатуры, то их управление может выполняться как с помощью манипулятора «мышь», так и с применением пяти клавиш кнопочной клавиатуры, подключенной к рабочей станции пользователя (клавиши со стрелками «вверх», «вниз», «вправо», «влево», а также клавиша «ввод»).

С помощью клавиатурного почерка можно проводить реаутентификацию для подтверждения личности пользователя перед выполнением критичных операций, а также осуществлять так называемую скрытную аутентификацию.

2.2. Лабораторное задание

Работа выполняется совместно двумя студентами. Для этого необходимо:

1. Запустить файл index в браузере Mozilla Firefox.

2. 1-й студент должен произвести регистрацию в системе посредством набора парольного слова из восьми букв. 2-й студент должен наблюдать за динамикой клавиатурного набора.

3. 2-й студент, который знает пароль и наблюдал за динамикой клавиатурного набора, должен аутентифицироваться в системе (10 попыток).

4. 1-й студент должен произвести регистрацию в системе посредством набора парольного слова из восьми букв. 2-й студент не должен наблюдать за динамикой клавиатурного набора.

5. 2-й студент, который знает пароль, но не наблюдал за динамикой клавиатурного набора, должен аутентифицироваться в системе (10 попыток).

6. 1-й студент, который помнит свой пароль, должен аутентифицироваться в системе (10 попыток).

7. Произвести расчет коэффициентов ложного доступа (ошибок 1-го рода) и коэффициента ложного отказа в доступе (ошибок 2-го рода).

8. На основании рассчитанных значений ошибок 1-го и 2-го родов, а также на основании характеристик динамики клавиатурного набора, выданных системой (файлом index), сделать выводы.

2.3. Содержание отчета

Отчет по лабораторной работе №2 должен содержать:

1. Цель работы.

2. Описание основных полученных результатов.

3. Вывод по работе.

4. Ответы на контрольные вопросы.

2.4. Контрольные вопросы

1. К какому типу биометрических характеристик относится клавиатурный почерк?

2. Каковы основные свойства, характеризующие клавиатурный почерк?

3. Каковые основные этапы методики, используемой для тестирования системы аутентификации по клавиатурному почерку?

4. Что такое многофакторная аутентификация?

5. Что такое реаутентификация?

ЛАБОРАТОРНАЯ РАБОТА №3
АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПО ГОЛОСУ

Цель: изучить основные принципы функционирования алгоритмов аутентификации пользователей информационных систем по голосу. Ознакомиться с назначением и работой программы VoiceChipher.

3.1. Теоретическая часть

Голос относится к физиологическим динамическим биометрическим характеристикам, т. к. зависит от эмоционального состояния и самочувствия человека.

В зависимости от принципа функционирования системы аутентификации пользователей информационных систем по голосу условно делятся на две группы:

– системы, основанные на сравнительном анализе спектра сигнала, полученного в результате произнесения пользователем парольной фразы (как правило, фраза произносится трижды), и так называемого эталонного спектра образца сигнала, хранящегося в базе данных и полученного аналогичным способом на этапе обучения системы;

– системы, основанные на сравнительном анализе спектра сигнала, полученного в результате ответа пользователем на ряд контрольных вопросов, и так называемого эталонного спектра образца сигнала, хранящегося в базе данных и полученного аналогичным способом на этапе обучения системы.

В системах первой группы необходимо использовать парольные фразы, большая часть фонем которых является огласованными ([э], [о], [л], [а], [и] и т. п.). Это связано с тем, что спектр сигнала, полученного в результате произнесения указанных фонем диктором, зависит от индивидуальных особенностей голоса последнего. Неогласованные фонемы – это шипящие (шумоподобные) [ц], [ч], [ш], [щ] и т. д. Использование таких фонем в парольной фразе,

применяемой для аутентификации по голосу, повышает вероятность ложного доступа. Это связано с тем, что спектр сигнала, полученного в результате произнесения указанных фонем диктором, не зависит от индивидуальных особенностей голоса последнего.

Аутентификация пользователей информационных систем по голосу выполняется в соответствии со следующим алгоритмом:

1. Запись звукового сигнала, получаемого в результате произнесения пользователем парольной фразы или ответа им на ряд контрольных вопросов.

2. Фильтрация от шумов записанного звукового сигнала.

3. Спектральное преобразование сигнала, как правило, с применением быстрого преобразования Фурье.

4. Разбиение спектра на фрагменты.

5. Вычисление спектральной мощности каждого из фрагментов.

6. Вычисление коэффициента сходства величин спектральной мощности соответствующих фрагментов спектра записанного сигнала и эталонного спектра, хранящегося в базе данных.

7. Принятие решения о сходстве или несходстве спектров сигналов путем сравнения вычисленных величин коэффициентов сходства с пороговыми значениями, устанавливаемыми в процессе настройки рассматриваемых систем аутентификации.

3.2. Лабораторное задание

Этапы выполнения лабораторного задания:

1. Ознакомиться с особенностями использования программы VoiceCipher в целях выполнения процедуры аутентификации пользователя по голосу.

VoiceCipher – программа, относящаяся к биометрическим системам безопасности и осуществляющая шифрование/дешифрование файлов, используя для генерации ключа голос пользователя. Эта система позволяет выполнять три этапа:

– обучение;

– шифрование файлов;

– дешифрование файлов.

Этап обучения. На этапе обучения осуществляется регистрация в базе данных нового пользователя. Для реализации данной стадии в окне программы необходимо выбрать вкладку *Study* (рис. 3.1), после чего трижды поочередно произвести запись одной и той же фразы (клавиша *Record*), ее прослушивание с целью контроля качества записи (клавиша *Play*) и добавление в базу данных (клавиша *Add phrase*). Для того чтобы исключить получение трех фраз, произнесенных с одинаковой интонацией, разработчики программы рекомендуют делать перерыв 15–20 мин между записями.

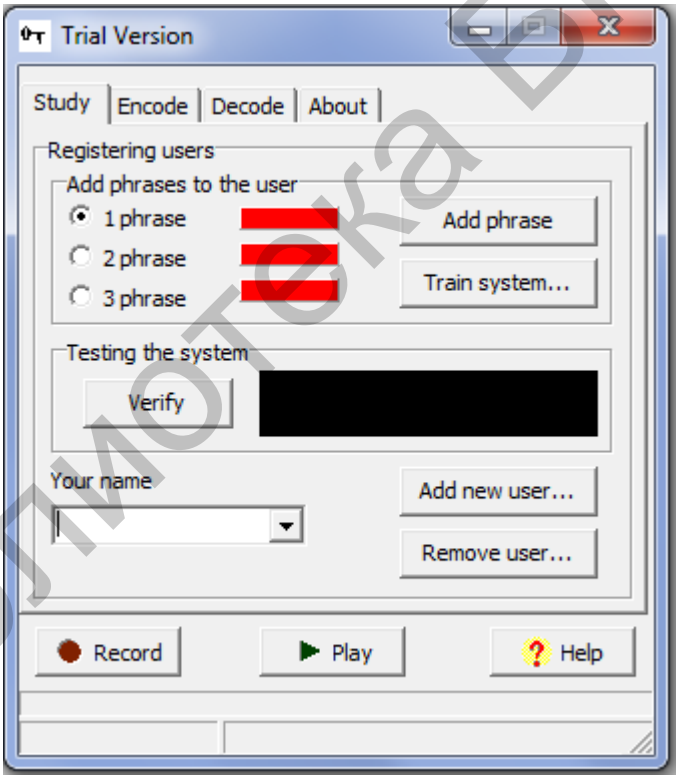


Рис. 3.1. Внешний вид окна программы при выбранной вкладке *Study*

Изменение цвета полосы индикации с красного на зеленый является признаком того, что добавление записанной фразы в базу данных произведено успешно.

После добавления трех вариантов фразы в базу необходимо осуществить в настройках выбор требуемого уровня безопасности данных, для чего нажать клавишу *Train system...*. В результате появится диалоговое окно *Security parameters*.

Выбор высокого уровня безопасности способствует установлению минимального порога признания, т. е. в определенных ситуациях даже реальному пользователю системы проблематично будет осуществить шифрование/дешифрование файлов.

После выбора уровня безопасности диалоговое окно необходимо закрыть нажатием клавиши *OK*.

Далее можно приступить к тестированию системы распознавания. Для этого необходимо вновь осуществить запись кодовой фразы, после чего нажать клавишу *Verify*. Результат работы системы распознавания отобразится в соответствующей области окна программы.

Осуществив запись кодовой фразы, установку уровня безопасности и тестирование системы распознавания, необходимо задать имя пользователя (клавиша *Add new user…*), а далее при необходимости перейти к выполнению следующего этапа программы – шифрованию файлов.

Этап шифрования. Для осуществления шифрования требуется открыть вкладку *Encode*. После выбора имени пользователя из списка необходимо нажать клавишу *Open file(s) for encoding...*, в результате чего откроется окно, в котором следует выбрать файлы, подлежащие шифрованию.

Выбор папки, в которую требуется сохранить зашифрованные файлы, можно осуществить после нажатия клавиши *Change folder*.

После нажатия в диалоговом окне программы клавиши *OK* произойдет шифрование выбранных файлов. Если перед шифрованием отметить флажком блок *Delete encoded files after decoding*, то по окончании оригинальные файлы будут удалены (в противном случае отметку блока *Delete encoded files after decoding* следует убрать).

Этап дешифрования. При реализации этапа дешифрования необходимо выбрать вкладку *Decode*. Дешифрование можно осуществить при помощи голоса либо при помощи ключа, для чего необходимо отметить блок *Voice decoding* либо блок *Enter security key* в диалоговом окне программы. После этого требуется произвести выбор файлов для дешифрования *Open file(s) to decode*... (рис. 3.2, 3.3).

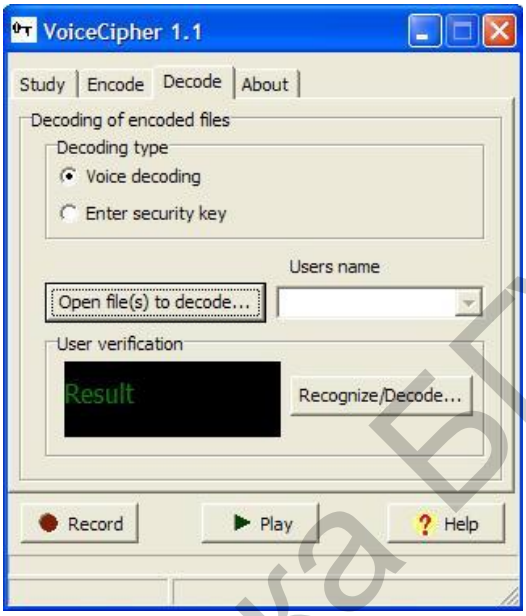


Рис. 3.2. Внешний вид окна программы при выбранной вкладке *Decode*

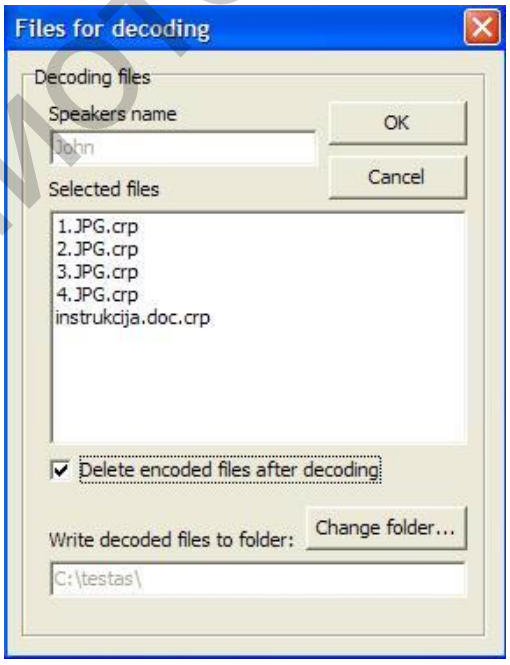


Рис. 3.3. Внешний вид окна программы после выбора файлов для дешифрования и получения положительного результата верификации

При первом способе дешифрования необходимо выполнить запись кодовой фразы, нажав для этого клавишу *Record* (по окончании записи ее необходимо нажать повторно). Далее после нажатия клавиши *Recognize/decode…* осуществляется верификация пользователя (результат верификации отображается в соответствующей области диалогового окна программы. Если результат верификации окажется положительным, то появится диалоговое окно с перечнем имен файлов, подлежащих дешифрации. Выбор директории, в которую необходимо сохранить расшифрованные файлы, можно осуществить после нажатия клавиши *Change folder*. Расшифрование выбранных файлов производится нажатием клавиши *OK*.

Расшифрованные файлы будут сохранены в директории *Write decoded (original) files to folder*, при этом их имена не изменятся. Если перед расшифрованием отметить флажком блок *Delete encoded files after decoding*, то по окончании оригинальные файлы будут удалены (в противном случае отметку блока *Delete encoded files after decoding* следует убрать).

2. Разработать парольную фразу, с использованием которой может быть реализован ложный доступ к ресурсам информационной системы в результате аутентификации пользователя с помощью программы VoiceCipher. Установить, каким образом должна быть настроена программа, чтобы вероятность ложного доступа пользователя к ресурсам системы была максимальной. Оценить значение этой вероятности (в процентах).

3. Разработать парольную фразу, при использовании которой для аутентификации пользователей с помощью программы VoiceCipher значения вероятности ложного доступа и ложного отказа в доступе минимальны. Установить, каким образом должна быть настроена программа для того, чтобы выполнялись указанные условия.

3.3. Содержание отчета

Отчет по лабораторной работе №3 должен содержать:

1. Цель работы.

2. Письменную формулировку разработанной парольной фразы в соответствии с требованиями, изложенными в п. 2 подразд. 3.2, а также описание процесса настройки программы.

3. Письменную формулировку разработанной парольной фразы в соответствии с требованиями, изложенными в п. 3 подразд. 3.2, а также описание процесса настройки программы.

4. Ответы на контрольные вопросы.

3.4. Контрольные вопросы

1. К какому типу биометрических характеристик относится голос?

2. Какие фонемы русского языка не рекомендуется использовать для построения парольной фразы? Какой звук является наиболее устойчивым в спектральном отношении к шумам акустической обстановки и искажениям?

3. Какие шаги включает в себя алгоритм, в соответствии с которым функционирует система аутентификации по голосу?

4. Каким путем можно осуществить защиту парольной фразы от перехвата?

5. В чем заключаются достоинства и недостатки метода идентификации по голосу?

