ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Томский государственный университет систем управления и радиоэлектроники
(ТУСУР)

Кафедра радиоэлектроники и защиты информации
(РЗИ)

УТВЕРЖДАЮ
Зав.каф. РЗИ
_____ А.С. Задорин
10 апреля 2007 г.

КОНТРОЛЬ ТЕЛЕФОННЫХ ЛИНИЙ И ЦЕПЕЙ ЭЛЕКТРОПИТАНИЯ НА ОТСУТСТВИЕ ЗАКЛАДНЫХ УСТРОЙСТВ

Руководство к практическим занятиям и лабораторным работам по курсам «Инженерно-техническая защита информации» и "Технические средства защиты информации" для студентов специальностей 075300, 075400, 075500, 075600

Разработчик:

Старший преподаватель каф. РЗИ, к.т.н.
«___» _____ Р.С. Круглов

2007

Содержание

Введение

Инженерно-техническая защита информации – одна из основных компонент комплекса мер по защите информации, составляющей государственную, служебную, коммерческую и личную тайну [1]. Этот комплекс включает нормативно-правовые документы, организационные и технические меры, направленные на обеспечение безопасности секретной и конфиденциальной информации. С возрастанием роли информации в обществе повышаются требования ко всем аспектам ее защиты и, прежде всего, к инженерно-технической защите.

Инженерно-техническая защита информации включает комплекс организационных и технических мер по обеспечению безопасности информации техническими средствами. Она решает следующие задачи:

1. Предотвращение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения.
2. Защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего, пожара и воды (пены) при его тушении.
3. Предотвращение утечки информации по различным техническим каналам.

Способы и средства решения первых двух задач не отличаются от способов и средств защиты любых материальных ценностей, третья задача решатся исключительно способами и средствами инженерно-технической защиты информации.

Целью данной лабораторной работы является изучение студентами способов и средств контроля телефонных линий и цепей электропитания, направленных на предотвращение утечки информации с помощью закладных устройств.

1 Принципы контроля телефонных линий и цепей электропитания

1.1 Основные методы прослушивания телефонных линий

Ценность информации, передаваемой по телефонным линиям, а также существующее убеждение о массовом характере прослушивания этих линий вызывает наибольшую обеспокоенность у организаций и частных лиц о сохранении конфиденциальности своих переговоров именно по телефонным каналам. Для защиты своих секретов необходимо знать методы, посредством которых могут быть выполнены операции по перехвату.

Можно выделить шесть основных зон прослушивания (рисунок 1.1) [2]:

- телефонный аппарат;
- линия от телефонного аппарата к распределительной коробке;
- кабельная зона;
- зона АТС;
- зона многоканального кабеля;
- зона радиоканала.

Наиболее вероятна организация прослушивания первых трех зон, потому что именно в них наиболее легко подключиться к телефонной линии. Специалисты, которые занимаются защитой информации, утверждают, что чаще всего используется прослушивание посредством параллельного аппарата. В большинстве случаев для этого даже не требуется прокладывать дополнительные провода: телефонная сеть настолько запутанная, что всегда есть неиспользуемые линии. Кроме того, нетрудно подключится в парадном к распределительной коробке.

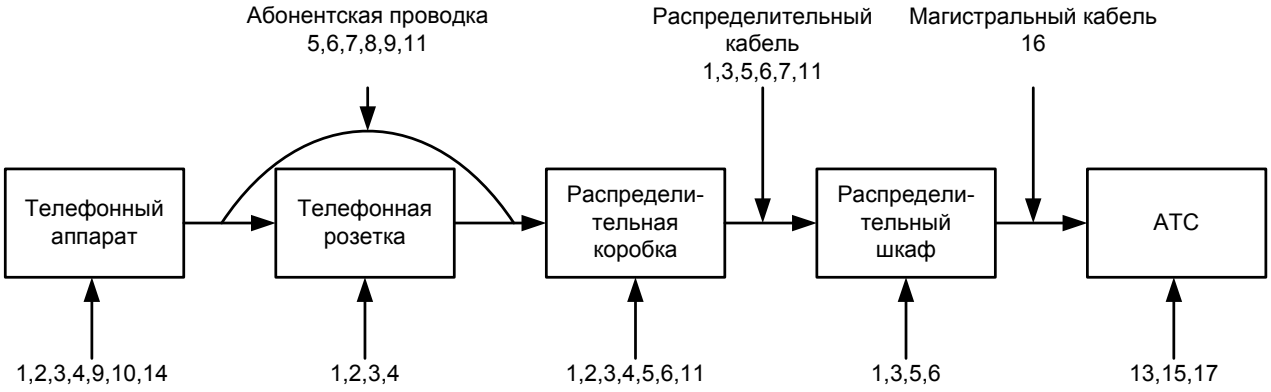

Рисунок 1.1 – Структурно-топологическая схема абонентской телефонной линии [2]

