

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине
«Фундаментальные проблемы информационной
безопасности на современном этапе»
для студентов направления подготовки
10.04.01 Информационная безопасность

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Практическое занятие № 1

Тема: *«Изучение основных положений «Стратегии национальной безопасности РФ 2015 г.»*

В результате настоящего занятия и последующей самостоятельной работы студенты **должны:**

знать: требований Стратегии национальной безопасности РФ 2015 г. по вопросам обеспечения национальной безопасности РФ в различных сферах жизнедеятельности государства

уметь: применять в своей деятельности основные положения "Стратегии" в области обеспечения информационной безопасности структурных образований РФ

владеть: практическими навыками формальной постановки и решения задачи обеспечения информационной безопасности предприятий различных форм собственности

Формируемые компетенции или их части: ПК-5

Распределение времени занятия

I. Вступительная часть

Проверка наличия студентов - 2 мин.

Проверка готовности студентов к занятию. - 3 мин.

II. Учебные вопросы занятия:

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства. - 35 мин.

2. Угрозы информационному обеспечению государственно политики Российской Федерации. - 50 мин

III. Заключение

Подведение итогов занятия - 3 мин.

Задание студентам для самостоятельной работы - 2 мин.

СОДЕРЖАНИЕ ЗАНЯТИЯ

В процесс изучения программного материала студентам следует особое внимание обратить на следующие вопросы

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства

Определение понятия национальной безопасности.

Виды безопасности и сферы жизнедеятельности личности, общества и государства.

Интересы личности в информационной сфере.

Интересы общества в информационной сфере.

Интересы государства в информационной сфере.

2. Угрозы информационному обеспечению государственной политики Российской Федерации.

Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности.

Угрозы конституционным правам и свободам человека и гражданина в области индивидуальному, групповому и общественному сознанию.

Угрозы конституционным правам и свободам человека и гражданина в области духовному возрождению России.

Угрозы информационному обеспечению государственной политики Российской Федерации.

Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи.

Угрозы обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок.

Угрозы обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Рекомендованная литература

Основная

1. Федеральный государственный образовательный стандарт ВПО по специальности компьютерная безопасность
2. Основы информационной безопасности. Учебное пособие для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М: Горячая линия – Телеком, 2006. – 544 с.: ил.

Интернет ресурсы

1. Конституция РФ
2. Стратегия национальной безопасности РФ до 2020г

Задания для развития и контроля владения компетенциями

1. Дать определение понятию национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Виды защищаемой информации.
4. Основные понятия и общеметодологические принципы теории информационной безопасности.
5. Роль информационной безопасности в обеспечении национальной безопасности государства.
6. Интересы личности в информационной сфере.
7. Интересы общества в информационной сфере.
8. Интересы государства в информационной сфере.
9. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

III. Заключение

Подведение итогов занятия

По результатам собеседования с каждым студентом устанавливается

степень усвоения ими программного материала и выставляется оценка.

Задание студентам для самостоятельной работы

1. Оформить отчет о лабораторной работе в соответствии с требованиями

2. Представить отчет для утверждения и защиты.

Практическое занятие № 2

«Изучение основных положений «Доктрины информационной безопасности РФ 2000 г.»

В результате настоящего занятия и последующей самостоятельной работы студенты **должны:**

знать: цели, задачи, принципы и основные направления обеспечения информационной безопасности государства;

уметь: применять в своей практической деятельности основные термины по проблематике информационной безопасности;

владеть: навыками использования знаниями по вопросам обеспечения структурными образованиями РФ национальных интересов Российской Федерации в информационной сфере

Формируемые компетенции или их части: ПК-5

I. Вступительная часть

Проверка наличия студентов - 2 мин

Проверка готовности студентов к занятию. - 3 мин

II. Учебные вопросы занятия:

1. Виды угроз информационной безопасности Российской Федерации - 45 мин

2. Источники угроз информационной безопасности Российской Федерации - 45 мин

III. Заключение

Подведение итогов занятия - 3 мин.

Задание студентам для самостоятельной работы - 2 мин.

СОДЕРЖАНИЕ ЗАНЯТИЯ

В процесс изучения программного материала студентам следует особое внимание обратить на следующие вопросы

1. Виды угроз информационной безопасности Российской Федерации

Основные понятия и общеметодологические принципы теории информационной безопасности.

Роль информационной безопасности в обеспечении национальной безопасности государства.

Интересы личности в информационной сфере.

Интересы общества в информационной сфере.

Интересы государства в информационной сфере.

Основные составляющие национальных интересов Российской Федерации в информационной сфере.

Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства.

2. Источники угроз информационной безопасности Российской Федерации

Содержание информационного противоборства на межгосударственном уровне

Информационная безопасность и информационное противоборство.

Субъекты информационного противоборства. Цели информационного противоборства.

Составные части и методы информационного противоборства.

Рекомендованная литература

Основная

1. Федеральный государственный образовательный стандарт ВПО по специальности компьютерная безопасность
2. Основы информационной безопасности. Учебное пособие для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М: Горячая линия – Телеком, 2006. – 544 с.: ил.

Интернет ресурсы

1. Конституция РФ
2. Доктрина информационной безопасности РФ

Задания для развития и контроля владения компетенциями

1. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности.
2. Угрозы конституционным правам и свободам человека и гражданина в области индивидуальному, групповому и общественному сознанию.
3. Угрозы конституционным правам и свободам человека и гражданина в области духовному возрождению России.
4. Угрозы информационному обеспечению государственной политики Российской Федерации.
5. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи.
6. Угрозы обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок.
7. Угрозы обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.
8. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

III. Заключение

Подведение итогов занятия

По результатам собеседования с каждым студентом устанавливается степень усвоения ими программного материала и выставляется оценка.

Задание студентам для самостоятельной работы

1. Оформить отчет о лабораторной работе в соответствии с требованиями
2. Представить отчет для утверждения и защиты.

Практическое занятие №3

***«Демонстрация портативных средств защиты информации:
профессионально сканирующего приемника AR3000A,
детектора поля D 006, генератора шума ГШ-1000М»***

В результате настоящего занятия и последующей самостоятельной работы студенты **должны:**

знать: технические характеристик и возможности работы профессионально сканирующего приемника **AR3000A**, детектора поля **D 006**, генератора шума **ГШ-1000М**.

уметь: применять в своей практической деятельности профессионально сканирующий приемник **AR3000A**, детектор поля **D 006**, генератор шума **ГШ-1000М**.

владеть: навыками настройки, регулировки профессионально сканирующий приемник **AR3000A**, детектор поля **D 006**, генератор шума **ГШ-1000М**.

Формируемые компетенции или их части: ПК-5

Распределение времени занятия

I. Вступительная часть

Проверка наличия студентов	- 2 мин
Проверка готовности студентов к занятию.	- 3 мин

II. Учебные вопросы занятия:

1. Профессионально сканирующий приемник AR3000	- 55 мин
2. Детектор поля D 006	
3. Генератора шума ГШ-1000М	- 55 мин
	- 60 мин

III. Заключение

Подведение итогов занятия	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

СОДЕРЖАНИЕ ЗАНЯТИЯ

1. Профессионально сканирующий приемник AR3000A

Теоретическая часть

Сканирующий широкодиапазонный приемник **AR3000A** является сложным устройством, в котором используются последние достижения в электронной технологии и схемотехнике, а также одним из лучших мобильных сканирующих устройств на сегодняшний день.

С помощью **AR3000A** расширяются горизонты восприятия эфира. Диапазон принимаемых частот простирается от **100 кГц** до **2036 МГц** без пропусков. Приемник предлагает самый широкий на сегодняшний день на рынке диапазон частот от длинных, коротких, УКВ и далее вплоть до СВЧ в сочетании с превосходным исполнением и функциональной многосторонностью.

Широкий диапазон приемника **AR3000A** обеспечивает прием сигналов с амплитудной (**AM**), узкополосной (**NFM**) и широкополосной (**WFM**) частотной модуляцией. Кроме указанных типов принимаются сигналы с амплитудной однополосной модуляцией (**SSB**) в режиме приема верхней боковой полосы (**USB**) и нижней боковой полосы (**LSB**), а также телеграфных сигналов (**CW**).

Режим **SSB** специально используется многими службами на коротких волнах (включая любителей, морскую, воздушную службы) для расширения возможности их трансиверов. Его включение в **AR3000A** является положительным моментом.

Высокий уровень исполнения высокочастотной части достигнут благодаря **13 полосовым** фильтрам перед арсенид-галлиевыми усилителями в отличие от других приемников, где больше полагаются на полосовые усилители. Это позволяет иметь высокую чувствительность во всем диапазоне частот в сочетании с широким динамическим диапазоном и отсутствием интермодуляции. По основным параметрам, таким как чувствительность, избирательность и диапазон приема, **AR3000A** находится на одной ступени со значительно более дорогими моделями (например, ICOM IC-R9000). Несомненна надежность конструкции, выполненная на металлическом шасси. Расположение кнопок управления, ручек настройки, размеры жидкокристаллического индикатора – все сделано для удобства управления.

Дискрет перестройки (шаг настройки) выбирается в диапазоне от ультрамалого 50-и герцового шага для **SSB** и **CW** и до 999.95 килогерцового (кратно 50 Гц) для телевизионного диапазона и Band-2. Две кнопки на передней панели:

×10 и **«Slow»(×5)** позволяют соответственно увеличить (в 10 раз) или уменьшить (в 5 раз) шаг простым нажатием, что делает работу

разнообразной и комфортной. Ручка «свободного сканирования» (ручка настройки) создаёт лучшие условия для пользователя, особенно на **SSB**.

Крупный жидкокристаллический индикатор расположен под удобным для наблюдения углом и отражает информацию о частоте, канале памяти, режимах поиска/сканирования, мощности принимаемого сигнала, включении/выключении аттенюатора, перебора каналов памяти и дополнительных функциях. На дисплее отображается время таймера, позволяющего точно определить время перехвата, включать и выключать приемник в установленное время. Для работы в условиях недостаточной освещенности предусмотрена подсветка индикатора.

400 каналов памяти разбиты на 4 банка по 100 каналов в каждом. Каждый канал содержит: частоту, состояние ВЧ-аттенюатора, позволяет зафиксировать частоту или ее отсутствие, шаг перестройки. Первый канал каждого банка может использоваться как канал приоритета и, таким образом, обеспечивается 4 канала приоритета в целом. Вся информация, содержащаяся в памяти, а также информация о диапазонах сканирования поддерживаются внутренним встроенным литиевым источником.

Все четыре банка спроектированы так, что каждый из них можно запрограммировать для работы в любой точке частотного диапазона приемника. Для целей поиска 100 частот можно исключить из прослушивания, чтобы приемник не останавливался на нежелательных или на постоянно присутствующих частотах. Улучшенный программный захват частоты сигнала и различные функции паузы реализованы в режимах поиска, сканирования, приоритета канала, отсюда высокая разносторонность приемника.

Технические характеристики сканирующего приемника **AR3000A** приведены в таблице

Характеристика	Значение			
Диапазон Принимаемых частот	100 кГц – 2036 МГц			
Режимы работы	USB, LSB, CW, AM, NFM, WFM			
Способы набора частоты	Ручной / Ручной поиск / Программный поиск / Вызов канала памяти / Сканирование памяти / приоритетный канал			
Шаг перестройки	Любой кратный 50Гц (от 50Гц до 999.95кГц)			
Схема построения Приемника	Супергетеродин с тройным (на LSB, USB, AM, CW, NMF) и 4-х кратным преобразованием (на WFM) частоты			
Каналы памяти	400 (по 100 в каждом банке памяти)			
Банки поиска	4, программируемых пользователем			
«Закрытые» частоты	по 100 на банк поиска, всего 400			
Длительность паузы	1-60 секунд			
Задержка на частоте в режиме поиска или сканирования	от 1 до 9 секунд			
Число каналов приоритета	4, по одному в каждом банке			
Время прослушивания канала приоритета	от 1 до 19 секунд			
Скорость перестройки по частоте	50 шагов в секунду (типовая – 30 шагов)			
Скорость сканирования	50 каналов / с			
Чувствительность приемника в диапазоне частот: 100 кГц – 2,5 МГц	10 дБ S / N		12 дБ SINAD	
	SSB / CW	AM	NFM	WFM
	1,0 мкВ	3,2 мкВ	-	-

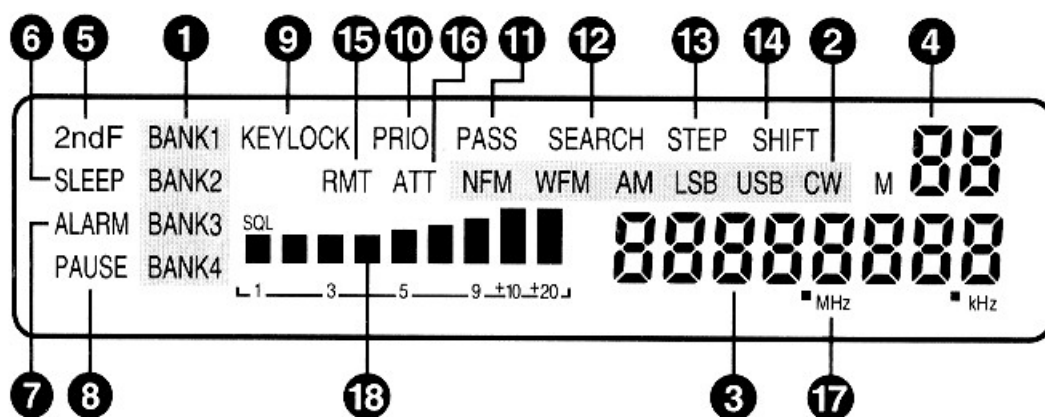
2,5 МГц – 1,8 ГГц	0,25 мкВ	1,0 мкВ	0,35 мкВ	1,0 мкВ
1,8 ГГц – 2,0 ГГц	0,75 мкВ	3,0 мкВ	1,25 мкВ	3,0 мкВ
Избирательность приемника	2,4 кГц /по –6 дБ, 4,5 кГц /по –60 дБ (USB, LSB, CW)			
	12 кГц /по –6 дБ, 15 КГц /по –70 дБ (AM, NFM)			
	180 кГц /по –6 дБ, 800 кГц /по –50 дБ (WFM)			
Подключение антенны	Один байнетный разъем			
Аудио выход	1,2 Вт при коэффициенте нелинейных искажений 10% (4 Ом)			
	0,7 Вт при коэффициенте нелинейных искажений 10% (8 Ом)			
Дисплей	Жидкокристаллический			
Питание памяти	Встроенная литиевая аккумуляторная батарея			
Питание	13,8 В постоянного тока (потребляемый ток 500 мА)			
Размеры	138 мм(ширина)×80 мм(высота)×200 мм(глубина)			
Вес	1,2 кг			

Прибор оборудован энергонезависимой памятью. Вся информация, находящаяся в ней, остается без изменений даже при выключении питания благодаря встроенной литиевой батарее.

Скорость поиска и сканирования максимально возможная - 50 переключений в секунду, хотя типичная - 30 переключений в секунду.

Приемник позволяет осуществлять программируемое сканирование с задержкой до пропадания сигнала и паузой, время которой составляет от 1 до 60 с и задается пользователем.

Порт **RS232C** позволяет осуществлять полное дистанционное управление с компьютера основными функциями приемника, подключаться к большинству компьютеров (с соответствующим программным обеспечением). Контролируемыми параметрами являются: частота, режим приема, шаг настройки, запись/считывание из памяти, уровень сигнала, ВЧ-аттенюатор, выбор банка памяти и т.д. Переключение в режим дистанционного управления производится при помощи переключателя на задней панели прибора: клавиатура/ **RS232C**.



Описание дисплея (управление и функции):

1. <BANK(1,2,3,4)> индикатор банка памяти.
2. <NFM>, <WFM>, <AM>, <LSB>, <USB>, <CW> индикатор режима приема.

3. Индикатор частоты.
4. Индикатор памяти.
5. Индикатор вторичных функций.
6. <SLEEP> индикатор автоматического выключения.
7. <ALARM> индикатор автоматического включения.
8. <PAUSE> индикатор паузы.
9. <KEYLOCK> индикатор отключения клавиатуры.
- 10.<PRIO> индикатор приоритета.
- 11.<PASS> индикатор пропуска частоты.
- 12.<SEARCH> индикатор режима поиска.
- 13.<STEP> индикатор шага.
- 14.<SHIFT> индикатор расстройки.
- 15.<RMT> индикатор режима дистанционного управления.
- 16.<ATT> индикатор вкл/выкл аттенюатора.
17. Индикатор скорости перестройки.
18. Индикатор уровня сигнала.

Практическая часть

Работа с приемником (основные операции):

1.Подсоединить соответствующую антенну к баянному разъему на задней панели.

2.Подсоедините к приемнику нужный источник питания, используя либо данный блок питания, либо 12-ти вольтовой кабель. ***Никогда не подключайте приемник прямо в сеть!***

3.После включения установите уровень громкости в положение «10», ручку бесшумной настройки в положение 12 и убедитесь, что переключатель дистанционного управления в положении (OFF).

4.Включите питание. Убедитесь, что ни один из указанных символов <KEYLOCK>, <RMT>, <PAUSE> не появился на ЖКИ-дисплее при первом включении.

Уберите эти символы с дисплея при их появлении как указано выше. После указанной процедуры приемник готов к вводу частоты и режима приема.

Действия в каждом отдельном режиме приема

Режим ввода

В этом режиме можно выбрать частоту для немедленного прослушивания, ввод частоты произойдет после нажатия кнопки (DIAL). Выбор частоты приема можно осуществить с помощью десятичных кнопок, кнопок (UP/DOWN) или ручки настройки.

Прямой ввод с помощью кнопок

Пример 1.

Ввести частоту “Radio 1” на средних волнах 1089 кГц, режим АМ.

1. Нажать (DIAL).
2. Нажать (MODE).

Нажать (UP/DOWN) или вращать ручку настройки пока не появится <АМ> на дисплее. Для ввода нажать (ENTER).

Помните (ENTER) нажимается для завершения последовательности действий.

3.Нажать (STEP), (9), затем (ENTER).

Т.к. станции на средних волнах расположены через 9 кГц, то в дальнейшем эта установка позволит правильно настраиваться с помощью ручки настройки. Если Вы хотите слушать только частоту 1089 кГц, то можете проигнорировать эти действия.

4.Нажмите (1), (.), (0), (8), (9) затем (ENTER).