6. Какие объекты могут быть зашифрованы с помощью программы VoiceCipher?

7. Каким образом выполняется процесс шифрования с помощью программы VoiceCipher? Что является ключом шифрования?

ЛАБОРАТОРНАЯ РАБОТА №4
ПАССИВНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКИМ КАНАЛАМ

Цель работы: изучить принципы использования оборудования методики для измерения звукоизоляции воздушного шума однослойными и многослойными конструкциями из звукоизолирующих материалов. Получить практические навыки по оценке индекса звукоизоляции материалов.

4.1. Теоретическая часть

Под понятием канала утечки речевой информации (РИ) обычно понимается совокупность источника информационного (речевого) сигнала, среды распространения информационного сигнала, специальных технических средств для негласного получения информации (СТСНПИ).

Параметрами речевого сигнала являются:

– частотный диапазон (70…7000 Гц);

– уровень громкости речи (60…70 дБ для нормального разговора);

– динамический диапазон (20…45 дБ).

Основная энергия акустических колебаний (около 95 %) лежит в диапазоне частот 125…5600 Гц.

Перехват речевых сигналов может быть реализован с применением одного из следующих методов:

– заходовый (требуется проникновение внутрь выделенного помещения);

– беззаходовый (не требуется проникновение внутрь выделенного помещения).

В качестве СТСНПИ при использовании заходовых методов применяют радиозакладки, закладки с передачей речевого сигнала в инфракрасном диапазоне и по цепям электропитания, закладки с передачей речевого сигнала по телефонной линии, а также диктофоны, проводные микрофоны, «телефонное ухо». При использовании беззаходовых методов используют аппаратуру высокочастотного навязывания, стетоскопы, лазерные микрофоны.

В зависимости от среды распространения и используемых для перехвата СТСНПИ технические каналы утечки речевой информации подразделяются на следующие виды (табл. 4.1): прямой акустический; виброакустический; акустоэлектрический; оптоэлектронный; параметрический.

Таблица 4.1

Виды акустических каналов утечки информации

Наименование канала утечки РИ	Среда распространения	СТСНПИ
Прямой акустический	Воздух или ограждающие конструкции зданий и помещений (стены, потолки, полы, окна)	Акустические закладки (микрофоны, соединенные с миниатюрными звукозаписывающими устройствами и передатчиками), миниатюрные диктофоны и т. п.
Виброакустический	Воздух и ограждающие конструкции зданий и помещений (стены, потолки, полы, окна), инженерные коммуникации (трубы водоснабжения, отопления, вентиляции)	Электронные стетоскопы (контактный вибродатчик, соединенный с усилителем), виброметры, акселерометры
Акустоэлектрический	Электрические цепи (явление «микрофонного эффекта»)	Высокочувствительные низкочастотные усилители, генераторы высокочастотного (более 100 кГц) сигнала, приемники-демодуляторы
Оптоэлектронный	Оконные стекла	Лазерные микрофоны
Параметрический	Элементы высокочастотных генераторов	Приемники-демодуляторы

На рис. 4.1 представлены наиболее вероятные способы утечки РИ из выделенного помещения.

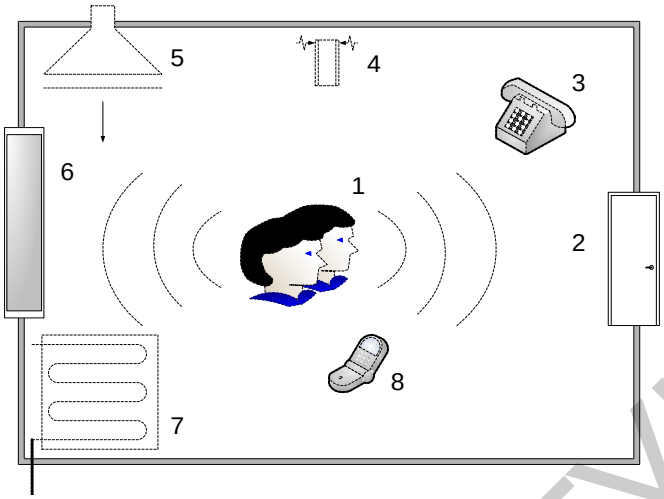


Рис. 4.1. Наиболее вероятные способы утечки РИ из выделенного помещения:
1 – источник РС (прямой акустический канал); 2 – дверь; 3 – телефон;
4 – батарея; 5 – лампа; 6 – окно; 7 – вентиляция; 8 – сотовый телефон

Для защиты информации от утечки по акустическим каналам могут использоваться активные и пассивные средства. Использование таких средств обеспечивает снижение отношения сигнал/шум на входе СТСНПИ. К активным техническим средствам защиты информации от утечки по акустическим каналам относят генераторы акустического шума (белого, окрашенного, речеподобных помех и т. п.). Применение таких средств обеспечивает снижение отношения сигнал/шум на входе СТСНПИ за счет увеличения уровня шума. К пассивным техническим средствам защиты информации от утечки по акустическим каналам относят звукоизолирующие и звукопоглощающие материалы и конструкции. Применение таких материалов и конструкций обеспечивает снижение отношения сигнал/шум на входе СТСНПИ за счет снижения уровня речевого сигнала. Это снижение обусловлено особенностями взаимодействия акустических волн с различными материалами. При своем распространении акустическая волна, взаимодействуя с материалом, частично отражается от его поверхности, частично проходит внутрь него. Энергия акустической волны,

прошедшей внутрь материала, зависит от соотношения акустических сопротивлений первичной среды ее распространения и материала, внутрь которого эта волна прошла (рис. 4.2). Акустическое (волновое) сопротивление среды (Z) – это отношение звукового давления (ρ) плоской волны к колебательной скорости частиц среды (v): $Z = \frac{\rho}{v}$, (Па·с/м). Этот параметр может также быть выражен следующим образом: $Z = \rho \cdot c$, где c – скорость звука в среде.

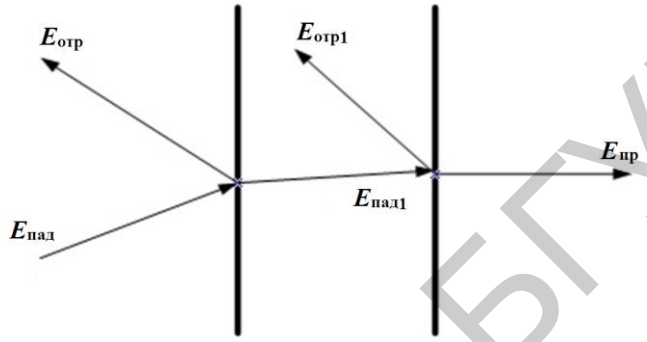


Рис. 4.2. Взаимодействие акустической волны со средой:
$E_{пад}$ – энергия падающей звуковой волны; $E_{отр}$ – энергия отраженной звуковой волны; $E_{пр}$ – энергия прошедшей звуковой волны

Звукоизолирующие материалы обеспечивают ослабление энергии акустической волны за счет явления ее отражения от границы раздела между ними и первичной средой распространения этой волны. Звукопоглощающие материалы обеспечивают ослабление энергии прошедшей внутрь их акустической волны за счет преобразования большей части ее энергии в тепловую.

В зависимости от формы звукоизолирующие и звукопоглощающие материалы подразделяются на следующие виды:

– штучные (блоки, плиты);

– рулонные (маты, полосовые прокладки, холсты);

– рыхлые;

– сыпучие (вата минеральная, стеклянная, керамзит, шлак).

По величине относительного сжатия (жесткости) звукоизолирующие и звукопоглощающие материалы подразделяются на следующие виды:

– мягкие;

– полужесткие;

– жесткие;

– твердые.

Мягкие звукопоглощающие материалы изготавливаются на основе минеральной ваты или стекловолокна с минимальным объемом (связующего до 3 % по массе) или без него. К ним относятся маты или рулонные полотна с объемной массой до 70 кг/м^3, которые обычно применяются в сочетании с защитными перфорированными листовыми экранами (из алюминия, гипсокартона, жесткого ПВХ) или с покрытием пористой пленкой. Коэффициент звукопоглощения этих материалов на средних частотах (250…1000 Гц) достигает значений 0,7…0,95.

К полужестким материалам относятся минераловатные или стекловолокнистые плиты, поверхность которых покрыта пористой краской или пленкой. Коэффициент звукопоглощения полужестких материалов на средних частотах составляет 0,5…0,75.

У твердых материалов объемная масса составляет 300…400 кг/м^3 и коэффициент звукопоглощения – порядка 0,5. Их производят на основе гранулированной или суспендированной минеральной ваты и коллоидного связующего. К ним относятся материалы, в состав которых входят пористые заполнители (перлит, вермикулит, пемза).

В зависимости от структурных признаков звукоизолирующие и звукопоглощающие материалы подразделяются на следующие виды:

– пористо-волокнистые;

– пористо-ячеистые;

– пористо-губчатые.

Для создания звукоизолирующих конструкций, как правило, используются жесткие и твердые строительные материалы. Величина звукоизоляции таких

конструкций зависит от следующих параметров:

– масса;

– изгибная жесткость;

– количество слоев.

Установлено, что при увеличении (наращивании) массы однослойной конструкции в два раза ее звукоизоляция возрастает примерно на 6 дБ. Однако, как правило, увеличение звукоизоляции однослойной конструкции путем наращивания ее массы представляется малоэффективным решением. Более эффективным является способ, при котором обеспечивается следующее:

– снижение изгибной жесткости этой конструкции путем добавления к ней взаимно перпендикулярных ребер жесткости (звукоизоляция такой конструкции может быть при этом увеличена на десятки децибел в диапазоне частот 500…3150 Гц);

– формирование многослойной конструкции, включающей в себя несколько (минимум два) жестких слоев, разделенных мягкими материалами либо воздушной прослойкой; жесткие материалы отражают акустические волны, мягкие материалы – поглощают. Многослойные конструкции являются наиболее эффективными с точки зрения ослабления энергии акустических волн.

Основными характеристиками, определяющими звукоизолирующую способность многослойных конструкций, являются следующие:

– тип материалов;

– толщина слоев;

– вид каркаса;

– способ крепления к каркасу материалов;

– расстояние между слоями.

Использование несущего каркаса в многослойных конструкциях приводит к тому, что звуковые колебания первого жесткого слоя передаются через ребра этого каркаса на последний жесткий слой и затем переизлучаются. Это приводит к появлению так называемых звуковых мостиков, что обуславливает

снижение эффективности ослабления энергии акустических волн конструкцией. Исследования показали, что звуковые мостики могут снижать на 10…15 дБ в области средних и высоких частот звукоизолирующую способность двухслойных конструкций. Для снижения влияния звукового мостика на звукоизоляцию многослойных конструкций в ребра их каркаса включают упругие материалы (мягкая резина) либо при монтаже таких конструкций на стены звукоизолируемых помещений используются виброизолирующие прокладки. Звукопоглощающие материалы, как правило, характеризуются сквозной пористостью, вязкоупругими свойствами и величиной динамического модуля упругости не более 150 кгс/см^2. Звукопоглощающая способность таких материалов обусловлена их пористой структурой и наличием большого числа открытых сообщающихся между собой пор, максимальный диаметр которых обычно не превышает 2 мм (общая пористость должна составлять не менее 75 % по объему). Большая удельная поверхность материалов, создаваемая стенками открытых пор, способствует активному преобразованию энергии акустических волн в тепловую энергию вследствие потерь на трение. На рис. 4.3 представлена частотная зависимость коэффициента звукопоглощения волокнистых материалов от величины их пористости.

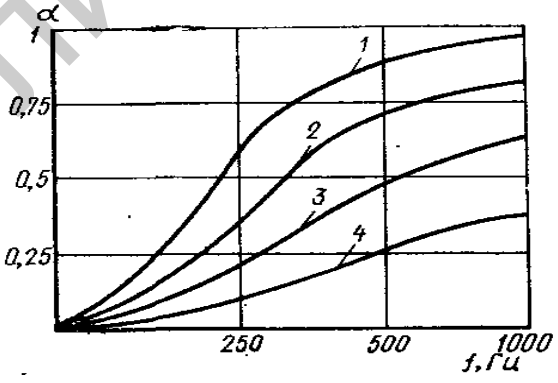


Рис. 4.3. Зависимость коэффициента звукопоглощения волокнистых материалов от пористости:
1 – 95 %; 2 – 50 %; 3 – 25 %; 4 – 15 %

К основным параметрам пористых звукопоглощающих материалов относятся следующие: пористость; распределение по объему; вид пористости (открытая, закрытая, полуоткрытая или тупиковая); форма и извилистость пор; удельная поверхность пор; состояние поверхности пор; вязкостный и инерционный коэффициенты; физико-механические свойства. В волокнистых звукопоглощающих материалах превращение энергии акустических волн в тепловую происходит вследствие вязкости воздуха в межволоконном пространстве и колебаний частиц микрообъемов воздуха внутри материала, что приводит к трению. Также происходит рассеяние энергии из-за трения волокон.

Пористо-губчатые звукоизоляционные материалы изготовливают механическим или химическим вспениванием полимеров. Звукопоглощающие материалы могут характеризоваться плоской или рельефной формой поверхности (рис. 4.4).

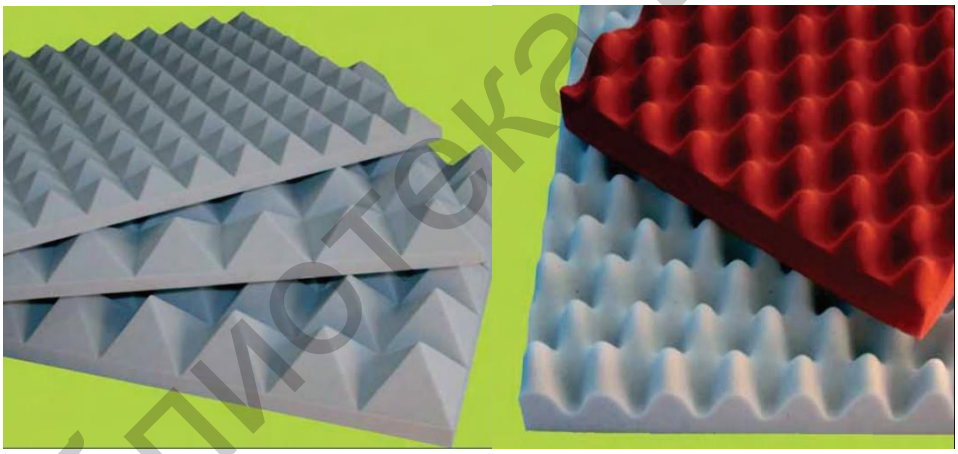


Рис. 4.4. Внешний вид звукопоглощающих материалов с пирамидальной формой поверхности, изготовленных из вспененного полиамида

Звукопоглощающие материалы, характеризующиеся плоской формой поверхности, закрепляют вплотную к стене звукоизолируемого помещения, звукопоглощающие материалы, характеризующиеся рельефной формой поверхности, – на небольшом расстоянии от стены, вплотную друг к другу. При закреплении материала вплотную к стене следует обеспечить значительную толщину слоя, т. к. поглощение звука будет происходить только в нем.

