Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Кафедра Автоматическая электросвязь
Специальность: Радиотехника, электроника и телекоммуникации

Допущен к защите
Зав. кафедрой АЭС
Чежимбаева К.С. к.т.н., доцент_____
(Ф.И.О.)подпись«_____»_____2014г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ
пояснительная записка

Тема Исследование модели устройства защиты речевой информации в канале связи

Магистрант_____ Аманова А.Д.
подпись(Ф.И.О.)

Руководитель диссертации_____ д.т.н., проф. Якубова М.З.
подпись (Ф.И.О.)

Рецензент_____
подпись (Ф.И.О.)

Консультант по ВТ_____ к.т.н., проф. Туманбаева К.Х.
подпись (Ф.И.О.)

Нормоконтроль_____ ст.препод. Абиров Д.А.
подпись (Ф.И.О.)

Алматы 2014г.

Некоммерческоеакционерноеобщество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Факультет Радиотехники и связи
Специальность: Радиотехника, электроника и телекоммуникации
Кафедра Автоматическая электросвязь

ЗАДАНИЕ

на выполнение магистерской диссертации

Магистранту Амановой Айгул Джумасатовне
(фамилия, имя, отчество)

Тема диссертации Исследование модели устройства защиты речевой информации в канале связи
утверждена Ученым советом университета №108от «16»ноября2012 г.
Срок сдачи законченной диссертации «_26__» ___мая 2014 г.
Цель исследования: Исследование устройства защиты информации в канале связи, разработка принципиальной схемы и компьютерного моделирования в пакете SystemView, выбор и расчет надежности его элементов.
Перечень подлежащих разработке в магистерской диссертации вопросов или краткое содержание магистерской диссертации:
В данной магистерской диссертации представлен анализ всех формальных моделей безопасности, разработаны критерий и требований по информационной безопасности, выбран оптимальный вариант устройства защиты речевой информации, разработана принципиальная схема и компьютерное моделирование в пакете SystemView, рассчитана надежность устройства.
Перечень графического материала (с точным указанием обязательных чертежей)
1. Ролевая модель управления доступом. 2. Структурная схема устройства защиты речевой информации. 3. Биквадратный фильтр. 4. Сдвоенный ПФ с внутренней частотной коррекцией. 5. Полосовой RC - фильтр с внутренней частотной коррекцией. 6. АЦП последовательного приближенияю 7. Типовая схема включения ЦАП. 8. Графическое изображение регистра К589ИР12. 9. Типовая схема включения К555ЛН1. 10. Генератор тактируемых импульсов на ИМС К555ЛА3. 11. Графическое изображение микросхемы К555Л1А3. 11. Графическое изображение скремблера на ИМС 1146ФП4. 12. Принципиальная схема устройства защиты речевой информации. 13. Модель схемы в пакете SystemView. 14. Исходный и результирующий сигналы смоделированной системы

Рекомендуемая основная литература

1. Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонных каналах. - М.: Энергоатомиздат, 2006.
2. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь,1999.
3.Тарабрин Б.В. Интегральные микросхемы справочник. – М.: Энергоатомиздат,1995.
4. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ,2007.
5. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь 2000..
6. National Bureau of Standards, Data encryption Standard, Federal Information Processing Standard Publication 46, (NTIS NBS-FIPS PUB 46), January 2005.

Г Р А Ф И К
подготовки магистерской диссертации

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
1. Обзор существующих методов и средств защиты информации	15.11.2013 г.	Выполнено
2. Разработка критериев и требований по информационной безопасности	17.01.2014 г.	Выполнено
3. Выбор оптимального варианта устройства защиты речевой информации	3.03.2014 г.	Выполнено

Дата выдачи задания 5.11.2012 г.

Заведующий кафедрой _____ (к.т.н., доцент Чежимбаева К.С.)
(подпись) (Ф.И.О.)

Руководитель диссертации _____ (д.т.н., проф. Якубова М.З)
(подпись) (Ф.И.О.)

Задание принял к исполнению
магистрант _____ (Аманова А.Д.)
(подпись) (Ф.И.О.)

Аңдатпа

Осы аталған магистерлік диссертацияда бүкіл формалды қауіпсіздік модельдердің талдауы жүргізіліп, ақпаратты қорғау талаптары қарастырылды. Ақпаратты қорғау құрылғысының оңтайлы нұсқасы таңдалынды, және де құрылғының принципиалды схемасы мен SystemView бағдарламасында компьютерлік моделі құрастырылды. Соңында құрылғының сенімділігі есептелінді.