1 – радиозакладка параллельного подключения; 2 – комбинируемая телефонно-акустическая радиозакладка; 3 – радиозакладка последовательного подключения; 4 – закладка типа "длинное ухо"; 5 – низкоомный адаптер; 6 – высокоомный адаптер; 7 – бесконтактный адаптер; 8 – наводки телефонного сигнала на другие круги; 9 – акустоэлектрическое преобразование; 10 – ВЧ излучение схем телефонного сигнала; 11 – ВЧ навязывание; 12 – паразитные излучения усилителя; 13 – снятие информации на АТС; 14 – радиоизлучение телефонного удлинителя; 15 – перехват информации из линии связи; 16 – сложная высокочувствительная аппаратура; 17 – утечка информации на линиях отвода от АТС (вневедомственная охрана и т.п.)

Подключение в третьей зоне менее распространено, потому что необходимо проникать в систему телефонных коммуникаций, которая состоит из труб с проложенными внутри них кабелями, а также разобраться в этой системе и определить требуемую пару среди сотен других. Однако не следует считать, что это невыполнимая задача, поскольку необходимая для этого аппаратура уже существует [2].

В техническом плане самым простым способом является контактное подключение. Возможно временное подключение к абонентской проводке с помощью стандартной «монтерской трубки», однако подключение такого типа легко определяется посредством простейших средств контроля напряжения телефонной сети. Уменьшить эффект падения напряжения можно путем подключения трубки через резистор с сопротивлением 0,6-1 кОм. Подключение осуществляется с помощью очень тонких игл и тонких, покрытых лаком проводов, которые прокладываются в какой-либо существующей или изготовленной щели. Щель может быть зашпаклевана и окрашена так, что визуально определить подключение очень сложно.

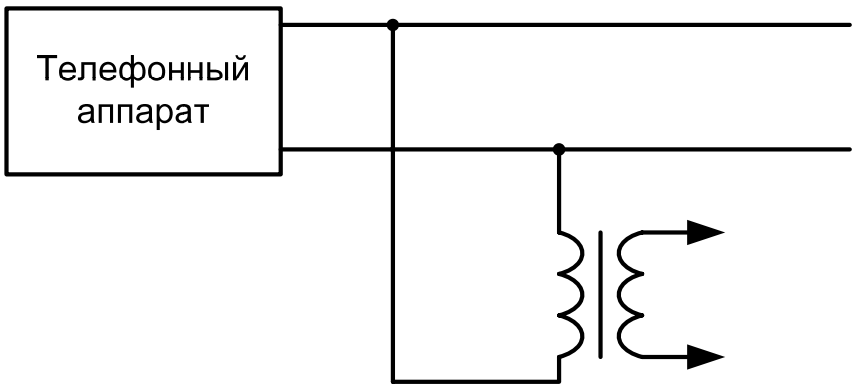

Рисунок 1.2 – Подключение с помощью согласующего устройства [3]

Наиболее удачным типом подключения является подключение с помощью согласующего устройства (рисунок 1.2).