Материал будет эффективно поглощать звуковые волны при толщине слоя минимум в половину длины волны. Для волн с большей длиной эффективность поглощения будет незначительна. Материалы, характеризующиеся рельефной формой поверхности, обеспечивают большее звукопоглощение, чем плоские материалы.

4.2. Лабораторное задание

Выполнить измерения параметров, необходимых для расчета индекса звукоизоляции образцов материалов. Схема экспериментальной установки для таких измерений представлена на рис. 4.5.

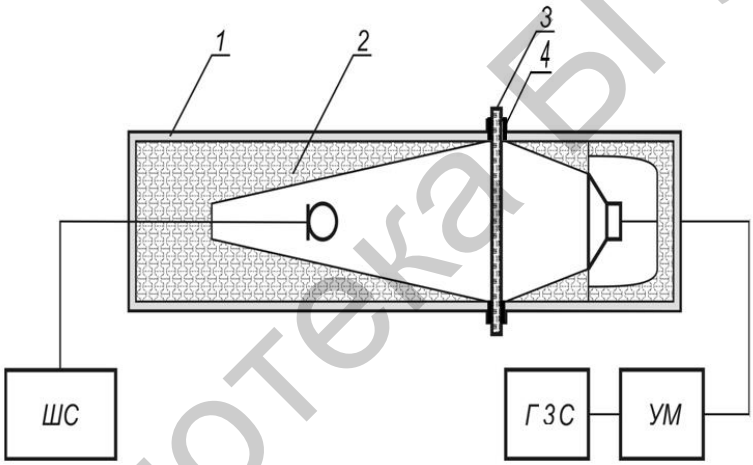


Рис. 4.5. Схема экспериментальной установки:
1 – металлическая труба; 2 – звукопоглощающий материал;
3 – исследуемый образец; 4 – прокладки из пористой резины;
ШС – анализатор акустического шума;
ГЗС – генератор звуковых сигналов; УМ – усилитель мощности

Установка состоит из двух частей металлической трубы. Внутренние поверхности обеих частей трубы облицованы звукопоглощающим материалом на основе стеклянной ваты, характеризующимся формой конуса, расширяющегося в направлении открытой части (для уменьшения диффузности звукового поля и для исключения возникновения в трубе стоячих волн). Одна часть трубы явля-

ется стационарной, другая может передвигаться. В стационарной части трубы установлен микрофон с микрофонным предусилителем, который соединен с анализатором акустического шума, используемого для регистрации параметров звуковых сигналов. В подвижной части трубы установлен динамик, который через усилитель мощности соединен с генератором звуковых сигналов.

При оценке индекса звукоизоляции образцов материалов весь диапазон частот измерений условно делился на третьоктавные полосы со среднегеометрическими частотами 200, 250, 315, 400, 500, 630, 800, 1 000, 1 250, 1 600, 2 000, 2 500, 3 150, 4 000, 5 000, 6 300, 8 000 Гц.

Индекс звукоизоляции (R, дБ) конструкции определяется как разность уровней звукового сигнала, зарегистрированного в определенной точке пространства с помощью анализатора акустического шума, при отсутствии между ГЗС и анализатором акустического шума этой конструкции (L_{m1}) и при ее наличии (L_{m2}): $R = L_{m1} - L_{m2}$.

Используемые приборы и оборудование:

1) анализатор акустического шума МАНОМ-4;

2) микрофон марки М-101;

3) источник звукового сигнала.

4.3. Содержание отчета

Отчет по лабораторной работе №4 должен содержать:

1. Величины измеренных и рассчитанных параметров на каждой из среднегеометрических частот, занесенные в таблицу, имеющую следующий вид:

№ п/п	Наименование образца материала	L_{m1}, дБ	L_{m2}, дБ	R, дБ

2. Частотные зависимости индекса звукоизоляции.

3. Ответы на контрольные вопросы.

4.4. Контрольные вопросы

1. В чем различие между прямым акустическим и виброакустическим каналами утечки информации?

2. В чем различие между звукоизолирующими и звукопоглощающими материалами?

3. Какие существуют подходы к несанкционированному перехвату речевой информации?

4. Какие способы утечки речевой информации из выделенного помещения являются наиболее вероятными?

5. Каким образом может быть оценена величина звукоизоляции конструкций?

6. Какие характеристики конструкций определяют величину их звукоизоляции?

7. Какими основными параметрами характеризуются звукопоглощающие материалы и конструкции?

8. Каким основным недостатком характеризуются многослойные конструкции для ослабления энергии акустических волн? Каким образом может быть исключен этот недостаток?

ЛАБОРАТОРНАЯ РАБОТА №5
АКТИВНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ

Цель работы: 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 защиты речевой информации.

5.1. Теоретическая часть

Под воздействием акустических волн строительные конструкции совершают колебания. Если зафиксировать такие колебания, то возможно реализовать перехват переносимой ими информации по виброакустическому каналу. Например, под воздействием звука, характеризующегося амплитудой 70 дБ, кирпичная стена толщиной 0,5 м совершает вибрационные колебания с ускорением, равным $3 \cdot 10^{-5} \mathrm{g}$.

Современные строительные материалы и конструкции характеризуются низкими показателями затухания механических колебаний в диапазоне звуковых частот. Это обеспечивает возможность распространения таких колебаний на значительные расстояния и перехвата переносимой ими информации. Например, существует реальная возможность перехвата информации по несущей стене из выделенного помещения, расположенного через 1, 2 этажа от места установки специального технического средства негласного получения информации. 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. Трубы различных коммуникаций (отопления, водоснабжения, электропитания и пр.) представляют собой волноводы вибрационных колебаний. По ним возможна реализация волноводного распространения сигналов на значительные расстояния.

Для защиты информации от утечки по виброакутическим каналам могут быть использованы звукоизолирующие и звукопоглощающие материалы и конструкции, а также генераторы акустического шума, ко входу которых подключаются колонки и вибродатчики, предназначенные для закрепления на ограждающих конструкциях помещений (двери, окна, стены и т. п.).

5.2. Лабораторное задание

Структурная схема аппаратного комплекса представлена на рис. 5.1.

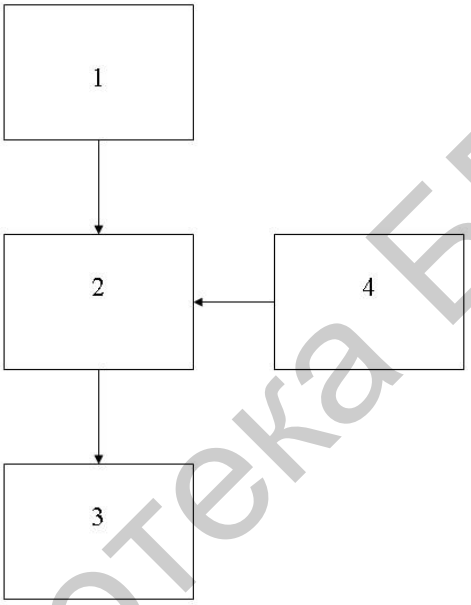


Рис. 5.1. Структурная схема аппаратного комплекса имитации утечки информации и ее защиты:

1 – источник звука; 2 – среда распространения колебаний;

3 – приемное устройство; 4 – устройство активного зашумления

В качестве источника звука используется низкочастотный генератор гармонических сигналов Г3-112 (рис. 5.2), нагруженный на динамическую головку (рис. 5.3). В качестве среды распространения может использоваться любой твердый материал: оргстекло, бетон и т. д. В данном комплексе используется модель ограждающей конструкции из листа оргстекла размером 300×400 мм.

Рис. 5.2. Внешний вид и назначение органов управления генератора Г3-112: 1 – тумблер сети электропитания; 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

Рис. 5.3. Внешний вид модели ограждающей конструкции помещения и размещение элементов комплекса на ней: 1 – разъем виброэлектрического датчика; 2 – виброэлектрический преобразователь; 3 – крепление электромеханического преобразователя; 4 – электромеханический преобразователь; 5 – динамическая головка

Приемное устройство (электронный стетоскоп) представляет собой электронное устройство, которое преобразует механические колебания в электрический сигнал (рис. 5.4) и состоит из виброэлектрического преобразователя, усилителя, источника питания и наушников.

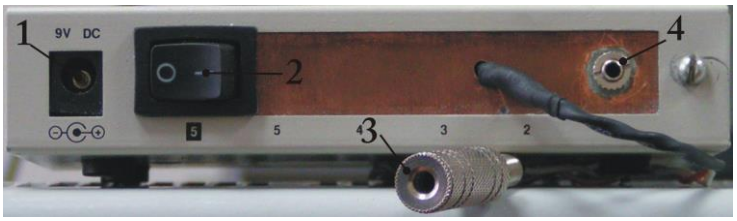


Рис. 5.4. Назначение органов управления приемного устройства:
1 – разъем для подключения источника питания; 2 – тумблер электропитания;
3 – разъем для подключения наушников; 4 – разъем для подключения
виброэлектрического преобразователя

Виброэлектрический преобразователь выполнен на основе пьезокерамического преобразователя ЗП-3, который крепится на поверхность твердой среды (в данном случае оргстекло).

Схема электрическая принципиальная приемного устройства представлена на рис. 5.5.

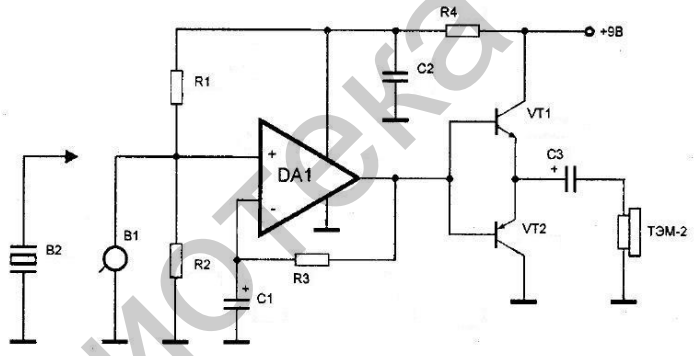


Рис. 5.5. Схема электрическая принципиальная приемного устройства

Микросхема DA1 (см. рис. 5.5) представляет собой операционный усилитель средней точности со встроенной коррекцией и защитой входа и выхода от перегрузки, выполняет функцию предварительного усилителя. Режим работы DA1 по постоянному току задается делителем R1 и R2. Глубина отрицательной обратной связи определяется параметрами цепи C1 и R3. Усилитель мощности представлен двухтактной схемой на транзисторах VT1 и VT2 (режим класса В).

Питание усилителя происходит от сети напряжением 220 В через блок питания, преобразующий напряжение сети в постоянное 9 В, либо от элемента питания типа «Крона».

В качестве устройства активного зашумления используется устройство защиты речевой информации (УЗРИ) «Кабинет», которое предназначено для предотвращения несанкционированного перехвата речевой информации через ограждающие конструкции и инженерные коммуникации выделенных помещений. Устройство защиты речевой информации «Кабинет» обеспечивает защиту от следующих технических средств перехвата информации:

– устройств, использующих контактные микрофоны (электронные, проводные и радиостетоскопы);

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

– закладных устройств, внедряемых в строительные элементы конструкций.

Технические характеристики устройства «Кабинет» приведены в табл. 5.1.

Таблица 5.1

Технические характеристики УЗРИ «Кабинет»

Технические параметры	Значение параметра
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 В·А
Габариты акустического генератора шума (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 шт.

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. 5.6, а наименования и расположение его органов управления – на рис. 5.7.

В состав АГШ входят:

– генератор шума (ГШ);

– усилитель мощности;

– модуль питания (МП);

– эквалайзер (Э);

– устройство контроля (УК).

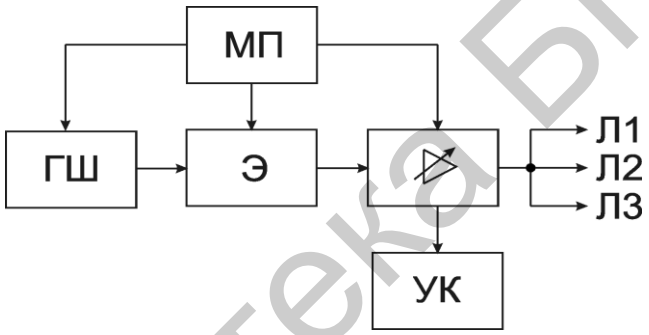


Рис. 5.6. Схема электрическая структурная устройства защиты речевой информации «Кабинет»

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. Глубина регулировки усиления по полосам составляет не менее ±20 дБ, глубина регулировки общего уровня сигнала – не менее 40 дБ.

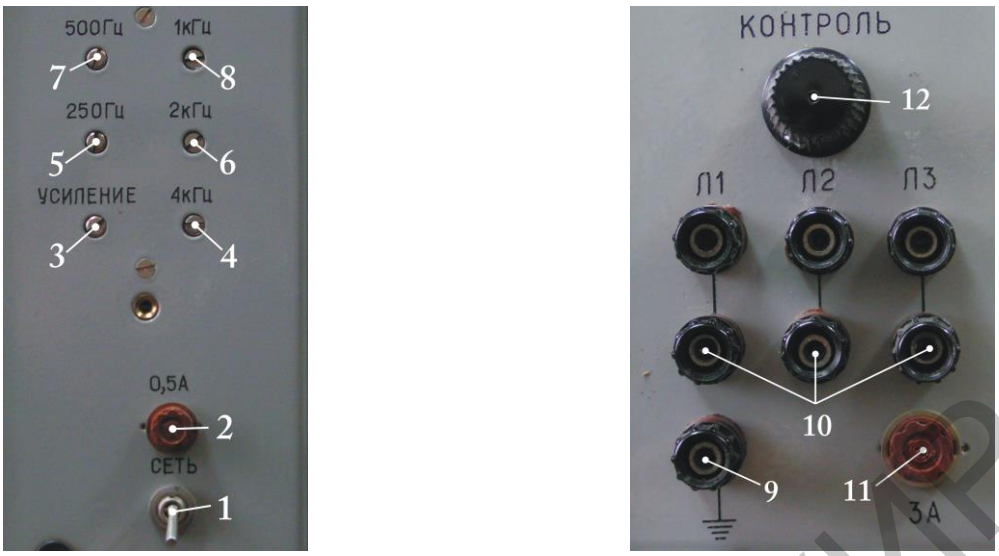


Рис. 5.7. Назначение органов управления УЗРИ «Кабинет»:
1 – тумблер сети питания; 2 – сетевой предохранитель; 3 – регулятор усиления; 4, 5, 6, 7, 8 – регуляторы эквалайзера для соответствующих октавных частот; 9 – разъем подключения заземления; 10 – разъемы для подключения электромеханических преобразователей; 12 – ручка плавной регулировки уровня шума на встроенной динамической головке

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.