Аннотация

В данной магистерской диссертации представлен анализ всех формальных моделей безопасности, разработаны критерий и требований по информационной безопасности. Был выбран оптимальный вариант устройства защиты речевой информации, а также разработана принципиальная схема и компьютерное моделирование в пакете SystemView. В конце была рассчитана надежность устройства.

Annotation

This master's thesis presents an analysis of all formal security models. And at project was developed criteria and requirements for information security. There was chosen the best option for information security device, and developed concept and computer simulation model on the package SystemView. At the end there was calculated reliability of this device.

Введение

С развитием средств телекоммуникаций все больше информации стало передаваться по каналам связи, используя при этом различные методы и информационные технологии.

Эволюция средств телекоммуникаций и систем позволило не только передавать и принимать информацию, но и получать ее несанкционированным путем посредством перехвата. Поэтому возникла проблема сохранности информационного сообщения. Большое внимание в настоящее время уделяется информационным технологиям, когда обработке и передаче информации с помощью компьютера и на данном направлении достигнуты высокие результаты. Но следует отметить, что большинство информации передающейся по каналам связи является речевая. Вследствие этого в данной работе рассмотрены средства и методы защиты речевой информации, которая может передаваться по обычному стационарному телефону, мобильным и спутниковым средствам связи, а также при помощи компьютера, используя т.н. IP-сеть.

Основной целью в данной работе является выработка конкретного метода и средства защиты речевой информации на базе существующих методов и средств защиты информации, подбора оптимальной математической модели защиты, а также разработка устройства защиты информации работающего в диапазоне тональной частоты. Проведя рассмотрение и изучение методов защиты информации необходимо было сделать обзор существующих и возможных каналов утечки на объектах телекоммуникации, а также изучить основные приемы сбора акустической (телефонной) информации. При рассмотрении существующих средств защиты речевой информации и проведя обзор существующего рынка по защите информации необходимо было все устройства классифицировать по способу контроля за несанкционированным доступом, виду защиты, степени защиты и степени сложности устройств. Необходимо на базе существующих математических моделях безопасности выбрать оптимальную модель защиты информации в тональном диапазоне. На базе проведенных исследований должна быть предложена разработка устройства защиты речевой информации. При разработке необходимо также учитывать актуальность поставленной задачи и насыщенность рынка различными средствами защиты.

Степень информатизации в данный момент времени достигла очень высоких показателей по скорости передачи, по виду обработки и по виду хранения. Но следует отметить, что средства взлома и устройства несанкционированного доступа намного опережают рынок существующих средств защиты информации. Если в компьютерных системах в этом отношении уже достигнут небольшой паритет, то на телекоммуникационных системах средства защиты информации почти не применяются. Поэтому в задачу магистерской диссертации поставлено научное исследование всей

проблемы в целом и исходя из требований по стойкости и защите предлагается оптимальный вариант устройства защиты речевой информации, который также должен будет удовлетворять выбранному методу защите и математической модели безопасности. Немаловажным фактором при данном анализе и проектировании устройства является выявление критерия защиты исходя из конкретного случая.

Теоретическая значимость работы заключается в выборе математической модели безопасности и оценки степени защиты информации.

Научная новизна данной работы заключается в разработке формул для оценки прочности защиты информации и разработке новых алгоритмов программно-аппаратной защиты информации.

По имеющимся литературным источникам в области соответствующих средств обработки и передачи данных, защита информации проводилась в основном средствами шифрования. Поэтому практическая значимость этой работы состоит в том, что использована комбинация шифрования и скремблирования и предложено конкретное средство защиты речевой информации в любых каналах где осуществляется передача голоса.

1 Обзор существующих методов и средств защиты информации

Ценность информации является критерием при принятии любого решения о ее защите. Существуют следующие виды информации по уровню важности:

- жизненная, незаменимая информация;
- важная информация, которая может быть заменена или восстановлена с большими расходами;
- полезная информация, которая является трудно восстанавливаемой, но пользователь без нее может эффективно функционировать;
- незначительная информация, которая не необходима для пользователя.

Однако нельзя отнести информацию только к одной из этих категорий, т.к. одна и та же информация для отдельных пользователей может быть отнесена к различным категориям важности. Применительно к современным условиям и назначению систем телекоммуникации все виды информации можно поделить на три группы:

- секретную;
- конфиденциальную (важную);
- открытую.