Приемник сейчас настроен точно на 1089 кГц, режим АМ. *Всегда нажимайте (.), при вводе мегагерц, например (.), (5), (9),(4), для частоты кГц, заканчивайте последовательность нажатием (ENTER). Нажмите (4), (.), (7), (2), (2) для 4.722 МГц. При ошибке нажмите (ENTER) и повторите набор.

Пример 2

Ввод частоты коммерческого диапазона 466.0 МГц, режим FM.

1.Нажать (DIAL).

2.Нажать (MODE).

Нажать (UP/DOWN) или вращать ручку настройки до появления символа <FM> на ЖКИ-дисплее.

Для ввода нажать (ENTER).

3.Нажать (STEP), (5), затем (ENTER). Установили шаг перестройки диапазона 5 кГц.

4.Нажмите (4), (6), (6), (.), (0) затем (ENTER).

Приемник сейчас настроен точно на 466.0 МГц, режим FM. При ошибке нажмите (ENTER) и повторите набор.

Пример 3

Ввод частоты УКВ диапазона 101.8 МГц, режим FM («Русское радио»)

1. Нажать (DIAL).

2.Нажать (MODE).

Нажать (UP/DOWN) или вращать ручку настройки до появления символа <WFM> на ЖКИ-дисплее.

Для ввода нажать (ENTER).

3.Нажмите (1), (0),(1), (.), (8) затем (ENTER).

Сейчас приемник настроен точно на 88.3 МГц, режим WFM.

2. Детектор поля D 006

Теоретическая часть

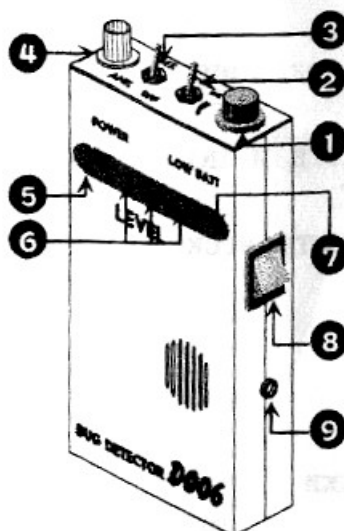
Детектор D 006 предназначен для оперативного обнаружения радиопередающих прослушивающих систем промышленного шпионажа (РС).

Данный прибор является конечным элементом поиска подобных устройств и позволяет в конкретной обстановке выявить и локализовать скрытно установленные РС.

Принцип действия D 006 основан на широкополосном детектировании электрического поля, что дает возможность регистрировать РС независимо от вида модуляции.

Технические характеристики детектора D 006:

Характеристика	Значение
Питание	9В
Потребляемый ток	30 Ма
Габариты D 006	128×63×20(мм)
Диапазон частот	50÷1000(МГц)
Чувствительность (f=110МГц)	0,5мВ
Чувствительность (f=800МГц)	3мВ
Динамический диапазон индикатора	40дБ



Общее описание

1. Выключатель питания и регулятор порога срабатывания
2. Выключатель тонального звукового сигнала
3. Выключатель аттенюатора
4. Разъем для подключения антенны
5. Индикатор включения питания
6. Индикатор уровня электрического поля
7. Индикатор разряда аккумулятора
8. Выключатель системы акустической обратной связи
9. Разъем для подключения зарядного устройства

Радиус обнаружения детектора зависит от излучаемой мощности прослушивающей системы, электромагнитной обстановки в обследуемом помещении и составляет при мощности РС 5мВт порядка 1м.

Возможность включения аттенюатора облегчает работу в условиях сложной электромагнитной обстановки, присущей крупным промышленным центрам, за счет ослабления входного сигнала. Данный режим полезен и в случае точного обнаружения мощных РС.

Наличие системы акустической обратной связи («акустической завязки») позволяет исключить ложные срабатывания детектора на локальные электромагнитные поля и идентифицировать находящееся в помещении РС по характерному звуковому сигналу.

Восьмисегментная логарифмическая светодиодная шкала и тональный звуковой сигнал обеспечивают наглядность и удобство при работе с прибором.

Практическая часть

Порядок работы

1. Установите регулятором (1) положение тах чувствительности. Для этого, находясь на относительном удалении от предполагаемых мест установки РС (например, в свободном от мебели центре комнаты), поворачивайте ручку регулятора вправо до начала загорания второго сегмента шкалы индикатора (6) (выключатель (3) при этом должен находиться в положении «OFF»).

2. В случае, если при максимальном закручении чувствительности детектора (регулятор (1) повернут против часовой стрелки до упора) на индикаторе (6) горит более двух сегментов, что говорит о высоком уровне электромагнитных полей на объекте, включите аттенюатор (выключатель (3) в положении «ATT»). Это позволит Вам работать в данных условиях при соответствующем уменьшении максимальной дальности обнаружения примерно в 2–3 раза.

3. В процессе работы с прибором могут создавать помехи побочные излучения бытовых электроприборов, телевизоры, компьютеры, различные наводки от проводов сети 220В×50Гц. Предварительно изучите характер их действия и особенности распространения.

4. При осмотре объекта проводите антенной прибора вдоль предполагаемых мест установки РС. Увеличение количества одновременно горящих светодиодов индикатора (6) и усиление тона звукового сигнала позволят Вам точно установить их месторасположение.

5. Для уменьшения чувствительности и соответственно повышения точности локализации РС плавно поворачивайте регулятор (1) против часовой стрелки.

Для однозначной идентификации включите акустическую завязку (систему акустической обратной связи) (выключатель (8) в положении «AUD»). На нахождение РС в зоне обнаружения детектора однозначно укажет характерный звуковой тон. В противном случае будет прослушиваться хаотичный шум.

6. Для более точного определения меняйте ориентацию антенны.

Дополнительные рекомендации

1. Некоторые типы РС включают свои радиопередающие блоки только в случае наличия какого-либо звукового шума в помещении. Поэтому перед проведением осмотра включите один из стандартных источников звука: например радиоприемник.

2. Во избежание отключения на время проверки дистанционно управляемых систем не ведите предварительных и сопутствующих разговоров во время осмотра помещения, дающих представление о Вашей деятельности.

3. Детектор эффективен при обнаружении телефонных РС. В качестве передающей антенны используется в основном телефонный провод. Для обнаружения таких устройств проведите следующие действия:

3.1. замерьте уровень излучения в непосредственной близости от телефонного провода при опущенной телефонной трубке;

3.2. поднимите трубку и повторите измерения; увеличение сигнала укажет на наличие подключенной к линии РС.

4. Для зарядки аккумулятора проведите следующие действия:

4.1. подключите в разъем (9) ответную часть зарядного устройства, предварительно выключив детектор;

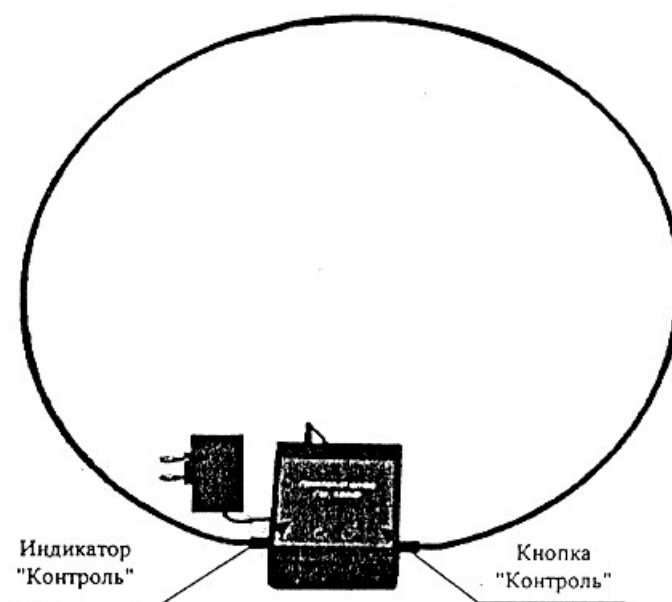
4.2. подключите зарядное устройство к сети 220В; время полной зарядки составляет 14 часов.

!!! Во избежание выхода из строя детектора запрещается использование Д 006 в непосредственной близости от радиопередающих устройств мощностью более 1 Вт.

3. Генератор шума ГШ-1000М

Теоретическая часть

Генератор шума предназначен для маскировки побочных, информативных электромагнитных излучений персональных компьютеров, компьютерных сетей и комплексов на объектах вычислительной техники первой, второй и третьей категорий путем формирования и излучения в окружающее пространство электромагнитного поля шума (ЭМПШ) в диапазоне частот 0,1–1000МГц.



Работа генератора основана на использовании нелинейных свойств транзистора и организации широкополосной обратной связи для генерации широкополосного шумового сигнала и его усиления. Сформированный шумовой сигнал излучается в окружающее пространство. Его интенсивность значительно превышает интенсивность радиоизлучения от средств вычислительной техники, что обеспечивает надежную защиту обрабатываемой ими информации от несанкционированного доступа.

В состав генератора шума входит устройство контроля нормального режима работы генератора.

Если уровень сигнала на выходе генератора превышает заданный уровень, то горит светодиод «Контроль», служащий индикатором нормального режима работы генератора.

Если же уровень сигнала на выходе генератора окажется ниже заданного уровня, что может быть обусловлено как падением уровня выходной мощности генератора, так и изменением характера спектра генерируемого им сигнала, то индикаторный светодиод гаснет и запускается генератор звукового сигнала. Это является признаком нарушения нормального режима работы генератора.

В состав генератора шума входит устройство дистанционного контроля нормального режима работы генератора.

Внешнее контрольное и/или управляющее устройство может быть подключено к коаксиальному разъему DJK-10A, причем положительный контакт – внешний, отрицательный – внутренний. Так как выходным элементом схемы дистанционного контроля является транзисторная оптопара АОТ128А, то значения параметров коммутируемых напряжения и тока не должны превышать максимально допустимых для этой оптопары, а именно, максимально допустимое коммутируемое напряжение не более 50В, максимально допустимый ток нагрузки не более 8мА.

Если уровень сигнала на выходе генератора превышает заданный уровень, то транзистор оптопары открыт и поданное на него напряжение передается в нагрузку.

Если же уровень сигнала на выходе генератора окажется ниже заданного уровня, что может быть обусловлено как падением уровня выходной мощности генератора, так и изменением характера спектра генерируемого им сигнала, то транзистор оптопары закрывается и поданное на него напряжение в нагрузку не передается. Это является признаком нарушения нормального режима работы генератора.

Технические характеристики генератора шума ГШ-1000М:

Частота, МГц	0,1	0,5	1	5	10	30	100	200	300	500	700	1000
Норма по ТУ Еш, дБ.	35	40	40	45	50	50	45	45	45	40	40	35
Результат измерения Еш, дБ.	42	56	64	65	73	65	46	57	46	44	43	37
Норма по ТУ рНш, дБ.	60	55	55	55	50	45	-	-	-	-	-	-
Результат измерения рНш, дБ.	67	77	81	72	71	60						

1. Значения спектральной плотности напряженности магнитного (рНш) и электрического (Еш) компонентов нормированного электромагнитного поля шума (ЭМПШ) децибелах к 1мкВ/м*√кГц, формируемого генератором на расстоянии d=1м для Нш и d=3м для Еш не ниже, значений указанных в таблице.

2. Нормализованный коэффициент качества ЭПМШ (К), формируемого генератором не менее 0,8.

3. Генератор обеспечивает визуальную и звуковую индикацию выполнения требований нормального режима работы.

4. Генератор обеспечивает возможность дистанционного контроля выполнения требований нормального режима работы.

2. Электропитание генератора осуществляется от сети переменного тока напряжением 220±22 и частотой 50 Гц.

3. Генератор сохраняет свои технические характеристики в интервале температур от +5 до +40°С.

Практическая часть

Порядок работы

1. Установить генератор вблизи защищаемого компьютера. Один генератор обеспечивает маскировку (защиту) информации устройств вычислительной техники, размещенной в помещении площадью – 40м².

2. Для защиты информации от утечки по побочным электромагнитным каналам на больших вычислительных центрах, в терминальных залах, мощных вычислительных комплексах рекомендуется использовать несколько генераторов ГШ-1000М, размещая их по периметру объекта. Максимальное расстояние между соседними генераторами должно быть не более 20 метров.

3. Отключение генератора производится в следующем порядке: - подключить разъем блока питания к генератору, - включить блок питания в сеть.

4. Провести инструментальную проверку защищенности информации.

5. При нормальной работе генератора должно наблюдаться свечение индикатора «Контроль» на передней панели блока генератора. При нажатии кнопки «Контроль» на передней панели корпуса блока генератора индикатор «Контроль» должен гаснуть и излучаться прерывистый звуковой сигнал. Нормальный режим работы генератора устанавливается не более 10 секунд.

6. К разъему «Дист. контроль» на задней панели корпуса блока генератора может быть подключено внешнее устройство дистанционного контроля, позволяющего автоматически блокировать работу систем вычислительной техники в случае возникновения неполадок в работе генератора во время работы операторов с информацией с ограниченным доступом или индицировать работу генератора на центральном пульте контроля, если таковой установлен.

7. В случае возникновения нештатной ситуации (индикатор погас и подается прерывистый звуковой сигнал) следует прекратить работу с указанной информацией до выяснения причин нарушения работы генератора.

8. В выделенных помещениях первой, второй и третьей категорий при проведении режимных мероприятий (переговоры, совещания), генератор должен быть отключен от цепи питания или применены специальные меры защиты информации.

9. Для защиты информации от утечки по каналам ПЭМИ на объектах информатизации первой категории рекомендуется использовать несколько генераторов, размещая их по периметру объекта и располагая антенные системы в трех взаимно перпендикулярных плоскостях.

Меры безопасности

1. Работы по установке генератора производить только при выключенном напряжении питания.

2. Соблюдать требования по работе с электроаппаратурой, питающейся от сети с напряжением 220В и частотой 50Гц и с постоянным напряжением 12В при токах порядка 0,3А.

3. Электромагнитные поля, создаваемые генератором на расстоянии более 1м от антенны не превышают допустимого уровня на рабочих местах и соответствуют ГОСТам «Электромагнитные излучения радиочастотного диапазона (ЭМИ РЧ). Санитарные нормы и правила»

Рекомендуемая литература

Основная

1. Основы информационной безопасности. Учебное пособие для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М: Горячая линия – Телеком, 2006. – 544 с.: ил.

2. Введение в специальность. Методические рекомендации студентам по выполнению лабораторных работ. – Ставрополь, Изд-во СГУ, 2006 – 50с.

Задания для развития и контроля владения компетенциями

1. Режимы принимаемых сигналов приемником *AP – 3000 А* и их краткая характеристика.

2. Назначение сканирующего приемника *AP – 3000 А*.

3. Основные характеристики приемника *AP – 3000 А*.

4. Основные режимы работы сканирующего приемника *AP – 3000 А*.

5. Режим ручного ввода принимаемых частот.

6. Назначение и принцип действия детектора поля.

7. Основные характеристики детектора поля.

8. Принцип действия акустической завязки.

9. Порядок поиска подслушивающих устройств.

10. Порядок поиска при высоком уровне помех.

11. Назначение и принцип работы генератора шума ГШ-1000 М.

12. Технические характеристики ГШ-1000 М.

13. Контроль работоспособности генератора.

14. Порядок использования генератора шума.

III. Заключение

Подведение итогов занятия

По результатам собеседования с каждым студентом устанавливается степень усвоения ими программного материала и выставляется оценка.

Задание студентам для самостоятельной работы

1. Оформить отчет о лабораторной работе в соответствии с требованиями

2. Представить отчет для утверждения и защиты

Практическое занятие №4
«Демонстрация портативных средств защиты информации:
индикатор электрических сигналов в проводных системах
ПСЧ-5 и генератора шума ГРОМ-ЗИ-6»

В результате настоящего занятия и последующей самостоятельной работы студенты **должны:**

знать: технические характеристик и возможности работы профессионально *индикатор электрических сигналов в проводных системах ПСЧ-5 и генератора шума ГРОМ-ЗИ-6»*

уметь: применять в своей практической деятельности *индикатор электрических сигналов в проводных системах ПСЧ-5 и генератора шума ГРОМ-ЗИ-6»*

владеть: навыками настройки, регулировки *индикатора электрических сигналов в проводных системах ПСЧ-5 и генератора шума ГРОМ-ЗИ-6»*

Формируемые компетенции или их части: ПК-5

I. Вступительная часть

Проверка наличия студентов	- 2 мин
Проверка готовности студентов к занятию.	- 3 мин

II. Учебные вопросы занятия:

1. Индикатор электрических сигналов в проводных системах ПСЧ-5	- 85 мин
2. Генератора шума ГРОМ-ЗИ-6	- 85 мин

III. Заключение

- | | |
|---|----------|
| 1. Подведение итогов занятия | - 3 мин. |
| 2. Задание студентам для самостоятельной работы | - 2 мин. |

СОДЕРЖАНИЕ ЗАНЯТИЯ

1. Индикатор электрических сигналов в проводных системах ПСЧ-5

Теоретическая часть

Комплект аппаратуры ПСЧ-5 предназначен для:

- исследования электрических сигналов в проводных системах, силовых и слаботочных сетях (телефонной линии, системах охранной, пожарной сигнализации и др.);
- выявление акустических и вибрационных каналов утечки речевой информации;
- для выявления подслушивающих устройств, передающих информацию в инфракрасном диапазоне.

Основные технические характеристики (рис. в приложении № 1):

Полоса рабочих частот ПУ

В режиме АМ/ФМ	20 кГц – 10 МГц;
(амплитудная модуляция/ фазовая модуляция)	
В режиме АФ	200 Гц – 7 кГц;
(аудио частота)	
Шаг перестройки частоты	2.5 кГц;
Чувствительность ПУ	
В режиме АМ/ФМ	30 мкВ
В режиме АФ	100 мкВ
Точность измерения частоты сигнала	± 2.5 кГц

Органы управления и индикации.

На лицевой панели ПУ находится жидкокристаллический индикатор (ЖКИ), служащий для отображения текущей информации:

- частоты и направления настройки приемного устройства;
- уровня входного сигнала;
- напряжения источника питания прибора.

Частота настройки приемного устройства отображается на

верхней строке ЖКИ и указывается в кГц. Направление настройки указывается знаками «>» либо «<» соответственно. Уровень сигнала на низкой частоте индицируется на нижней строке ЖКИ в логарифмическом масштабе. Засветка первого сегмента шкалы соответствует входному сигналу 50 мкВ, засветка каждого последующего сегмента происходит при увеличении входного сигнала на 10 дБ (в три раза), засветка всех 16 сегментов соответствует входному сигналу напряжением более 30 мВ.