В ходе выполнения лабораторной работы необходимо обеспечить невозможность перехвата акустических колебаний в ограждающей конструкции в частотном диапазоне 175…5600 Гц средствами акустической разведки. Для этого необходимо:

1. К выходу генератора Г3-112 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. Параллельно к электромеханическому преобразователю подключить электронный вольтметр.

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

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

9. Установить на генераторе значение частоты, равное 1 кГц.

10. Включить в электрическую сеть генератор и УЗРИ «Кабинет».

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

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

13. 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.

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

15. 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. Измерить с помощью электронного вольтметра напряжение на электромеханическом преобразователе.

16. 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. После выполнения измерения регуляторы вернуть в крайнее левое положение.

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

18. Построить частотную зависимость измеренного значения напряжения шума.

19. Оформить отчет.

5.3. Содержание отчета

Отчет по лабораторной работе №5 должен содержать:

1. Цель работы.

2. Структурную схему аппаратного комплекса имитации утечки информации и ее защиты.

3. Измеренные значения напряжения шума, частотную зависимость напряжения шума.

4. Вывод по работе.

5. Ответы на контрольные вопросы.

5.4. Контрольные вопросы

1. Что такое октава? Приведите пример центральных частот стандартных октавных полос.

2. Что такое речевой сигнал и какими параметрами он характеризуется?

3. К чему может привести явление волнового совпадения в помещении, где циркулирует речевая информация?

4. Сформулируйте основные рекомендации по применению систем активной защиты информации.

ЛАБОРАТОРНАЯ РАБОТА №6
ОБНАРУЖЕНИЕ С ПОМОЩЬЮ НЕЛИНЕЙНОГО ЛОКАТОРА СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ

Цель: изучить демаскирующие признаки нелинейных объектов и получить практические навыки по их обнаружению и идентификации с использование нелинейного локатора.

6.1. Теоретическая часть

Закладное устройство – устройство, конструктивно объединяющее в себе приемный и передающий модуль и, как правило, источник питания, предназначенное для перехвата речевой информации.

В зависимости от демаскирующих признаков закладных устройств методы их поиска можно разделить на три группы:

– с использованием видовых демаскирующих признаков;

– с использованием сигнальных демаскирующих признаков;

– с использованием вещественных демаскирующих признаков.

Поиск закладных устройств по видовым демаскирующим признакам характеризуется наименьшими затратами по сравнению с другими методами поиска и выполняется сотрудниками службы безопасности путем визуального осмотра помещения и размещенных в нем объектов (в том числе технических средств) на предмет наличия в них закладных устройств. В целях обеспечения полноты визуального осмотра его целесообразно проводить, перемещаясь от двери по или против часовой стрелке от периферии к центру помещения. Во время осмотра 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 и т. п. Для визуального осмотра при поиске закладных устройств могут применяться фонари, досмотровые зеркала и технические эндоскопы.

Поиск закладных устройств, вмонтированных в технические средства, проводят путем сравнения топологии схемы таких средств с эталонной топологией, которая зафиксирована в документации.

Метод поиска закладных устройств по сигнальным демаскирующим признакам реализуется одним из следующих способов:

– путем регистрации с помощью сканирующего приемника параметров электромагнитных сигналов, мощность которого превышает мощность электромагнитного фона;

– путем регистрации с помощью селективного приемника электромагнитных сигналов, мощность и частота которых соответствует аналогичным параметрам побочных электромагнитных сигналов закладных устройств;

– путем обнаружения изменений электрических характеристик линий связи, к которым могут быть подключены закладные устройства.

Вещественные демаскирующие признаки закладных устройств обусловлены наличием в них полупроводниковых элементов, которые являются нелинейными объектами, т. е. характеризующимися нелинейной вольт-амперной характеристикой (ВАХ) – зависимостью тока, протекающего по их p-n-переходу, от величины подводимого к ним напряжения. Поиск закладных устройств по вещественным демаскирующим признакам выполняется с использованием метода нелинейной локации, при котором применяются устройства, называемые нелинейными локаторами. Нелинейная локация – метод обнаружения и определения местоположения нелинейных объектов, основанный на воздействии на эти объекты первичным электромагнитным излучением (зондирующим сигналом) и дальнейшем анализе амплитуды вторичного электромагнитного излучения (сигналов, переизлученных нелинейным объектом) на высших гармониках его спектра.

При воздействии на полупроводник первичным электромагнитным излучением через его p-n-переходы начинают протекать вихревые токи, которые

обуславливают формирование вторичного электромагнитного излучения. Первичное излучение – совокупность непрерывных гармонических или импульсных сигналов, характеризующихся некоторой частотой f. Источником такого излучения является нелинейный локатор. Так как полупроводники являются нелинейными объектами, то спектр вторичного электромагнитного излучения, формируемого вихревыми токами, протекающими через их p-n-переходы, может быть разложен в ряд Фурье по частотам f, 2f, 3f и т. д., т. е. такой спектр характеризуется наличием высших гармоник. Приемник нелинейного локатора настроен таким образом, чтобы регистрировать вторичное электромагнитное излучение на частотах 2f и 3f.

Нелинейными свойствами характеризуются не только полупроводниковые элементы, но так называемые структуры металл – окисел – металл (МОМ-структуры), формируемые в местах контактов металлических предметов или конструкций помещения и здания. Поэтому для обнаружения полупроводников необходимо учитывать различия в спектральной мощности вторичного электромагнитного излучения на частотах 2f и 3f. Для истинных полупроводников спектральная мощность вторичного электромагнитного излучения на частоте 2f превышает величину аналогичного параметра на частоте 3f. Для ложных (МОМ-структур) наблюдается противоположное соотношение указанных параметров. Кроме того, так как соединение слоев МОМ-структуры является непрочным, то соотношение мощности вторичного электромагнитного излучения на частотах 2f и 3f может изменяться в результате оказания механического воздействия на объект, где сформировалась такая структура.

Нелинейные локаторы (НЛ) могут работать в следующих режимах:

– непрерывный;

– импульсный.

Максимальная мощность излучения локатора в непрерывном режиме не превышает 3…5 Вт, чтобы не оказывалось негативное воздействие на оператора. При импульсном режиме работы локатора мощность одного импульса мо-

жет составлять 300 Вт, а средняя мощность излучения – 1,5 Вт. В связи с этим более вероятным представляется обнаружение закладных устройств с помощью нелинейных локаторов, функционирующих в импульсном режиме. Средняя мощность излучения таких локаторов определяется по формуле $P_{ср} = \frac{P_{имп}}{Q}$, где $P_{имп}$ – мощность одного импульса, Вт; $Q = 1/F\tau$ – скважность; F – частота следования импульсов, Гц; τ – длительность одного импульса, с. В связи с этим все локаторы, функционирующие в импульсном режиме, по параметру мощности генерируемого электромагнитного излучения удовлетворяют санитарно-гигиеническим требованиям.

6.2. Лабораторное задание

Перед выполнением задания ознакомиться с органами управления нелинейного локатора SP-61/M «Катран» в соответствии с Руководством по эксплуатации ЕЛКБ 464415.810 РЭ.

При выполнении лабораторного задания необходимо определить сигнальные демаскирующие признаки сотового телефона. Для этого:

1. Включить нелинейный локатор. Подключить наушники. Установить мощность излучения передатчика 0,08 Вт.

2. Разместить сотовый телефон на поверхности стола в таком месте, где при его отсутствии нелинейный локатор не регистрирует вторую и третью гармоники.

3. Определить сигнальные демаскирующие признаки сотового телефона, используя режимы излучения ЧМ- и АМ-сигналов, а также тракты приема сигналов второй и третьей гармоник.

4. Полученные результаты записать в отчет. Определить наиболее «удобный» режим для обнаружения сотовых телефонов.

5. Выключить сотовый телефон. Выполнить повторное обнаружение его демаскирующих признаков. Полученные результаты записать в отчет. Сравнить результаты, отметить различия.

6. Получить у преподавателя имитаторы нелинейных объектов. Используя нелинейный локатор, идентифицировать нелинейные объекты.

7. Полученные результаты записать в таблицу, имеющую следующий вид:

№ имитатора	Демаскирующие признаки	Наименование нелинейного объекта

6.3. Содержание отчета

Отчет по лабораторной работе №6 должен содержать:

1. Цель работы.
2. Результаты выполнения пп. 3, 4, 5 лабораторного задания.
3. Результаты выполнения пп. 6, 7 лабораторного задания.
4. Вывод по работе.
5. Ответы на контрольные вопросы.

6.4. Контрольные вопросы

1. Каково назначение нелинейного локатора?
2. Какой признак является характерным при обнаружении полупроводника?
3. Какой признак является характерным при обнаружении МОМ-структуры?
4. Каково назначение демодулятора аудиосигналов НЛ?
5. Как отличается способность НЛ обнаруживать закладные устройства при работе в импульсном и непрерывном режимах работы?

ЛАБОРАТОРНАЯ РАБОТА №7
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.

7.1. Теоретическая часть

Сканирующие приемники обеспечивают прием радиосигналов в широком диапазоне частот (100 кГц…3 ГГц) с различными видами модуляции. Основными отличительными функциями таких приемников является возможность сканирования (просмотра) заданного диапазона частот, контроль приоритетной частоты, возможность создания банков контролируемых частот. Более широкие возможности по обнаружению предоставляются при получении спектрограммы диапазона, что может быть реализовано при подключении к приемнику специальной панорамной приставки или компьютера со специальным программным обеспечением, которое значительно расширяет возможности обнаружения подслушивающих устройств. Сканирующие приемники подразделяются на две группы: переносимые сканирующие приемники и перевозимые портативные сканирующие приемники. К переносимым относятся малогабаритные сканирующие приемники весом 150…350 г, имеющие автономные аккумуляторные источники питания.

Сканирующие приемники (как переносимые, так и перевозимые) могут работать в одном из следующих режимов:

– режим автоматического сканирования в заданном диапазоне частот;

– режим автоматического сканирования по фиксированным частотам;

– ручной режим работы.

Первый режим работы приемника является основным при выявлении частот работающих радиоэлектронных средств (при решении задач радиоразведки и радиоконтроля), а также при поиске излучений радиозакладок. При этом режиме устанавливаются начальная и конечная частоты сканирования, шаг перестройки по частоте и вид модуляции.

Второй режим работы приемников используется при ведении радиоразведки и радиоконтроля, если известны и записаны в каналы памяти возможные частоты работы радиосредств. Для каждого канала памяти вводится значение частоты, вид модуляции и для некоторых видов приемников – ослабление входного аттенюатора. Информация, хранящаяся в каждой ячейке (канале) памяти, может легко вызываться на жидкокристаллический дисплей с помощью функциональных клавиш. Сканирование каналов памяти осуществляется последовательно, при этом так же, как и при первом режиме работы, предусмотрены возможность сканирования с пропуском частот, записанных в маскированные каналы, и возможность автоматической записи в память частот обнаруженных сигналов.

Третий режим работы приемников применяется для детального обследования всего или ряда частотных диапазонов и отличается от первого режима тем, что перестройка приемников осуществляется оператором с помощью ручки изменения частоты, при этом информация о частоте настройки, виде модуляции, уровне входного сигнала и т. п. выводится на жидкокристаллический дисплей. Перестройка частоты осуществляется с выбранным шагом перестройки. Для более быстрого изменения частоты используется режим поразрядного набора, при котором частота изменяется последовательно по разрядам (например, 100 МГц, 10 МГц, 1 МГц, 100 кГц и т. д.). Данный режим работы позволяет довольно быстро и легко выйти в нужный частотный диапазон.

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 радиоприемное

устройство, выделить и зафиксировать частоты всех постоянно присутствующих в эфире радиовещательных и телевизионных станций, организационных каналов сетей радиосвязи общего пользования, несущих частот радиорелейных линий (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 радиосистем передачи извещений (РСПИ), необходимо проводить еще в более узких пределах (2…3 МГц).

Сканирующие приемники широко используются для решения задач радиомониторинга:

– выявления загрузки диапазона частот зарегистрированными источниками радиоизлучений;

– измерения параметров радиоизлучений на основе их спектрального анализа;

– обнаружения побочных электромагнитных излучений специальных технических средств негласного получения информации;

– выявления побочных электромагнитных излучений технических средств объекта защиты (оргтехники, компьютеров и т. п.);

– выявления наличия преднамеренных и непреднамеренных помех;

– поиска облучающих объект сигналов (радиолокационных, ВЧ-навязывания, НЧ-навязывания, лазерных);

– контроля соблюдения дисциплины связи при использовании персоналом на объекте открытых каналов связи (по частотам, режимам работы, характеру передаваемой информации, графику работы и т. д.);

– оценки эффективности используемых на объекте технических средств защиты.

7.2. Лабораторное задание

Перед выполнением задания ознакомиться с органами управления скоростного поискового приемника «Скорпион XL» и многофункционального имитатора сигналов «Шиповник-2» в соответствии с руководствами по их эксплуатации.

В ходе выполнения лабораторного задания необходимо обнаружить и классифицировать радиочастотные излучения в полосе приема сканирующего приемника. Для этого выполнить следующее:

1. С помощью многофункционального имитатора сигналов «Шиповник-2» поочередно на частотах 144 МГц, 433 МГц, 1,2 ГГц и 2,4 ГГц сгенерировать сигналы следующих видов модуляции: ШЧМ, УЧМ.

