САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ

МОРСКОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ МОРСКОГО ПРБОРОСТРОЕНИЯ

Кафедра №50

КУРСОВОЙ ПРОЕКТ

УСТРОЙСТВО ЗАПРЕТА ТЕЛЕФОННОЙ СВЯЗИ

ПО ЗАДАННЫМ НОМЕРАМ

{п.5 и п.6 неверно}

ВЫПОЛНИЛ:

СТУДЕНТ ГРУППЫ 34РК1

СУХАРЕВ Р.М.

ПРОВЕРИЛ:

доцент к.т.н.

ФИЛИМОНОВ А.К.

#### САНКТ-ПЕТЕРБУРГ

2000

СОДЕРЖАНИЕ

1. Введение 3

2. Техническое задание 9

3. Устройства пассивной и активной технической защиты 10

3.1. Способы получения информации о подключении 10

3.2. Совмещенный индикатор подключения и обрыва телефонной линии 12

3.3. Световой индикатор с автоматическим отключением 12

3.4. Счетчик времени разговора 13

3.5. Устройство криптографической защиты информации 14

4. Назначение, принцип действия и функциональная схема 25

5. Принципиальная электрическая схема 27

6. Конструкция лабораторного макета (печатная плата) 29

Список использованных источников 30

# 1. Введение

Огромное влияние на системный анализ проблем противодействия самовольному коммерческому использованию телефонных линий оказала теория и многолетняя практика радиоэлектронной борьбы (РЭБ) в ВС.

С введением в большинстве городов повременной оплаты за телефонные услуги, эта проблема чрезвычайно обострилась. Для некоторых абонентов 40-50% оплаты за телефон приходится на так называемых "пиратов" (от греческого peirates - грабитель, разбойник, морской разбойник).

Сейчас уже невозможно точно определить то время, когда появились первые случаи самовольного или т.н. "пиратского" подключения к телефонным линиям с целью проведения дорогостоящих разговоров без соответствующей оплаты. Очевидно, это произошло практически одновременно с развертыванием первых общенациональных телефонных сетей в начале XX века. С большой вероятностью можно утверждать, что и в те времена находились люди, которые эпизодически или постоянно пользовались телефоном бесплатно. Другое дело, что отсутствие поминутного учета разговоров и суммарная абонентская плата, взимаемая с владельцев отдельных номеров, не позволяли нанести существенный финансовый урон как телефонным компаниям, так и отдельным гражданам. Автоматизация телефонных станций, возможность установления связи по всему миру, высокие тарифы на услуги связи, все это привело к тому, что на рубеже XXI века проблема финансового обеспечения связи чрезвычайно обострилась. В периодической печати описано множество случаев, когда действия махинаторов приводили к значительным финансовым потерям.

Приведу лишь несколько возможных примеров.

В офис Вашей фирмы приходит посетитель с пакетом документов по торговому сотрудничеству. Пока происходит ознакомление с документами, он просит позвонить по телефону и некоторое время с кем-то разговаривает. После его ухода, не позднее конца месяца Вы получаете счет с телефонной станции за разговор с .... Впрочем, это уже дело его фантазии. Документы, разумеется, фиктивные.

За рубежом, где некоторые телефонные компании устанавливают плату за входящую связь, данный посетитель мог бы "перекачать" некоторую сумму с вашего счета непосредственно на свой (счет фирмы - владельца номера, куда он звонил). Хорошо еще, что до нас подобная автоматизация перевода денег еще не дошла (или дошла в ограниченном масштабе).

Второй случай для нас более реален.

Некто, арендовав квартиру в центре города, за месяц успевает обзвонить все соседние страны и благополучно съезжает до выставления счета за телефонные разговоры.

Известен случай, когда мошенники, арендовав квартиру, установили в ней радиотелефон и, работая на "выезде", в машине у переговорного пункта, предлагали всем желающим за "половинные" расценки воспользоваться междугородним телефоном.

И, наконец, на бытовом уровне, все знают про рекламу интимных услуг по телефону, в сети которой попадаются дети и доверчивые простаки. Счет на оплату разговоров может стать неподъемным для семьи.

Во всех таких случаях, администрация линейных узлов связи требует погасить возникшую задолженность, обещая в виде санкций отключение телефона.

Все эти проблемы можно если не устранить вообще, то значительно облегчить, если в полной мере ознакомиться с теорией и практикой "Противодействия Самовольному Коммерческому Использованию Телефонных линий".

***Способы подключения к линии***

Для того, чтобы рассмотреть все возможные места подключения к телефонной линии, представим себе упрощенную схему линии связи приведенную на Рис.1.

На схеме показана распределительная коробка, к которой подключены четыре пары:

* радиотелефон;
* таксофон;
* обычный телефонный аппарат;
* встроенное устройство имитации сигналов АТС.

Необходимо уточнить, что анализ возможных подключений проводится исключительно в "последней миле" телефонных коммуникаций, т.е. на участках шлейфа, в которых информация передается в аналоговой форме.

Стационар-ный блок р/телефона

Переносной блок р/телефона

 Зона радиоканала

Распределительная коробка

 шлейф

Таксофон

шлейф

Телефон-ный аппарат (факс, модем)

АТС

 шлейф

шлейф

Телефон-ный аппарат (факс, модем)

Имитатор сигналов АТС

Пиратский ТА

Рис.1. Схема линии связи

Из этой схемы видно, что можно выделить пять основных зон пиратского подключения:

* телефонный аппарат (таксофон);
* линия от телефонного аппарата, включая распределительную коробку;
* кабельная зона (шлейф АТС);
* зона АТС (машинный зал);
* зона радиоканала радиотелефона.

В этих зонах подключение с целью коммерческого использования линии наиболее вероятно.

На Рис.2 показаны ожидаемые способы подключения.

*Кратковременное подключение.*

Характеризуется малым временем контакта пиратского ТА с линией в точке подключения. Как правило, наблюдаются единичные случаи использования различных телефонных аппаратов или линий с отсутствием или незначительной маскировкой мест подключения.

Достаточно хорошо поддаются выявлению и предупреждению и, в условиях длительной эксплуатации ТА (например, в течении года), в суммарном выражении, не наносят значительного финансового ущерба.

Возможные способы использования линии (кратковременные и длительные)

С внешним подключением

Без разрыва шлейфа

С разрывом шлейфа

Параллельное подключение в распределительной коробке

Подключение в распределительной коробке

Параллельное подключение в кабельной зоне телефонных коммуникаций или АТС

Подключение в кабельной зоне

Подключение с установкой спец. устройства, имитирующего сигнал «занято» для владельца линии

Использование неисправного таксофона междугородной и городской связи

Подключение модема для занятия линии компьютером

Бесконтактное

Подключение к радиотелефону в зоне радиоканала

Подключение в зоне связи для сотовых телефонов

Без внешнего подключения (использование ТА не по назначению)

Междугородные разговоры работников предприятия и случайных посетителей

Использование ТА для подключения различных платных (например интимных) услуг по телефону

Рис.2. Возможные способы пиратского использования линии

*Длительное подключение.*

Уже сам факт длительного использования линии посторонними лицами говорит о том, что эти лица в процессе жизни (или производственной деятельности) находятся где-то рядом (члены семьи, соседи, сотрудники), либо показывает особую уязвимость данного абонентского комплекта ТА для пиратского подключения (вскрытые шкафы и распределительные коробки, отсутствие контроля за использованием телефона, отсутствие элементарных средств защиты).