Кнопки «FREQ» обеспечивают перестройку приемного устройства по всему диапазону:

- кнопка « << » вниз по частоте;
- кнопка « >> » вверх по частоте;

Уровень сигнала при работе в режиме АМ/ФМ показывает стрелочный индикатор.

Клавишами «АМ, FM, АF/RF» (*амплитудная модуляция, фазовая модуляция, аудио частота / радио частота*) производится выбор соответствующего режима работы поискового устройства.

Клавиша «АТТ» служит для ослабления входного сигнала в режиме АМ/ФМ в 10 раз.

Для подачи напряжения в исследуемую линию в режиме АF служит кнопка « +5В ».

Ручка «SQV» служит для установки порога срабатывания системы бесшумной настройки в режиме АМ/ФМ и усиления в режиме АF.

Ручка «VOLUME» совмещенная с выключателем питания прибора служит для регулирования громкости в режиме АМ/ФМ и усиления в режиме АF.

На нижней крышке корпуса расположен громкоговоритель и отсек питания.

Верхнее гнездо на правой стороне корпуса служит для подключения микрофона. Среднее гнездо на правой боковой стенке «REC» служит для подключения магнитофона в режиме АМ/ФМ.

Нижнее гнездо на правой стороне корпуса служит для подключения головных телефонов.

На торце корпуса расположен сетевой ввод, предназначенный для подключения прибора к силовой сети и слаботочным проводным линиям в режиме RF (*радио частота*)

Работоспособность ПУ в режиме контроля сети и режиме детектирования ИК-излучения, а также контроль прохождения сигналов по силовой сети осуществляется при помощи контрольного устройства.

Практическая часть

Подготовка ПУ к работе:

Перед началом работы снарядить контейнер питания и произвести предварительные установки:

- «VOLUME» – в положении OFF;
- «SQV» – в крайне левое положение;

кл. «FM», «ATT» – нажаты;

кн. «AF/RF» – отжата.

Стандартным тестовым оборудованием (портативные тестеры, мультиметры) определить категорию проводных линий, подлежащих обследованию: силовые (напряжение более 70В) и сигнальные (напряжение менее 70В).

Проверка работоспособности поискового устройства и выявление сигналов радиомикрофонов в силовой сети.

1.Подключить поисковое устройство к исследуемой силовой сети кабелем «8».

2.Вставить КУ в розетку на расстоянии 1,5 ... 2 м от поискового устройства и установить переключатель рода работ в положение ТОН.

3.Включить ПУ и установить ручку «VOLUME» в среднее положение.

4.Настроить приемное устройство на сигнал КУ, добиваясь наиболее чистого звучания частоты модуляции.

5.Перевести переключатель модуляции КУ в положение «MIC» и установить ручку «VOLUME» ПУ в крайнее правое положение.

6. Ориентируя громкоговоритель ПУ в сторону КУ добиться акустической завязки (свиста переменного тона, свидетельствующего об исправности поисковой аппаратуры).

7.Перестраивая приемник кнопками «FREQ», произвести поиск FM сигналов радиомикрофонов в силовой сети во всем диапазоне рабочих частот ПУ.

8.Нажатием клавиши AM перевести поисковое устройство, а режим приема AM сигналов и произвести поиск сигналов радиомикрофонов во всем диапазоне рабочих частот.

9.Поиск и локализация радиомикрофонов производится путем подключения ПУ к различным точкам силовой сети с одновременным контролем уровня прослушиваемых сигналов. При прослушивании сигналов на громкоговоритель обнаружение микрофонов облегчается образованием акустической завязки. Уменьшая громкость регулятором «VOLUME» и снижая чувствительность поискового устройства по входному сигналу, произвести локализацию радиомикрофона в обследуемом помещении.

Поиск и локализация радиомикрофонов в слаботочных проводных линиях

Методика поиска и локализации радиомикрофонов в слаботочных проводных линиях аналогична методике поиска в силовых сетях.

Поиск и локализация низкочастотных подслушивающих устройств в слаботочных проводных линиях.

1. Выполнить предварительные установки:
ручка «VOLUME» - в положение OFF;
ручка «SQV» - в крайнем левом положении;
кл. «AF/RF» - нажата.
2. Подключить ПУ к исследуемой проводной линии кабелем .
3. Включить ПУ и плавно увеличить громкость до максимума.

При наличии подслушивающего устройства в обследуемом помещении в громкоговорителе должны прослушиваться свисты переменного тона (эффект акустической завязки) либо характерные звуковые сигналы – шумы помещения, речь и т.п.

При отсутствии названных звуковых сигналов убавить громкость до минимума и, нажав кл. «+5 В» для активизации электретных микрофонов, увеличить громкость до максимума.

4. Отжав клавишу «АТТ», сменить полярность подключения кабеля исследуемой линии и повторить вышеуказанные действия.

Поиск акустических и вибрационных каналов утечки речевой информации

1. Подключить к ПУ головные телефоны и выносной микрофон.
2. Включить ПУ и установив уровень громкости близкий к максимальному, произвести обследование помещения в предполагаемых местах утечки речевой информации.
3. Поиск вибрационных каналов утечки информации производится с помощью выносного вибродатчика по той же методике.

Поиск микрофонов с ИК-каналами

Поиск микрофонов с ИК-каналами производится с помощью выносного ИК-детектора, подключаемого к гнезду «MIS» поискового устройства.

ИК-детектор обеспечивает детектирование ИК-излучения как прямой модуляции, так и модуляции с поднесущей.

В первом случае поиск источников ИК-излучения производится выносным ИК-детектором в местах возможного расположения подслушивающих устройств в режиме «MIS».

При использовании встроенного громкоговорителя возможно прослушивание ранее оптимальных звуковых эффектов.

Детектирование ИК-излучения с поднесущей производится поисковым устройством в режиме AM/FM во всем диапазоне рабочих частот.

Проверка работы в этом режиме производится при помощи КУ.

2. Генератор шума «ГРОМ-ЗИ-6»

Теоретическая часть

Общие сведения. Устройство и назначение

1.1. Генератор шума "ГРОМ-ЗИ-6" (далее по тексту прибор) предназначен для защиты переговоров по телефонной линии (далее по тексту линия) от утечки информации. Прибор предотвращает прослушивание переговоров по линии от Вашего телефонного аппарата (ТА) до автоматической телефонной станции (АТС). Принцип действия прибора основан на маскировке спектра речи широкополосным шумом. Прибор предотвращает прослушивание с помощью различных устройств, подключаемых к линии (параллельные ТА, диктофоны, индуктивные датчики, устройства с радиоканалом и т.д.). Прибор не требует подстройки под параметры линии и обеспечивает высокое значение подавления в Вашем ТА помех, генерируемых по линии.

1.2. Прибор обеспечивает регулировку тока в линии, что предотвращает прослушивание устройствами, реагирующими на "поднятие трубки" Вашего ТА.

1.3. Прибор предотвращает прослушивание Вашего ТА устройствами, работающими по принципу высокочастотного навязывания.

1.4. Прибор может работать в автоматическом и неавтоматическом режимах. В автоматическом режиме прибор контролирует напряжение линии, при этом Ваш ТА гальванически изолирован от линии. Защита включается автоматически при:

- поднятии трубки Вашего ТА;
- снижении напряжения линии при подключении к ней параллельного ТА или прослушивающих устройств.

1.5. Прибор имеет зуммер, срабатывающий при вызывании Вашего ТА.

1.6. Прибор блокирует устройства, использующие электрическую сеть помещения в качестве канала утечки информации.

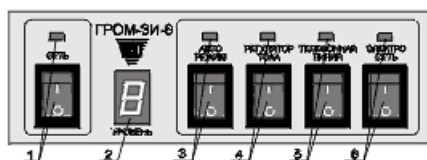


Рис.1 Лицевая панель прибора

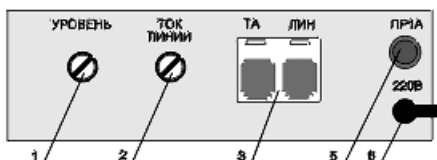


Рис.2 Задняя панель прибора

1.7. На лицевой панели прибора (рис.1.) расположены:

- включатель сетевого напряжения "СЕТЬ" и индикатор включения прибора (1);
- индикатор уровня защиты линии "УРОВЕНЬ" (2).
- включатель защиты линии в автоматическом режиме "АВТО РЕЖИМ" и индикатор автоматического режима работы прибора (3);
- включатель регулятора тока линии "РЕГУЛЯТОР ТОКА" и индикатор включения (4);
- включатель защиты линии "ТЕЛЕФОННАЯ ЛИНИЯ" и индикатор включения защиты (5);
- включатель защиты электрической сети "ЭЛЕКТРО СЕТЬ" и индикатор включения (6);

1.8. На задней панели прибора (рис.2.) расположены:

- регулятор уровня защиты линии "УРОВЕНЬ" (1).
- регулятор тока линии ТОК ЛИНИИ (2);
- гнезда ТА и ЛИН для подключения телефона и линии к прибору (3);
- кабель для подключения прибора к электросети 220 В (5) и сетевой предохранитель (4).

Технические данные и характеристики

2.1. Максимальное значение напряжения, генерируемого прибором по телефонной линии в диапазоне частот 6 - 40 кГц не менее 3 В ср. кв.

2.2. Отношение напряжения помех, генерируемых прибором по линии, к напряжению помех на клеммах ТА не менее 30 дБ. (Типовое значение 40 дБ).

2.3. Диапазон регулировки тока линии не менее 10 мА.

2.4. Порог включения прибора в автоматическом режиме 55+-3 В.

2.5. Напряжение помех, генерируемых прибором по электросети относительно 1 мкВ:

- в диапазоне частот 0,1-1 МГц не менее 60 дБ;
- в диапазоне частот 1-5 МГц не менее 30 дБ.

2.6. Электропитание прибора: сеть переменного тока напряжением 220 В +10 % -15 % частотой 50 Гц -2 %

2.7. Потребляемая мощность прибором не более 10 В × А.

2.8. Габаритные размеры 150 × 280 × 50 мм.

2.9. Масса не более 1,5 кг.

2.9.1. Время непрерывной работы прибора 8 часов.

Указание мер предосторожности.

При замене предохранителя в приборе необходимо отключить прибор от электросети. В приборе имеется напряжение 220 В 50 Гц, поэтому при эксплуатации и ремонте следует соблюдать соответствующие меры предосторожности.

Практическая часть

Подготовка прибора к работе и работа с прибором

3.1. Подключите прибор к электросети 220 В 50 Гц. Подключите ТА к гнезду "ТА" прибора. Подключите линию к гнезду "ЛИН" прибора.

3.2. Включите прибор клавишей "СЕТЬ" и проконтролируйте включение по индикатору.

3.3. Перед эксплуатацией прибора необходимо предварительно установить ток и уровень защиты линии.

3.3.1. Регулировка тока линии.

Регулятор "ТОК ЛИНИИ" установите в крайнее положение против часовой стрелки (соответствует минимальному току линии). Включите регулятор тока клавишей "РЕГУЛЯТОР ТОКА" и проконтролируйте включение по индикатору. Подняв трубку ТА Вы услышите тональный сигнал. Если он отсутствует, то медленно вращайте ручку регулятора "ТОК ЛИНИИ" по часовой стрелке до появления устойчивого тонального сигнала. Для проверки регулятора тока линии сделайте несколько контрольных звонков. Если при поднятой трубке ТА линия не соединяется или слишком низкий уровень громкости переговоров по ТА, то необходимо увеличить ток линии, повернув ручку регулятора "ТОК ЛИНИИ" по часовой стрелке.

3.3.2. Регулировка уровня защиты линии.

Регулятор "УРОВЕНЬ" установите в крайнее положение против часовой стрелки (соответствует минимальному уровню защиты). Включите защиту клавишей "ТЕЛЕФОННАЯ ЛИНИЯ" и проконтролируйте включение по индикатору. Сделайте контрольный звонок Вашему абоненту. Во время разговора медленно вращайте ручку регулятора "УРОВЕНЬ" по часовой стрелке до появления шума в трубке Вашего ТА и абонента. Индикатор "УРОВЕНЬ" показывает величину уровня защиты линии. Проконтролировать уровень шума в линии можно, подключив к линии параллельный телефон.

3.4. Работа прибора в неавтоматическом режиме.

Режим включается после нажатия клавиш "СЕТЬ" и "ТЕЛЕФОННАЯ ЛИНИЯ" прибора. Прибор защищает линию и Ваш ТА постоянно, как при "поднятой", так и при "положенной" трубке Вашего ТА. Возможна работа в данном режиме совместно с режимами "РЕГУЛЯТОР ТОКА" и "ЭЛЕКТРО СЕТЬ".

3.5. Работа прибора в автоматическом режиме.

Режим включается после нажатия клавиш "СЕТЬ", "ТЕЛЕФОННАЯ ЛИНИЯ" и "АВТО РЕЖИМ" прибора. В автоматическом режиме прибор контролирует напряжение линии. Индикатор "АВТО РЕЖИМ" показывает работу прибора в автоматическом режиме. Индикатор "АВТО РЕЖИМ" горит при:

- "положенной" трубке Вашего ТА;

В этом случае Ваш ТА гальванически изолирован от линии и

зашумление линии отсутствует. Индикаторы "УРОВЕНЬ" и "ТЕЛЕФОННАЯ ЛИНИЯ" погашены. Индикатор "АВТО РЕЖИМ" гаснет, а индикаторы "УРОВЕНЬ" и "ТЕЛЕФОННАЯ ЛИНИЯ" зажигаются при:

- "поднятой" трубке Вашего ТА;
- снижении напряжения линии при подключении к ней параллельного ТА или прослушивающих устройств;

В этом случае Ваш ТА автоматически соединяется с линией и прибор производит зашумление линии. Автоматическое переключение прибора из режима "поднята трубка" Вашего ТА в режим "положенная трубка" происходит с задержкой около 5 сек. Обратное переключение происходит без задержки. Возможна работа в данном режиме совместно с режимами "РЕГУЛЯТОР ТОКА" и "ЭЛЕКТРО СЕТЬ".

3.6. Для защиты прибором электрической сети необходимо включить защиту клавишей "ЭЛЕКТРО СЕТЬ" и проконтролировать включение по индикатору.

Рекомендуемая литература

Основная

1. Основы информационной безопасности. Учебное пособие для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М: Горячая линия – Телеком, 2006. – 544 с.: ил.

2. Введение в специальность. Методические рекомендации студентам по выполнению лабораторных работ. – Ставрополь, Изд-во СГУ, 2006 – 50с.

Задания для развития и контроля владения компетенциями

1. Общее назначение прибора ПСЧ-5.
2. Режимы работы прибора и их краткая характеристика.
3. Технические характеристики ПСЧ-5.
4. Состав комплекта ПСЧ-5.
5. Порядок поиска радиомикрофонов в силовой сети.
6. Порядок поиска акустических и виброакустических каналов утечки информации.
7. Назначение и принцип действия прибора ГРОМ-ЗИ-6.
8. Основные режимы работы прибора ГРОМ-ЗИ-6.
9. Технические характеристики прибора ГРОМ-ЗИ-6.
10. Порядок работы прибора в режиме регулировки и ограничения тока линии.
11. Работа прибора в автоматическом режиме.

III. Заключение

Подведение итогов занятия

По результатам собеседования с каждым студентом устанавливается степень усвоения ими программного материала и выставляется оценка.

Задание студентам для самостоятельной работы

1. Оформить отчет о лабораторной работе в соответствии с требованиями
2. Представить отчет для утверждения и защиты

Практическое занятие № 5

Тема: *«Демонстрация портативных средств несанкционированного доступа к информации и ее защиты: портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»*

В результате настоящего занятия и последующей самостоятельной работы студенты **должны:**

знать: технические характеристик и возможности работы портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

уметь: применять в своей практической деятельности портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

владеть: навыками настройки, регулировки портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

Формируемые компетенции или их части: ПК-5

I. Вступительная часть

Проверка наличия студентов	- 2 мин
Проверка готовности студентов к занятию.	- 3 мин

II. Учебные вопросы занятия:

1. Портативный диктофон OLYMPUS L140	- 55 мин
2. Миниатюрная камера KPC-400	- 55 мин
3. Акустический шумогенератор ANG-2000	- 60 мин

III. Заключение

Подведение итогов занятия	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

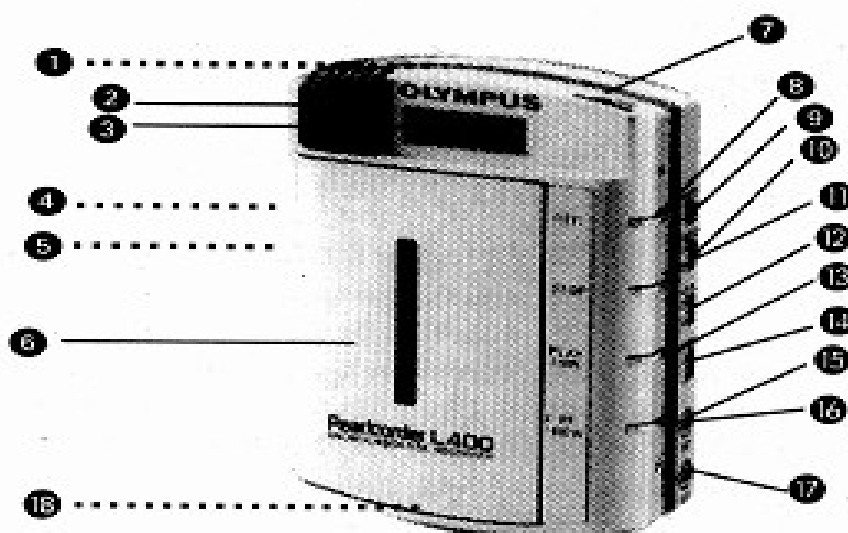
СОДЕРЖАНИЕ ЗАНЯТИЯ

1. Портативный диктофон OLYMPUS L140

Теоретическая часть

Если заинтересованное лицо не имеет постоянного доступа в контролируемое помещение, но имеется возможность его кратковременного посещения под различными предлогами, для ведения акустической разведки могут использоваться портативные диктофоны. В настоящее время выпускается огромное количество портативных диктофонов, легко маскируемых и обеспечивающих время непрерывной записи от 30 мин до нескольких часов. Современные портативные диктофоны оборудованы встроенными и миниатюрными выносными микрофонами, имеют автоматическую регулировку уровня записи (АРУЗ), устройство управления голосом включения записи (VAS), автореверс и автостоп, счетчик ленты. Последние модификации оборудованы эквалайзерами и устройством фиксации времени записи разговоров. Портативные диктофоны, как правило имеют две скорости записи 2,4 см/с и 1,2 см/с. Наличие автореверса позволяет без изъятия микрокассеты или ее перемотки осуществлять запись на второй дорожке, изменяя лишь направление движения пленки, что повышает время непрерывной записи на одну микрокассету в два раза. С целью уменьшения уровня излучения двигателей некоторые диктофоны выпускаются в металлических корпусах.