2. На расстоянии 1, 3 и 5 м от антенн имитатора с использованием скоростного поискового приемника «Скорпион-XL» провести обнаружение сигналов генерируемых имитатором сигналов «Шиповник-2». Оценить максимальные значения мощности этих сигналов, а также значения частот, на которых мощность максимальна. Результаты систематизировать в таблице, форма которой имеет следующий вид:

№ п/п	Вид модуляции	Расстояние, м	Частота, МГц	Мощность, Вт

Таблицу с результатами занести в отчет.

3. С использованием полученных результатов построить графические зависимости амплитуды сигналов от расстояния и частоты. Сделать вывод на основе результатов построенной зависимости.

7.3. Содержание отчета

Отчет по лабораторной работе №7 должен содержать:

1. Цель работы.

2. Таблицу с результатами выполненных измерений.

3. Построенные графические зависимости.

4. Вывод по работе.

5. Ответы на контрольные вопросы.

7.4. Контрольные вопросы

1. Каково назначение сканирующего приемника?

2. Для чего предназначен имитатор сигналов «Шиповник-2»?

3. Что относится к перечню задач радиомониторинга?

4. Какова классификация сканирующих приемников?

5. В каких случаях используется ручной режим работы сканирующего приемника?

ЛАБОРАТОРНАЯ РАБОТА №8
АППАРАТНЫЕ И ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ СТИРАНИЯ ИНФОРМАЦИИ С ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ

Цель: изучить принципы работы аппаратных и программных средств для стирания информации с магнитных и полупроводниковых носителей.

8.1. Теоретическая часть

Информация ограниченного распространения на сегодняшний день документируется не только посредством бумажных, но и посредством электронных носителей (магнитных или полупроводниковых). Для сохранения режима ограниченного доступа к информации, документируемой посредством электронных носителей, при возникновении опасности ее утечки, разглашения, хищения возникает необходимость ее полного стирания, в результате которого она не может быть восстановлена. Для этих целей используются аппаратные или программные средства.

Аппаратные средства для стирания информации с магнитных носителей

Выделяют два типа магнитных носителей:

– нежесткие;

– жесткие.

Модификация аппаратных средств для стирания информации с магнитных носителей:

– автономные устройства (для стирания информации с обоих типов магнитных носителей) (рис. 8.1);

– устройства, встраиваемые в типовой компьютерный корпус (для стирания информации с жестких магнитных носителей) (рис. 8.2).

Рис. 8.1. Автономное устройство стирания информации
с магнитных носителей «Раскат»

Рис. 8.2. Устройство стирания информации, встроенное
в системный блок персональной электронной вычислительной машины

Стирание информации с магнитных носителей реализуется в результате воздействия магнитного поля на их элементы. При этом может выполняться их размагничивание или намагничивание до насыщения. Наиболее просты в реализации устройства стирания информации, выполняющие намагничивание до насыщения элементов носителя. Это обусловлено тем, что такое воздействие выполняется посредством мощного импульса магнитного поля, который генерируется более просто, чем переменное магнитное поле с затухающей до нуля напряженностью, необходимое для выполнения размагничивания.

Основными параметрами, определяющими величину напряженности магнитного поля, требуемую для стирания информации, являются коэрцитивная сила и прямоугольность петли гистерезиса материалов магнитных носителей информации. Для современных нежестких магнитных носителей информации значения указанных параметров составляют соответственно не менее 200 кА/м и 0,85…0,95. Ориентация воздействующего на носитель магнитного поля должна соответствовать ориентации поля, которым выполнялась запись информации. В табл. 8.1 представлены основные технические характеристики устройств для стирания информации с магнитных носителей «Раскат».

Таблица 8.1

Основные технические характеристики устройств для стирания информации с магнитных носителей «Раскат»

Наименование параметра	Значения параметра
1	2
Напряженность стирающего магнитного поля	не менее 450 кА/м
Количество стираемых носителей	1…4 шт.
Длительность стирания информации на магнитном носителе	не более 0,1 с
Время готовности устройства к стиранию информации после включения питания или предыдущего срабатывания	не более 20 с

Окончание табл. 8.1

1	2
Номинальное напряжение питания: – от сети; – от автономного источника питания	 220 В, 50 Гц 12 В
Потребляемая мощность при работе от сети 220 В, 50 Гц: – в режиме ожидания; – импульсная потребляемая мощность	 не более 5 Вт не более 90 Вт
Диапазон рабочих температур	5…40 °С
Масса	до 4,5 кг

На рис. 8.3 представлена функциональная схема устройства для стирания информации с магнитных носителей «Раскат». Устройство для стирания информации с магнитных носителей содержит источник постоянного напряжения (ИПН), первый и второй конденсаторы (C_1 и C_2 соответственно), катушку индуктивности L и двухпозиционный ключ (ДК). Устройство работает следующим образом. До осуществления стирания информации ДК устанавливается в положение 1, при котором происходит заряд первого конденсатора C_1 от ИПН ($U_0 = E$). Для стирания информации ДК переводится в положение 2. Первый конденсатор C_1 отключается от ИПН и включается в цепь спиральной катушки индуктивности L, причем первый конденсатор C_1 разряжается через катушку индуктивности L и активное сопротивление цепи, что приводит к возникновению мощного импульса магнитного поля, одновременно происходит заряд конденсатора C_2. По окончании разряда первого конденсатора C_1 устройство ДК автоматически переключается в положение 1. Конденсатор C_2 также разряжается через спиральную катушку индуктивности L. В параллельном контуре LC_2 возникают затухающие резонансные колебания с частотой, определяемой параметрами контура ($\omega = (\omega_0^2 - \delta^2)^{1/2}$ – угловая частота затухающего колебания, где $\omega_0 = (LC_2)^{-1/2}$ – резонансная частота, $\delta = R/2L$ – коэффициент затухания), что приводит к возникновению серии разнополярных затухающих электромагнит-

ных импульсов с амплитудой $U_0e^{-\delta t}$. В результате воздействия мощного импульса магнитного поля на магнитный носитель, возникающего вследствие разряда первого конденсатора C_1, происходит намагничивание носителя и стирание информации. Благодаря появлению серии разнополярных импульсов, носитель перемагничивается несколько раз в разных направлениях с затухающей амплитудой воздействия. Вследствие изменения направления и интенсивности воздействующего магнитного поля происходит дополнительное перемагничивание носителя, который в результате остается размагниченным.

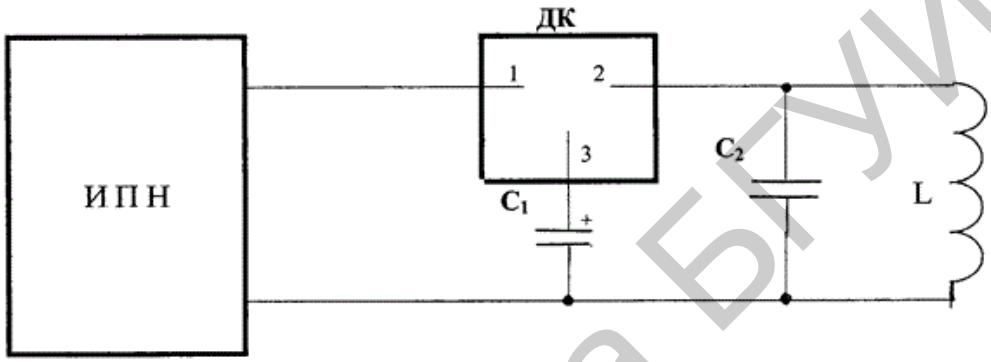


Рис. 8.3. Функциональная схема устройства стирания информации с магнитных носителей «Раскат»

Основными элементами устройств для стирания информации с жестких магнитных носителей являются следующие: аккумулятор; зарядное устройство; устройство подключения сети; преобразователь напряжения; стабилизатор напряжения; микроконтроллер; устройство индикации; накопитель энергии; коммутатор; демпфер; устройство переключения коммутирующих устройств, изменяющих направление тока в катушках индуктивности; электронный ключ; устройство блокировки; три катушки индуктивности полеобразующей системы; источник питания персональной электронной вычислительной машины. Механическая часть устройства содержит привод вращения носителя на жестком магнитном диске. Устройство размещается в системном блоке персональной электронной вычислительной машины (см. рис. 8.2).

Аппаратные средства для стирания информации с полупроводниковых носителей

Основные преимущества полупроводниковых носителей информации по сравнению с магнитными:

– низкое значение времени доступа;

– высокая скорость перезаписи информации при последовательном доступе за счет того, что ненужная информация стирается блоками;

– низкая себестоимость производства.

При стирании информации с полупроводниковых носителей с помощью аппаратных средств выполняется прямое воздействие на управляющие выводы микросхем этих носителей электрическими импульсами высокого напряжения и/или непосредственное воздействие на них мощным импульсным электромагнитным излучением (длительность электромагнитных импульсов – 3…20 нс, энергия – до $4{,}5 \cdot 10^{-2}$ Дж (энергия импульсов может быть пропорционально увеличена путем их многократного излучения)).

Первый способ может быть использован для стирания информации с полупроводниковых носителей с параллельным доступом, у которых микросхемы имеют выводы шины данных или адреса. В этом случае подача высокого напряжения на эти выводы позволяет либо полностью уничтожить систему адресации микросхемы, либо записать во все ее ячейки логический нуль. В результате реализации одного из таких процессов прочитать существовавшую ранее информацию будет невозможно.

При использовании для стирания информации второго способа происходит следующее. Импульсное электромагнитное поле индуцирует изменяющееся электрическое поле, создающее на управляющих затворах дополнительное высокое напряжение, изменяющее пороговое напряжение, и носители-электроны переносятся через потенциальный барьер. Иными словами, транзисторы переходят в другие состояния, или происходит простой пробой. Напряжение пробоя полевого транзистора с размером 1 мкм приблизительно равно 10 В. Следова-

тельно, необходимо создать импульсное электромагнитное поле, обеспечивающее такую крутизну, чтобы в зазоре, где помещается транзистор, сформировать напряжение порядка 10 кВ/см.

Программные средства для стирания информации с электронных носителей

Основное преимущество программных средств для стирания информации с электронных носителей по сравнению с аппаратными средствами – носители не повреждаются и пригодны для повторной записи данных. Основной недостаток – длительность процесса стирания.

Процесс стирания информации с электронных носителей с использованием программных средств называют форматированием. Выделяют следующие виды форматирования:

– форматирование на низком уровне;

– форматирование на высоком уровне:

а) в обычном режиме;

б) быстрое форматирование.

Форматирование электронного носителя на высоком уровне выполняется одним из следующих образов:

– полная перезапись информации на носитель;

– частичная перезапись информации на носитель.

Форматирование электронного носителя информации на низком уровне. Такое форматирование выполняется на заводе-изготовителе. Основной его целью является инициализация и тестирование изготовленного носителя. При форматировании на низком уровне жесткого магнитного диска на его магнитную поверхность с использованием специального оборудования наносятся сервометки (информация, которая в дальнейшем используется для позиционирования головок такого носителя). Информация, записанная во время этого процесса, является служебной и не может быть перезаписана без использования спе-

циального программного обеспечения. Перезапись такой информации является актуальной в том случае, когда жесткий магнитный диск начал работать некорректно. Эта проблема в наибольшей степени актуальна для носителей типа ATA (Advanced Technology Attachment) и SCSI (Small Computer System Interface). Для выполнения форматирования на низком уровне носителей указанных типов необходимо использовать специальное программное обеспечение, выпущенное заводом-изготовителем носителя. Как правило, оно выпускается для носителей каждой из моделей (рис. 8.4).

Рис. 8.4. Месторасположения названия производителя и номера модели на корпусе жесткого магнитного диска

В зависимости от модели жесткого магнитного диска необходим определенный набор команд для того, чтобы разблокировать доступ к секторам, на которых записана служебная информация. В случае если эти сектора являются поврежденными, то с использованием специального программного обеспечения выполняется их замена на резервные, которые создаются на заводе-изготовителе в процессе «первого» форматирования выпущенного жесткого магнитного диска.

Форматирование в обычном режиме – процесс, который заключается в создании главной загрузочной записи с таблицей разделов и/или структур пу-

стой файловой системы, установке загрузочного сектора и тому подобных действий. В процессе форматирования также проверяется целостность носителя для блокировки дефектных секторов.

Быстрое форматирование – процесс, практически аналогичный форматированию в обычном режиме с той лишь разницей, что в ходе такого процесса не выполняется проверка носителя на наличие дефектных секторов.

Форматирование методом полной перезаписи информации на носитель. Существует большое количество алгоритмов для стирания информации с электронных носителей путем их полной перезаписи. Однако в основе всех этих алгоритмов лежат N-кратные процедуры форматирования и записи на носитель двоичных единиц, нулей и псевдослучайных чисел.

Для того чтобы выполнить форматирование на высоком уровне одного из дисков или разделов операционной системы Windows, необходимо в командной строке прописать следующее:

format «буква, обозначающая наименование форматируемого системного диска:» (например, format C:) или format «путь к разделу, который необходимо отформатировать» (например, format D:/folder 1).

Для операционной системы Linux синтаксис команды для форматирования следующий:

:dd if =/dev/zero of=/dev/sda bs=

Вместо «/dev/sda» необходимо указать адрес устройства для форматирования.

Форматирование методом частичной перезаписи информации на носитель. С использованием API-драйвера (Application Programming Interface) электронного носителя можно установить адреса ячеек памяти, в которые занесены файлы, подлежащие стиранию. После этого с использованием указанного драйвера нужно выполнить форматирование методом полной перезаписи информа-

ции в ячейки памяти по установленным адресам. Форматирование с применением рассматриваемого метода является более сложным с точки зрения реализации программного обеспечения, однако для его реализации требуется меньшее количество времени. Кроме того, в процессе такого форматирования доступ к форматируемому носителю сохраняется. Работа с API-драйвером включает в себя два этапа. Первый этап – получение адресов ячеек памяти и количество бит стираемой информации, занесенных в каждую из ячеек. В результате выполнения этого этапа формируется массив данных, включающих в себя значения адресов и количества бит информации, записанной по этим адресам. Второй этап – запись псевдослучайных чисел по полученным адресам ячеек памяти.

8.2. Лабораторное задание

В ходе выполнения лабораторной работы необходимо:

1. Изучить внешний вид и принцип работы устройства стирания информации с магнитных носителей «Раскат». Для этого использовать руководство по его эксплуатации.

2. Разработать структурную схему устройства стирания информации с магнитных носителей «Раскат».

3. Разработать структурную схему устройства стирания информации с полупроводниковых носителей.

4. Решить задачу. Скорость записи информации на электронный носитель составляет 70 Мбит/с. Объем носителя – 500 Гбайт. Рассчитать, какое количество времени понадобится для того, чтобы выполнить форматирование такого носителя методом полной перезаписи информации, если количество циклов перезаписи равно 7.