Для пиратского подключения используются либо обычные ТА, либо специальные устройства подключения, обеспечивающие скрытое подсоединение к двухпроводному шлейфу и имитацию всех основных сигналов АТС для хозяина линии. В течение собственно момента самовольных разговоров владельцу абонентской линии имитируется либо сигнал "занято", либо сигнал "контроль посылки вызова". В остальное время владелец линии пользуется ТА беспрепятственно. Выявление таких приборов достаточно сложно, но возможно путем анализа статистики по оплате телефонных разговоров (например, по выставленным распечаткам - счетам за междугородные переговоры). Как правило, в подобных случаях нелегалы не злоупотребляют телефонным временем, боясь огласки. Для них важна сама возможность постоянно пользоваться линией. К области длительных подключений относится так же использование телефонного аппарата не по назначению, например, сотрудниками предприятия, фирмы либо детьми в собственной квартире. Вероятность подобного развития событий достаточно велика.

*Самовольное подключение без разрыва шлейфа.*

К такому виду подключений относится: параллельное подключение в распределительной коробке, в кабельной зоне АТС либо использование неисправного телефона (а также некоторых особенностей механизма кассирования монеты, жетона). Для этих подключений характерно прослушивание (подзвякивание) набора номера на аппарате владельца линии, что заставляет нелегалов пользоваться линией в отсутствие хозяина. Но это же обстоятельство служит средством выявления самого факта подключения. Подзвякивание ТА, перехват чужих разговоров, все это верные признаки параллельного самовольного подключения.

Подсоединение к двухпроводному шлейфу производится чаще всего с помощью обычного ТА разъемами типа "крокодил" либо иголками в открытых распределительных шкафах, колодцах, после чего практически не остается никаких следов подключения (естественно кроме финансового ущерба).

Самовольное неоплаченное использование таксофонов также ощутимо влияет на величину финансовых потерь линейных узлов связи. Один из возможных способов: длительное повторное использование первой неоплачиваемой минуты на некоторых типах междугородных таксофонов. Кроме этого, для таксофонов так же характерно и подключение к проводному шлейфу, как и для обычных ТА. Достаточно часто встречается и применение самодельных жетонов, монетозаменителей, карточек.

*Самовольное подключение с разрывом шлейфа.*

Бывает: в распределительной коробке, в кабельной зоне АТС, подключение имитатора либо модема (факса).

Характеризуется высокой степенью скрытности проведения самовольных разговоров. Практически невозможно выявить факт подключения в момент его проведения. Если после подключения проводка линии восстанавливается и место соединения маскируется, это говорит о длительном (устойчивом) использовании вашей телефонной линии.

*Бесконтактное подключение.*

Проявляется в зоне радиоканала между стационарным и переносным блоком радиотелефона. Путем электронного сканирования распознается кодовая посылка сигнала снятия трубки, и далее, связь происходит обычным образом, только вместо переносного блока владельца линии используется пиратский аппарат, "прошитый" соответствующим образом. Таким образом происходит мошенничество в области сотовых систем связи. Есть несколько методов, с помощью которых третья сторона может собрать данные об опознавательных (телефонных) номерах, последовательных электронных индексах абонентов сети и воссоздать копию-клон, реализующую возможности оригинала в упрощенном варианте. Запущенные в сеть клоны опознавательного номера сотового телефона могут быть использованы для ведения за день телефонных разговоров (в том числе международных) на ощутимую сумму.

Существуют также "телефоны-вампиры", которые непрерывно "обнюхивают" эфир и вытягивают опознавательный номер и электронный последовательный индекс санкционированного пользователя для однократного разговора.

*Использование телефона не по назначению.*

Эта область подключений включает в себя все возможные варианты использования телефона владельца линии. Как правило, это одна из самых вероятных ситуаций, характерных для крупных производств, фирм. Проведение личных разговоров сотрудниками без соответствующей оплаты за них. Это дополнительная статья расходов, а также головная боль руководящего персонала.

Обычный домашний телефон тоже может стать источником финансового ущерба при неразумном использовании. Выросшая оплата за междугородные разговоры приводит к увеличению количества случаев, когда абоненты не могут оплатить счета.

***Способы противодействия самовольному использованию телефона***

Все способы противодействия можно разбить на две основные группы:

* организационные;
* технические.

Под организационными способами понимается комплекс мер по регламентированию и контролю за использованием телефонной линии. Они проводятся работниками линейных узлов связи, а также индивидуальными абонентами АТС. Особенно большой эффект от организационных мер получают предприятия и организации, на балансе которых имеется достаточно много городских телефонных линий. Под техническими способами противодействия понимается применение специальных устройств защиты, ограничивающих возможности нелегальных абонентов по доступу к линиям связи.

По воздействию на телефонные линии технические способы подразделяются на:

* пассивные;
* активные.

Пассивные устройства защиты предназначены для регистрации факта подключения и самовольного использования линии. Они не вмешиваются в процесс связи, а только помогают владельцу линии оперативно реагировать на начальный процесс возникновения самовольного использования линии.

Способы противодействия пиратскому подключению к телефонной линии

Организационные

Регламентирование и контроль за использованием телефона на производстве

Установка телефона в месте, недоступном посторонним лицам

Контроль линии с опломбированием шкафов и распределительный щитков, ограничение доступа к шкафам и колодцам

Отключение выхода на межгород

на АТС

Технические

Пассивные

Активные

Сигнализаторы подключения и обрыва линии

Устройства защиты от параллельного подключения

Счетчики времени разговора

Блокираторы выхода на межгород

Устройства контроля увеличения количества междугородних разговоров

Устройства кодирования доступа к телефонной линии

Программирование цифровых АТС на работу с номерным телефонным аппаратом

Устройство ограничения продолжительности разговора

Настройка «в резонанс» системы АТС-ТА по различным параметрам

Рис.3. Способы противодействия пиратскому подключению к линии

Активные устройства защиты предусматривают вмешательство в процесс установления и проведения связи с целью предотвратить реальные финансовые затраты в случаях самовольного подключения. Основные способы противодействия приведены на Рис.3.

# 2. Техническое задание

*Исходные данные*

Разработать устройство запрета телефонной связи ври импульсном наборе номера 061.

Устройство запрета разработать в виде лабораторного макета.

*Основные технические характеристики*

- ток потребления в режиме ожидания от линии, не более, мкА\_\_500;

- допустимое напряжение постоянного тока АТС, В\_\_\_\_\_\_\_\_\_\_\_\_55-70;

- температура окружающей среды, градусы С\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_+10+40;

- габариты макета, мм\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_30040050;

- масса, не более, кг\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2.

*Перечень вопросов подлежащих разработке*

Аналитический обзор устройств пассивной и активной технической зашиты. Назначение, принцип действия, функциональная схема. Принципиальная электрическая схема лабораторного макета. Временная диаграмма работы макета при наборе цифры 061. Конструкция лабораторного макета.