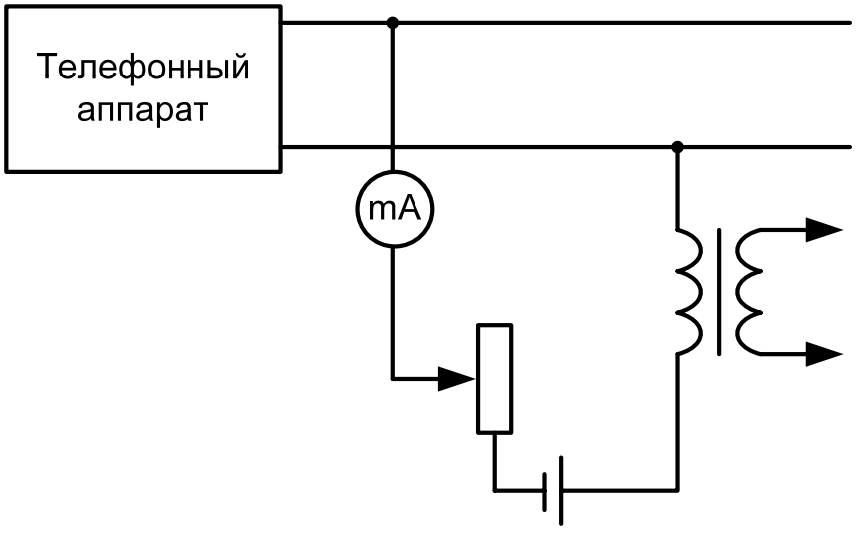

Рисунок 1.3 – Подключение с компенсацией падения напряжения [3]

Такой способ существенно снижает напряжение в телефонной сети и осложняет выявление факта прослушивания. Также существует способ

подключения к линиям связи аппаратуры с компенсацией падения напряжения (рисунок 1.3).

Существенными недостатками контактного способа подключения является нарушение целостности проводов и влияние подключенного устройства на характеристики линий связи. С целью устранения этого недостатка применяется индуктивный датчик, выполненный в виде трансформатора. Существуют также датчики, принцип работы которых основан на эффекте Холла.

1.2 Классификация средств обнаружения и локализации закладных устройств прослушивания телефонных линий

Способы контроля телефонных линий основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий: напряжения и тока в линии, значений емкости и индуктивности линии, активного и реактивного сопротивления. В зависимости от способа подключения подслушивающего устройства к телефонной линии (последовательного – в разрыв провода телефонного кабеля или параллельного) влияние подключаемого подслушивающего устройства может существенно отличаться. Так как закладное устройство использует энергию телефонной линии, величина отбора мощности закладкой из телефонной линии зависит от мощности передатчика закладки и его коэффициента полезного действия. Наилучшие возможности по выявлению этих отклонений существуют при опущенной трубке телефонного аппарата. Это обусловлено тем, что в этом состоянии в телефонную линию подается постоянное напряжение 60+10% В (для отечественных телефонных линий) и 25-36 В (для зарубежных АТС, мини-АТС). При поднятии трубки в линию поступают от АТС дискретный сигнал, преобразуемый в телефонной трубке в длинный гудок, а напряжение в линии уменьшается до 12 В [1]. Для контроля телефонных линий применяются следующие устройства:

- устройства оповещения световым и звуковым сигналом об уменьшении напряжения в телефонной линии, вызванном несанкционированным подключением средств подслушивания к телефонной линии;
- измерители характеристик телефонных линий (напряжения, тока, емкости, сопротивления и др.), при отклонении от которых формируется сигнал тревоги;
- «кабельные радары», позволяющие измерять неоднородности телефонной линии и определять расстояние до неоднородности (асимметрии постоянному току в местах подключения подслушивающих устройств, обрыва, короткого замыкания и др.).

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения с индикацией изменения его значения от номинального, которое фиксируется оператором в режиме настройки вращением регулятора на лицевой панели устройства. Предполагается, что при

установке номинального напряжения к телефонной линии подслушивающее устройство не подключено.

Но устройства контроля телефонной сети по изменению напряжения или тока в ней не обеспечивают надежного обнаружения подключаемых параллельно к линии современных средств подслушивания с входным сопротивлением более единиц МОм. Повышение реальной чувствительности устройств контроля ограничено нестабильностью параметров линии, колебаниями напряжения источников электропитания на АТС, помехами в линии. Для снижения вероятности ложных тревог в более сложных подобных устройствах увеличивают количество измеряемых характеристик линии, предусматривают возможность накопления и статистической обработки результатов измерений в течение достаточно длительного времени как контролируемой линии, так и близко расположенных.

Наиболее рациональным вариантом является совмещение в одном приборе функции обнаружения несанкционированного подключения к телефонной линии и противодействия подслушиванию. Активное противодействие осуществляется путем линейного зашумления телефонной линии.

2 Порядок выполнения работы

Перед выполнением задания студент обязан ознакомиться с правилами работы измерительного прибора, которые представлены в приложении А настоящего руководства.