В настоящее время в системах телекоммуникации существует много возможных способов несанкционированного доступа к информации [2]: просмотр, копирование данных, подмена данных; ввод ложных программ, команд и сообщений; подключение с этой целью к линии и каналам связи; использование отладочных и аварийных программ и устройств; чтение остатков информации; прием сигналов побочного электромагнитного излучения и наводок информации; использование неисправностей и сбоев аппаратуры, ошибок операторов, программных ошибок и т.д.

Далее мы будем рассматривать основные каналы утечки информации.

1.1 Каналы утечки информации

По каналам утечки информации можно группировать несанкционированное получение информации частного и коммерческого характера [3]:

- акустический контроль комнаты, автомобиля, непосредственно человека; контроль и слушание телефонных каналов связи, перехват факса и передача модема сообщений;
- перехват информации о компьютере (включая компьютерную эмиссию радио), несанкционированное введение в базах данных;

– скрытая фотография и видео, снимающееся с помощью специальной оптики;

– визуальное наблюдение по объекту;

– несанкционированное знакомство с открытыми публикациями фирмы (предприятие);

– аналитическое исследование процессов деятельности предприятия, его полезного продукта и производственных отходов.

1.2 Приемы сбора акустической (телефонной) информации

1. Перехват акустической (телефонной) информации с использованием радиомикрофонов («жучков»), которые используются для передачи по радиоканалу акустической информации об объекте.

Существуют следующие виды радиомикрофонов:

– непрерывно излучающие (простейшие);

– с включением на передачу при появлении в контролируемом помещении разговоров или шумов (акустоматы);

– дистанционно управляемые, т.е. включающиеся и выключающиеся при помощи передатчика дистанционного управления на время, необходимое для контроля объекта. Они могут быть приспособленными для ношения на теле человека и одежде, или же замаскированными под предметы обихода.

Например, в случае если установка «жучка» непосредственно на объекте невозможна, то используют стетоскопные передатчики. С помощью этих передатчиков можно прослушать переговоры через твердую преграду (стену, стекло, корпус автомобиля и т.д.). И чем тверже и однороднее преграда, тем лучше они работают [4].

«Жучки» различают по:

– диапазону используемых частот (40МГц…1,5ГГц);

– долговременности работы (от 5 ч. до 1 года);

– дистанции передачи (от 15м до 10 км);

– виду используемой модуляции: амплитудная (АМ), частотная (ЧМ), узкополосная ЧМ, широкополосная, шумоподобная и др.

Также «жучки» можно различить по тем или иным способам закрытия (фактически по шифровке сигнала).

Применение радиопередающих средств предполагает обязательное наличие приемника, и с помощью этого приемника осуществляется прием информации от «жучка». Они также бывают разные (бытовые и специальные).

2. Прослушивание с использованием метода «высокочастотной (ВЧ) наводки». Этот метод основан на подключении к одному телефонному проводу высокочастотного генератора, а к другому амплитудного детектора с усилителем. Оно позволяет прослушивать помещение через телефон с лежащей

трубкой. Физика процесса очень проста — ВЧ колебания проходят через микрофон или обмотки звонка, обладающие «микрофонным эффектом», и модулируются при помощи акустических сигнал помещения, где установлен телефонный аппарат.

3. Прослушивание с использованием «жучков». В качестве канала передачи они используют силовую сеть. «Жучки», которые встраиваются в электрические розетки, удлинители, тройники, бытовую аппаратуру, используют для передачи акустической информации силовую сеть 127, 220 В. У них есть такие преимущества как неограниченное время работы и сложность обнаружения. Только специально предназначенные приемники принимают информацию от таких «жучков». Эти приемники подключаются к силовой сети в радиусе до 300 м от «жучка» (по длине проводки) до силового трансформатора, обслуживающего здание или комплекс зданий.

4. Акустические закладки, ведущие передачу в инфракрасном диапазоне (ИК передатчики) и, соответственно, специальные приемники к ним. Можно сказать, что их очень сложно обнаружить. Срок работы этих изделий составляет 13 суток, но следует учесть, что прослушать их передачу можно только в прямом визуальном контакте, т.е. для этого надо непосредственно видеть закладку. Поэтому их размещают у окон, вентиляционных отверстий и т.п..

5. Акустические радиопередающие закладки, которые используют «двойную модуляцию». Физика процесса проста, акустический сигнал модулирует промежуточную несущую, а выходящий сигнал подается на вход непосредственно передатчика. Невозможно прослушать такую закладку (даже очень хорошим сканирующим приемником), слышен будет только шум. Так что это закладки с очень неплохим «закрытием».