*Задание по разделу* "Технологическая часть проекта".

Разработать печатные платы схем\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель

доцент, к.т.н. Филимонов А.К.

# 3. Устройства пассивной и активной технической защиты

## 3.1. Способы получения информации о подключении

Устройства пассивной технической защиты предназначены для регистрации факта подключения и самовольного коммерческого использования линии. Своевременная индикация позволяет абоненту предотвратить дальнейшие попытки подключения к его линии.

***Способы получения информации о подключении***

Основные технические способы получения информации о постороннем включении в линию базируются на следующих признаках:

* отсутствие напряжения в телефонной линии;
* падение напряжения в линии в 3-4 раза при положенной трубке основного ТА;
* наличие импульсов набора номера при положенной трубке ТА;
* наличие частотных посылок DTMF кода при неиспользовании основного ТА;
* непрохождение вызова с АТС на основной ТА.

Большинство отечественных АТС имеют рабочее напряжение 60В постоянного тока. Для индикации состояния линии с успехом может быть применена схема, приведенная на Рис. 4.

Данная схема позволяет отследить:

* падение напряжения в линии до уровня 35В;
* наличие импульсов набора номера частотой 10 Гц;
* наличие вызывного сигнала частотой 25 Гц;
* пропадание напряжения в линии (при наличии независимого источника питания микросхемы DD1).

Рис.4. Индикатор состояния линии

В состав схемы входят:

* мост униполярного подключения – VD1-VD4;
* специальный делитель контроля падения напряжения – VD5, R1, VD6, R2;
* переключающий элемент И-НЕ – DD1.1.

Сочетание в делителе резистивных (Rl, R2) и нелинейных элементов (в частности, стабилитрона VD6) позволяет подключить элемент DD1.1 непосредственно к линии, а также получить порог переключения элемента DD1.1 не ниже 35В. В результате, данная схема может уверенно отработать падение напряжения как при установке у абонента, так и при установке на кроссе АТС. Рис.5 поясняет сказанное.

Рис.5. Эквивалентная схема проводного шлейфа АТС-ТА

При Rэкв600, при снятой трубке телефона ТА напряжение в точках (ТА стандартный, при снятой трубке RT=500):

КТ1 – КТ1 = 30 Вольт

КТ2 - КТ2 = 15 Вольт

Следует учитывать, что для отдаленных от АТС абонентов эквивалентное сопротивление линии может составлять Кэкв ~ 1 кОм, что затрудняет работу устройства индикации, включающего только резистивный делитель (без стабилитрона), вследствие большой разницы в уровнях напряжений на коротком (Кэкв = 0) и длинном (Кэкв > 500 Ом) шлейфе.

Схема на Рис.4 свободна от этих недостатков и применяется в различных устройствах индикации и защиты. Очевидно, что с помощью данной схемы невозможно принять DTMF-посылки набора номера, но сам момент снятия трубки на пиратском аппарате регистрируется однозначно, что позволяет использовать данную схему во всех режимах подключения.

В дополнение на Рис.6 приведена схема индикатора состояния линии с использованием транзистора. В данной схеме используется обычный резистивный делитель Rl, R2. В качестве ключа применяются кремниевые транзисторы КТ3102 или КТ315. Подбор уровня срабатывания осуществляется изменением R2 при настройке схемы. Обычно он не превышает 30В и позволяет регистрировать те же режимы, что и схема на Рис.4.

Рис.6. Датчик состояния линии на транзисторе

## 3.2. Совмещенный индикатор подключения и обрыва телефонной линии

В соответствии с описанным выше способом контроля напряжения в линии разработан совмещенный индикатор подключения и обрыва линии.

Питание индикатора встроенное, батарея 9 BJ("Крона", "Корунд"...).

Благодаря высоким значениям Rl, R2, индикатор абсолютно не влияет на параметры линии в соответствии с ГОСТом. Естественно, что индикатор будет срабатывать и при подъеме трубки (ведении разговора) и самим хозяином линии. Можно порекомендовать встроить выключатель или выполнить индикатор в виде заглушки, подключаемой вместо телефонного аппарата.

## 3.3. Световой индикатор с автоматическим отключением

Для того, чтобы индикатор подключения не срабатывал при снятии трубки хозяином телефонной линии, необходимо ввести режим автоматического отключения. В этом случае индикатор включается последовательно с телефонным аппаратом через датчик тока. Принципиальная схема такого устройства приведена на Рис.7.

В состав схемы входят:

* датчик напряжения - VD1, R1, VD2, R2, DD1.1;
* датчик тока - R5, VT2, R6, DD1.2;
* ключ включения светодиода - R3, VT1, R4, HL1;
* схема автоматического отключения - R7, С1, DD1.3, VD3;
* элемент питания - 9 В.

Рис.7. Световой индикатор с автоматическим отключением

Принцип действия индикатора заключается в следующем.

Светодиод HL1 загорается в случаях:

* снижения напряжения в линии ниже 35В (попытка нелегального подключения);
* обрыва телефонной линии;
* прохождения сигнала вызова АТС - 25 Гц. Включение ключа VT1 происходит высоким уровнем с выхода 3 DD1.1 через R3. При снятии трубки телефонного аппарата с задержкой ~1с (определяется R7, С1) переключается элемент DD1.3 и принудительно поддерживает "О" на базе VT1, отключая тем самым HL1. Если кроме световой сигнализации в схему введена звуковая, она также будет выключаться при снятии трубки основного защищаемого ТА.

## 3.4. Счетчик времени разговора

Если совместить схему индикатора состояния линии с электронными часами, можно получить простой счетчик времени разговора. Заметим, что если индикатор линии реагирует как на попытку набора, так и на обрыв линии, то счетчик позволит произвести оценку времени пиратского подключения во время отсутствия хозяина телефона. Получается своеобразный индикатор с памятью.

Привязку датчика состояния линии с часами легче всего производить по запуску кварцевого задающего генератора. Тогда, часы запускаются при падении напряжения в линии ниже установленного уровня (разговор или обрыв) и останавливаются после восстановления уровня 60 В (окончание разговора).

Если часы не обнулять, то счетчик времени суммирует время всех разговоров в течение суток и более (до 24-х часов разговорного времени). Счетчик времени может быть также применен для анализа частоты использования телефонного аппарата.

Для примера, на Рис.8 представлена схема счетчика времени разговора с задающим генератором на микросхемах 561 серии.

В исходном состоянии, когда на линии 60 В, вход 1 DD2.1 шунтируется диодом VD9 на корпус. Задающий генератор выключен, счет часов остановлен. При снятии трубки на линии, на выходе 10 DD1.3 с задержкой в 1 с (R4, С1) появляется логическая единица, осуществляя запуск генератора. Счет времени осуществляется пока на выходе 10 DD1.3 не появится логический "ноль" (через 1 с после появления на линии напряжения 60 В).

По описанному принципу можно осуществить сопряжение датчика линии с любыми другими схемами электронных часов. Для конструирования желательно использовать готовые часы с питанием от батареек, так как в этом случае осуществляется страховка от пропадания напряжения в сети 220 В.