Внешний вид диктофона OLYMPUS L140.



Основные технические характеристики:

Портативный диктофон OLYMPUS L400 имеет следующие технические характеристики:

Система записи	2-дорожечная 1-канальная монофоническая.
Скорость пленки	2,4 см/сек – стандартная 1,2 см/сек – пониженная
Частотный диапазон	400-4000 Гц при скорости 2,4 см/с 400-2700 Гц при скорости 1,2 см/с
Микрофонный вход	1,2 кОм
Выход на наушник	8 Ом
Максимальная выходная мощность	100 мВт
Электропитание	1 батарея 1,5В
Габариты	73x52x20 мм
Вес	90 г

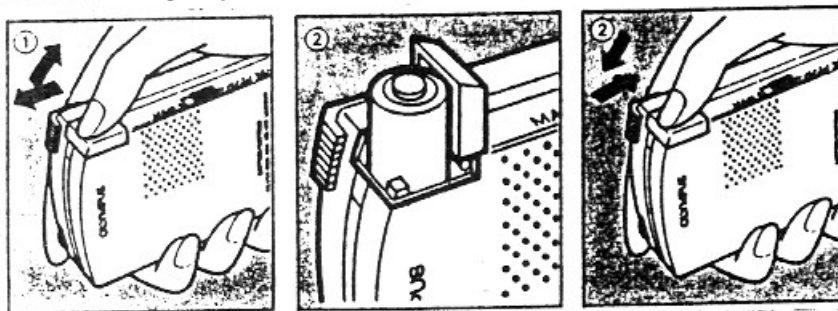
Органы управления и индикации

1. Отделение для батареек.
2. Встроенный микрофон.
3. Жидкокристаллический дисплей.
4. Громкоговоритель.
5. Переключатель режимов удерживания (MAIN – основной, HOLD/REMOTE – удержание/дистанционное управление)
6. Крышка отделения для микрокассеты.
7. Ручка регулятора громкости.
8. Кнопка записи.
9. Гнездо для подключения переключателя дистанционного управления.
10. Реверс.
11. Кнопка СТОП.
12. Переключатель ON/OFF режима VCVA.
13. Кнопка ВОСПРОИЗВЕДЕНИЕ/НАПРАВЛЕНИЕ ДВИЖЕНИЯ ЛЕНТЫ (PLAY/DIR)
14. Переключатель скорости движения ленты.
15. Кнопка открывания крышки отделения для кассеты (Open).
16. Гнездо для подключения внешнего микрофона (Mic).
17. Кнопка БЫСТРАЯ ПЕРЕМОТКА ВПЕРЕД / ОБРАТНАЯ ПЕРЕМОТКА (FF/REW).
18. Гнездо для подключения наушников (EAR).

Практическая часть

Установка батарей питания

Диктофон запитывается от одной батареи 1,5 В. Батарея устанавливается в специальный отсек, находящийся на левой стороне от дисплея. Для установки батареи необходимо сдвинуть крышку отсека в направлении, указанном стрелкой, и открыть отсек. Батареи устанавливаются положительным потенциалом к крышке. Через 2-3 сек после установки батареи, на дисплее появится надпись «000 FWD». Если после установки



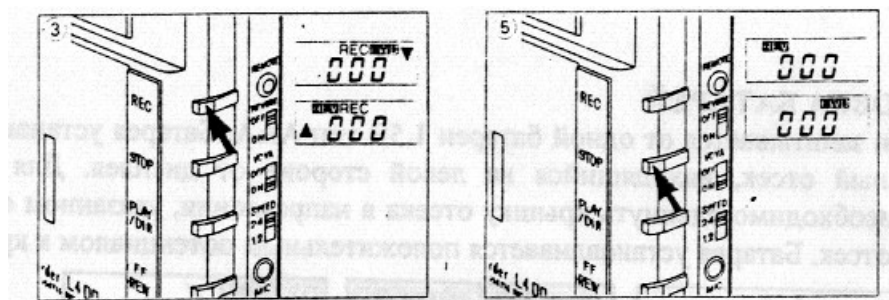
Для этого переведите переключатель HOLD в положение MAIN. Затем одновременно нажмите кнопки REC и REW.

Запись через встроенный микрофон

1. Установите необходимую скорость записи с помощью переключателя скоростей. Если переключатель реверса AUTO REVERSE находится в положении ON, то запись будет произведена на обе стороны кассеты. Время работы механизма автореверса составляет около 5 сек., при этом диктофон не записывает. По окончании записи на вторую сторону, диктофон автоматически остановится. Если переключатель находится в положении OFF, то запись будет произведена только на одну сторону.

2. Нажмите кнопку REC (запись). Запись будет производиться через встроенный микрофон.

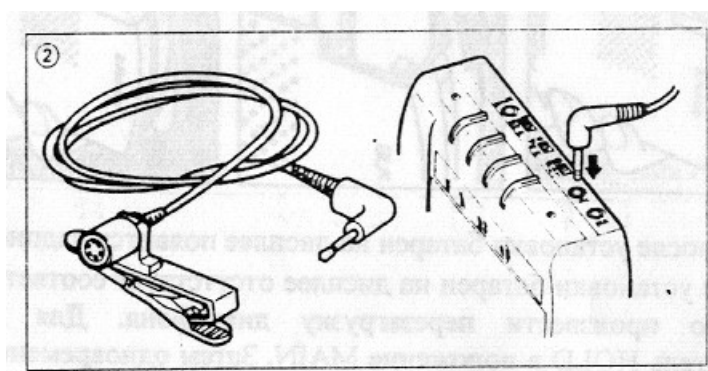
3. Для завершения записи нажмите кнопку STOP.



Запись через выносной микрофон:

1. Подключить входящий в комплект поставки микрофон к микрофонному гнезду MIC.

2. Включение на запись аналогично записи на встроенный микрофон.



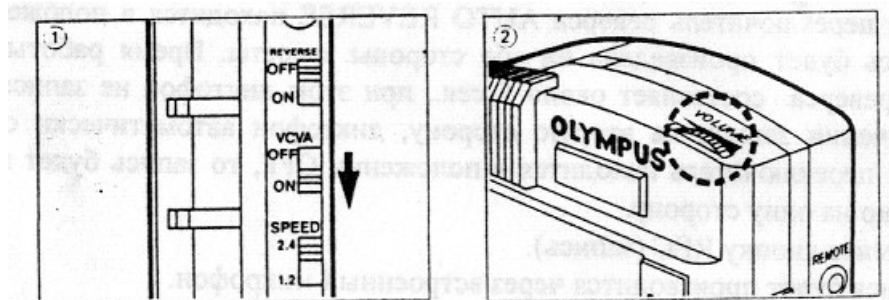
Использование акустопуска (система VCVA)

1. Переведите переключатель VCVA в положение ON.

2. С помощью регулятора громкости VOLUME установите требуемый уровень срабатывания акустопуска (при предварительной установке рекомендуется устанавливать среднее положение регулятора). Максимальный уровень громкости соответствует максимальному уровню срабатывания акустопуска и наоборот.

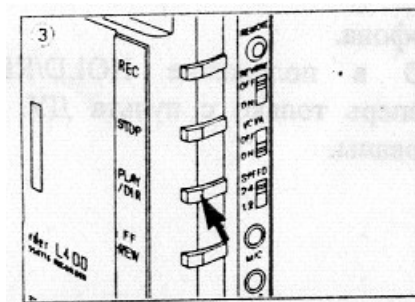
3.Нажмите кнопку REC (запись).

4.При появлении звука диктофон автоматически начнет запись и на дисплее появится надпись REC. При пропадании звука, диктофон в течении 3 сек продолжает запись, затем запись прекращается и он переходит в режим ожидания. При этом надпись REC начинает мигать.



Воспроизведение

Установите необходимую скорость записи с помощью переключателя скоростей.

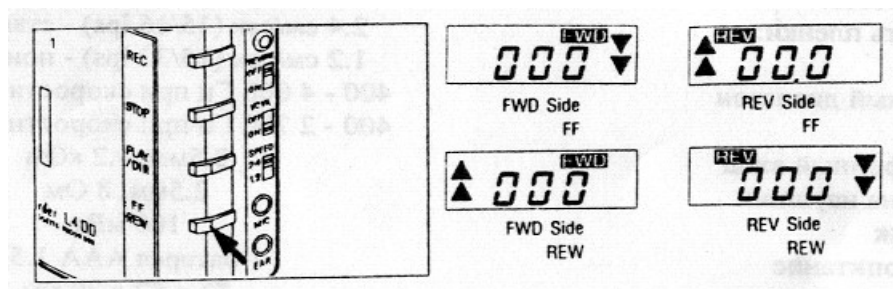


1.Установите, при необходимости, автореверс.

2.Нажмите кнопку PLAY/DIR для воспроизведения записи. Направление движения пленки высветится на дисплее. Если при воспроизведении необходимо прослушать запись на второй стороне микрокассеты, то нужно нажать кнопку PLAY/DIR.

Перемотка ВПЕРЕД/НАЗАД

1. Для перемотки назад необходимо нажать кнопку FF.REW (при этом диктофон должен быть остановлен).

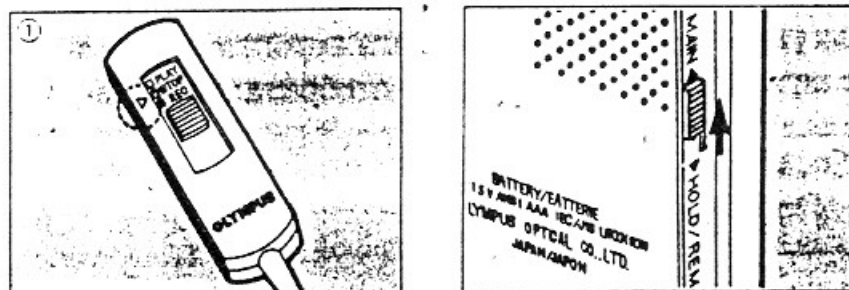


2.Для перемотки вперед необходимо дважды нажать кнопку FF.REW. В обоих случаях направление движения пленки высветится на дисплее.

3. Во время записи или воспроизведения можно осуществлять перемотку пленки вперед или назад. Для этого необходимо нажать и удерживать кнопку FF.REW.

Использование пульта дистанционного управления RS17

1. Убедитесь, что переключатель пульта ДУ, находится в положении STOP.



2. Подключите пульт к разъему REMOTE диктофона.

3. Переведите переключатель MAIN-HOLD в положение HOLD/REMOTE. Управление диктофона осуществляется только с пульта ДУ. Кнопки управления на корпусе диктофона заблокированы.

2. Миниатюрная камера KPC-400

Теоретическая часть

Нет необходимости напоминать об огромной важности использования видеотехники для обеспечения безопасности различных объектов.

Основным компонентом систем телевизионного наблюдения является видеокамера, предназначенная для преобразования оптического изображения в электрический телевизионный сигнал, пригодный для передачи и воспроизведения.

Одним из основных элементов видеокамеры является датчик изображения, т.е. устройство преобразования спроецированного объективом оптического изображения наблюдаемого объекта в электрический сигнал. Как правило, в качестве такого датчика используются передающие телевизионные трубки и твердотельные преобразователи свет-сигнал.

В последнее время все большее применение находят твердотельные преобразователи. Это фоточувствительные приборы с зарядовой связью (ПЗС). Практически все современные малогабаритные камеры наблюдения строятся на основе матричных ПЗС. Поверхность матрицы ПЗС состоит из множества светочувствительных ячеек – пикселей (обычно от 270000 до 440000). Чем большее количество пикселей размещается на матрице ПЗС, тем выше качество и четкость получаемого изображения. Разрешающая способность по горизонтали измеряется в «твл» (телевизионных линиях) и как правило составляет 300-600 твл.

Размер матрицы ПЗС определяется ее форматом. Формат – это диагональный размер видикона, формирующего изображение, эквивалентное изображению, формируемому матрицей ПЗС. Чем меньше формат матрицы ПЗС, тем миниатюрнее видеокамера. Для увеличения угла обзора матрицы малого формата должны иметь объектив с малым фокусным расстоянием. При этом качество изображения будет определяться светосилой объектива, т.е. количеством света, которое будет проходить через него и попадать на преобразователь свет – сигнал. Чем выше светосила объектива, тем меньше нужно времени для освещения матрицы ПЗС до получения изображения необходимого качества. Светосила объектива зависит от двух величин: диаметра входного зрачка “D” и фокусного расстояния “f “. Еще одним важным параметром видеокамеры является ее чувствительность. Под чувствительностью понимают минимальную освещенность объекта, при которой еще можно различать черно-белые переходы на изображении. Измеряют чувствительность в «люксах».

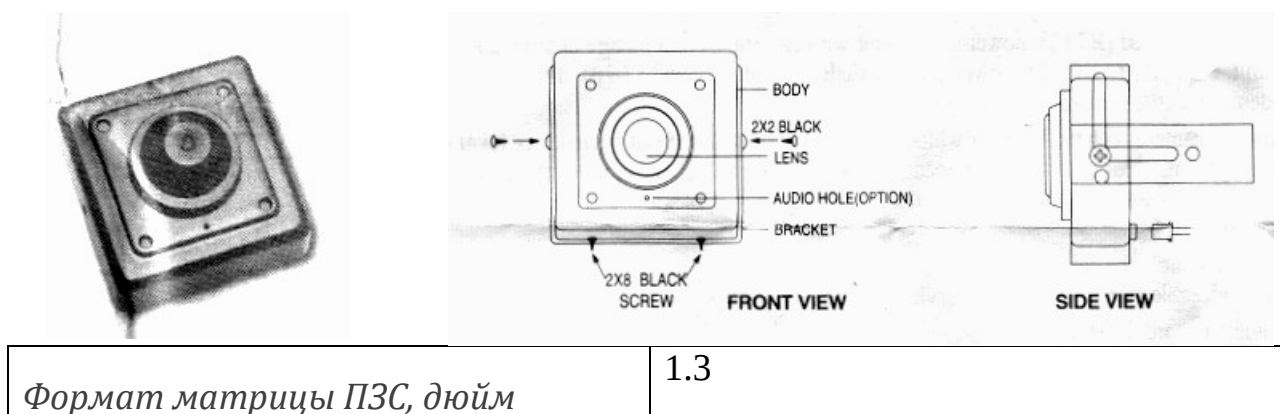
Следующая характеристика – это электронный затвор, скорость электронного затвора видеокамеры определяет качество воспроизведения быстро перемещающихся объектов. В современных камерах используются затворы со скоростью срабатывания от 1/50 до 1/10000 сек.

В настоящее время быстрыми темпами развиваются методы цифровой обработки видеосигнала. В таких системах аналоговый сигнал, снимаемый с матрицы ПЗС, проходит через аналогово-цифровой преобразователь, размещенный внутри видеокамеры. Затем сигнал разделяется на яркостную и цветовую компоненты, обрабатывается микропроцессором и поступает на цифровой монитор. Это позволяет существенно улучшить разрешение и качество изображения.

Телевизионные системы наблюдения можно рассматривать как надежный охранный комплекс любого учреждения.

Теперь ознакомимся с техническими характеристиками системы видеонаблюдения, состоящей из миниатюрной видеокамеры КРС-400РА1 и монитора В/М ТС-4312АС.

Миниатюрная видеокамера КРС-400РА1

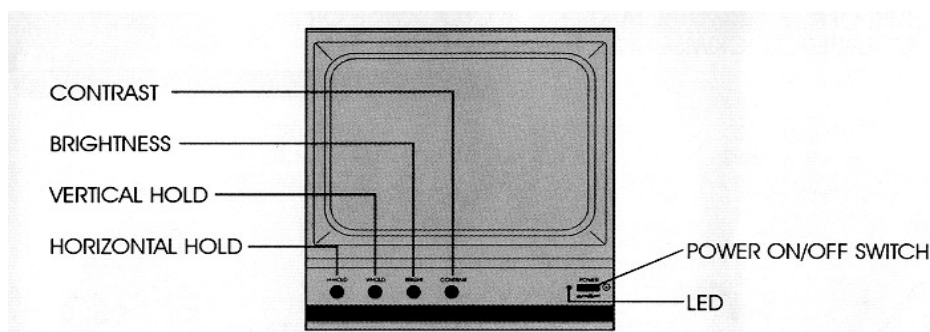


<i>Фокусное расстояние, мм</i>	3.7
<i>Относительное отверстие объектива</i>	F:2.0
<i>Разрешение, pix</i>	500(H)x582(V)
<i>Разрешение по горизонтали, твл</i>	420
<i>Электро-затвор, сек</i>	1/50-1/100000
<i>Чувствительность, люкс</i>	0.05
<i>Выходное сопротивление, ом</i>	75
<i>Источник питания, вольт</i>	9-12
<i>Размеры, мм</i>	30(H)x30(V)x28(D)

Видеомонитор TC-4312AS

Видеомонитор предназначен для отображения видеоинформации, получаемой с видеокамеры. В/В TC-4312AS имеет следующие характеристики:

- четыре входных канала для видео и аудиосигнала;
- один выходной канал для видео и аудиосигнала;
- автоматический режим выбора канала;
- разрешающая способность по горизонтали 800 твл;
- входное сопротивление 75 ом;



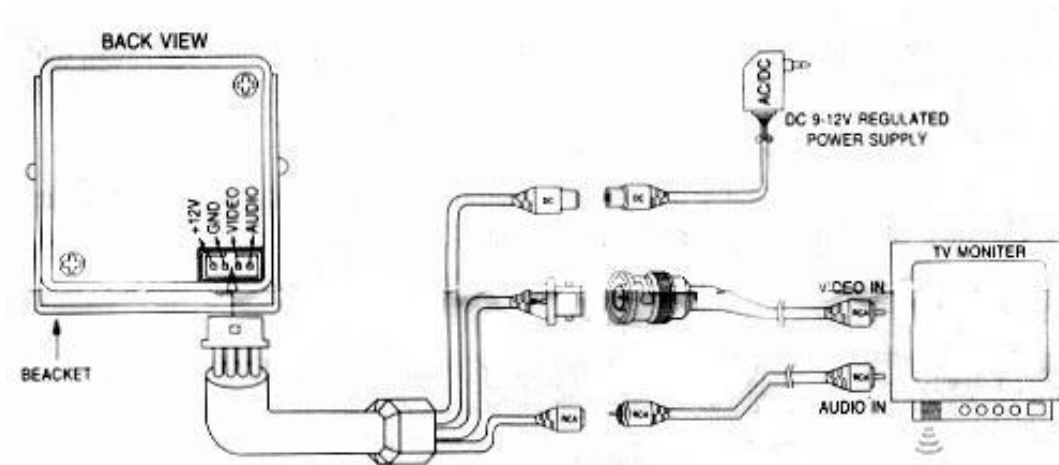


Схема подключения видеокамеры к монитору

Практическая часть

Подключить видеокамеру к монитору согласно схемы подключения. Включить монитор и источник питания камеры. Получить изображение на мониторе, проверить прохождение звук.