6. Закладки и переговорные устройства, которые используют в качестве канала передачи элементы конструкций зданий, воду и другие среды.

7. Системы накапливания информации и скоростной передачи ее по команде от оператора.

8. Прослушивание помещения при помощи лазерного микрофона, который представляет собой систему, которая позволяет на расстоянии до 300 м считывать вибрацию оконных стекол и преобразовывать ее в слышимую речь. Есть два типа лазерных микрофонов: для работы первого типа необходимо «метить» стекло, т.е. наносить на него пятно специальной краски, которая будет отражать лазерный луч обратно в место излучения, где он принимается фотоприемным устройством; для работы второго типа ничего этого не требуется.

9. Системы, использующие перемодуляцию радиоизлучения на нелинейных элементах, входящих в состав различной электронной техники или специально помещаемых в контролируемых помещениях. Такие системы стоят очень дорого, и они также сложны в эксплуатации.

10. Системы магнитной записи звука. К этим системам можно отнести диктофоны и регистраторы. Обычно они используются людьми, которые

входят в состав группы, ведущей какие-либо переговоры, или же людьми, которые являются просто собеседником.

Если у диктофона есть система включения от голоса (акустомат), а противник регулярно посещает контролируемое помещение, то в таких случаях диктофон используется как закладка. Диктофоны могут комплектоваться дополнительными устройствами такими, как выносные микрофоны с отдельным питанием и усилителем; выносные вибромикрофоны (стетоскопные), позволяющие записать разговор через стену; микрофоны с достаточно длинным кабелем (применяются для записи разговоров, например на кухне, через вентиляционную шахту).

11. Прослушивание переговоров группы лиц с использованием направленных микрофонов. С помощью направленных микрофонов можно прослушивать и записывать разговор на довольно значительных расстояниях (до 70 м). Есть три вида направленных микрофонов: микрофон-зеркало имеет параболический отражатель, в фокусе которого находится чувствительный обычный микрофон; микрофон-трубка, который может камуфлироваться (маскироваться) под трость или зонтик; плоские направленные микрофоны могут встраиваться в стенку, атташе-кейса или носиться в виде жилета под рубашкой и пиджаком. Они наиболее удобны в использовании, так как у оператора в руках нет никаких предметов, которые привлекали бы внимание и вызывали настороженность информанта.

12. «Междугородная закладка» дает всемирно-дистанционную возможность прослушивания помещения. «Междугородная закладка» представляет собой устройство, которое подключается к телефонной линии или встраивается в телефон и имеет свой встроенный или выносной микрофон. Позвонив, даже из другого города, на телефон, оборудованный таким образом, и передав специальный код включения, оператор отключает телефон абонента, не позволяя ему зазвонить, и начинает прослушивать разговоры и акустические шумы контролируемого помещения по телефонной линии. Если абонент в момент прослушивания вдруг решит куда-либо позвонить и снимет трубку, то устройство мгновенно отключится, и телефон будет работать совершенно нормально.

13. Самым распространенным способом несанкционированного получения информации частного и коммерческого характера стало прослушивание телефонных переговоров объекта благодаря тому, что: для того чтобы установить аппаратуру для прослушивания, не требуется особых навыков, не требуется вторжения в помещение, где установлен телефон объекта; по стоимости аппаратура для телефонного прослушивания вполне доступна даже малообеспеченным гражданам; телефонные переговоры представляют большой интерес для лиц, занимающихся сбором информации.

Для прослушивания телефонных переговоров объекта [1] можно непосредственно подключить к линии телефонный капсюль или магнитофон с системой автоматического включения записи с началом разговора объекта по телефону (подключение может осуществляться как в помещении, где

установлен телефон, так и в любом месте линии от абонента до АТС включительно) или установить на линии радиопередающую закладку (телефонный «жучок»). Существуют два типа телефонных «жучков»: с параллельным подключением к линии (они труднее всего обнаруживаются, но требуют внешний источник питания); с последовательным включением в разрыв одного провода телефонной линии. Питание «жучка» осуществляется от АТС по телефонной линии и в эфир он выходит (т.е. начинает передачу) как только абонент поднимет трубку. Для того, чтобы принимать информации от радиопередающих телефонных закладок используются такие же приемники, как и для акустических «жучков».

14. Специальные двухканальные приемники. Они позволяют принимать на довольно значительном расстоянии разговоры объекта по радиотелефонам.