1. С помощью генератора Г4-151 сымитировать сигнал закладного устройства, для этого установить частоту гармонического колебания соответствующую рабочему диапазону анализатора проводных линий; включить внутреннюю амплитудную модуляцию.
2. С помощью осциллографа проконтролировать параметры АМ сигнала. Амплитудное значение сигнала должно быть 0,1-0,15 В. Определить частоту моделирующего колебания.
3. Подключить анализатор проводных линий RRL – 002 к генератору. В режиме автоматического сканирования зафиксировать АМ сигнал. С помощью анализатора определить частоту сигнала F_c и сравнить ее с показаниями генератора. В отчет занести уровень детерминированного сигнала и его частотные параметры.
4. С помощью источника постоянного напряжения сымитировать телефонную линию в состоянии с положенной трубкой. Значение напряжение должно соответствовать напряжению, подаваемому **мини-АТС** (32 В). Значение напряжения проконтролировать с помощью вольтметра.
5. Произвести подключение к телефонной линии закладного устройства.
6. Подключить анализатор проводных линий RRL – 002 к телефонной линии. С помощью анализатора обнаружить имитатор закладного

устройства, установить его тип и принцип действия. Полученные результаты занести в отчет.

Список литературы

1. Торокин А. А. Основы инженерно-технической защиты информации. – М.: Издательство «Ось-89», 1998. – 336 с. – ISBN 5-86894-215-9.
2. Петраков А.В., Лагутин В.С. Защита абонентского телетрафика. – М.: Радио и связь, 2002. – 504 с.
3. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных системах. – К.: «МК-Пресс», 2005. – 288 с.
4. Куприянов А. И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А. И. Куприянов, А.В. Сахаров, В.А. Шевцов. – М.: Издательский центр «Академия». 2006. – 256 с. – ISBN 5-7695-2438-3.

Приложение А. Анализатор проводных линий RRL – 02

Анализатор проводных линий RRL-02 предназначен для контроля проводных линий (электросеть, телефонные линии, ОПС и т.д.) на наличие радиопередатчиков, работающих в низкочастотном диапазоне (10- 10 000 кГц). Прибор позволяет автоматически обнаруживать активные передатчики в любых двухпроводных линиях, демодулировать AM/FM сигналы и воспроизводить звук через встроенный громкоговоритель. Кроме того, прибор позволяет обнаруживать выносные микрофоны, работающих в НЧ диапазоне частот на любых двухпроводных линиях напряжением до 60 В. В комплект поставки входят внешние адаптеры для проверки сети переменного напряжения 220В, телефонных линий. Принцип работы прибора основан на сканировании диапазона частот. При обнаружении источника излучения, уровень которого превышает установленный пользователем, прибор останавливает сканирование и переходит в режим прослушивания сигнала на данной частоте. Уровень и частота обнаруженного источника сигнала высвечивает на ЖК-дисплее с подсветкой. Продолжение сканирования возобновляется пользователем, при нажатии на кнопки «+» или «-». Сканирование по частоте может осуществляться с шагом 1,25 кГц, 5,0 кГц. Прибор работает от внутренних Ni-Cd аккумуляторов.

Условия эксплуатации:

Прибор предназначен для работы внутри помещений

- при температуре 0...+55град;
- относительной влажности воздуха не более 98% при 25С без конденсации.

Основные технические характеристики

Диапазон рабочих частот, кГц	10-10000
Вид модуляции	AM/NFM
Чувствительность прибора (сигнал/шум 12 дБ), мВ	< 0,5
Шаг сканирования, кГц	1,25 / 5,00
Время сканирования при шаге 1,25 кГц, мин	< 5
Погрешность установки частоты, Гц	< 100
Динамический диапазон индикатора, дБ	> 40
Напряжение питания (от аккумулятора), В	4,8
Время работы от внутренних аккумуляторов емкостью 600 мА/ч, ч	> 3
Габаритные размеры, мм	180x150x55

Прибор имеет три режима работы:

- «Автоматическое сканирование» – сканирование всего рабочего диапазона частот с остановкой на сигнале, превышающем установленный уровень;
- «Ручное сканирование» – сканирование всего рабочего диапазона частот;

- «Проверка микрофона» – проверка наличия микрофона в любой двухпроводной линии напряжением до 60 В.

Внешний вид прибора RLL – 02, расположение органов управления и разъемов показаны на рисунке А.1.