3. Виброакустический шумогенератор ANG-2000 Теоретическая часть

Виброакустический шумогенератор **ANG-2000** разработан специалистами фирмы REI для нейтрализации подслушивающих устройств, выявление которых затруднено традиционными средствами обнаружения.



Прибор **ANG-2000** обеспечивает противодействие таким видам подслушивающих устройств как проводные микрофоны, вмонтированные в ограждающие конструкции, контактные или прокалывающие микрофоны, радиопередатчики, установленные в электрические розетки, а также лазерные и микроволновые системы съема информации с окон строительных

конструкций.

Вышеперечисленные возможности реализуются посредством постановки сплошной шумовой нефилтруемой вибропомехи на ограждающие конструкции и строительные коммуникации помещения.

ANG-2000 является незаменимым дополнением к комплексу самых современных средств противодействия информационному шпионажу, а также может применяться самостоятельно с целью обеспечения периметральной защиты от утечки речевой информации.

Вибропреобразователи ANG-2000 возбуждают шумовые виброколебания в ограждающих конструкциях, обеспечивая при этом минимальный уровень помехового акустического сигнала в помещении практически не влияющий на комфортность проведения переговоров.

Шумовая помеха, генерируемая ANG-2000 сформирована специальным образом с целью оптимального маскирования сигналов речевого диапазона частот.

Комплект поставки предусматривает все необходимые установочные элементы для монтажа вибропреобразователей.

ANG-2000 целенаправленно разработан для обеспечения Вашей защиты от средств и методов подслушивания не подлежащих выявлению традиционными методами аппаратурного и физического поиска.

АКУСТИЧЕСКОЕ ПОДСЛУШИВАНИЕ

Звук, проходя через ограждающие и вентиляционные конструкции, вызывает их вибрацию. Контактные микрофоны или приборы лазерного или микроволнового зондирования активно используют эту способность звука, улавливая вибрации вентиляционных каналов, водопровода, строений, стен, окон, дверей, пола и др. и преобразовывая их обратно в звук. Микрофон может быть установлен не обязательно в той же комнате, где проходит разговор, может быть вмонтирован в ограждающие конструкции. Это значительно затрудняет их поиск и обнаружение. ANG-2000 предназначен для нейтрализации таких приборов.

ХАРАКТЕРИСТИКИ

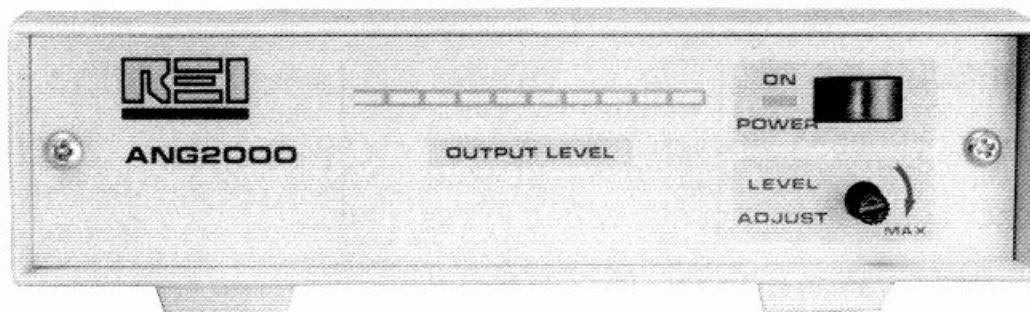
Акустический шумогенератор ANG-2000

Размер:	43 x 152 x 254 мм;
Вес:	1,36 кг;
Диапазон выходного напряжения:	0- 14 В 6 Ом;
Минимальная нагрузка:	1 Ом;
Диапазон частот:	250 Гц - 5 кГц ? 3 дБ;

Мощность (адаптера): 120 В перем. тока
(прибора): 50/60 Гц 24 Вт;
12 - 18 В перем. тока;

Датчики TRN-2000

Размер: 101 x 38 мм;
Вес: 907 г;
Сопротивление: 6 Ом.



Комплект поставки ANG-2000 предусматривает 3 базовых установочных элемента:

- прямой винт для твердых поверхностей;
- крепление, рассчитанное на стены сухой кладки, штукатурку и другие мягкие или хрупкие материалы;
- пластиковый диск для плоских гладких поверхностей (стекло, пластик, и т.д.)

Предупреждения:

- Не подсоединяйте больше 4-х датчиков параллельно или нагрузку меньше 1 Ом к выходу ANG-2000.
- Не допускайте проникновения в прибор влаги.
- Не бросайте прибор.
- Обеспечьте соответствующую вентиляцию вокруг корпуса ANG-2000.
- Не оставляйте прибор при температуре ниже - 30° и выше +50°.

Для ремонта прибора обращайтесь к специалистам. При самостоятельном вскрытии прибор снимается с гарантийного обслуживания

Рекомендуемая литература

Основная

1. Основы информационной безопасности. Учебное пособие для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М: Горячая линия – Телеком, 2006. – 544 с.: ил.

2. Введение в специальность. Методические рекомендации студентам по выполнению лабораторных работ. – Ставрополь, Изд-во СГУ, 2006 – 50с.

Задания для развития и контроля владения компетенциями

1. Технические характеристики диктофона.
2. Назначение и принцип действия системы VCVA и автореверса.
3. Достоинства и недостатки 2-х скоростного режима записи на диктофон.
4. Технические характеристики миниатюрной телекамеры **KPC – 400**.
5. Характеристики ПЗС.
6. Что характеризует чувствительность видеокамеры?
7. Понятие светосилы объектива.
8. Основные характеристики видеомонитора **ТС-4312AS**.
9. Назначение виброакустического шумогенератора **ANG – 2000**.
10. Технические характеристики акустического шумогенератора.
11. Принцип маскировки акустических сигналов.
12. Принцип работы устройств лазерного и микроволнового зондирования.

III. Заключение

Подведение итогов занятия

По результатам собеседования с каждым студентом устанавливается степень усвоения ими программного материала и выставляется оценка.

Задание студентам для самостоятельной работы

1. Оформить отчет о лабораторной работе в соответствии с требованиями

2. Представить отчет для утверждения и защиты

Практическое занятие № 6

Тема: *«Демонстрация и ознакомление со средствами защиты от несанкционированного доступа к информации в персональных компьютерах и компьютерных сетях»*

В результате настоящего занятия и последующей самостоятельной работы студенты **должны:**

знать: технические характеристик и возможности работы портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

уметь: применять в своей практической деятельности портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

владеть: навыками настройки, регулировки портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

Формируемые компетенции или их части: ПК-5

I. Вступительная часть

Проверка наличия студентов	- 2 мин
Проверка готовности студентов к занятию.	- 3 мин

II. Учебные вопросы занятия:

- | | |
|--|----------|
| 1. Портативный диктофон OLYMPUS L140 | - 55 мин |
| 2. Миниатюрная камера KPC-400 | - 55 мин |
| 3. Акустический шумогенератор ANG-2000 | - 60 мин |

III. Заключение

- | | |
|--|----------|
| Подведение итогов занятия | - 3 мин. |
| Задание студентам для самостоятельной работы | - 2 мин. |

СОДЕРЖАНИЕ ЗАНЯТИЯ

Цель работы: знать: методологию создания систем защиты информации; перспективные направления развития средств и методов защиты информации;

технических характеристик и демонстрация работы системы охранно-пожарной сигнализации и стандартных средств защиты информации от несанкционированного доступа в персональных компьютерах и локальных сетях.

Занятие проводится с использованием кафедрального виртуального комплекса на базе программных эмуляторов

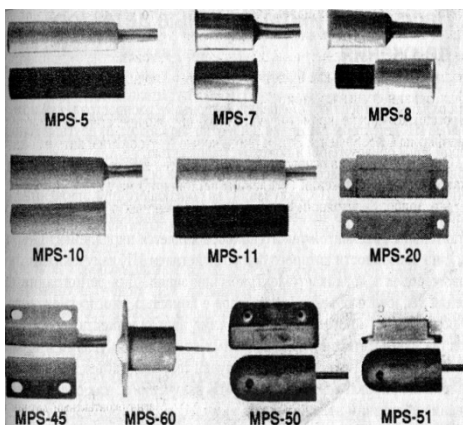
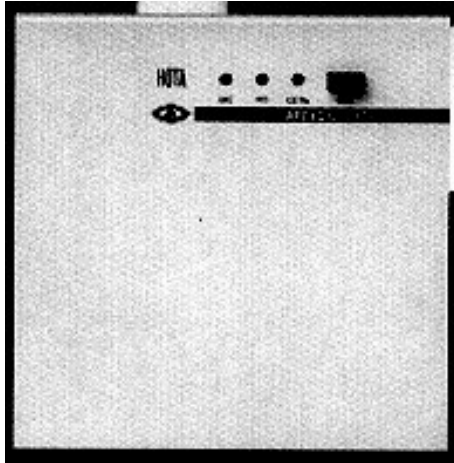
Учебные вопросы

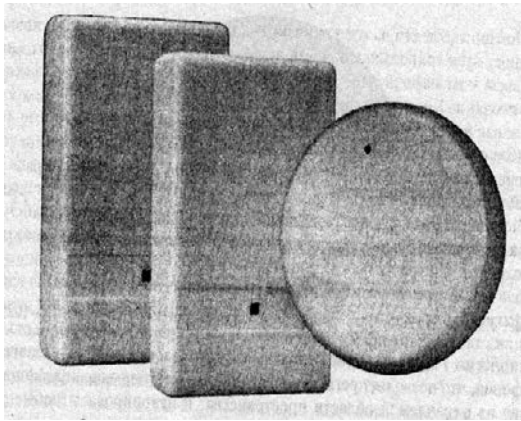
1. Системы охранно–пожарной сигнализации
2. Защита информации на персональном компьютере и в локальной вычислительной сети.

Приборы и принадлежности: система охранно-пожарной сигнализации в аудитории № 122, компьютеры на базе процессора Intel Pentium II, операционная система Windows NT.

Время, отводимое на занятие – 4 часа

Методические рекомендации

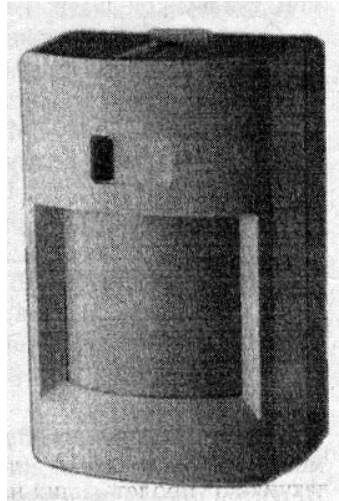




Детекторы битого стекла

Детекторы битого стекла (ДБС) предназначены для регистрации преднамеренного разрушения стеклянных конструкций: окон, витрин и др. Они реагируют на звук бьющегося стекла и удара о стекло, а также анализируют спектр звуковых шумов в помещении, позволяют бесконтактно контролировать целостность стекла размером более 20×20 см.

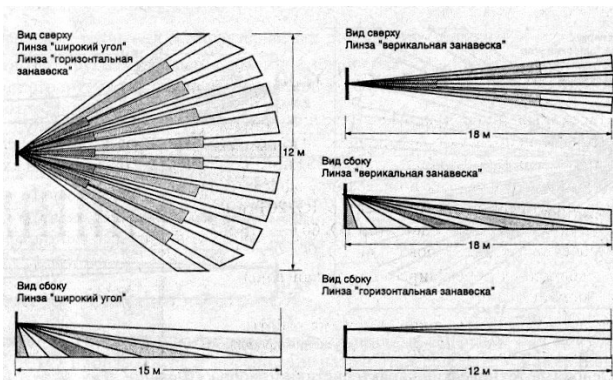
Пассивные и активные ИК детекторы движения



Детекторы движения предназначены для обнаружения движения теплового объекта в охраняемой зоне. По принципу действия они подразделяются на пассивные и активные. В настоящее время первые находят более широкое применение. Они имеют регулируемые зоны обнаружения, защиту от ложных срабатываний, вызываемых домашними животными и насекомыми. Различаются пассивные детекторы размером зоны обнаружения (20 - 360°), методами обработки сигнала, конструкцией и т.п. Активные детекторы используются, как правило, для охраны периметров объектов.

Недостатком самых простых и дешевых ИК детекторов движения является низкая помехоустойчивость – они срабатывают даже при возникновении теплового потока, например, из-за прогрева солнцем помещения.

Более совершенные детекторы лишены этого недостатка. Их надежность и стойкость к тепловым помехам обеспечивается многоканальными пироэлементами и сложной электронной обработкой сигнала в самом детекторе. В простых моделях обработка сигналов осуществляется аналоговыми методами, а в более сложных – цифровых, например, с помощью встроенного процессора.



Способы подключения извещателей

Системы охранно-пожарной сигнализации по способу подключения извещателей подразделяются на проводные и беспроводные. В первых связь между всеми устройствами системы осуществляется по проводам. Совокупность соединительных проводов, датчиков, детекторов, соединительных коробок, разъемов и т.п. называется *шлейфом*. С помощью шлейфов формируются зоны охраны. При своей надежности проводные системы менее гибкие, чем беспроводные. В беспроводных системах каждый извещатель оснащается собственным передатчиком, а контрольная панель – многоканальным приемником. Надежность связи определяется характеристиками приемника и передатчиков, архитектурой здания и уровнем промышленных радиопомех. Дальность связи обычно составляет от 30 до 1000 м. Беспроводные системы сигнализации более удобны при монтаже и использовании, они могут дополняться устройствами дистанционного управления.

Исполнительные устройства

Исполнительные устройства предназначены для передачи информации пользователю или компетентным органам о срабатывании системы охраны путем подачи звукового и (или) светового сигналов или путем автоматического дозвона по телефонной линии связи до заранее определенных абонентов, а также для управления различными механизмами, обеспечивающими усиление безопасности.

К исполнительным устройствам относятся лампы наружного освещения, прожекторы, стробоскопы, сирены, автодозвончики, блоки электромагнитных реле, электрозамки и т.п.

Прожекторы, лампы наружного освещения и стробоскопы освещают охраняемую территорию и включаются в случае срабатывания сигнализации, привлекая внимание окружающих. Яркая вспышка стробоскопа в темное время суток или в плохо освещенном помещении может ошеломить преступника и на некоторое время вывести его из строя.

Сирены или ревуны издают громкий звуковой сигнал мощностью до 130 дБ, который может быть услышан на расстоянии нескольких сотен метров. Сирены имеют различное оформление и размеры,

некоторые из них оборудованы автономным источником питания. Длительность звучания сирены может быть различной и устанавливается по желанию пользователя.

Устройства автоматического дозвона (автодозвончики, или коммуникаторы) подключаются к телефонной линии и могут дозваниваться в автоматическом режиме до одного или нескольких абонентов в зависимости от логики работы системы охраны.

Блоки электромагнитных реле обеспечивают включение мощных исполнительных механизмов и приборов.

2. Защита информации на персональном компьютере и в локальной вычислительной сети.

Теоретическая часть

Степень защищенности информации в персональном компьютере или локальной вычислительной сети в большой степени зависит от того какая операционная система используется пользователем. Условно операционные системы можно разделить на защищенные и частично защищенные.

Защищенная операционная система обязательно должна содержать средства разграничения доступа пользователей к своим ресурсам, а также средства проверки подлинности пользователя, начинающего работу с операционной системой. Кроме того, защищенная операционная система должна содержать средства противодействия случайному или преднамеренному выводу операционной системы из строя.

Если операционная система предусматривает защиту не от всех основных классов угроз, а только от некоторых, такую операционную систему называют *частично защищенной*.

Для оценки защищенности операционных систем специальных стандартов нет, но используются стандарты, разработанные для компьютерных систем вообще.

В России, наиболее часто применяются две системы стандартов:

- **«Оранжевая книга»;**
- **Руководящие документы Гостехкомиссии.**

Если операционная система сертифицирована по какому-либо классу защищенности некоторой системы стандартов, это вовсе не означает, что информация, хранящаяся и обрабатываемая в этой системе, защищена согласно соответствующему классу. Защищенность операционной системы определяется не только ее архитектурой, но и текущей политикой безопасности.