8.3. Содержание отчета

Отчет по лабораторной работе №8 должен содержать:

1. Цель работы.

2. Структурную схему и описание принципа работы устройства стирания информации с магнитных носителей «Раскат».

3. Структурную схему и описание принципа работы устройств стирания информации с полупроводниковых носителей.

4. Решение задачи.

5. Вывод по работе.

6. Ответы на контрольные вопросы.

8.4. Контрольные вопросы

1. Какие существуют способы документирования информации?

2. В каких случаях возникает необходимость стирания информации?

3. Какие выделяют типы электронных носителей информации?

4. Какие существуют модификации аппаратных средств для стирания информации с магнитных носителей?

5. Каким образом выполняется стирание информации с электронных носителей с помощью программных средств?

ЛАБОРАТОРНАЯ РАБОТА №9
ИЗУЧЕНИЕ СИСТЕМЫ ОХРАННОГО ТЕЛЕВИДЕНИЯ

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

9.1. Теоретическая часть

Назначение и состав системы видеонаблюдения

Системы видеонаблюдения предназначены для обнаружения и идентификации человека и автотранспортных средств.

Основные технические средства, применяемые для построения таких систем (рис. 9.1):

1) видеокамеры – обеспечивают формирование телевизионного изображения;

2) видеомонитор – применяется для отображения видеоданных;

3) устройство видеорегистрации – используется для записи и хранения видеоданных;

4) устройство коммутации – позволяет транслировать изображения с видеокамер на видеомонитор.

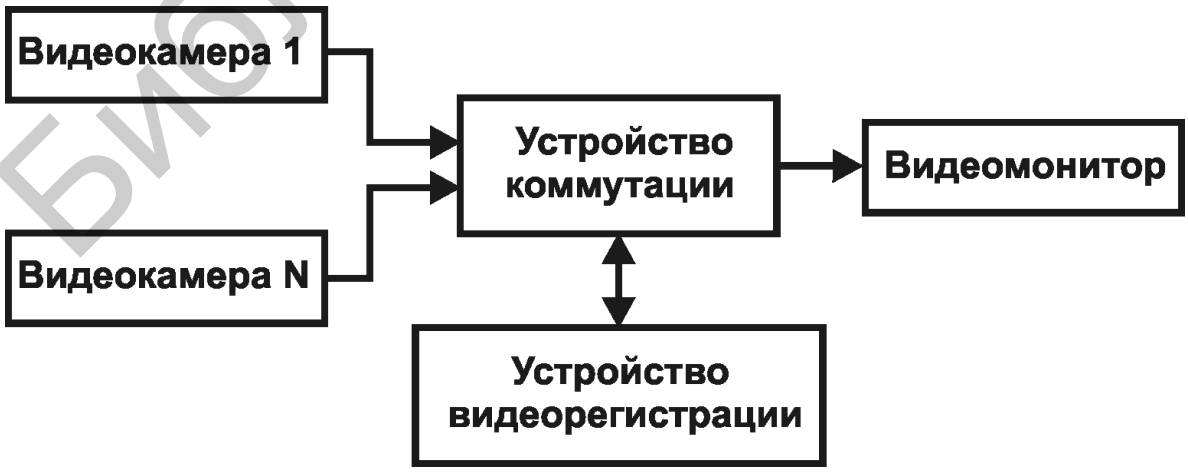


Рис. 9.1. Упрощенная схема системы видеонаблюдения

Состав изучаемой системы видеонаблюдения (рис. 9.2):

1) персональный компьютер;

2) цифровой видеорегистратор (DVR) NVB-025/4A (Novus, Польша);

3) беспроводная система аудио- и видеонаблюдения W413C.

Состав беспроводной системы аудио- и видеонаблюдения 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.).

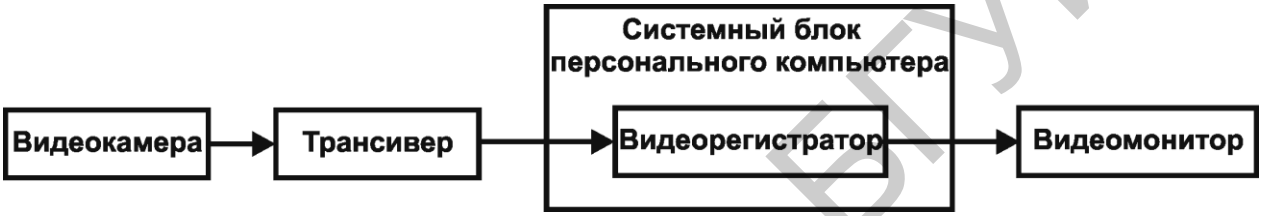


Рис. 9.2. Упрощенная схема изучаемой системы видеонаблюдения

Система охранного телевидения выполнена на базе персонального компьютера с платой цифрового видеорегистратора NVB-025/4A (рис. 9.3, табл. 9.1).

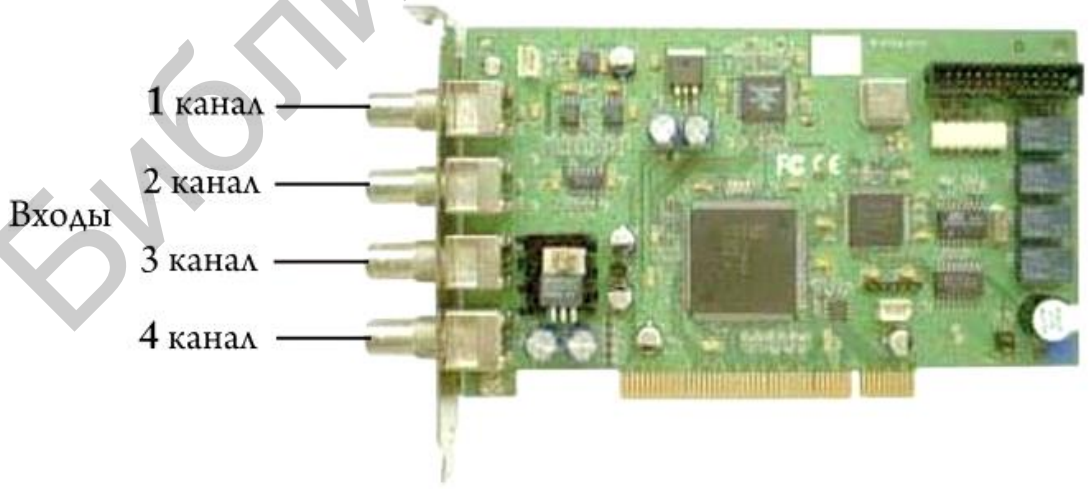


Рис. 9.3. Внешний вид платы цифрового видеорегистратора (DVR) NVB-025/4A

Таблица 9.1

Основные технические характеристики цифрового видеорегистратора NVB-025/4A

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

Рассмотрим 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 четыре 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 включает 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 аудио- и видеонаблюдения W413C (табл. 9.2) предназначена для эфирной передачи аудио- и видеосигналов на частоте 2,4 ГГц и имеет защиту от интерференции частоты 900 МГц.

Таблица 9.2

Основные технические характеристики беспроводной системы аудио- и видеонаблюдения W413C

Характеристика	Описание
1	2
Разрешение видеокамер, пикселей	628×628 (PAL), 510×429 (NTSC)
Разрешение по горизонтали, ТВЛ	380

Окончание табл. 9.2

1	2
Выходная мощность видеокамеры, мВт	10
Чувствительность приемника, дБ	–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, шт.	4
Настройка частоты	Автоматическая

Внешний вид аппаратуры беспроводной системы аудио- и видеонаблюдения W413C и назначение органов ее управления

На рис. 9.4 представлен внешний вид адаптеров для трансивера и видеокамер, на рис. 9.5 – внешний вид и расположение органов управления трансивера, на рис. 9.6 – внешний вид видеокамеры.

а *б*

Рис. 9.4. Внешний вид адаптеров для трансивера (*а*) и видеокамер (*б*)

а

б *в*

Рис. 9.5. Внешний вид и расположение органов управления трансивера (*а*), вариант вертикального (*б*) и вертикального с поворотом на 90° (*в*) размещения антенны трансивера:

1 – выход аудио (правый канал); 2 – выход аудио (левый канал); 3 – выход видео; 4 – разъем источника питания; 5 – антенна; 6 – ИК-приемник сигналов пульта ДУ; 7 – кнопка управления переключением видеокамер; 8 – пульт дистанционного управления

Рис. 9.6. Внешний вид видеокамеры:

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

Порядок работы с системой охранного телевидения:

1. Выключить персональный компьютер.

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

3. Соединить кабелем выход «видео» трансивера (см. рис. 9.5) с одним из видеовходом DVR (например, первый канал) (см. рис. 9.3).

4. Антенну трансивера поднять в вертикальное положение.

5. Подключить блок питания (12 В) к трансиверу (см. рис. 9.4, *а*).

6. Позиционировать видеокамеры в помещении.

7. Подключить блок питания (8 В) к видеокамерам (рис. 9.4, *б*).

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

9. Включить персональный компьютер.

Выключение оборудования выполняется в обратной последовательности.

9.2. Лабораторное задание

В ходе выполнения лабораторной работы необходимо получить практические навыки по настройке и технической эксплуатации системы охранного телевидения. Для этого:

1. Собрать систему охранного телевидения.

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

3. Запустить программу конфигурирования DVR – DVR Settings.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. Установить минимально возможное разрешение для видеокамер.

7.6. Настроить степень сжатия видеопотока по своему усмотрению.

7.7. Включить уведомление о потери видеосигнала.

7.8. Настроить детектор движения по своему усмотрению.

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

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

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

7.12. 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:/361402) и просмотреть его (DVR AVI Viewer.exe).

14. Сохранить отдельные три кадра записанного видеопотока (директория для сохранения E:/номер группы, например E:/361402) 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.

9.3. Содержание отчета

Отчет по лабораторной работе №9 должен содержать:

1. Цель работы.

2. Таблицу результатов (см. ниже).

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

4. Вывод по работе.

5. Ответы на контрольные вопросы.

9.4. Контрольные вопросы

1. Каково назначение цифрового видеорегистратора?

2. Что такое водяной знак для изображения?

3. Каково назначение детектора движения?

4. Каково назначение трансивера в составе изучаемой системы охранного телевидения?

5. К чему приведет увеличение разрешения видеоизображения?

ЛАБОРАТОРНАЯ РАБОТА №10
ИЗУЧЕНИЕ СИСТЕМ ОБНАРУЖЕНИЯ СКРЫТЫХ ВИДЕОКАМЕР

Цель работы: изучить разновидности и особенности функционирования систем обнаружения скрытых видеокамер; получить практические навыки по работе с такими системами и по оформлению протокола проведения специальных проверок.

10.1. Теоретическая часть

Специальная проверка помещения (объекта информатизации) проводится с целью обнаружения в нем возможных специальных технических средств негласного получения информации. Не стоит путать названный процесс со специальным исследованием помещения (объекта информатизации), выполняемым с целью выявления технических каналов утечки защищаемой информации в помещении и оценки соответствия мероприятий по защите информации требованиям нормативных и правовых документов в области безопасности информации.

В зависимости от целей, задач и используемых средств можно выделить следующие виды специальных проверок:

– проверка радиоэлектронной аппаратуры, устанавливаемой в помещении;

– проверка помещения по предмет наличия в нем закладных устройств;

– радиомониторинг помещения;

– проверка помещения на предмет наличия в нем скрытых видеокамер;

– визуальный осмотр и специальная проверка новых предметов (подарков, предметов интерьера, бытовых приборов и т. п.) и мебели, размещаемых или устанавливаемых в помещении;

– комплексная проверка помещения.

Периодичность и виды специальных проверок помещения зависят от его категории и порядка допуска в него посторонних лиц.

Рассмотрим более подробно особенности реализации способов обнаружения скрытых видеокамер в помещениях.

Обнаружение скрытых видеокамер в помещениях

Выделяют четыре способа обнаружения скрытых видеокамер в помещениях:

1) визуальный осмотр;

2) способ, основанный на нелинейных эффектах в полупроводниках;

3) способ, основанный на оптическом эффекте;

4) способ, основанный на регистрации параметров побочного электромагнитного излучения скрытых видеокамер, находящихся в активном состоянии.

Для реализации первого способа обнаружения не требуется использование специальных технических средств. Для реализации второго способа целесообразно применение нелинейных локаторов, третьего и четвертого – обнаружителей скрытых видеокамер.

Обнаружители скрытых видеокамер, основанные на оптическом эффекте

С использованием рассматриваемых обнаружителей можно локализовывать как проводные, так и беспроводные видеокамеры, находящиеся в активном или пассивном состоянии. Диаметр объектива таких видеокамер должен составлять более 1 мм. Функционирование обнаружителей рассматриваемого типа основано на оптическом эффекте световозвращения или так называемого «обратного блика» линзы, входящей в состав объектива скрытой видеокамеры.

В состав рассматриваемых обнаружителей входят следующие элементы:

– корпус;

– объектив;

– красные светодиоды, общая мощность которых на сегодняшний день может составлять 280 кд (расположены вокруг объектива);

– токоограничивающие резисторы, обеспечивающие длительную бесперебойную работу светодиодов;

– зеленые светодиоды в качестве дополнительной подсветки, с помощью которой может быть увеличена вероятность обнаружения скрытых видеокамер в ближней зоне (как правило, вмонтированы в корпус);

– окуляр(-ы);

– кнопка включения/выключения и переключения режимов работы (изменения частоты мерцания красных светодиодов).

На рис. 10.1 представлен внешний вид одного из используемых в настоящее время обнаружителей скрытых видеокамер, основанных на оптическом эффекте.

Рис. 10.1. Внешний вид обнаружителя скрытых видеокамер, основанного на оптическом эффекте, и расположение на нем основных элементов

Задача оператора, который проводит специальную проверку помещения с их применением, заключается в том, чтобы направлять объектив обнаружителя в места потенциального расположения скрытых видеокамер и анализировать элементы изображения, получаемого в результате приема объективом излучения красных светодиодов, отраженного от мест потенциального расположения скрытых видеокамер (рис. 10.2).

а *б*

Рис. 10.2. Потенциально возможные места установки скрытых видеокамер (*а*) и примеры изображений этих мест, полученных с помощью обнаружителей скрытых видеокамер, основанных на оптическом эффекте (*б*)

Просмотр такого изображения выполняется через окуляры. О наличии видеокамеры в анализируемой области помещения можно судить в случае, если на получаемом изображении этой области удалось зарегистрировать мерцающую точку. При этом частота ее мерцания должна изменяться после изменения режима работы обнаружителя.