15. Средства прослушивания телефонных переговоров позволяют получить смысловую информацию и определить номер телефона, на который звонит объект.

16. Есть техника, которая позволяет непосредственно, либо используя магнитофонную запись обмена двух факсов или модемов, получить расшифровку и распечатку документа. Речь можно также записать в память компьютера для последующей передачи.

17. Перехват компьютерной информации. Существует два распространенных способа для дистанционного несанкционированного считывания содержимого чьего-либо компьютера. Первый — это прием паразитных радиоизлучений компьютера, а точнее говоря, его дисплея, с синхронизацией изображения приемом импульсов развертки, излучаемых строчным трансформатором. Аппаратура для этого вида технической разведки достаточно проста и изготавливается на базе обычного малогабаритного телевизора. Появились устройства, которые позволяют на удалении до 50 м получать устойчивую картинку-копию содержимого контролируемого дисплея. Второй способ, базируется на приеме высокочастотных наводок в силовую сеть через блок питания компьютера. Он требует непосредственного подключения к силовой сети и последующей чрезвычайно сложной обработки принятой информации.

18. Несанкционированное внедрение в базы данных пока не получило (в нашей стране) широкого распространения из-за низкого уровня развития компьютерной обработки информации в коммерческих кругах. Компьютерные «взломщики» пока ограничиваются проработкой вопросов бесплатного получения коммерческой информации из информационных сетей общего пользования.

1.3 Сбор оптической (визуальной) информации

Этот сбор информации включает в себя скрытые фото- и видеосъемки, визуальное наблюдение и досмотр обеспечиваются фото- и видеокамерами различных типов:

- камкордеры (камеры, совмещенные с видеомагнитафоном);
- скрытые (миниатюрные), т.е. камуфлированные под обычные предметы, встраиваемые в бытовую технику и передающие видеоинформацию либо по кабелю, либо с помощью собственных миниатюрных телевизионных передатчиков;
- камеры, замаскированные под пачку сигарет, заколку для галстука, сумку, кейс, книгу, наручные часы.

Эта техника может снабжаться специальными насадками и объективами, включающими:

- эндоскопы – гибкие световые насадки, снабженные объективами и системой управления (поворот объектива относительно оси гибкого шнура световода), которые могут дополняться системой подсветки для осмотра и фотографирования темных помещений и полостей (например, бензобак автомобиля);
- объективы- иглы – устройства, устанавливаемые на стандарте фото- и видеокамеры и предназначенные для съемки через отверстия небольшого диаметра (до 5…6мм);
- телескопические объективы (телевики), дающие возможность вести съемку с дальних дистанций (существуют объективы с увеличением до 1500 раз);
- -объективы-камуфляжи, помогающие приспособить фото- и видео-камеры для скрытой съемки из сумок, кейсов и т.п.;
- объективы, совмещенные с прибором ночного видения (с ИК подсветкой или безтактовой) и предназначенные для съемки в темное время суток.

1.4 Методы защиты речевой информации

Основные методы защиты информации от несанкционированного доступа можно разделить на две группы:

1 Организационные или организационно технические;

2 Аппаратные или программно аппаратные.

Рассмотрим эти методы защиты.

1.4.1 Организационно - технические методы защиты. В эту группу входят:

– организация охраны помещения, где размещается аппаратура связи, защита его от акустического контроля и разработка мероприятий по противодействию визуального наблюдения;

– использование приборов обнаруживающих подслушивающие устройства при несанкционированном подключении к телефонным каналам связи, перехвата факсовой и модемной связи;

– использование кабелей в герметичной оболочке с контролем разгерметизации (появление утечки газового или другого наполнителя) при повреждении этой оболочки;

– экранирование кабелей и их зануление (часть жил используется для передачи по ним шумовых сигналов с большим уровнем);

– прокладка кабелей в трудно доступных траншеях с устройствами сигнализации о проникновении в них;

– зашумление помещений и строительных конструкций с помощью специальных генераторов акустических, электрических и вибрационных помех.

В первую группу также входят такие методы как:

– использование шумоподобных несущих в каналах радиосвязи;

– использование в подвижной радиосвязи сотовых структур (вместо радиальных), когда при перемещении абонента по территории сети изменяются несущие частоты;

– использование систем типа ограничения доступа;

– отказ от использования радиоканалов.