Для примера рассмотрим некоторые (далеко не все) требования к конфигурации операционной системе Windows NT, которые должны выполняться для соответствия защищенности операционной системы классу **C2** «Оранжевой книги»:



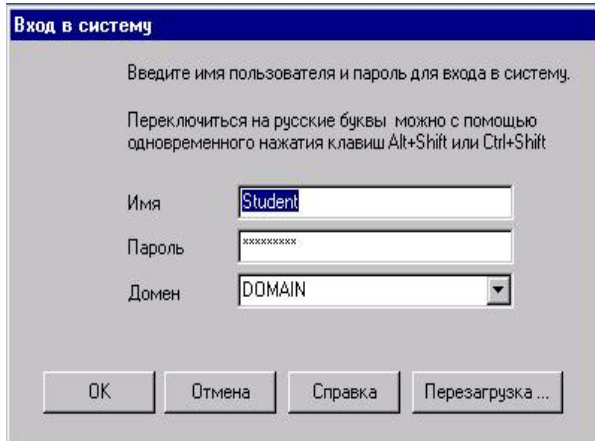
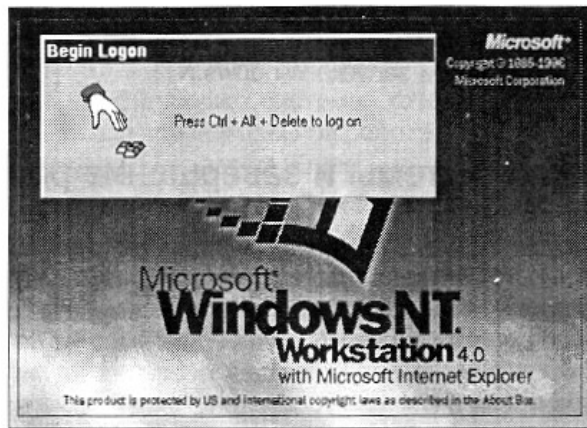
- ❖ Загрузка компьютера невозможна без ввода пароля;
- ❖ Запрещено использование паролей короче 6 символов;
- ❖ Запрещен анонимный и гостевой доступ;
- ❖ Запрещен запуск любых отладчиков;
- ❖ Запрещена запись в системную директорию;
- ❖ Запрещено разделение между пользователями ресурсов сменных носителей информации и др.

Однако следует иметь в виду, что операционная, сертифицированная по очень высокому классу защиты, оказывается уязвимой для некоторых угроз даже при соответствии политики безопасности требованиям соответствующего класса защиты. Например, операционная система, защищенная по классу **C2** «Оранжевой книги», уязвима для несанкционированных действий администратора.

Практическая часть

Защита документов и права доступа:

В Windows NT каждый пользователь должен регистрироваться в системе перед началом работы индивидуально. Это необходимо как на локальной рабочей станции без подключения к сети, так и на станции в компьютерной сети. После окна приветствия через некоторое время появляется окно с приглашением зарегистрироваться в системе. Для входа в систему нужно выполнить следующие действия:



Нажмите комбинацию клавиш [Ctrl] + [Alt] + [Del]. Появляется окно регистрации пользователя. В поле имени указано имя пользователя, который последним работал с Windows NT.

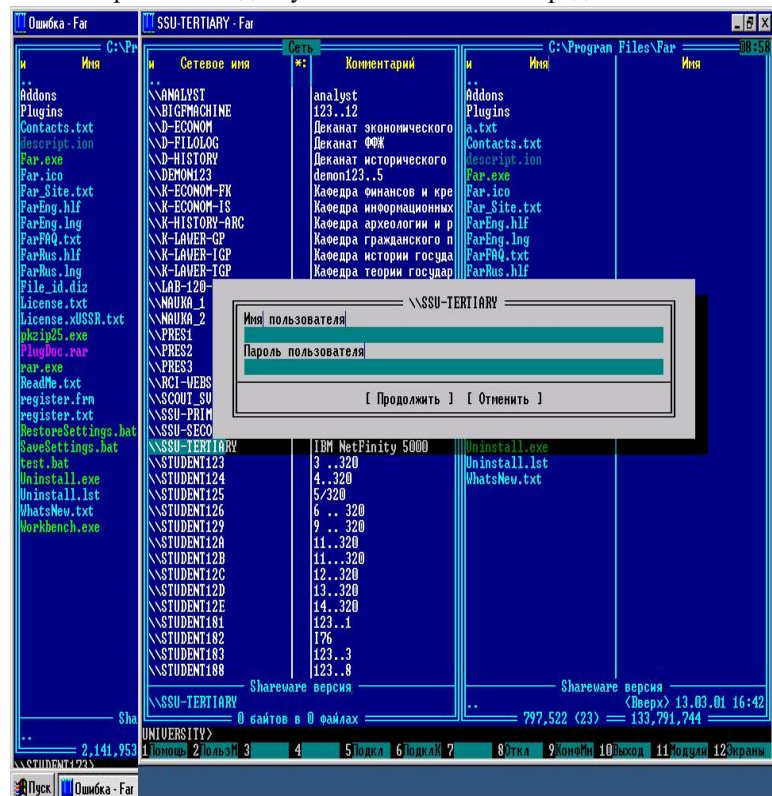
Если нужно задать другое имя пользователя, то оно вводится в поле (ИМЯ). Пароль вводится в поле (ПАРОЛЬ).

- ♦ Переход между полями осуществляется щелчком мыши или клавишей [Tab].

- ♦ После ввода имени и пароля пользователя нужно нажать клавишу [Enter] или щелкнуть на кнопке ОК. После этого введенная информация анализируется системой, и если имя пользователя и пароль соответствуют списку пользователей, которые имеют доступ к работе, осуществляется запуск системы.

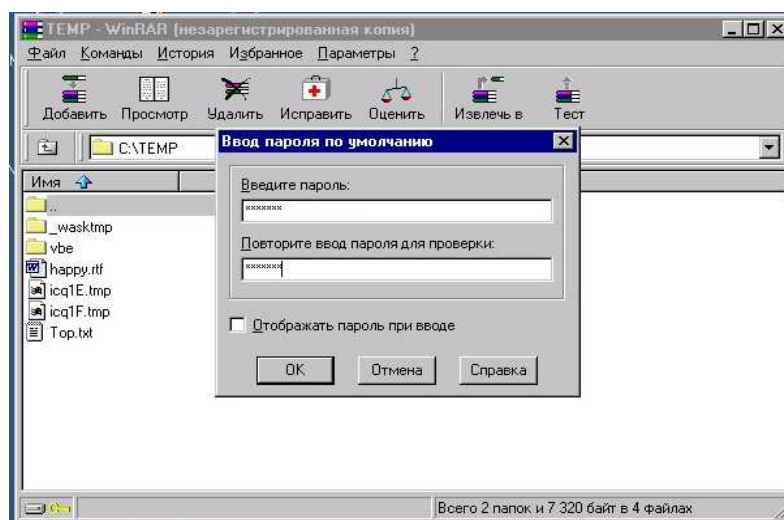
Ограничение доступа к папкам и файлам.

Ограничение доступа – это важнейшее средство



защиты в компьютерной сети, обеспечивающее возможность предоставления доступа к данным только определенным пользователям. Ограничивая доступ, можно установить, какими правами обладает пользователь в отношении каталога, папки и содержащихся в них файлов. (Ограничение доступа демонстрируется программистами с использованием программы FAR manager).

Защита архивов.

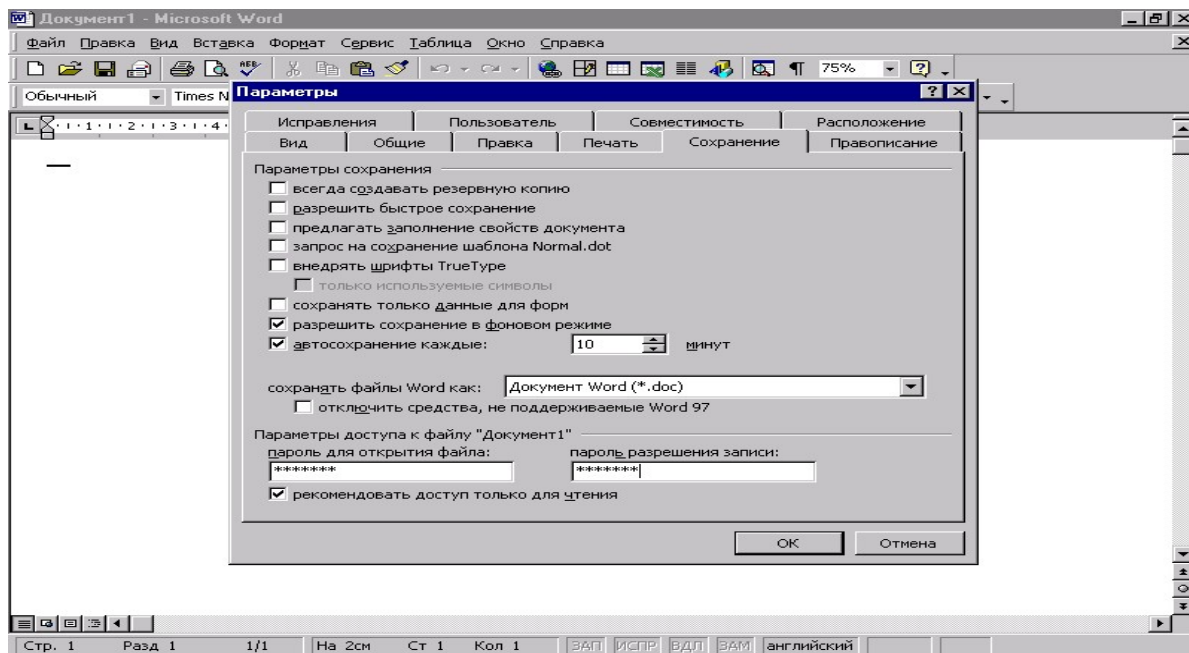


Чтобы уменьшить потери информации, необходимо иметь резервные копии файлов и папок. Для этих целей используются программы-упаковщики, которые позволяют за счет применения специальных методов сжатия информации создавать копии нескольких файлов в один архивный файл.

При помещении файлов в архив программы-упаковщики позволяют указывать пароль. При этом помещаемые в архив файлы зашифровываются с помощью этого пароля. Извлечение файлов из архива возможно только при указании правильного пароля.

Запустим программу – упаковщик WinRAR. С помощью программистов кафедры заархивируем несколько файлов и зашифруем их паролем. Затем проведем разархивацию, при этом вначале введем неправильный пароль, а затем правильный.

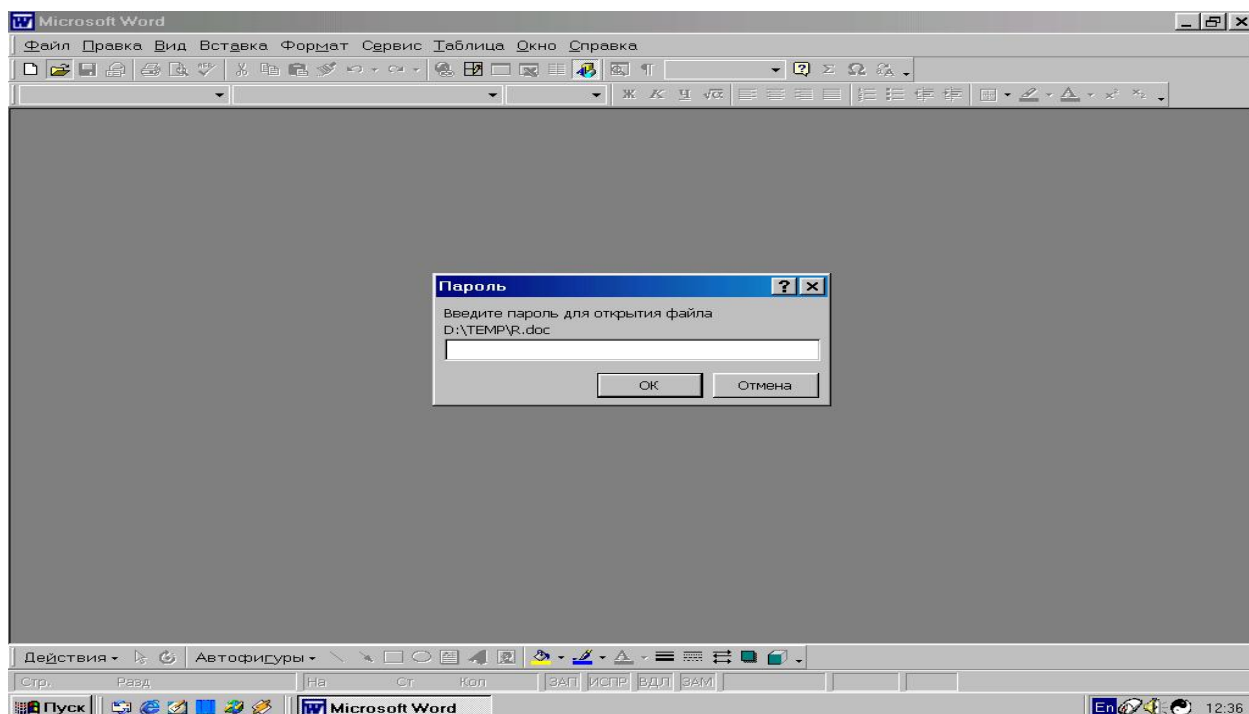
Защита документов



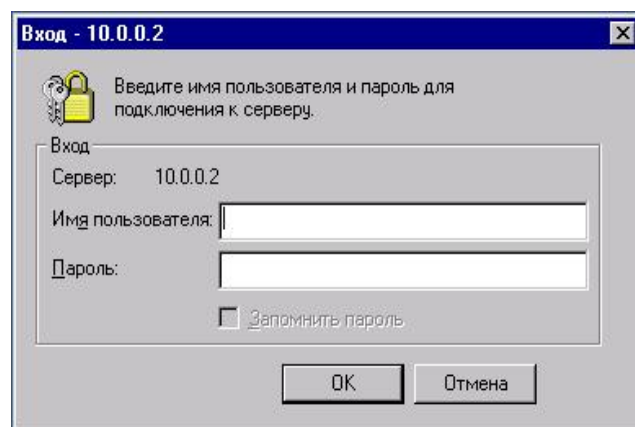
Запустим программу Microsoft Word. Осуществим набор произвольного текста. Сохраним текст: в меню ФАЙЛ – СОХРАНИТЬ КАК, в диалоговом окне наберем имя файла и нажмем кнопку СОХРАНИТЬ.

Затем откроем меню СЕРВИС – ПАРАМЕТРЫ и выберем вкладку СОХРАНЕНИЕ. В полях ПАРОЛЬ ДЛЯ ОТКРЫТИЯ ФАЙЛА; ПАРОЛЬ ДЛЯ РАЗРЕШЕНИЯ ЗАПИСИ введем пароль и нажмем кнопку ОК. Закроем документ.

Вновь откроем сохраненный документ. При этом появятся диалоговые окна для ввода пароля: на открытие файла и на разрешение записи. Вначале введем неправильный пароль, затем правильный.



Защита электронной почты



Для защиты от несанкционированного чтения электронной почты используется логин и пароль. Как только вы запускаете почтовую программу и она подключает вас с серверу появляется диалоговое окно, где необходимо ввести имя пользователя и пароль. (Демонстрация защиты от несанкционированного доступа чтения электронной почты проводится программистами кафедры с использованием программы Outlook Express).

Рекомендуемая литература

Основная

1. Основы информационной безопасности. Учебное пособие для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М: Горячая линия – Телеком, 2006. – 544 с.: ил.

2. Введение в специальность. Методические рекомендации студентам по выполнению лабораторных работ. – Ставрополь, Изд-во СГУ, 2006 – 50с.

Задания для развития и контроля владения компетенциями

1. Предназначение систем охрано-пожарной сигнализации.
2. Основные компоненты систем охрано-пожарной сигнализации.
3. Предназначение контрольной панели.
4. Типы извещателей.
5. Предназначение исполнительных устройств.
6. Краткая характеристика защищенных ОС.
7. Какие ОС называют частично защищенными.
8. Основные требования к конфигурации ОС для соответствия защищенности по классу С2 «Оранжевой книги».

III. Заключение

Подведение итогов занятия

По результатам собеседования с каждым студентом устанавливается степень усвоения ими программного материала и выставляется оценка.

Задание студентам для самостоятельной работы

1. Оформить отчет о лабораторной работе в соответствии с

требованиями

2. Представить отчет для утверждения и защиты

Практическое занятие № 7

Тема: «Демонстрация портативных средств защиты информации: анализатора поля «АРР-7», универсального поискового прибора D008, устройства предотвращения утечки информации по каналам систем мобильной связи «Мозаика».

В результате настоящего занятия и последующей самостоятельной работы студенты **должны:**

знать: технические характеристик и возможности работы портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

уметь: применять в своей практической деятельности портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

владеть: навыками настройки, регулировки портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

Формируемые компетенции или их части: ПК-5

I. Вступительная часть

Проверка наличия студентов	- 2 мин
Проверка готовности студентов к занятию.	- 3 мин

II. Учебные вопросы занятия:

1. Портативный диктофон OLYMPUS L140	- 55 мин
2. Миниатюрная камера KPC-400	- 55 мин
3. Акустический шумогенератор ANG-2000	- 60 мин

III. Заключение

Подведение итогов занятия	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

СОДЕРЖАНИЕ ЗАНЯТИЯ

Цель работы:

знать: методологию создания систем защиты информации;
перспективные направления развития средств и методов защиты информации;
технических характеристик и демонстрация работы:
анализатора поля «АРР–7», универсального поискового прибора D008, устройства предотвращения утечки информации по каналам систем мобильной связи «Мозаика».

Занятие проводится с использованием кафедрального виртуального комплекса на базе программных эмуляторов

Учебные вопросы

1. Анализатора поля «АРР–7»
2. Универсальный поисковый прибор D008,
3. Устройства предотвращения утечки информации по каналам систем мобильной связи «Мозаика»

Приборы и принадлежности: анализатор поля «АРР–7», универсальный поисковый прибор D008, устройство предотвращения утечки информации по каналам систем мобильной связи «Мозаика».

Время, отводимое на занятие – 4 часа

Методические рекомендации

1. Анализатор поля «АРР–7»

Теоретическая часть

Анализатор поля АРР–7 представляет собой широкополосное радиоприемное устройство, предназначенное для поиска и локализации маломощных источников электромагнитного излучения в диапазоне от 30 до

3600 МГц.

Анализатор поля АРР-7 позволяет не только выявить сигналы радиомикрофонов, негласно установленных в проверяемом помещении, но и измерить частоту их сигналов, а также оценить мощность излучения в точке приема.

Анализатор поля АРР-7 позволяет выявить даже сигналы средств съема информации, работающих с прикрытием, включая устройства, использующие маскировку сигнала.

Работа АРР-7 основана на принципе интегральной оценки электромагнитного излучения.

Основные режимы работы прибора

LEVEL – основной режим работы, используемый для поиска и локализации источников радиоизлучений.

AUDIO – режим, применяемый для слухового контроля принимаемых сигналов.

В этом режиме можно осуществить поиск радиомикрофонов по методу «акустической завязки».

RANGE – пороговый режим. Он применяется при выявлении сигналов средств съема информации, возможно внедренных в контролируемое помещение.