Дальность обнаружения скрытых видеокамер с использованием рассматриваемых устройств достигает на сегодняшний день 20 м. В случае если скрытая видеокамера вмонтирована в картину, написанную масляными красками, ее обнаружение с помощью рассматриваемых устройств представляется проблематичным, т. к. поверхность таких картин является источником так называемых пассивных помех.

Обнаружители скрытых видеокамер, основанные на регистрации параметров побочного электромагнитного излучения

В большинстве скрытых видеокамер в качестве фотоприемника (устройства для трансформации светового сигнала в электрический) используется ПЗС-матрица (прибор с зарядовой связью). Управление ею выполняется процессором, который затем формирует видеосигнал. В состав процессора входит осциллятор, являющийся источником побочного электромагнитного излучения, спектр которого представляет собой совокупность гармоник. Эти гармоники кратны основной частоте побочного электромагнитного излучения осциллятора. Некоторые из них транслируются на расстояния порядка десятков метров от корпуса видеокамеры.

Обнаружители видеокамер рассматриваемого типа предназначены для регистрации параметров таких гармоник и сравнения их величин с эталонными, сведения о которых занесены в их память. Обнаружители функционируют согласно следующему алгоритму:

1. Прием побочного электромагнитного излучения (если амплитуда этого излучения превышает чувствительность приемника обнаружителя).

2. Регистрация частоты принятого излучения (значение основной частоты побочного электромагнитного излучения осциллятора видеокамеры может колебаться в узком интервале, в связи с этим обнаружитель «разбивает» полосу спектра принятого излучения на небольшие фрагменты, после чего для каждого из этих фрагментов выполняет регистрацию частоты, на которой амплитуда принятого излучения максимальна).

3. Принятие решения о том, является ли зарегистрированная частота частотой осциллятора видеокамеры или случайной помехой.

Локализация камеры выполняется путем анализа отображаемого на дисплее значения амплитуды принятого излучения операторами в процессе изменения местоположения обнаружителя в помещении, в котором проводится специальная проверка. В большинстве случаев чем выше амплитуды принятого излучения, тем ближе расположен обнаружитель рассматриваемого типа к видеокамере.

Выделяют две группы обнаружителей в зависимости от того, каким образом в них налажен процесс отображения амплитуды принятого излучения:

1) обнаружители, на дисплее которых отображается интегральное значение амплитуд гармоник спектра принятого сигнала;

2) обнаружители, на дисплее которых отображается значение максимальной амплитуды гармоники спектра принятого сигнала.

Использование обнаружителей второй группы является более предпочтительным, т. к. нередко несколько гармоник спектра принятого излучения оказываются в так называемой «мертвой зоне», что обусловлено явлением интерференции электромагнитного излучения видеокамеры и иных радиоэлектронных устройств, располагаемых вблизи нее. Это приведет к снижению интегрального значения амплитуд гармоник спектра принятого сигнала и затруднит реализации процесса локализации видеокамеры в помещении, в котором проводится проверка.

Дальность обнаружения скрытых видеокамер рассматриваемыми устройствами составляет от нескольких единиц до нескольких десятков метров и зави-

сит в основном от типа камеры. Время поиска в большей степени зависит от количества типов видеокамер, сведения о параметрах побочного электромагнитного излучения которых внесены в память обнаружителя и, как правило, в настоящее время не превышает 5 мин.

С использованием современных обнаружителей рассматриваемого типа можно проводить скрытый поиск видеокамер благодаря тому, что они оснащены световой, звуковой и вибрационной индикацией, а также в ряде случаев скрытой антенной. Однако стоит отметить, что прилегание антенны к телу человека в значительной степени снижает его чувствительность, поэтому рациональнее проводить поиск, держа обнаружитель на вытянутой руке в открытом пространстве. В некоторых обнаружителях рассматриваемого типа предусмотрена функция постоянного мониторинга электромагнитной обстановки в помещении и отправки данных о подозрительном излучении на удаленную ПЭВМ.

Оформление результатов проведения специальной проверки помещения

Результаты проведения специальной проверки помещения описываются в протоколе. Примерное содержание протокола проведения специальной проверки помещения на предмет наличия в нем скрытых видеокамер следующее:

1. Дата проведения специальной проверки.

2. Сведения о лицах, выполнивших специальную проверку.

3. Цель проведения специальной проверки.

4. Схема помещения, в котором проводилась специальная проверка.

5. Объекты помещения, подлежавшие проверке.

6. Методы проведения специальной проверки.

7. Параметры спектрограммы зарегистрированных сигналов скрытых видеокамер (при их наличии).

8. Результаты локализации скрытых видеокамер (для представления таких результатов используется план помещения, в котором проводилась специальная проверка).

10.2. Лабораторное задание

В ходе выполнения лабораторного задания необходимо:

1. Ознакомиться с руководством по эксплуатации обнаружителя скрытых видеокамер SEL SP-102 «Аркам». Ответить на вопросы преподавателя по содержанию указанного руководства.

2. С помощью обнаружителя «Аркам» выполнить специальную проверку помещения на предмет наличия в нем скрытых видеокамер.

10.3. Содержание отчета

Отчет по лабораторной работе №10 должен содержать:

1. Протокол с результатами проведения специальной проверки.

2. Ответы на контрольные вопросы.

10.4. Контрольные вопросы

1. Что такое специальная проверка помещений?

2. Какие этапы включает в себя процесс специальной проверки помещений?

3. Какие выделяют разновидности способов обнаружения скрытых видеокамер? Проанализируйте эти способы на предмет их достоинств и недостатков.

4. На каких физических принципах основывается функционирование систем обнаружения скрытых видеокамер?

5. В каких единицах измерения оценивается величина чувствительности приемников систем обнаружения скрытых видеокамер? Каков физический смысл этого параметра?

ЛАБОРАТОРНАЯ РАБОТА №11
ОЦЕНКА КАЧЕСТВА ИЗОБРАЖЕНИЯ ВИДЕОМОНИТОРОВ

Цель работы: получить практические навыки по применению универсальных электронных испытательных таблиц и настройке видеомониторов с их использованием.

11.1. Теоретическая часть

Если качество видеомонитора не эквивалентно качеству видеокамеры (или хуже), то общее качество видеосистемы будет снижено. Для оценки качества изображения видеомонитров наиболее широко используются специальные универсальные электронные испытательные таблицы (УЭИТ) (рис. 11.1).

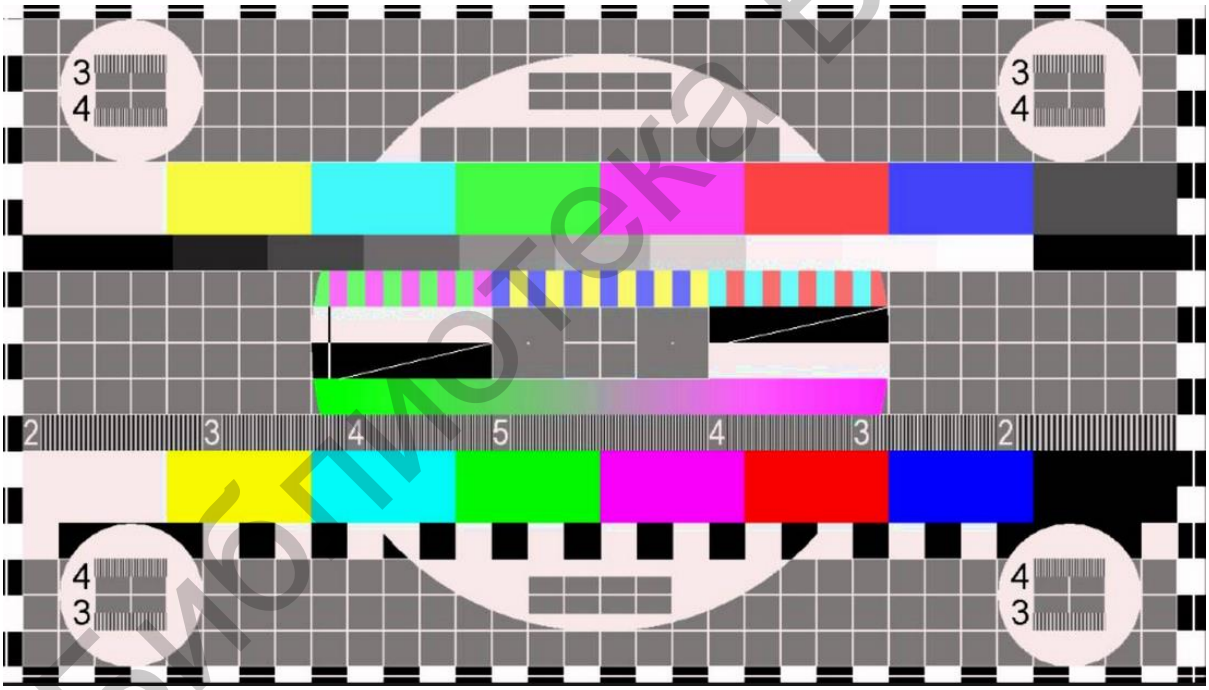


Рис. 11.1. Внешний вид УЭИТ 16:9

В табл. 11.1 изложены наименования элементов УЭИТ и описание их назначения.

Таблица 11.1

Описание назначения элементов УЭИТ

№ п/п	Наименование элемента УЭИТ	Номер строки УЭИТ, где расположен элемент	Назначение элемента УЭИТ
1	2	3	4
1	Сетчатое поле (фон таблицы)	–	Настройка сведения лучей
2	Окантовка (реперные (опорные) метки)	1	Установка размера изображения
3	Малые круги	2…5	Контроль геометрических искажений растра; оценка разрешающей способности
4	Цветные полосы насыщенностью 75 %	6, 7	Контроль цветопередачи
5	Серая шкала	8	Установка яркости, контрастности, баланса белого и уровня черного
6	Контрастные цветные полосы	9	Регулировка четкости цветовых переходов
7	Наклонные полосы	10, 11	Контроль точности чересстрочной развертки
8	Плавный цветовой переход	12	Проверка линейности канала цветности
9	Вертикальные штрихи	13	Оценка разрешающей способности

Окончание табл. 11.1

1	2	3	4
10	Цветные полосы насыщенностью 100 %	14, 15	Контроль цветопередачи
11	Чередующиеся черные и белые квадраты	16	Оценка АЧХ-видеотракта по всем каналам
12	Малые круги	17…19	Контроль геометрических искажений растра; оценка разрешающей способности

Требования к элементам УЭИТ изложены в ГОСТ 14872–82 «Таблицы испытательные оптические телевизионные».

Рассмотрим параметры и свойства изображения, которые могут быть определены с использованием УЭИТ:

1. Размер изображения. Размер изображения по вертикали и горизонтали на экране определяется расстоянием между верхними и нижними, левыми и правыми соответственно реперным линиям, которые должны быть совмещены с краями обрамления монитора. Точность совмещения можно оценить по квадратам и кругам в составе таблицы. Размер изображения на экране на 10…15 % меньше реального размера.

2. Геометрические искажения. Они обусловлены нелинейностью сигналов, формируемых генераторами строчной и кадровой разверток. Оценить рассматриваемый параметр можно с использованием малых кругов УЭИТ или квадратов. При наличии искажений указанные элементы будут принимать форму эллипса и прямоугольника (реже – параллелограмма) соответственно. Для количественной оценки искажения (расчета коэффициента искажения изображения в процентах) необходимо выполнить следующее:

– провести измерение величин сторон одного из искаженных квадратов;

– рассчитать отношение измеренных величин малой и большой сторон;

– отнять от единицы величину рассчитанного отношения;

– умножить результат вычитания на 100 %.

3. Разрешающая способность изображения. Оценивается с использованием вертикальных штрихов, расположенных в строке 13 УЭИТ. Эти штрихи сформированы посредством пачек синусоидальных сигналов частотой 2, 3, 4 и 5 МГц и соответствуют разрешающей способности, равной 220, 330, 440 и 550 линий (в центре расположен участок, соответствующий наибольшей частоте).

4. Наличие побочного электромагнитного излучения. Оценивается с использованием одиночных штрихов, расположенных под полосами, размещенными в строках 10 и 11 УЭИТ. При наличии побочного электромагнитного излучения, воздействующего на интерфейсный кабель видеомонитора, будет наблюдаться смещение этих штрихов. Если измерить величину этого смещения, то можно определить частоту побочного электромагнитного излучения.

5. Правильность передачи цвета изображения. Для оценки названной характеристики используются два ряда цветных прямоугольников, расположенных в строках 6, 7, 14, 15 УЭИТ. На прямоугольниках, расположенных в строках 6, 7, насыщенность цвета должна быть ~ 75 %, а в строках 14, 15 – ~ 100 %. Неправильная цветопередача может быть обусловлена расстройкой схемы матрицирования и нарушением цветовой синхронизации.

11.2. Лабораторное задание

В ходе выполнения лабораторного задания необходимо:

1. Среди УЭИТ, представленных в файлах UEMT1.jpg, UEMT2.jpg, UEMT3.jpg, UEMT4.jpg, выбрать ту, которая соответствует требованиям ГОСТ 14872–82. Обосновать, почему оставшиеся невыбранными таблицы не соответствуют требованиям ГОСТ 14872–82.

2. Определить размер изображения.

3. Оценить наличие побочного электромагнитного излучения (ответ обосновать).

4. Рассчитать размеры элемента, предназначенного для проверки размаха видеосигнала и искажений.

5. Оценить величину нелинейности изображения.

6. Оценить разрешающую способность изображения.

7. Провести настройку изображения видеомонитора с использованием выбранной таблицы.

11.3. Содержание отчета

Отчет по лабораторной работе №11 должен содержать:

1. Цель работы.

2. Обоснование выбора УЭИТ.

3. Значения параметров УЭИТ и видеомонитора.

4. Описание процесса настройки.

5. Выводы по работе.

6. Ответы на контрольные вопросы.

11.4. Контрольные вопросы

1. Что такое УЭИТ?

2. Что представляют собой элементы УЭИТ?

3. С помощью каких элементов УЭИТ может быть оценена разрешающая способность видеомонитора?

4. Каким образом с помощью УЭИТ можно определить коэффициент искажения изображения?

5. Как с использованием УЭИТ определить частоту побочного электромагнитного излучения, воздействующего на интерфейсный кабель видеомонитора?