В последнее время стало широко применяться аппаратура технического противодействия (АТП) несанкционированному доступу и информации на объектах связи. Необходимо выполнить три условий, чтобы эта аппаратура эффективно действовала и приносила реальную помощь:

1) Правильного подбора техники и ее соответствие заявленной фирмой изготовителем техническим параметрам;

2) Грамотного проекта оборудования помещения в соответствии с индивидуальными особенностями и качественного монтажа;

3) Соблюдение правил эксплуатации аппаратуры и рекомендаций по оперативному использованию имеющихся технических средств.

Минимальный набор АТП позволяющий эффективно обеспечить информационную безопасность должен включать в себя следующие устройства:

а) подавление акустических закладок по радиоканалу;

б) защита стен, потолков, пола и оконных стекол от стетоскопов и лазерного микрофона;

в) подавление телефонных закладок и автоматических диктофонов подключенных к телефонной линий;

г) криптографической защиты телефонных разговоров при ограниченном числе телефонных собеседников;

д) постановки помех по пути напряжения питания 127…220В.

По данным специалистов [1] в области защиты речи, имеющееся в продаже оборудование обнаружения негласного съема информации с проводных каналов реагирует лишь на изменение импеданса линии связи. Поэтому использование такого оборудования не может гарантировать его владельцу надежную защиту от утечки информации. Можно также отметить, что сотовая связь значительно более защищена, если сравнивать с другими системами радиосвязи. Но нельзя исключать возможность перехвата с помощью имеющихся в продаже сканеров (приемников используемых для прочесывания радиоканалов).

Организационные и организационно-технические методы могут быть достаточными для защиты конфиденциальной информации. Однако в ряде случаев в коммерческих сетях экономически выгоднее и более надежно можно защититься от утечки информации путем использования аппаратных (аппаратура конфиденциальной связи – АКС) и программно-аппаратных (устройства конфиденциальной связи – УКС) устройств.

1.4.2 Аппаратные или программно - аппаратные методы. По степени защиты аппаратные или программно - аппаратные методы можно условно классифицировать на три группы.

1) Простейшие (маскираторы), где осуществляется простое кодирование;

2) Средней сложности (скремблеры или перемешиватели). Здесь используется не очень сложное динамическое кодирование. При подслушивании с использованием современной вычислительной техники, полезная информация может быть раскрыта за ограниченный отрезок времени. Это такие методы, при которых законы кодирования изменяются в процессе передачи информации. В каналах ТЧ – это коммутируемая инверсия, частотные перестановки, а также комбинация этих методов. При использовании рассмотренных методов не устраняются некоторые признаки исходного речевого сигнала в канале связи, т.е. в канале связи может сохраниться остаточная разборчивость речи или такие признаки, которые позволяют восстановить исходный сигнал с помощью устройств типа «видимая речь» (спетрограф, с помощью которого получается трехмерное изображение в координатах время, частота, амплитуда) [5];

3) Высокой сложности (шифраторы или шифрирующие устройства – аппараты засекречивания АЗ или ЗАС), в которых используются достаточно сложные алгоритмы преобразований, поэтому для извлечения полезной информации потребуется необозримый срок (например, более длительный, чем средняя продолжительность жизни человека). Остаточная разборчивость в канале нулевая, что дает ей большое преимущество по сравнению с двумя предыдущими группами.

Место включения устройства или аппарата конфиденциальной связи (УКС или АКС) в канале связи может быть различным и зависит от ряда факторов. Если необходимо защититься от утечки по любым сетям, то включают его на входе в телефонный аппарат (т.е. перед микротелефонной

трубкой). Ну а если стоит задача защититься от утечки информации по каналам связи, то достаточно будет включить УКС на выходе телефонного аппарата (в абонентскую линию). Если же необходимо предотвратить утечку информации только на отдельных участках телефонной сети, то в таком случае достаточно включить УКС на входе этого участка. Очевидно, что в любом случае для правильного приема информации должно быть включено ответное устройство на приемной стороне.

Место включения зависит также от условий эксплуатации или от того, к какой группе относится абонент. Таких групп три: стационарные, подвижные, блуждающие. Стационарные абоненты находятся в определенных точках сети. Подвижные находятся на перемещающихся средствах (автомобилях, самолетах, поездах), имеющих телефонные аппараты, включенные в сеть общего пользования. У стационарных и подвижных абонентов телефонные номера закреплены. У блуждающих абонентов номера не закреплены и они могут вести разговоры с чужих телефонов.