Рис.8. Счетчик времени разговора

DD1 – К561ЛА7

DD2 – К561ЛЕ5

## 3.5. Устройство криптографической защиты информации

В современных условиях информация играет решающую роль как в процессе экономического развития, так и в ходе конкурентной борьбы на национальном и международном рынках. Противоборство развернулось за превосходство в тех областях, которые определяют направления научно-технического прогресса. В мире реального бизнеса конкуренция ставит участников рынка в такие жесткие рамки, что многим из них приходится поступать в соответствие с принципами “победителей не судят”, “цель оправдывает средства”.

В этих условиях становится реальностью промышленный шпионаж как сфера тайной деятельности по добыванию, сбору, анализу, хранению и использованию конфиденциальной информации. Это обусловлено тем, что получение сколько-нибудь достоверной информации об объектах заинтересованности законным путем становится невозможным из-за создания и поддержания определенной системы защиты ценной информации от несанкционированного, то есть противоправного, доступа со стороны злоумышленников.

Анализ различных способов получения информации о конкурентах позволил установить, что подслушивание телефонных переговоров в ряде случаев может являться одним из эффективных способов несанкционированного доступа к конфиденциальной информации. Это объясняется тем, что в настоящее время обмен информацией по телефону является очень распространенным и практически во всех случаях, когда абонентам не требуется письменного документа и имеется возможность воспользоваться телефонной связью, они ею пользуются. Мало того, даже в тех случаях, когда требуется письменный документ, абоненты довольно часто ведут по телефону предварительные переговоры, оправдывая это срочностью согласования определенных позиций.

Самым эффективным способом защиты телефонных сообщений от несанкционированного доступа является их криптографическое преобразование.

Действительно, для того, чтобы скрыть от злоумышленников смысловое содержание передаваемого телефонного сообщения, его необходимо определенным образом изменить. При этом изменить его так, чтобы восстановление исходного сообщения санкционированным абонентом осуществлялось бы очень просто, а восстановление сообщения злоумышленником было бы невозможным или требовало бы существенных временных и материальных затрат, что делало бы сам процесс восстановления неэффективным.

Именно такими свойствами и обладают криптографические преобразования, задачей которых является обеспечение математическими методами защиты передаваемых конфиденциальных телефонных сообщений. Даже в случае их перехвата злоумышленниками и обработки любыми способами с использованием самых быстродействующих суперЭВМ и последних достижений науки и техники смысловое содержание сообщений должно быть раскрыто только в течение заданного времени, например, в течение нескольких десятков лет.

***Общие принципы криптографического преобразования телефонных сообщений***

Рассмотрим общие принципы криптографического преобразования телефонных сообщений (см. рис.9).

X(t) Y(t)=Fk[X(t)] X(t)=Zk{Fk[X(t)]} X(t)

Шифратор

Дешифратор

Приемник сообщения

Источник сообщения

Источник ключа

**Рис.9. Обобщенная схема криптографической системы**

Будем называть исходное телефонное сообщение, которое передается по радио- или проводному каналу, открытым сообщением и обозначать X(t).Это сообщение поступает в устройство криптографического преобразования (шифрования), где формируется зашифрованное сообщение Y(t) с помощью следующей зависимости:

Y(t) = Fk[X(t)],

где Fk[.] - криптографическое преобразование;

k - ключ криптографического преобразования,

Здесь под ключом криптографического преобразования будем понимать некоторый параметр k, с помощью которого осуществляется выбор конкретного криптографического преобразования Fk[.]. Очевидно, что чем больше мощность используемого множества ключей криптографического преобразования K, тем большему числу криптографических преобразований может быть подвергнуто телефонное сообщение X(t), а, следовательно, тем больше неопределенность у злоумышленника при определении используемого в данный момент криптографического преобразования Fk[.].

Вообще говоря, при шифровании сообщения X(t) должны использоваться такие криптографические преобразования, при которых степень его защиты определялась бы только мощностью множества ключей криптографического преобразования K.

Зашифрованное сообщение Y(t) передается по радио- или проводному каналу связи. На приемной стороне это сообщение расшифровывается с целью восстановления открытого сообщения с помощью следующей зависимости:

X(t) = Zk[Y(t)] = Zk{Fk[X(t)]},

где - Zk[.] - обратное по отношению к Fk[.] преобразование.

Таким образом, наличие у абонентов одинаковых ключей k и криптографических преобразований Fk[.], Zk[.] позволяет без особых сложностей осуществлять зашифрование и расшифрование телефонных сообщений.

Очевидно, что для рассмотрения способов криптографического преобразования телефонных сообщений необходимо иметь представление о тех процессах, которые лежат в основе формирования этих сообщений.

Телефонное сообщение передается с помощью электрических сигналов, которые формируются из акустических сигналов путем преобразования микрофоном телефонного аппарата этих акустических сигналов в электрические, обработки электрических сигналов и усиления до необходимого уровня. На приемной стороне в телефонном аппарате электрические сигналы подвергаются обработке и преобразованию в акустические с помощью телефона.

Любое сообщение X(t) характеризуется длительностью и амплитудно-частотным спектром S(f), т.е. сообщение X(t) может быть представлено эквивалентно как во временной, так и в частотной областях.

Заметим, что человеческое ухо может воспринимать акустический сигнал в диапазоне от 15 Гц до 20 кГц, хотя могут иметь место некоторые индивидуальные расхождения. Однако для того, чтобы сохранить узнаваемость голоса абонента по тембру, чистоту и хорошую разборчивость звуков совершенно необязательно передавать акустический сигнал в этом частотном диапазоне. Как показала практика, для этого достаточно использовать частотный диапазон от 300 Гц до 3400 Гц. Именно такую частотную полосу пропускания имеют стандартные телефонные каналы во всем мире.

Исходя из временного и частотного представлений открытого телефонного сообщения X(t) на практике могут использоваться криптографические преобразования, применяемые к самому сообщению X(t) или к его амплитудно-частотному спектру S(f).

Все криптографические преобразования, с точки зрения стойкости, представляется возможным разделить на две группы.

Первую группу составляют вычислительно стойкие и доказуемо стойкие криптографические преобразования, а вторую - безусловно стойкие криптографические преобразования.

К вычислительно стойким и доказуемо стойким относятся криптографические преобразования, стойкость которых определяется вычислительной сложностью решения некоторой сложной задачи. Основное различие между этими криптографическими преобразованиями заключается в том, что в первом случае имеются основания верить, что стойкость эквивалентна сложности решения трудной задачи, тогда как во втором случае известно, что стойкость, по крайней мере, большая. При этом во втором случае должно быть предоставлено доказательство, что раскрытие передаваемого зашифрованного сообщения Y(t) эквивалентно решению сложной задачи.

Примером вычислительно стойких криптографических преобразований являются сложные криптографические преобразования, составленные из большого числа элементарных операций и простых криптографических преобразований таким образом, что злоумышленнику для дешифрования перехваченного сообщения Y(t) не остается ничего другого, как применить метод тотального опробования возможных ключей криптографического преобразования, или, как еще называют, метод грубой силы. С помощью таких криптографических преобразований представляется возможным обеспечить гарантированную защиту передаваемого сообщения X(t) от несанкционированного доступа.