В этом случае анализатор АРР-7 используется в качестве сторожевого устройства. При превышении некоторого порога, устанавливаемого Пользователем, прибор выдает тревожный звуковой сигнал, подтверждаемый загоранием красного светодиода.

Основные технические характеристики анализатора АРР-7

Диапазон рабочих частот, MHz	30 – 3600 (не менее)
------------------------------	----------------------

Диапазон измерения уровня

входного сигнала, dB	не менее 70
----------------------	-------------

Чувствительность в режиме

измерения уровня сигнала (режим поиска), мВ

в НЧ диапазоне (30 – 500 MHz)	не менее 1
в ВЧ диапазоне (500 – 2500 MHz)	не менее 3

Чувствительность при измерении частоты, мВ

в НЧ диапазоне (30 – 500 MHz)	не менее 3
в ВЧ диапазоне (500 – 2500 MHz)	не менее 10

Уровень ослабления аттенюатора, dB	0, 10, 20
------------------------------------	-----------

Точность измерения частоты	$\pm 2 \times 10^{-6}$.
----------------------------	--------------------------

Напряжение питания, В

4 элемента АА	6
---------------	---

2. Универсальный поисковый прибор D008

Теоретическая часть

Общие сведения. Устройство и назначение

Универсальный поисковый прибор D008 предназначен для оперативного обнаружения и локализации специальных технических средств негласного добывания информации.

Использование D008 позволяет обнаружить следующие виды

- радиомикрофоны;
- телефонные радиоретрансляторы;
- радиостетоскопы;
- скрытые видеокамеры с передачей информации по радиоканалу;
- технические средства систем пространственного высокочастотного облучения;
- радиомаяки систем слежения за перемещением объектов;
- несанкционированно включенные радиостанции и радиотелефоны;
- ПУ, использующие для передачи информации линии сети переменного тока 220В, абонентские телефонные линии, линии систем пожарной и охранной сигнализации и т.п.

D008 предназначен для решения задач в пределах помещения (или непосредственной близости к нему), в транспортных средствах и т.п.

D008 имеет два канала обнаружения:

- радиодетектор (РД), предназначенный для поиска радиопередающих ПУ;
- анализатор проводных линий (АПЛ), предназначенный для поиска ПУ, использующих для передачи информации проводные линии с напряжением до 500В.

Принцип действия D008 в режиме РД основан на широкополосном амплитудном детектировании электрического поля, что дает возможность регистрировать радиопередающие ПУ независимо от вида модуляции.

Радиус обнаружения зависит от излучаемой мощности, частоты ПУ и электромагнитной обстановки в обследуемом помещении. Для ориентировки – дальность обнаружения ПУ (5 мвт, 160 МГц) составляет примерно 1 м.

Аттенюатор позволяет работать в условиях сложной электромагнитной

обстановки, присущей крупным промышленным центрам. Он также полезен в случае локализации мощных радиопередающих ПУ–устройств (в том числе несанкционированно включенные радиостанции и сотовые радиотелефоны).

Высокочастотная антенна, за счет встроенного усилителя, облегчит обнаружение ПУ с частотой передачи выше 400 МГц.

Режим акустической обратной связи (АОС) позволяет исключить ложные срабатывания детектора на локальные электромагнитные поля и идентифицировать ПУ по характерному звуковому сигналу.

АПЛ состоит из внешнего проводного адаптера и, собственно, супергетеродинного приемника с ручной перестройкой частоты.

Контроль звуковой информации осуществляется посредством головных телефонов либо через встроенные громкоговоритель, причем как АМ, так и ЧМ–сигналов.

Десятисегментная светоидная шкала и звуковой сигнал, с меняющейся частотой тона, обеспечивают наглядность и удобство при работе с D008.

Основные технические характеристики универсального поискового прибора D008:

РД	
Диапазон рабочих частот, МГц	50 – 1500
Чувствительность по входу, мВ:	
F=100 МГц	2
F=400 МГц	2
F=800 МГц	1,5
F=1400 МГц	6
Ослабление аттенюатора, дБ	20
Диапазон частот активной антенны, МГц	400 – 1500
входного сигнала, дВ	не менее 70
Усиление активной антенны, дБ	7
Динамический диапазон индикатора, дБ	20
Диапазон рабочих частот, МГц	
нижняя граница, не более	0,05
верхняя граница, не менее	7
Чувствительность при отн. с/ш 20 дБ, г	
лубина АМ 30%, мВ	4
Полоса пропускания, кГц	200

Вид модуляции	АМ, ЧМ
Максимальное входное напряжение	
проводного адаптера, В	500
Напряжение питания, В	9
Потребляемый ток, не более, мА	
дежурный режим	30
рабочий режим	100

3. Устройство предотвращения утечки информации по каналам систем мобильной связи МОЗАИКА

Теоретическая часть

Общие сведения. Устройство и назначение

Изделие «МОЗАИКА» предназначено для блокирования работы подслушивающих устройств, использующих каналы систем мобильной связи стандартов GSM–900/1800, E– GSM, AMPS/DAMPS, CDMA и блокирования работы телефонов названных систем мобильной связи в пределах выделенных помещений, предназначенных для ведения переговоров, проведения совещаний. Используется в целях предотвращения утечки информации за пределы выделенного помещения через подслушивающие устройства указанного выше типа, через включенный телефон мобильной связи, а также для обеспечения рабочей обстановки во время проведения переговоров, совещаний.

Изделие излучает в диапазоне работы систем мобильной связи, мощность излучения в других диапазонах незначительна. Изделие имеет небольшую мощность излучения (меньше мощности мобильных телефонов!), блокирование каналов систем мобильной связи осуществляется за счет применения специального вида модуляции. Изделие не оказывает влияния на работу других технических средств – бытовой электронной техники (теле–, видео–, аудио–, и др.), компьютеров, оргтехники.

Зона эффективного действия изделия зависит от расстояния до ближайшей базовой станции сети мобильной связи и составляет от 3 до 25 м. Для регулировки мощности излучения (для установки оптимальной мощности в зависимости от площади защищаемой территории) имеется регулятор на лицевой панели изделия. Для охвата большей площади необходимо использовать несколько изделий, разнесенных по защищаемой территории.

Изделие конструктивно исполнено в виде законченного блока в пластмассовом корпусе, имеет небольшие габариты, автономное питание и поэтому может быть использовано не только в стационарном режиме.

Питание изделия осуществляется от сети 220В через блок питания (который одновременно подзаряжает аккумуляторы), или от встроенного блока аккумуляторов. Продолжительность работы от полностью заряженного блока аккумуляторов – не менее 1 часа.

Основные технические характеристики устройства «МОЗАИКА»

Диапазон рабочих частот	869 – 960 МГц; 1805 – 1880 МГц
Мощность излучения	не более 100 мВт/диапазон
Радиус действия (зависит от расстояния до ближайшей базовой станции)	3 – 25 м
Питание изделия	– от сети 220 В; – от блока аккумуляторов
Потребляемая мощность	не более 8 ВА
Продолжительность работы изделия от полностью заряженного аккумулятора	не менее 1 часа.

Рекомендуемая литература

Основная

1. Основы информационной безопасности. Учебное пособие для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М: Горячая линия – Телеком, 2006. – 544 с.: ил.

2. Введение в специальность. Методические рекомендации студентам по выполнению лабораторных работ. – Ставрополь, Изд-во СГУ, 2006 – 50с.

Задания для развития и контроля владения компетенциями

1. Назначение анализатора поля «АРР-7».
2. Назначение универсального поискового прибора D008.
3. Устройство предотвращения утечки информации по каналам систем мобильной связи «Мозаика».
4. Основные режимы работы АРР-7
5. Основные технические характеристики АРР-7
6. Основные технические характеристики D008
7. Основные технические характеристики устройства «Мозаика»

III. Заключение

Подведение итогов занятия

По результатам собеседования с каждым студентом устанавливается степень усвоения ими программного материала и выставляется оценка.

Задание студентам для самостоятельной работы

1. Оформить отчет о лабораторной работе в соответствии с требованиями
2. Представить отчет для утверждения и защиты

Практическое занятие № 8

Тема: *«Демонстрация портативных средств защиты информации: комплекта для оценки каналов утечки информации «ПКУ-6», устройства информационной защиты телефонных линий «NG 305», телефонного проверочного устройства «ТПУ-7»».*

В результате настоящего занятия и последующей самостоятельной работы студенты **должны:**

знать: технические характеристик и возможности работы портативный диктофон OLYMPUS L140, миниатюрная камера КРС-400, акустический шумогенератор ANG-2000»

уметь: применять в своей практической деятельности портативный диктофон OLYMPUS L140, миниатюрная камера КРС-400, акустический шумогенератор ANG-2000»

владеть: навыками настройки, регулировки портативный диктофон OLYMPUS L140, миниатюрная камера КРС-400, акустический шумогенератор ANG-2000»

Формируемые компетенции или их части: ПК-5

I. Вступительная часть

Проверка наличия студентов	- 2 мин
Проверка готовности студентов к занятию.	- 3 мин

II. Учебные вопросы занятия:

1. Портативный диктофон OLYMPUS L140	- 55 мин
2. Миниатюрная камера КРС-400	- 55 мин
3. Акустический шумогенератор ANG-2000	- 60 мин

III. Заключение

Подведение итогов занятия	- 3 мин.
Задание студентам для самостоятельной работы	- 2 мин.

СОДЕРЖАНИЕ ЗАНЯТИЯ

Цель работы:

знать: методологию создания систем защиты информации;
перспективные направления развития средств и методов защиты информации;
технических характеристик и демонстрация работы:
комплекта для оценки каналов утечки информации «ПКУ–6», устройства информационной защиты телефонных линий «NG 305», телефонного проверочного устройства «ТПУ–7».

**Занятие проводится с использованием кафедрального
виртуального комплекса на базе программных эмуляторов**

Учебные вопросы

1. Комплект для оценки каналов утечки информации «ПКУ–6»
2. Устройство информационной защиты телефонных линий «NG 305»,
3. Телефонное проверочное устройство «ТПУ–7»

Приборы и принадлежности: комплект для оценки каналов утечки информации «ПКУ–6», устройство информационной защиты телефонных линий «NG 305», телефонное проверочное устройство «ТПУ–7».

Время, отводимое на занятие – 4 часа

Методические рекомендации

1. Комплект для оценки каналов утечки информации «ПКУ–6»

Теоретическая часть

«ПКУ–6» представляет собой портативную многофункциональную поисковую систему, предназначенную для обнаружения средств съема информации и выявления других каналов ее утечки.

При создании системы использованы богатый опыт разработки и использования подобных технических средств.

Система предназначена для выявления:

- средств съема информации с передачей сигнала по «легальным» проводным коммуникациям;
- утечки речевой информации по акустическому и вибро–акустическому каналам;
- средств съема информации с передачей сигнала по оптическому каналу;
- оценки магнитных и электрических полей, излучаемых техническими средствами обработки информации и соответствующими кабельными линиями.

Система обеспечивает:

- прием сигналов с амплитудой (АМ) и частотной (ЧМ) модуляцией в рабочем диапазоне частот $20 - 25 \times 10^6$ Гц;
- автоматическую перестройку в рабочем диапазоне частот;
- визуальное отображение спектров принимаемых сигналов на встроенном жидкокристаллическом дисплее;
- прослушивание принимаемого сигнала при помощи встроенного громкоговорителя или головных телефонов.

В состав системы входит комплект датчиков, позволяющих оценить:

- утечку акустической информации по вентиляционным каналам, имеющимся сквозным щелям, трещинам и нарушениям уплотнителей;
- вибро–акустические свойства ограждающих конструкций и инженерных коммуникаций;
- электрические сигналы в линиях силового и слаботочного электрооборудования в полосе 20 Гц – 24,5 МГц;
- оптическое излучение осветительных приборов, индикаторов, датчиков сигнализации, блоков дистанционного управления в видимом и инфракрасном (ИК) диапазонах.

Основные режимы работы прибора:

АТТ – включение аттенюатора – 40 dB.

15 V – подача постоянного напряжения ± 15 V в проверяемую линию.

BAND – ввод начальной и конечной границ диапазона сканирования.

OSC – осциллографическое представление сигнала в режиме RF.

[←] или [→] – кнопки многофункциональные, которые могут использоваться вместо Ручки настройки.

AM/FM – переключатель вида модуляции.

ENTER – подтверждение введенной частоты настройки

Состав комплекта:

- Основной блок – анализатор
- Микрофон
- Вибро–электрический преобразователь
- Оптический датчик видимого и инфракрасного диапазонов
- Головные телефоны
- Входной сетевой кабель
- Съёмные зажимы и щупы
- Имитатор многофункциональный.

Основные технические характеристики основного блока ПКУ–6:

Основной блок

Диапазон частот, Гц	20 – 24,5×10 ⁶
Чувствительность, мкВ	
в диапазоне 20 – 20000 Гц	не хуже 50
в диапазоне 0,02 – 25 Гц	не хуже 30
Точность измерения частоты, кГц	±2

Разрешающая способность

спектроанализатора, кГц	0,3
-------------------------	-----

ИМФ–1 – Имитатор многофункциональный

Имитатор ИМФ–1 многофункциональный, поставляемый в составе системы ПКУ–6 предназначен для имитации работы средств съема информации в ходе проведения поисковых мероприятий.

Кроме того, имитатор может использоваться для проверки работоспособности таких поисковых приборов, как ИПФ–6, ПКУ–6, ТПУ–7, ППЛ–2, а также оценки достаточности мер защиты, обеспечиваемых приборами Соната–АВ, Соната–С2, спектр, NG–305Т.

Символы и номера режимов работы Имитатора ИМФ–1

- 2 – «WIRE» – Проводной низкочастотный генератор
3 – «RADIO» – Генератор электромагнитного излучения
4 – «IR-LIGHT» – Инфракрасный излучатель

Основные технические характеристики ИМФ–1 имитатора многофункционального:

Озвучивающее устройство (для ПКУ–6):

меняющийся тон, кГц	1/3,5
звуковое давление, дБ	74

Проводной низкочастотный генератор
(для ПКУ–6):

рабочая частота, кГц	260 (365)
модуляция	ЧМ
девиация, кГц	30

Генератор электромагнитного
излучения (для АПП–7):

рабочая частота, МГц	400
модуляция	ЧМ/АМ
девиация, кГц	30

ИК–излучатель (для ПКУ–6):

поднесущая частота, кГц	260
модуляция	ЧМ/АМ
девиация, кГц	30

Имитатор телефонного передатчика (для АПП–7):

рабочая частота, МГц	400
модуляция	ЧМ
девиация, кГц	50

2. Устройство информационной защиты телефонных линий «NG 305»

Теоретическая часть

Общие сведения. Устройство и назначение

Изделие является комплексным устройством защиты информации. Оно обеспечивает:

- защиту телефонных переговоров от прослушивания всеми известными средствами добывания акустической информации, включаемыми в телефонную линию последовательно или параллельно с помощью как контактных, так и индукционных датчиков;

- блокировку несанкционированного использования параллельного телефонного аппарата;

- сигнализацию о «пиратском» подключении к телефонной линии.

Основные технические характеристики «NG 305»

Защита телефонных переговоров и помещения от прослушивания осуществляется путем формирования и подачи в каналы связи специальных шумовых маскирующих сигналов, обеспечивающих:

Отношение сигнал/шум в устройстве прослушивания – не хуже минус 20 дБ

Отношение сигнал/шум в телефонном аппарате (ТА) – не менее 14 дБ

Электропитание изделия осуществляется от сети переменного тока напряжением $220\text{ В} \pm 10\%$

Потребляемая мощность – не более 15 Вт.

Функционально изделие состоит из 4-х модулей:

- генератора помех SN, предназначенного для подавления последовательных телефонных передатчиков и индукционных датчиков;

- генератора помех PN, предназначенного для подавления параллельных телефонных передатчиков и аппаратуры магнитной записи;

- модуля ZL, обеспечивающего подавление телефонных передатчиков, питающихся от телефонной линии и работающих при снятой трубке;

- модуля BL, обеспечивающего сигнализацию несанкционированного подключения параллельного телефона и блокировку его работы.

3. Телефонное проверочное устройство ТПУ–7

Общие сведения. Устройство и назначение

Телефонное проверочное устройство ТПУ–7 предназначено для обнаружения в телефонных линиях, без отключения от АТС, гальванических подключений цепей съема, передачи и питания средств съема информации. ТПУ–7 работает с телефонными линиями городских и местных АТС различных стандартов, а также с проводными линиями, свободными от источников питания и нагрузок.

ТПУ позволяет обнаружить и идентифицировать:

- 1) высокочастотные сигналы в диапазоне частот 20 – 10000 кГц напряжением от 10 мВ и выше;
- 2) последовательные подключения с сопротивлением от 50 Ом и выше;
- 3) параллельные подключения с потреблением от незанятой телефонной линии тока более 0,3 мА;
- 4) параллельные подключения с потреблением от занятой телефонной линии тока более 0,5 мА;
- 5) параллельное подключение высокоомных цепей с сопротивлением до 50 Мом;
- 6) высокоомные цепи с сопротивлением до 50 Мом, параллельно подключенные к линии через разделительный конденсатор.

ТПУ имеет несколько дополнительных режимов:

- аудиоконтроль низкочастотных сигналов от встроенных микрофонов;
- постоянный автоматический контроль телефонных линий;
- поиск трассы и места подключения цепей;
- включение/выключение подсветки ЖКИ;
- включение/выключение звука нажатия на кнопки клавиатуры;
- включение/выключение автоматическое определение типа АТС.

Порядок подключения телефонного проверочного устройства ТПУ–7:

Перед проведением измерений необходимо отключить от проверяемой телефонной сети все телефонные аппараты и другие устройства!

Необходимо соблюдать следующие меры безопасности

- Перед подключением ТПУ в сеть убедитесь в исправности шнура питания, вилки и розетки.
- Подключайте ТПУ к телефонной линии только после подключения к сети 220 В и проверки работоспособности устройства.
- Не допускается эксплуатация ТПУ в помещениях с повышенной влажностью воздуха.
- Запрещается при включенном в сеть ТПУ одновременно касаться выходных контактов соединительного телефонного провода и предметов,

имеющих естественное заземление (трубы отопления, водопроводные трубы, оголенные контакты телефонной сети и т.п.).

- Не рекомендуется длительно (более 2 часа) эксплуатировать ТПУ во включенном состоянии.