Обязательной составляющей аппаратов конфиденциальной связи (кроме тех, в которых осуществляется простое кодирование) является наличие шифрообразующего блока (криптоблока). В устройствах функции шифроблока могут быть реализованы с помощью программных методов. Алгоритмы работы при этом могут быть «фирменными» (т.е. используемыми только в изделиях данной фирмы) или стандартными, которые используются для возможности встречной работы изделий различных фирм.

К устройствам и аппаратам конфиденциальной связи предъявляются, обычно, специальные требования, такие как отсутствие побочных излучений, по уничтожению «ключевой» информации при попытках несанкционированного проникновения внутрь устройства и т.п.

Устройства конфиденциальной связи должны также удовлетворять основным требованиям рекомендаций МККТТ и ГОСТ на оконечные устройства связи и алгоритмы стыков. Это необходимо для того, чтобы получить сертификат на право подключения и обеспечивать работу по стандартным каналам связи.

1.5 Средства защиты информации

1.5.1 Шифровальные и криптографические средства защиты информации при ее передаче по каналам связи. Информацию при передаче ее по каналам связи защищают с помощью средств, криптографической защиты (СКЗИ). Их доля на рынке, по литературным данным [2] составляет 13,2%. Эти средства можно охарактеризовать тем, что они обеспечивают одну из самых надежных защит информации от несанкционированного доступа к ней. Помимо всего этого, СКЗИ защищают информацию от модификации. Но, несмотря на высокую степень защиты информации, применение СКЗИ имеет и свои

недостатки. Так, например, стойкость СКЗИ потенциальная. А это значит, что гарантируется при соблюдении определенных требований, реализация которых на практике очень сложна.

1.5.2 Средства защиты информации от ее утечки по побочным каналам. Для защиты информации от утечки по физическим полям (их доля составляет 2,4% в общей сегментации рынка [3]) используют следующие методы и средства защиты:

– электромагнитное экранирование устройств или помещений, в которых расположена вычислительная техника;

– активная радиотехническая маскировка с использованием широкополосных генераторов шума, которые широко представлены на нашем рынке.

Наибольшее распространение на рынке сегодня имеют средства второй группы – генераторы шума. Тем не менее наиболее радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако этот способ требует значительных капитальных затрат и поэтому сегодня практически не применяется.

1.5.3 Средства защиты информации при ее пересылке или транспортировке. Рассмотрим средства и методы защиты информации, обеспечивающих безопасность хранения, транспортировки носителей информации и защиту их от копирования. В основном это специальные тонкопленочные материалы с изменяющейся цветовой гаммой или голографические метки, которые наносятся на документы и предметы (в том числе и элементы компьютерной техники автоматизированных систем). Они позволяют:

– идентифицировать подлинность объекта;
– контролировать несанкционированный доступ к ним.

Критерии выбора, на которых основываются предпочтения потребителей на рынке СЗИ, распределились следующим образом:

– надежность;
– стоимость;
– удобство эксплуатации;
– гарантийное обслуживание;
– надежность фирмы поставщика;
– быстрота действия.

Кроме того, специалисты отметили [4], что при выборе техники и методов заказчики ориентируются на такие критерии, как эффективность выполнения своих услуг, качество технической поддержки, наличие сертификатов ГТК, а также возможность обучения.

В ближайшее время небольшим спросом на рынке СЗИ будут

пользоваться средства защиты информации при работе с персональными ЭВМ или циркулирующей в ЛВС (локально-вычислительная сеть), а именно: программные и программно-аппаратные средства защиты от НСД – 12,8%, межсетевые экраны – 11,2%, а также электронно-цифровая подпись – 9,6%(в силу наибольшей вероятности утечки информации через эти каналы) [5]. Кроме того, наибольшим спросом в ближайшее время будут пользоваться системы обнаружения атак и анализа защищенности, потому что они смогут обеспечить более высокий уровень защищенности, чем традиционные средства защиты информации, и потому что тони более адаптивны к постоянным изменениям в корпоративной сети.

По мнению ряда аналитиков, в ближайшие несколько лет будет активно развиваться сегмент рынка, связанный с услугами по созданию комплексных систем информационной безопасности, т.е. будут разрабатываться интеграционные проекты, включающие в себя различные технологии и средства защиты, объединенные единой идеей * технической политикой системного интегратора. В плане технологических направлений большой потенциал имеют биометрические технологии аутентификации пользователей. Особенно это связано с удаленным ON-LINE доступом к корпоративным информационным ресурсам системы. Сейчас качество подобных решений быстро возрастает , и в ближайшее время соотношение цена/качество позволит широко использовать такие продукты.