К вычислительно стойким криптографическим преобразованиям представляется возможным отнести и такие криптографические преобразования, при использовании которых злоумышленнику для несанкционированного доступа к сообщению X(t) требуется использовать лишь определенные алгоритмы обработки сообщения Y(t). Эти криптографические преобразования способны обеспечить лишь временную стойкость.

К безусловно стойким относятся криптографические преобразования, стойкость которых не зависит ни от вычислительной мощности, ни от времени, которыми может обладать злоумышленник. То есть такие криптографические преобразования, которые обладают свойством не предоставлять злоумышленнику при перехвате сообщения Y(t) дополнительной информации относительно переданного телефонного сообщения X(t).

Заметим, что безусловно стойкие криптографические преобразования реализовать очень сложно и поэтому в реальных системах телефонной связи они не используются.

***Криптографическое преобразование аналоговых телефонных сообщений***

Наиболее простым и распространенным способом криптографического преобразования аналоговых телефонных сообщений является разбиение сообщений X(t) на части и выдача этих частей в определенном порядке в канал связи.

 Временной интервал Временной интервал

 Т T

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| n-1 | n | 1 | 2 | 3 | 4 | 5 | … | … | n-1 | n | 1 | 2 | 3 | 4 | 5 | … | … | n-1 |

 t

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 | 4 | 3 | n-1 | 5 | n | … | … | 2 |

**Рис.10. Временные перестановки частей сообщения X(t)**

Этот способ заключается в следующем. Длительность сообщения X(t) (см.рис.10) делится на определенные, равные по длительности временные интервалы T. Каждый такой временной интервал дополнительно делится на более мелкие временные интервалы длительностью t. При этом для величины n=T/t , как правило, выполняется условие n = m ...10m , где m - некоторое целое число, m<10. Части сообщения X(t) на интервалах времени t записываются в запоминающее устройство, “перемешиваются” между собой в соответствие с правилом, определяемым ключом криптографического преобразованияk, и в виде сигнала Y(t) выдаются в канал связи. На приемной стороне канала связи, где правило перемешивания известно, т.к. имеется точно такой же ключ криптографического преобразования k, осуществляется “сборка” из сообщения Y(t) открытого сообщения X(t).

К преимуществам этого способа криптографического преобразования относится его сравнительная простота и возможность передачи зашифрованного телефонного сообщения по стандартным телефонным каналам. Однако этот способ позволяет обеспечить лишь временную стойкость. Это обусловлено следующим. Поскольку открытое телефонное сообщение X(t) является непрерывным, то у злоумышленника после записи сообщения Y(t) и выделения интервалов длительностью t (последнее достаточно легко сделать, т. к. в канале связи присутствует синхронизирующий сигнал) появляется принципиальная возможность дешифрования сообщения Y(t) даже без знания используемого ключаk. С этой целью необходимо осуществить выбор интервалов таким образом, чтобы обеспечивалась непрерывность получаемого сообщения на стыках этих интервалов. Очевидно, что при тщательной и кропотливой работе с использованием специальной техники можно достаточно быстро обеспечить такую непрерывность, выделив тем самым открытое сообщение X(t).

Поэтому такой способ криптографического преобразования открытых телефонных сообщений целесообразно применять только в тех случаях, когда информация не представляет особой ценности или когда ее ценность теряется через относительно небольшой промежуток времени.

Более высокую защиту от несанкционированного доступа можно обеспечить, если идею рассмотренного способа распространить на частотный спектр сообщения X(t). В этом случае полоса пропускания телефонного канала F делится с помощью системы полосовых фильтров на n частотных полос шириной D f, которые перемешиваются в соответствии с некоторым правилом, определяемым ключом криптографического преобразованияk. Перемешивание частотных полос осуществляется со скоростью V циклов в секунду, т.е. одна перестановка полос длится 1/V c, после чего она заменяется следующей.

Для повышения защиты от несанкционированного доступа после перемешивания частотных полос может осуществляться инверсия частотного спектра сообщения Y(t).

Рис.11 иллюстрирует рассмотренный способ криптографического преобразования. В верхней части рис.11 приведен частотный спектр сообщения X(t), а в нижней - спектр сообщения Y(t) на одном из циклов перемешивания при n = 5.

Рассмотренный способ позволяет обеспечить более высокую защиту телефонных сообщений от несанкционированного доступа по сравнению с предыдущим способом. Для восстановления открытого сообщения X(t) в этом случае злоумышленнику необходимо иметь дополнительные данные по относительным частотам появления звуков и их сочетаний в разговорной речи, частотным спектрам звонких и глухих звуков, а также формантной структуре звуков. В табл.1 приведены данные по относительным частотам появления некоторых звуков и границам формантных областей звуков русской речи, которые могут быть использованы злоумышленником при восстановлении перехваченных телефонных сообщений.

|  |
| --- |
|  |
| **Рис.11. Частотные спектры сообщений X(t) и Y(t)** |

*Таблица 1*

Данные по относительным частотам появления некоторых звуков и границам формантных областей

|  |  |  |  |
| --- | --- | --- | --- |
| Звук | Относительная частота появления, Гц | 1-ая формантная область, Гц | 2-ая формантная область, Гц |
| Гласный |  |  |  |
| А | 0,079 | 1100 - 1400 | - |
| И | 0,089 | 2800 - 4200 | - |
| О | 0,11 | 400 - 800 | - |
| У | 0,026 | 200 - 600 | - |
| Ы | 0,022 | 200 - 600 | 1500 - 2300 |
| Э | 0,002 | 600 - 1000 | 1600 - 2500 |
| Согласный |  |  |  |
| З | 0,016 | 0 - 600 | 4200 - 8600 |
| Ж | 0,008 | 200 - 600 | 1350 - 6300 |
| Л | 0,04 | 200 - 500 | 700 - 1100 |
| М | 0,031 | 0 - 400 | 1600 - 1850 |
| Н | 0,069 | 0 - 400 | 1500 - 3400 |
| Р | 0,05 | 200 - 1500 | - |
| С | 0,054 | 4200 - 8600 | - |
| Ф | 0,001 | 7000 - 12000 | - |
| Х | 0,012 | 400 - 1200 | - |
| Ш | 0,008 | 1200 - 6300 | - |

Очевидно, что наиболее высокую защиту телефонных сообщений от несанкционированного доступа представляется возможным обеспечить путем объединения рассмотренных способов. При этом временные перестановки будут разрушать смысловой строй, а частотные перемешивать гласные звуки.

Устройства, реализующие рассмотренные способы, называются скремблерами.

В этой связи представляет определенный интерес серия скремблеров, в качестве базового для которой был использован скремблер SCR - M1.2. Эти скремблеры реализуют рассмотренные способы криптографического преобразования аналоговых телефонных сообщений и довольно широко используются в различных государственных и коммерческих структурах. В табл.2 приведены основные характеристики некоторых скремблеров этой серии.

***Криптографическое преобразование цифровых телефонных сообщений***

На практике для преобразования телефонного сообщения X(t) в цифровую форму на передающей стороне и восстановления этого сообщения на приемной стороне используются речевые кодеки, которые реализуют один из двух способов кодирования телефонных сообщений: формы и параметров.