ЛАБОРАТОРНАЯ РАБОТА №12
ТЕПЛОВИЗИОННЫЕ СРЕДСТВА НАБЛЮДЕНИЯ

Цель работы: изучить метод теплового неразрушающего контроля, основные характеристики тепловизоров; получить практические навыки по работе с тепловизором и обработке термограмм.

12.1. Теоретическая часть

Любой объект является источником электромагнитного излучения инфракрасного (ИК) диапазона (так называемого «теплового излучения»), интенсивность которого зависит от температуры этого объекта. Так как ИК-излучение характеризуется низкой энергией, то оно не может быть зарегистрировано глазом человека. В связи с этим для указанной цели разработаны и применяются тепловизоры – пассивные оптоэлектронные приборы, преобразующие ИК-излучение в электрический сигнал с дальнейшими его усилением, обработкой и преобразованием в видимое изображение. Обобщенная структурная схема тепловизора представлена на рис. 12.1.

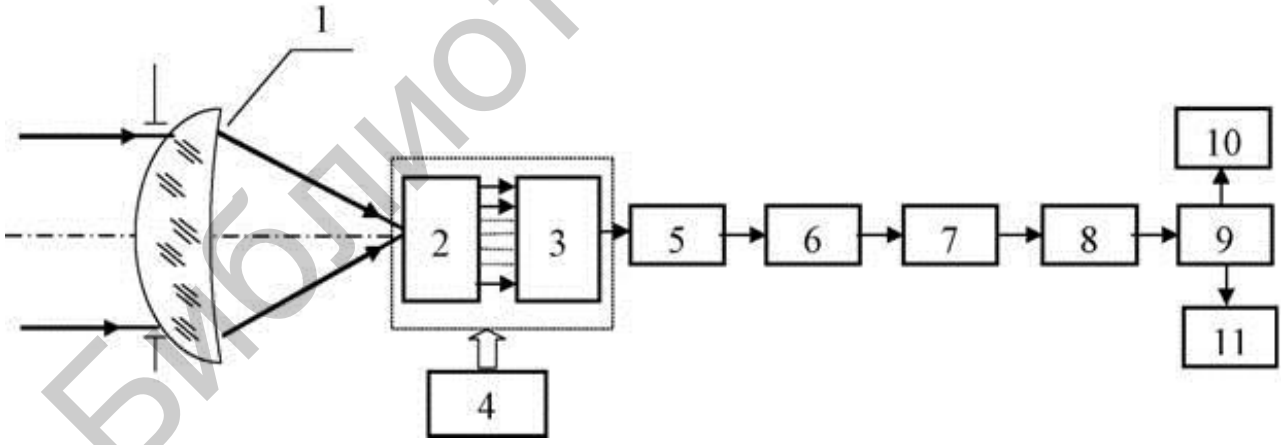


Рис. 12.1. Обобщенная структурная схема тепловизора:
1 – оптическая система; 2 – фокальная матрица с предусилителями; 3 – мультиплексор; 4 – система охлаждения; 5 – корректор неоднородности характеристик чувствительных элементов; 6 – аналого-цифровой преобразователь (АЦП); 7 – цифровой корректор неоднородности; 8 – корректор неработающих ячеек; 9 – формирователь изображения; 10 – дисплей; 11 – выход

Оптическая система 1 предназначена для приема ИК-излучения, которое далее поступает на фокальную матрицу 2, характеризующуюся избирательной чувствительностью к излучению определенного диапазона длин волн. На выходе матрицы формируется электрический сигнал, который подается на мультиплексор 3. Система охлаждения 4 используется для обеспечения высокого отношения сигнал/шум. В них может применяться жидкий азот (температура кипения – минус 195,7 °С) или элементы Пельтье (термоэлектрические преобразователи, которые охлаждаются при протекании по ним электрического тока). Корректор неоднородности характеристик чувствительных элементов 5 способствует обеспечению равномерности АЧХ-тепловизора. АЦП 6 преобразует сигнал из аналоговой формы в цифровую. Цифровой корректор неоднородности 7 и корректор неработающих ячеек 8 применяются для улучшения качества изображения. С использованием формирователя изображения 9 изображение выводится на дисплей 10. Выбор спектрального диапазона для обнаружения объектов реализуется с применением закона смещения Вина: $\lambda_{max} = \frac{2899}{T}$, где λ_{max} – длина волны с максимальной интенсивностью излучения; Т – температура.

Условия, которые должны выполняться для того, чтобы объекты были обнаружены с помощью теповизора, следующие:

1) наличие температурного контраста между объектом и фоном;

2) минимальная площадь объекта – не менее размера одного пикселя матрицы тепловизора (рис. 12.2, 12.3).

Корректно Некорректно Некорректно

Рис. 12.2. Схематичное изображение соотношения минимального размера обнаруживаемого объекта (изображен в виде пятна) с размером одного пикселя матрицы тепловизора

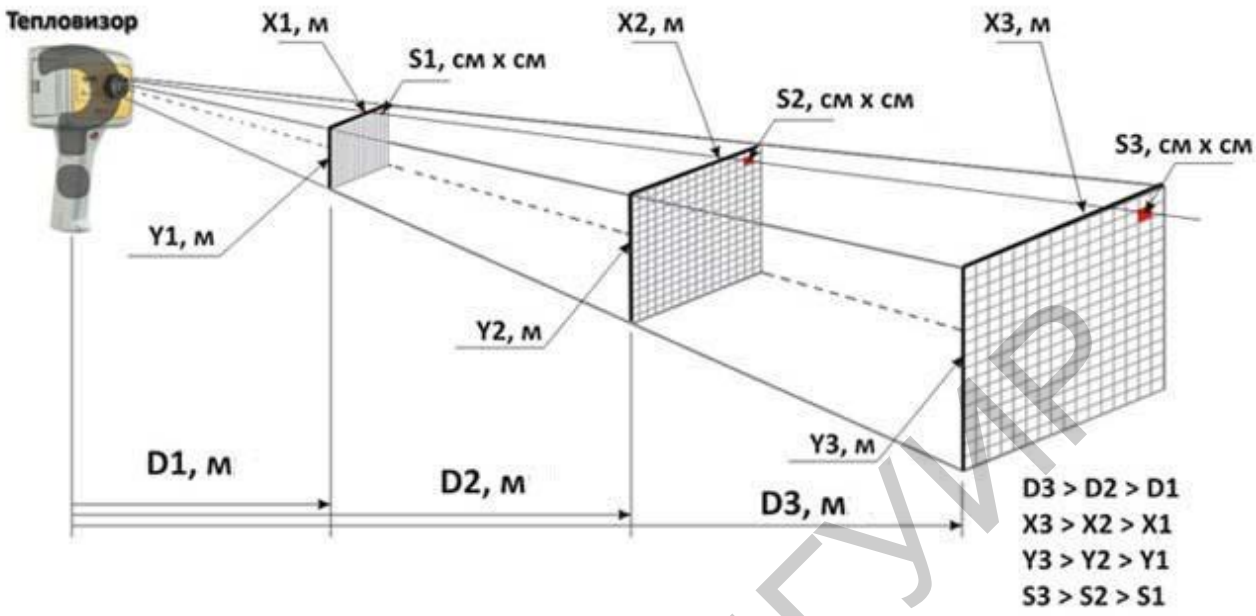


Рис. 12.3. Схематичное изображение изменения расстояния от тепловизора до объекта известной площади, с которого его возможно обнаружить: D1, D2, D3 – расстояние от тепловизора до объекта; X1, X2, X3 – ширина зоны обзора по горизонтали; Y1, Y2, Y3 – ширина зоны обзора по вертикали; S1, S2, S3 – минимальный размер объекта, наблюдаемый на заданном расстоянии

12.2. Лабораторное задание

Работа с тепловизором должна выполняться в соответствии с руководством по его эксплуатации. Запрещается:

– направлять тепловизионную камеру на источники с высокоинтенсивным излучением, такие как солнце, CO_2-лазер, на установку дуговой сварки;

– разбирать тепловизионную камеру;

– прикасаться к оптическим линзам объектива камеры;

– направлять лазерный указатель на биологические объекты.

При выполнении лабораторного задания необходимо:

1. Измерить линейные размеры ростовой фигуры человека (рост и максимальную ширину туловища), который стоит лицом и боком к наблюдателю. В данном случае ростовая фигура человека представляется в виде примитива, ко-

торый имеет форму прямоугольника, т. е. фигура человека должна вписываться в прямоугольник со следующими параметрами:

– высота прямоугольника – рост человека;

– ширина прямоугольника – максимальная ширина туловища человека.

2. Определить максимальное значение расстояния (с точностью до 1 м), с которого возможно обнаружение вышеуказанного объекта, стоящего лицом и боком к наблюдателю.

3. Включить тепловизор.

4. Выполнить обнаружение объекта:

а) фигура человека в полный рост, стоящего лицом к наблюдателю;

б) фигура человека в полный рост, стоящего боком к наблюдателю.

Расстояние, с которого выполняется обнаружение объекта, должно обеспечивать его отображение на дисплее тепловизора в полный рост и занимать наибольшую площадь дисплея тепловизора. Записать две термограммы.

5. Просматривая на экране тепловизора записанные термограммы, обнаружить поверхности объекта, которые имеют наибольший тепловой контраст по отношению к фону.

6. Выключить тепловизор.

7. Для одной из обнаруженных поверхностей объекта (выбирается в соответствие с заданием преподавателя) выполнить измерение ее линейных размеров (высота, ширина).

8. Определить максимальное расстояние (с точностью до 1 м), с которого возможно обнаружение вышеуказанной поверхности объекта.

9. Включить тепловизор.

10. С помощью программы Guide IrAnalyser переписать из flash-памяти тепловизора термограммы на персональный компьютер (ПК) для дальнейшей обработки.

11. Выключить тепловизор.

12. Открыть термограмму, где заданная поверхность тела человека имеет наибольшую площадь с помощью программы Guide IrAnalyser.

13. Для этой поверхности определить максимальную, минимальную и среднюю значения температур (используется кнопка «Многоугольник»).

14. Через точку с максимальным значением температуры провести линию и построить термопрофиль (используются кнопки «Добавить линию» и «Построить термопрофиль»). Сравнить максимальные значения температуры, наблюдаемые на термопрофиле и рассчитанные с помощью программы Guide IrAnalyser.

15. С помощью программы Guide IrAnalyser рассчитать разность температур между заданной поверхностью тела человека и фоном.

16. С помощью программы Guide IrAnalyser рассчитать среднее значение температуры фона.

17. Используя рассчитанные с помощью программы Guide IrAnalyser средние значения температур фона и поверхности объекта, выполнить расчет теплового контраста.

12.3. Содержание отчета

Отчет по лабораторной работе №12 должен содержать:

1. Цель работы.

2. Параметры ростовой фигуры человека, стоящего лицом и боком к наблюдателю.

3. Максимальное значение расстояния (с точностью до 1 м), с которого возможно обнаружение вышеуказанного объекта, стоящего лицом и боком к наблюдателю.

4. Наименования поверхностей объекта, которые имеют наибольший тепловой контраст по отношению к фону. Наименование заданной преподавателем поверхности объекта.

5. Значения линейных размеров поверхности (высота, ширина) объекта.

6. Максимальное значение расстояния (с точностью до 1 м), с которого возможно обнаружение вышеуказанной поверхности объекта.

7. Значения максимальной, минимальной и средней температур для поверхности объекта, указанной в п. 4.

8. Значения разности температур между контрастирующей поверхностью объекта и фоном.

9. Среднее значение температуры фона.

10. Результаты расчета теплового контраста.

11. Вывод по работе.

12. Ответы на контрольные вопросы.

12.4. Контрольные вопросы

1. Для каких целей используются тепловизоры и в каких спектральных диапазонах они способны регистрировать электромагнитное излучение?

2. Какие способы охлаждения матриц тепловизионной техники используются на практике?

3. Какие условия должны быть выполнены для обнаружения объекта с помощью тепловизионной техники?

4. Что такое поле зрения тепловизора?

5. Что такое пространственное разрешение тепловизора?

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Технические средства и методы защиты информации : учеб. для вузов / А. П. Зайцев [и др.] ; под. ред. А. П. Зайцева, А. А. Шелупанова. – М. : ООО «Издательство Машиностроение», 2009. – 508 с.

2. Аминов, В. П. Блокировка акустоэлектрических преобразователей в электронных технических средствах и системах общего применения / В. П. Аминов. – М. : Гелиос-АРВ, 2010. – 224 с.

3. Михайлов, В. Г. Измерение параметров речи / В. Г. Михайлов, Л. В. Златоустова ; под ред. М. А. Сапожкова. – М. : Радио и связь, 1987. – 168 с.

4. Ворона, В. А. Технические средства наблюдения в охране объектов / В. А. Ворона. – М. : Горячая линия – Телеком, 2011. – 188 с.

5. Пескин, А. Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации / А. Е. Пескин. – М. : Горячая линия – Телеком, 2013. – 256 с.

6. Гвоздек, М. Справочник по технике для видеонаблюдения. Планирование, проектирование, монтаж / М. Гвоздек. – М. : Техносфера, 2010. – 544 с.

7. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. – М. : Горячая линия – Телеком, 2014. – 594 с.

8. Руководство по составлению эксплуатационных требований к системам видеонаблюдения. Версия 5.0. М. : Security focus, 2013. – 80 с.

9. Беляев, Б. И. Методы и средства защиты объектов связи от несанкционированного доступа : курсовое проектирование / Б. И. Беляев. – Минск : БГУИР, 2011. – 98 с.

10. Бузов, Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г. А. Бузов. – М. : Горячая линия – Телеком, 2010. – 240 с.

11. Лыньков, Л. М. Активные средства защиты электронно-вычислительных машин / Л. М. Лыньков. – Минск : БГУИР, 2011. – 51 с.

12. ГОСТ 14872–82 «Таблицы испытательные оптические телевизионные».

Св. план 2016, поз. 53

Учебное издание

Лыньков Леонид Михайлович
Бойправ Ольга Владимировна
Рощупкин Яков Викторович
Борботько Тимофей Валентинович

ЗАЩИТА ОБЪЕКТОВ СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *Е. С. Юрец*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *А. А. Лущикова, В. М. Задоля*

Подписано в печать 11.09.2017. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 6,63. Уч.-изд. л. 6,5. Тираж 50 экз. Заказ 395.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014
ЛП №02330/264 от 14.04.2014.
220013, г. Минск, П. Бровки, 6