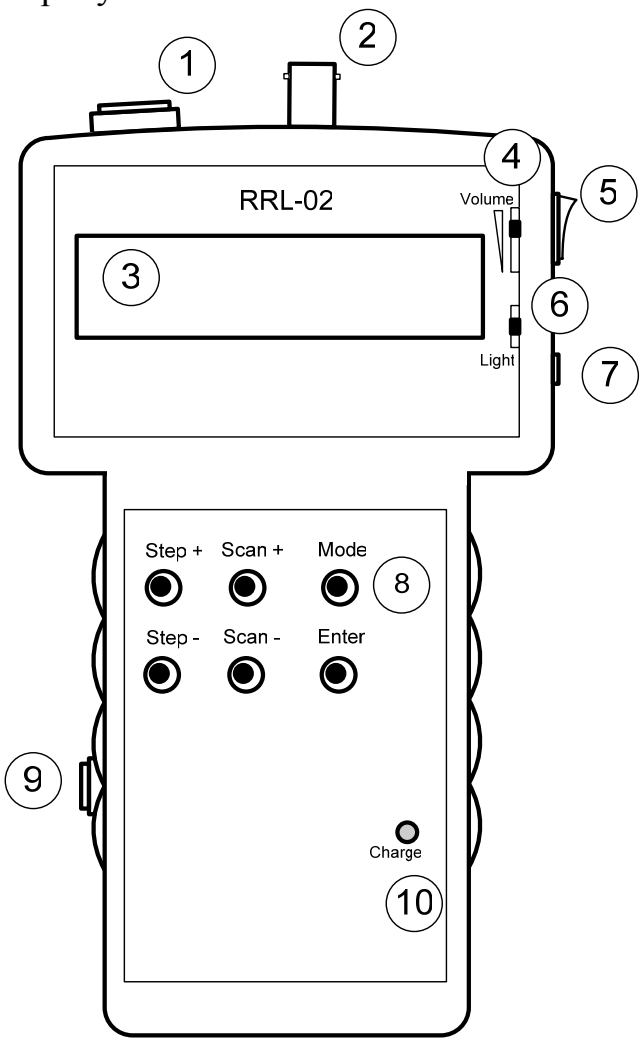

Рисунок А.1 – Внешний вид прибора RRL–02:

1 – разъем для подключения кабеля для проверки проводных коммуникаций с напряжением до 60В на наличие микрофонов работающих в НЧ диапазоне;
2 – разъем для подключения кабеля для проверки проводных коммуникаций на наличие передатчиков с АМ или NFM модуляций;
3 – жидкокристаллический индикатор, отображающий информацию о режимах работы прибора и состоянии процесса проверки;
4 – регулятор громкости демодулированного сигнала, поступающего на встроенный динамик или наушники;
5 – тумблер включения прибора;
6 – тумблер включения подсветки индикатора;
7 – разъем для подключения наушников;
8 – клавиатура управления прибором;
9 – разъем для подключения зарядного устройства;
10 – индикатор процесса зарядки.

Кнопки клавиатуры выполняют следующие функции:

- «Step+» – перестраивает приемник по частоте вверх в пределах рабочего диапазона на один шаг в соответствии с установленным шагом (5кГц по умолчанию);
- «Step–» – перестраивает приемник по частоте вниз в пределах рабочего диапазона на один шаг в соответствии с установленным шагом (5 кГц по умолчанию);
- «Scan+» – запускает приемник на санирование вверх по частоте в пределах рабочего диапазона частот. Если на индикаторе отображается, что уровень сигнала на данной частоте больше установленного порога прибор не переходит в режим сканирования. Для запуска прибора в режим сканирования необходимо кнопкой «Step+» перестроить его на свободный частотный участок или увеличить порог остановки;
- «Scan–» – запускает приемник на санирование вниз по частоте в пределах рабочего диапазона частот;
- «Mode» – предназначена для перевода приемника в режим настройки параметров;
- «Enter» – служит для выбора пункта меню для изменения режимов. В приемнике могут регулироваться следующие параметры: шаг перестройки по частоте (5 кГц или 1,25 кГц) тип модуляции (NFM или AM), переключение между входами приемника (проверка проводных коммуникаций на наличие низкочастотных передатчиков или проверка низковольтных цепей на наличие выносных микрофонов работающих в низкочастотном диапазоне) установка значения порога остановки сканирования.