Основу цифровой телефонии в настоящее время составляет кодирование формы сообщений, кодирование параметров сообщений или, как называют, вокодерная связь используется значительно реже. Это обусловлено тем, что кодирование формы сигнала позволяет сохранить индивидуальные особенности человеческого голоса, удовлетворить требования не только к разборчивости, но и к натуральности речи.

При кодировании формы сигнала широко используются импульсно-кодовая модуляция (ИКМ), дифференциальная ИКМ и дельта-модуляция.

Кратко рассмотрим принципы осуществления ИКМ, дифференциальной ИКМ и дельта-модуляции.

*Таблица 2*

Основные характеристики скремблеров, созданных на базе скремблера SCR-M1.2

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Скремблер | Режим работы | Идентификация абонента | Ввод сеансового ключа | Мощность множества ключей | Габариты, мм | Вес, кг | Питание |
| SCR-M1.2 | Дуплексная связь | Предусмотрена | Методом открытого распространения ключей | 2х1018 | 180х270х40 | 1,5 | 22В 50Гц |
| SCR-M1.2 mini | Дуплексная связь | Предусмотрена | Методом открытого распространения ключей | 2х1018 | 112х200х30 | 0,8 | От сетевого адаптера 9-15 В, или батарейного блока |
| SCR-M1.2 multi | Дуплексная связь | Может быть предусмотрена по желанию заказчика | Методом открытого распространения ключей | 2х1018 | 180х270х45 | 1,6 | 220В 50Гц |

ИКМ основана на дискретизации, квантовании отсчетов и кодировании номера уровня квантования (см. рис.12).

Телефонное сообщение X(t) длительностью T , имеющее ограниченный частотой fm спектр, после фильтрации преобразуется в последовательность узких импульсов X(l) = X(lD t), l =1,N, где N = T/D t, D t = 1/2fm, модулированных по амплитуде. Полученные мгновенные значения X(l),l=1,N, квантуются по величине с использованием равномерной, неравномерной или адаптивно-изменяемой шкалы квантования. Квантованные значения отсчетов Xкв(l), l=1,N, с помощью кодера преобразуются в кодовые слова, характеризуемые числом двоичных символов, которые выдаются в канал связи.

**X(t) X(l) XКВ(l) 0100…**

Кодер

Квантователь

Дискретизатор

Фильтр

НЧ

**X(t) XКВ(l) 0100…**

Декодер

Фильтр

НЧ

**Рис.12. Обобщенная схема системы с ИКМ**

На приемной стороне кодовые слова с помощью декодера преобразуются в значения отсчетов Xкв(l), l=1,N, из которых с помощью фильтра нижних частот осуществляется восстановление сообщения X(t).

Дифференциальная ИКМ и дельта-модуляция отличаются от ИКМ тем, что в них использовано нелинейное отслеживание передаваемого телефонного сообщения.

При этом дифференциальная ИКМ отличается от простой ИКМ тем, что квантованию подвергаются не сами отсчеты телефонного сообщения X(l), l=1,N, а разность между соответствующим отсчетом X(l) и результатом предсказания Xпр(l), формируемым на выходе предсказателя. При этом в канал связи выдаются кодовые слова, содержащие коды этой разности и ее знака (полярности). И, наконец, дельта-модуляция отличается от простой ИКМ тем, что в канал связи выдаются только коды знака (полярности) в виде последовательности импульсов, временное положение которых позволяет восстановить на приемной стороне переданное телефонное сообщение X(t), например, с помощью интегратора.

Необходимо отметить, что дифференциальная ИКМ является наиболее предпочтительной при формировании цифровых сообщений. Это обусловлено, в основном, тем, что использование дифференциальной ИКМ позволяет сократить длину кодовых слов, т.к. передаче подлежит только информация о знаке и величине приращения. Кроме того, использование дифференциальной ИКМ позволяет исключить перегрузку по крутизне, с которой приходится сталкиваться при линейной дельта-модуляции.

В системах синтетической или вокодерной связи по телефонному каналу передаются данные о деформациях периферического голосового аппарата говорящего. Приемное устройство в таких системах представляет собой модель голосового аппарата человека, параметры которой изменяются в соответствии с принимаемыми данными. При этом число параметров, характеризующих голосовой аппарат, сравнительно невелико (10...20) и скорость их изменения соизмерима со скоростью произношения фонем. В русской речи число фонем принимают равным 42 и они представляют собой эквивалент исключающих друг друга различных звуков.

Если считать, что фонемы произносятся независимо с одинаковой вероятностью, то энтропия источника будет равна log2 42 @ 5,4 бит/фонему. В разговорной речи за одну секунду произносится до 10 фонем, поэтому скорость передачи информации не будет превышать 54 бит/с. Учитывая статистическую связь между фонемами вследствие избыточности речи, представляется возможным снизить скорость передачи информации до 20...30 бит/c.

Система вокодерной связи функционирует следующим образом. В передающей части системы осуществляется анализ телефонного сообщения X(t), поступающего с микрофона, с целью выделения значений параметров, описывающих сигнал возбуждения, а также характеризующих резонансную структуру речевого тракта. Значения параметров в цифровом коде и передаются по каналу связи. На приемной стороне осуществляется синтез сообщения X(t) с использованием принятых значений параметров.

Таким образом, как при использовании кодирования формы сигнала с помощью ИКМ, дифференциальной ИКМ и дельта-модуляции, так и при кодировании параметров в канал связи выдаются последовательности символов.

Следовательно, к этим последовательностям могут быть применены известные и достаточно широко используемые на практике криптографические преобразования и алгоритмы.

В настоящее время наиболее известными криптографическими алгоритмами, обеспечивающими гарантированную защиту передаваемых цифровых сообщений от несанкционированного доступа, являются американский стандарт шифрования данных DES (Data Encryption Standart), который принят в качестве федерального стандарта США, и российский стандарт ГОСТ-28147-89.

Шифрование с помощью криптографического алгоритма DES осуществляется следующим образом.

Исходное сообщение, представляющее собой последовательность символов, делится на блоки по 64 символа каждый. Далее по отношению к каждому блоку осуществляется выполнение следующей последовательности операций.

1. Блок, обозначаемый L0R0, где L0 - блок, представляющий собой одну из частей блока L0R0 , состоящую из 32 символов; R0 - блок, представляющий собой другую часть блока L0R0, также состоящую из 32 символов, подвергается перестановке в соответствии с заранее определенным правилом.

2. Для каждой n-ой итерации, n = 1,16, выполняется следующая последовательность операций:

1. блок Rn-1 разбивается на 8 блоков по 4 символа каждый;
2. эти блоки преобразуются в 8 блоков по 6 символов путем добавления слева и справа к символам каждого блока очередных символов блока Rn-1. Так, например, если блок состоял из символов x0nx1nx2nx3n , то в результате добавления слева и справа указанных символов блок будет иметь следующий вид x31nx0nx1nx2nx3nx4n;
3. символы полученных 8 блоков складываются по mod2 с 48-ю символами ключа криптографического преобразования, соответствующего n-ой итерации и определяемого списком ключей;
4. далее 8 блоков подаются на входы соответствующих 8 блоков подстановки S[j],j = 0,7, которые преобразуют 8 блоков по 6 символов каждый в 8 блоков по 4 символа каждый в соответствии с заранее определенным правилом;
5. д) полученные в результате подстановки 32 символа подвергаются коммутации в соответствии с заранее определенным правилом;
6. далее осуществляется формирование блока Sn-1 путем сложения по mod2 символов, полученных при выполнении операции д), с символами блока Ln-1;
7. осуществляется запись символов блока Rn-1 на место блока Ln, а символов блока Sn-1 - на место блока Rn.