Питание ТПУ необходимо осуществлять непосредственно от сети 220 В, исключая различного рода устройства, такие как сетевые фильтры, разделительные трансформаторы, устройства бесперебойного питания и т.п.

Подключение к телефонной розетке ТПУ вилку соединительного телефонного шнура, ответную вилку которого подключите к розетке телефонной линии. При отсутствии подходящей телефонной розетки воспользуйтесь телефонным адаптером. При необходимости подключения непосредственно к линии, воспользуйтесь контактами типа «крокодил».

Отключение ТПУ, после проведения измерений, производите в обратной последовательности – сначала телефонную линию, затем сеть 220 В.

Порядок пользования устройством ТПУ–7

После подключения сетевого напряжения на ЖКИ в течение непродолжительного времени выводится заставка, содержащая следующую информацию: название устройства, название фирмы–изготовителя, номер версии программного обеспечения, месяц и год изготовления.

После заставки производится самотестирование устройства. Если тест завершается без ошибок, то на экран выводится сообщение Ок! Если в процессе тестирования будут выявлены ошибки, то выводится сообщение о кодах ошибок.

После тестирования на экран выводится изображение основного меню программы управления устройством, которое в зависимости от напряжения в исследуемой линии может выглядеть по–разному. Например для стандартной линии городской АТС основное меню программы может иметь следующий вид:

НДА 1234 Ул = 62.3 В

Автоматическая проверка

◀▶ Выбор Ent Ввод

Первая строка меню всех уровней используется для размещения выбираемых пунктов меню, вспомогательной информации (напряжение в линии или режим работы линии), результатов измерения и величин допустимых значений. Вторая и третья строки используются для ввода пояснительной информации. Четвертая строка используется для вывода информации о назначении клавиш управления.

Выбор требуемого пункта меню производится с помощью кнопок ◀▶, обеспечивающих передвижение влево / вправо по первой строке мигающего курсора. Вторая и третья строки содержат поясняющую информацию. Вход в подменю или запуск процесса измерения производятся кнопкой Ent.

Назначение пунктов основного меню:

Н – вход в подменю настроек устройства (п. 6.5);

Д – вход в подменю дополнительных режимов (п. 6.4);

А – запуск режима автоматической проверки линии (п. 6.3);

1234 – (возможно 12, для мини–АТС и электронных городских АТС при включенном автоопределении АТС, или 56, для свободных от напряжения линий) – номера возможных для подключенной линии режимов проверки;

После включения устройства или изменения состояния линии курсор устанавливается на пункте автоматическая проверка.

Порядок проведения измерений

Возможные режимы проверки:

1. наличие в линии сигнала высокой частоты;
2. наличие последовательно подключенных цепей;
3. наличие параллельно подключенных цепей, работающих от напряжения свободной линии (при ожидании вызова);
4. наличие параллельно подключенных цепей, работающих от напряжения занятой линии (при снятой трубке тел. Аппарата);
5. наличие высокоомных, параллельно подключенных цепей;
6. наличие высокоомных цепей, параллельно подключенных через конденсатор.

После выполнения измерения на первую строку экрана выводятся результат измерения (после строки Изм:) и допустимое значение (после строки Доп: и знака > или <).

Измерение можно повторить, нажав кнопку ◀ или ▶, или возвратиться в основное меню программы с помощью кнопки Ent.

Если результат измерения превышает допустимое значение, то прозвучит предупреждающий сигнал в виде короткой трели.

Рекомендуемая литература Основная

1. Основы информационной безопасности. Учебное пособие для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М: Горячая линия – Телеком, 2006. – 544 с.: ил.

2. Введение в специальность. Методические рекомендации студентам по выполнению лабораторных работ. – Ставрополь, Изд-во СГУ, 2006 – 50с.

Задания для развития и контроля владения компетенциями

1. Назначение комплекта для оценки каналов утечки информации «ПКУ–6».

2. Назначение устройства информационной защиты телефонных линий «NG 305»,

3. Назначение телефонного проверочного устройства «ТПУ–7».

4. Основные режимы работы ПКУ-6

5. Основные технические характеристики ПКУ-6

7. Основные технические характеристики NG-305

8. Основные режимы работы ТПУ-7

III. Заключение

Подведение итогов занятия

По результатам собеседования с каждым студентом устанавливается степень усвоения ими программного материала и выставляется оценка.

Задание студентам для самостоятельной работы

1. Оформить отчет о лабораторной работе в соответствии с требованиями
2. Представить отчет для утверждения и защиты

Практическое занятие № 9

Тема: «Изучение возможных деструктивных воздействий на информацию в компьютерных системах»

В результате настоящего занятия и последующей самостоятельной работы студенты **должны:**

знать: технические характеристик и возможности работы портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

уметь: применять в своей практической деятельности портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

владеть: навыками настройки, регулировки портативный диктофон OLYMPUS L140, миниатюрная камера KPC-400, акустический шумогенератор ANG-2000»

Формируемые компетенции или их части: ПК-5

I. Вступительная часть

Проверка наличия студентов - 2 мин

Проверка готовности студентов к занятию. - 3 мин

II. Учебные вопросы занятия:

1. Портативный диктофон OLYMPUS L140 - 55 мин

- | | |
|--|----------|
| 2. Миниатюрная камера КРС-400 | - 55 мин |
| 3. Акустический шумогенератор ANG-2000 | - 60 мин |

III. Заключение

- | | |
|--|----------|
| Подведение итогов занятия | - 3 мин. |
| Задание студентам для самостоятельной работы | - 2 мин. |

СОДЕРЖАНИЕ ЗАНЯТИЯ

Цель работы:

знать: методологию создания систем защиты информации;
перспективные направления развития средств и методов защиты информации;
возможные деструктивные воздействия на информацию, а также сертификационные требования, предъявляемые к компьютерным системам

Занятие проводится с использованием кафедрального виртуального комплекса на базе программных эмуляторов

Учебные вопросы

1. Изучение возможных деструктивных воздействий на информацию в компьютерных системах
2. Изучить сертификационные требования, предъявляемые к компьютерным системам

Методические рекомендации **Теоретическая часть**

В последние годы стала усиленно развиваться одна из ветвей информационного терроризма, о которой еще с десятков лет назад никто и не задумывался, — это так называемый электромагнитный терроризм. Применяя его, террористы могут без лишнего шума воздействовать на технические системы

государственного и военного управления и объекты инфраструктуры.

Благодаря активному развитию современных информационных технологий и систем безопасности появилась не только возможность успешно решать задачи обеспечения безопасности личности, объектов и информации, но и возникли новые проблемы. Одна из этих проблем — защита самих систем от силового разрушающего воздействия.

Современные технические средства силового разрушающего или поражающего (деструктивного) воздействия являются по существу электромагнитным оружием, которое способно дистанционно и без лишнего шума поразить практически любую информационную систему.

Главное в этом случае — обеспечить соответствующую мощность электромагнитного импульса, воздействующего на систему по трем основным каналам:

сети питания;

проводным линиям связи;

эффиру с использованием мощных коротких электромагнитных импульсов.

Простейшим примером мощного электромагнитного импульса является обычное и привычное для всех нас природное явление — молния. Это естественный электромагнитный импульс, воздействующий на различные радиоэлектронные устройства. Поскольку мы рассматриваем в основном преднамеренные деструктивные воздействия на элементы компьютерных сетей, то остановимся более подробно на рассмотрении электромагнитных импульсов искусственного происхождения.

На сегодняшний день уже разработаны специальные виды «электромагнитного оружия», способные генерировать электромагнитные импульсы огромной мощности, значительно превышающей электромагнитные импульсы, возникающие при ядерном взрыве. Такое оружие производится в виде боеголовок для ракет, бомб, специальных «высокочастотных пушек» и т. п. Для генерации поражающих электромагнитных импульсов созданы компактные, мобильные и одновременно мощные устройства.

Для поражения гражданских объектов вполне может быть достаточно воздействия электромагнитных импульсов сравнительно небольшой мощности. Технические средства, с помощью которых они получаются, носят название технических средств силового деструктивного воздействия. В Internet можно встретить подробные руководства, по созданию установок для генерации электромагнитных импульсов с целью поражения компьютеров, компьютерных сетей и другого электронного оборудования. Необходимые комплектующие можно купить в обычных магазинах. С помощью таких устройств можно, например, вывести из строя компьютер соседа, находящийся за стеной. Есть устройства, размещающиеся в обычном кейсе, которые способны вывести из строя 10—20 компьютеров среднего банка. Более мощные установки можно поместить в фургоне автомобиля. Стоимость таких устройств, в зависимости от их конструкции, размеров и мощности, составляет от 300 до 20 000 долларов. Такие суммы по карману даже террористу-одиночке.

Последствия же электромагнитного терроризма могут быть самыми чудовищными. Скрытность применения технических средств деструктивного

воздействия, компактность, высокая проникающая способность и эффективность действия, делают их идеальными орудиями преступления в руках террористов и других злоумышленников.

Эти средства могут быть использованы, например, для уничтожения компьютерной сети банка, в котором деньги предварительно были похищены хакерами. Они позволяют обеспечить беспрепятственное проникновение на охраняемый объект, преднамеренно разрушив систему охранной сигнализации или блокировав ее работу.

Такого рода «электронный ракет» для предприятий с большой долей электронного документооборота может оказаться гораздо опаснее, нежели традиционные приемы, применяемые криминальными структурами.

В отличие от других способов уничтожения информации, оборудования или методов проникновения на охраняемый объект, применение технических средств деструктивного воздействия требует существенно меньших интеллектуальных, а нередко и материальных затрат. Кроме того, последствия от такой атаки на объект могут быть отнесены пострадавшими на обычные нарушения функционирования объекта, например, нарушения в сети электропитания объекта.

Сертификационные требования для компьютерных систем

В Нашей стране и за рубежом все компьютеры и другая электронная техника проходят тестирование на предмет их правильного функционирования в сложных условиях электромагнитной обстановки. ГОСТ 29073-91 («Совместимость технических средств измерения, контроля и управления промышленными процессами электромагнитная. Устойчивость к электромагнитным помехам. Общие положения») устанавливает общие требования к техническим средствам в соответствии со стандартом МЭК 801 по устойчивости к воздействию электромагнитных помех (помехоустойчивость) следующих видов:

- электростатических разрядов;
- наносекундных и микросекундных импульсных помех;
- радиочастотных электромагнитных помех;
- динамических изменений напряжения сети электропитания.

Согласно этому документу, технические средства должны сохранять работоспособность в условиях эксплуатации при воздействии электромагнитных помех, создаваемых промышленным оборудованием различного назначения, сетью электропитания, молниями и электростатическими разрядами. Все Испытания проводят во время функционирования технических средств, а для качественной оценки используются показатели, представленные в табл. 1.

Таблица 1. Критерии качества функционирования технических средств

Критерии качества функционирования технических средств	Качество функционирования технических средств при испытаниях на помехоустойчивость
--	--

при испытаниях на помехоустойчивости	
A	Нормальное функционирование в соответствии с техническими условиями
B	Кратковременное нарушение функционирования или ухудшение параметров с последующим восстановлением нормального функционирования без вмешательства оператора
G	Кратковременное нарушение функционирования или ухудшение параметров, требующее для восстановления нормального функционирования вмешательства оператора
D	Нарушение функционирования или ухудшение параметров, требующее ремонта из-за выхода из строя оборудования или компонентов

Другой руководящий документ — ГОСТ 29191-91 (МЭК 801-2 — 88) «Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Технические требования и методы испытаний» — относится к группе государственных стандартов, регламентирующих устойчивость технических средств к электромагнитным помехам различного вида. Он подразделяет технические средства по степени жесткости испытаний (табл. 2) в зависимости от испытательного напряжения.

Таблица 2. Значения испытательного напряжения по степени жесткости

Степень жесткости	Испытательное напряжение, кВ	
	Контактный разряд	Воздушный разряд
1	2	2
2	4	4
3	6	8
4	8	15
5	По согласованию между потребителем и производителем	

Основной целью стандарта ГОСТ 29156-91 (МЭК 801-4-88) «Совместимость технических средств электромагнитная. Устойчивость к наносекундным импульсным помехам. Технические требования и методы испытаний» является установление общих методов оценки качества функционирования технических средств при воздействии наносекундных импульсных помех на цепи силового электропитания и цепи ввода вывода. Согласно этому документу, для испытаний устанавливаются степени жесткости, которые представлены в табл. 3.

Таблица 3. Степени жесткости по устойчивости технических средств к воздействию импульсных помех

Степень жесткости	Амплитуда импульсов ненагруженного испытательного генератора	выходного напряжения
	Цепь силового электропитания, кВ	Сигнальные цепи ввода/вывода, кВ
1	0,5	0,25
2	1,0	0,5
3	2,0	1,0
4	4,0	2,0
5	По согласованию между потребителем и производителем	

Как видно из табл. 3, степень жесткости 1 устанавливается для очень хорошей электромагнитной обстановки. Для данной степени жесткости в лабораториях испытания ограничивают воздействием коротких импульсных помех на цепи электропитания, а в условиях эксплуатации — воздействием на цепи заземления проверяемых технических средств.

Степень жесткости 2 устанавливается для хорошей электромагнитной обстановки. Примером условий, соответствующих этой степени жесткости, может служить электромагнитная обстановка в помещении для средств измерения, контроля и управления в промышленном или энергетическом предприятии.

Степень жесткости 3 устанавливается для промышленной электромагнитной обстановки. Примером условий, соответствующих степени жесткости 3, может служить электромагнитная обстановка на предприятиях энергетики и в релейных помещениях в подстанциях воздушных линий высокого напряжения.

Степень жесткости 4 устанавливается для тяжелой электромагнитной обстановки. Примером условий, соответствующих степени жесткости 4, может служить электромагнитная обстановка силовых подстанций, коммутационного оборудования воздушных линий высокого напряжения, газонаполненных переключателей на напряжение $U > 500$ кВ.

Степень жесткости 5 устанавливается для специальных условий эксплуатации технических средств по согласованию между потребителем и производителем.

ГОСТ 30374-95/ГОСТ Р 50007-92 — еще один стандарт, устанавливающий технические требования к степени жесткости испытаний и методы испытаний на устойчивость к микросекундным импульсным помехам большой энергии, образуемым в цепях электропитания переходными процессами от молниевых разрядов и различного рода переключений.

В зависимости от условий эксплуатации технических средств, этот документ устанавливает технические требования для нескольких степеней жесткости. Согласно этим требованиям, технические средства должны сохранять работоспособность в условиях эксплуатации при воздействии на цепи электропитания микросекундных импульсных помех в виде молниевых разрядов и коммутационных переходных процессов.

В отличие от предыдущих, рассматриваемый ниже стандарт ГОСТ 30375-95/ГОСТ Р 50008-92 регламентирует испытания, обеспечивающие защиту технических средств от высокочастотных помех.

ГОСТ 29216—91 («Радиопомехи промышленные от оборудования ин-

формационной техники. Нормы и методы испытаний») распространяется на оборудование информационной техники и устанавливает нормы и методы измерений промышленных радиопомех в полосе частот 0,15—1000,0 МГц.

По этому документу оборудование информационной техники подразделяют на два класса: А и В. К классу А относятся технические средства, которые эксплуатируют вне жилых зданий и не подключают к электросетям жилых зданий. Технические средства класса В эксплуатируют в жилых зданиях или подключают к электросетям этих зданий.

Как видно из приведенных выше документов, аппаратура информационных сетей с точки зрения сертификационных требований для 3 и 4 группы жесткости испытаний должна выдержать (данные для четвертой группы указаны в скобках):

одиночный импульс по цепям питания, ввода/вывода и корпуса с амплитудой тока 30 А в начальный момент, длительность пика 0,7—1,0 не, и далее 16 А в течение 60 не. (амплитуда импульса при контактном разряде емкости 6(8) кВ, а при воздушном разряде — 8(15) кВ);

пачки импульсов через емкостную связь, каждый из которых имеет в начальный момент длительность пика 5 не, общей длительностью до 50 не (амплитуда импульса 2(4) кВ по цепям питания и корпуса и 1(2) кВ по цепям ввода/вывода и корпуса);

не менее пяти импульсов с амплитудой 2(4) кВ через индуктивно-емкостную связь с длительностью фронта 1 мс и длительностью 50 мс по цепям питания и заземления.

Классификация воздействий основана на физике процессов и среды доставки энергии. Малые по энергетике наносекундные воздействия получаются из статического разряда и коммутационных помех по коммуникациям. Сильные воздействия оказывают в основном грозовые разряды и переходные процессы, связанные с коммутацией силовых цепей, особенно при срабатывании устройств защиты. К сожалению, это воздействие не рассматривается для кабельных информационных коммуникаций, а грозой «убита» не одна сотня видеокамер, модемов и прочего оборудования.

Выбор группы зависит от размещения технических средств (ТС) и их проводных коммуникаций. Компьютеры могут быть отнесены как к 3-й так и к 4-й группе жесткости, в зависимости от их назначения, производителя, наличия информационных коммуникаций. Домашний компьютер может быть отнесен ко 2-й группе, а что происходит в реальной жизни, к сожалению, неизвестно, особенно в случае закупки оборудования по принципу минимальной цены.

В случае с преднамеренными силовыми воздействиями не важна достоверность сертификата. Наоборот, он даже помогает определить необходимое силовое воздействие. Технология проста: берется класс исполнения технического средства, увеличивается в несколько раз энергетика (амплитуда, длительность и т. д.), по сравнению с указанными в ГОСТах, и можно атаковать противника. В этом случае для защиты техники нужно повысить класс устойчивости, добавить устройства защиты и не допускать «ближних контактов», чтобы сделать максимально бессмысленным применение средств создания преднамеренных силовых воздействий по коммуникациям.

Рекомендуемая литература

Основная

1. Основы информационной безопасности. Учебное пособие для вузов/ Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М: Горячая линия – Телеком, 2006. – 544 с.: ил.

2. Введение в специальность. Методические рекомендации студентам по выполнению лабораторных работ. – Ставрополь, Изд-во СГУ, 2006 – 50с.

Задания для развития и контроля владения компетенциями

1. Компьютерная система как объект информационной безопасности.

2. Методы оценки защищенности компьютерных систем от НСД.

3. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

3. Общие критерии, применяемые в США.

4. Общие критерии, применяемые в РФ.

5. Классификация и возможности технических разведок.

6. Компьютерная разведка, ее объекты и содержание.

7. Технические каналы утечки информации при эксплуатации АС.

8. Методы защиты информации, обрабатываемой в автоматизированных системах, от технических разведок.