3. Полученный после 16-и итераций блок L16R16 подвергается перестановке, обратной выполняемой при осуществлении операции 1.

Результатом выполнения операции 3 является зашифрованный блок, состоящий из 64 символов. Аналогичным образом осуществляется шифрование всех блоков исходного сообщения.

Заметим, что расшифрование зашифрованного криптографическим алгоритмом DES сообщения осуществляется достаточно легко благодаря обратимости используемого преобразования.

Поскольку длина входного ключа криптографического преобразования k составляет 56 символов, а на каждой итерации используются только 48 из 56 символов, то каждый символ входного ключа используется многократно.

Основными недостатками криптографического алгоритма DES, по мнению специалистов, являются:

* малая длина используемого ключа криптографического преобразования;
* малое число итераций;
* сложность практической реализации используемых перестановок.

Развитием стандарта DES является российский стандарт шифрования ГОСТ - 28147 - 89, который формировался с учетом мирового опыта, недостатков и нереализованных возможностей криптографического алгоритма DES. Этот стандарт рекомендован к использованию для защиты любых данных, представленных в виде двоичных последовательностей.

Необходимо отметить, что криптографический алгоритм ГОСТ-28147-89, как и криптографический алгоритм DES, применяется для криптографического преобразования сообщений, предварительно разбитых на блоки по 64 символа каждый. Алгоритм достаточно сложен, поэтому будет изложена в основном его концепция.

Алгоритм ГОСТ-28147-89 предусматривает следующие режимы работы: замены, гаммирования и гаммирования с обратной связью. Во всех этих режимах используется ключ криптографического преобразования k, состоящий из 256 символов.

Режим замены представляет собой итеративный процесс (число итераций равно 32), в котором используются операции сложения по mod2 и mod 232, перестановки, подстановки и циклического сдвига, применяемые к блокам, состоящим из 32 символов, и объединения двух блоков по 32 символа каждый в блок, состоящий из 64 символов.

В режиме гаммирования осуществляется криптографическое преобразование сообщения путем сложения по mod2 символов сообщения с символами последовательности (гаммы), вырабатываемой в соответствии с определенным правилом блоками по 64 символа.

Режим гаммирования с обратной связью отличается от режима гаммирования тем, что символы очередного блока гаммы формируются с учетом символов предыдущего зашифрованного блока.

В алгоритме ГОСТ - 28147 - 89 предусмотрена также операция выработки имитовставки, которая является одинаковой для всех режимов криптографического преобразования. Имитовставка представляет собой двоичную последовательность, состоящую из r символов, которая предназначена для защиты сообщения от имитации. При этом величина r выбирается исходя из условия обеспечения требуемого уровня имитозащиты.

Имитовставка передается по каналу связи после зашифрованного сообщения. На приемной стороне из принятого сообщения вырабатывается имитовставка, которая сравнивается с полученной. В случае несовпадения имитовставок принятое сообщение считается ложным.

Таким образом, использование в криптографическом алгоритме ГОСТ-28147-89 ключа криптографического преобразования k длиной 256 символов позволяет обеспечить более высокую стойкость по сравнению с криптографическим алгоритмом DES.

Действительно, если злоумышленник для раскрытия передаваемого телефонного сообщения использует тотальное опробование ключей криптографического преобразования, а ключи из множества, мощность которого равна K, назначаются равновероятно, то вероятность Pk(T) определения злоумышленником используемого ключа k за время T может быть оценена с помощью следующей зависимости

Pk(T) = TW/K,

где W - число опробований злоумышленником ключей криптографического преобразования в единицу времени.

В табл.3. в качестве иллюстрации приведены значения вероятности Pk(T) для алгоритмов DES и ГОСТ - 28147 - 89 при W = 109 1/с.

*Таблица 3*

Значения вероятности Pk(T) при W = 109 1/с.

|  |  |  |
| --- | --- | --- |
| Т | Алгоритм DES | Алгоритм ГОСТ-28147-89 |
| 1 год | 0,44 | 2,72х10-61 |
| 2 года | 0,88 | 5,44х10-61 |
| 10 лет | 1,0 | 2,72х10-60 |

Из анализа данных, приведенных в табл.3, следует, что задавая требуемое значение вероятности Pk, т.е. Pk=Pk.тр, всегда можно определить такие интервал времени T и алгоритм криптографического преобразования, при которых будет обеспечено выполнение заданного требования.

Таким образом, преимущества от использования вышерассмотренных алгоритмов криптографического преобразования цифровых телефонных сообщений по сравнению со способами криптографического преобразования аналоговых телефонных сообщений очевидны и заключаются главным образом в возможности обеспечения гарантированной стойкости передаваемых сообщений. Однако эти преимущества достигаются за счет применения сложной и дорогостоящей аппаратуры и отказа в большей части случаев от стандартного телефонного канала.

Действительно, если для передачи телефонного сообщения используется ИКМ, то для его восстановления на приемной стороне необходимо принимать не менее 6800 мгновенных значений в секунду. Далее, если для преобразования мгновенных значений в код используются 8-и разрядные аналого-цифровой и цифро-аналоговый преобразователи, то скорость передачи символов в канале связи будет составлять 54,4 кбит/c. Следовательно, для обеспечения передачи телефонного сообщения в этом случае необходимо существенно увеличить полосу пропускания канала связи. Кроме того, необходимо также создать шифратор (дешифратор), который осуществлял бы криптографическое преобразование сообщения со скоростью 54,4 кбит/с.

Здесь необходимо заметить, что без увеличения полосы пропускания канала связи представляется возможным передавать лишь последовательности символов в системах вокодерной связи. Однако, в этом случае, хотя речь и сохраняет приемлемую разборчивость, опознать абонента по тембру голоса часто бывает затруднительно, т.к. голос синтезируется речевым синтезатором и имеет “металлический” оттенок.

К сожалению, на отечественном рынке гарантированно защищенных от несанкционированного доступа к передаваемым телефонным сообщениям систем вокодерной связи чрезвычайно мало. Да и все они, как правило, характеризуются невысокой слоговой разборчивостью и сложностью опознания абонента по тембру голоса. Примером такой системы является система “Voice coder - 2400”, в которой совместно с криптографическим алгоритмом ГОСТ - 28147 - 89 используется достаточно “старый” алгоритм кодирования параметров телефонного сообщения LPC - 10.

Среди систем, выделяющихся в положительную сторону, представляется возможным отметить находящуюся на заключительной стадии разработки отечественную систему СКР - 511, которая предназначена для обеспечения конфиденциальности телефонных переговоров при работе на внутригородских и междугородних линиях связи.

Система размещается в корпусе телефонного аппарата “Panasonic KX-T2355/2365” и реализует наиболее современный алгоритм кодирования параметров телефонных сообщений CELP, что позволяет обеспечить высокое качество речи. Для защиты от несанкционированного доступа к передаваемым сообщениям используются криптографический алгоритм ГОСТ - 28147 - 89.

Электропитание системы осуществляется от сети 220 В 50/60 Гц или постоянного тока напряжением 9 - 12 В. При этом потребляемая электрическая мощность не превышает 5 Вт.

Что же касается способов криптографического преобразования аналоговых телефонных сообщений, то необходимо иметь в виду, что они не должны применяться для защиты сведений, которые являются секретными в течение сравнительно большого времени. Однако, для защиты коммерческой, а также личной информации, такие способы криптографического преобразования являются наиболее приемлемыми. Что обусловлено более низкой стоимостью устройств, реализующих эти способы, по сравнению с устройствами, реализующими криптографические алгоритмы DES и ГОСТ-28147-89, а также тем, что они могут быть использованы в самых распространенных в мире стандартных каналах связи.

# 4. Назначение, принцип действия и функциональная схема

Прибор запрета телефонной связи по заданным номерам является устройством охраной автоматики и предназначен для предотвращения несанкционированной связи абонента с платными телефонными службами.

Прибор анализирует набираемый импульсным способом номер и прерывает связь при наборе номера 061 путем кратковременного размыкания телефонной линии (отбой линии).

Прибор состоит из следующих блоков:

1. преобразователь полярности;
2. стабилизатор напряжения;
3. делитель напряжения;
4. схема подавления дребезга контактов;
5. схема выделения огибающей набора;
6. анализатор состояния линии;
7. счетчик-дешифратор набираемой цифры;
8. счетчик-дешифратор количества набранных цифр;
9. логический анализатор;
10. ждущий мультивибратор;
11. электронный коммутатор;
12. поляризованное реле;
13. схема питания поляризованного реле.

линия

преобразователь полярности

стабилизатор напряжения

 к цепям питания схемы

ТА

анализатор состояния линии

делитель напряжения

схема подавления дребезга контактов

схема выделения огибающей номера

схема питания поляризованного реле

счетчик дешифратор количества набранных цифр

счетчик дешифратор набираемой цифры

поляризованное реле

 2

 0 6 1

логический анализатор

электронный коммутатор

ждущий мультивибратор

Рис.13. Функциональная схема

*Прибор работает следующим образом:* Напряжение телефонной линии поступает на преобразователь полярности, который обеспечивает определенную полярность напряжения на своем выходе не зависимо от полярности напряжения в телефонной линии. Это обеспечивает работоспособность прибора при перекоммутации линии на АТС. С выхода преобразователя полярности напряжение поступает на делитель напряжения и стабилизатор напряжения, которые вырабатывают постоянное напряжение питания для схемы прибора независимо от состояния линии (линия свободна, когда трубка лежит на ТА, при этом постоянное напряжение в ней 60В; линия занята, когда трубка снята, при этом напряжение в линии 515В). Делитель напряжения необходим для изменения масштаба напряжения до величины, обеспечивающей работу логической схем прибора (при наборе номера амплитуда импульсов 60В, а для нормальной работы микросхем – 2-3В). С выхода делителя напряжения импульсы набора поступают на схему подавления дребезга контактов (дребезг может приводить к неправильному определению набранной цифры из-за того, что счетчик будет считать импульсы дребезга). С выхода схемы подавления дребезга контактов импульсы набора поступают на схему выделения огибающей набора и счетчик-дешифратор набираемой цифры. Схема выделения огибающей набора формирует на своем выходе импульс, длительность которого примерно равна длительности набираемой цифры. Этот сигнал поступает на вход управления счетчика-дешифратора набираемой цифры. На счетный вход этого счетчика поступают импульсы набора. Таким образом, при наборе номера счетчик считает количество импульсов набора, а после прекращения набора цифры показания счетчика с некоторой задержкой, необходимой для анализа, сбрасываются, подготавливая счетчик для счета второй цифры набора. В схеме счетчика-дешифратора счетчик считает в двоичном коде, а дешифратор преобразует этот код в десятичный, что выражается в изменении состояния соответствующего выхода (выход 0 соответствует состоянию цифры 10). На счетчик-дешифратор количества набранных цифр поступают сигналы с выхода схемы анализатора состояния линии (на вх. управления) и с выхода схемы выделения огибающей набора (на счетный вход). Анализатор состояния линии формирует определенное логическое состояние, когда линия занята (снята трубка ТА) независимо производится набор или нет. Когда трубка снята – разрешается счет количества набранных цифр, когда линия освобождается – показания счетчика сбрасываются, подготавливая его к счету последующего поднятия трубки. Счетчик-дешифратор количества набранных цифр считает только до двух (после набора второй цифры с выхода 2 этого счетчика сигнал блокирует его собственную работу и работу счетчика-дешифратора набираемой цифры), что уменьшает вероятность сбоя логического анализатора при дальнейшем наборе номера. На вход логического анализатора поступают сигналы 0, 6, 1 от счетчика-дешифратора набираемой цифры и сигналы с выхода 1 счетчика-дешифратора количества набранных цифр. Для увеличения помехоустойчивости схемы работа логического анализатора разрешается сигналом с выхода анализатора состояния линии только при снятой трубке. «Отбой линии», т.е. кратковременное ее размыкание, происходит следующим образом: после набора запретного номера 061, логический анализатор запускает схему ждущего мультивибратора, на выходах которого формируются короткие импульсы с заданной длительностью задержки 2-го импульса относительно 1-го. 1-ый импульс через электронный коммутатор включает поляризованное реле и при этом размыкая контакт реле в цепи ТА. Линия освобождается (эффект аналогичен тому, что абонент положил трубку), АТС при этом разъединяет абонента. 2-ой импульс выключает поляризованное реле и ТА снова подключен к линии. Поляризованное реле питается от линии связи через схему питания реле, обеспечивающую необходимую энергию для срабатывания реле и микропотребления в режиме ожидания.


# 5. Принципиальная электрическая схема

Для компактности представления принципиальной схемы, некоторые узлы объединены в один блок:

1. схема питания реле;
2. делитель напряжения и схема подавления дребезга;
3. преобразователь полярности и стабилизатор напряжения;
4. счетчик цифры и счетчик количества цифр;
5. логический анализатор и ждущий мультивибратор.

# 6. Конструкция лабораторного макета (печатная плата)

# Список использованных источников

1. Балахничев И.Н., Дрик А.В., Крупа А.И. Борьба с телефонным пиратством. -Минск: ОМО "Наш город". 1988.
2. Балахничев И.Н., Дрин А.В. Практическая телефония. –Минск: "Наш город”, 1998.
3. Каталог-справочник. Оружие шпионажа. -М.: Империал, 1994.
4. Шило В.Л. Популярные цифровые микросхемы: Справочник. –Челябинск: Челябинское отделение, 1988.
5. Якубовский С.В. и др. Цифровые и аналоговые интегральные микросхемы. -М.: Радио и связь, 1999.