Темпы развития информационных технологий заметно опережают темпы создания новых механизмов и средств защиты. Следовательно, недостатки средств защиты информации становятся существенным ограничением на пути развития и применения современных информационных технологий.

И не смотря на все разнообразие представленных рынке СЗИ, специалисты в этой обрасти почти единодушны в одном – средств, отвечающих такому критерию, как абсолютная надежность защиты, просто не существует. Поэтому, основной курс в стратегии построения системы защиты должен быть взят на то, чтобы она была достаточной, надежной, эффективной и управляемой. И что характерно, эффективность ее определяет даже не сумма финансовых средств, потраченных на нее, а способность адекватно реагировать на все попытки утечки информации. Любое мероприятие по защите информации от НСД должно носить комплексный подход, т.е. объединять разнородные меры, методы и средства противодействия угрозам, в том числе правовые, организационные и программно-технические.

1.5.4 Средства защиты речевой информации. Рассмотрим некоторые промышленные средства защиты, относящиеся к аппаратуре технического противодействия (АТП):

1) Скоростной поисковый приемник радиосигналов «Скорпион». Назначении этого прибора состоит в том, чтобы на время его включения выводить из работоспособного состояния радиопередающие телефонные закладки и диктофоны подключенные к линии защищаемого объекта;

2) Детектор радиопередатчиков ДМ-2 – профессиональный карманный детектор-локатор. Он используется для выявления и обнаружения маломощных радиосигналов даже на фоне сильных помех;

3) Детектор-сканер передатчиков ДМ-12 профессиональная система для обнаружения радиосигналов в широком диапазоне частот;

4) Нелинейный детектор-локатор ДМ-13 – высокоэффективный прибор для выявления, локализации радиосигналов практически любых средств подслушивания, а также скрыто установленных электронных взрывателей;

5) Детектор-локатор излучения ДМ-14 – переносной универсальный комплекс для обнаружения и локализации радиосигналов в широком диапазоне частот;

6) Радиоанализатор R9000 – ДМ-20 – профессиональный радиоприемный многофункциональный комплекс. Он используется для поиска, контроля и анализа любых радиосигналов в диапазоне 0,1…2000МГц;

7) Нелинейный детектор коммутаций ДМ-21 – современный комплекс для оценки параметров проводных коммуникаций, его цель состоит в обнаружении посторонних подключений, в том числе для подслушивания и снятия информации;

8) Нелинейный локатор «Орион» - изделие американской фирмы REI. Имеет анализатор второй и третьей гармоник, работающий в диапазоне 820…1000МГц;

9) Спектральный коррелятор OSCOR (OSC-5000) – этой же фирмы REI. Данный прибор является мощным средством для обнаружения всевозможных подслушивающих устройств. Он представляет собой сочетание спектрального прибора способного контролировать широкий диапазон 50Гц-3ГГц, и цифрового корректора производящего анализ частоты на принадлежность подслушивающему устройству;

10) Маскиратор телефонных разговоров «Туман» - выполнен в виде приставки, расположенной под телефонным аппаратом и включаемый между ним и микротелефонной трубкой. Принцип его работы основан на аналоговом преобразовании речевого сигнала. При этом постороннее лицо не сможет прослушивать телефонный разговор, если он не снабжен аналогичным преобразователем;

11) Абонентский терминал – маскиратор «Исса» позволяет передавать конфиденциальную информацию и данные по телефонным каналам сети общего пользования, а также через УКВ радиостанции, защищая их от преднамеренных и случайных искажений знаков и навязывание ложных сообщений;

12) Устройство передачи конфиденциальной информации «Вуаль», предназначена для засекречивания и передачи по телефонному каналу общего пользования конфиденциальных сообщений представляющих коммерческую тайну. В нее входят малогабаритная клавиатура калькуляторного типа, устройство ввода-вывода сообщений и блок питания;

13) Криптоплата «Мега» предназначена для шифрования информации, хранящейся на внутренних и внешних накопителях ПЭВМ и представляет собой высокоскоростную приставку с программным обеспечением;

14) Скремблеры аналого-цифрового типа предназначены для защиты телефонных разговоров от несанкционированного прослушивания по линии. Скремблер СТА-1000 выполнен в виде малогабаритной приставки под настольной телефонный аппарат любой марки, подключается к телефонной сети общего пользования, работает в дуплексном режиме. Приставка О-135/Р и SCR-M1,2 аналогичны скремблеру СТА-1000, только имеют дополнительное число кодовых комбинаций до 10^7;

15) Аппаратура засекречивания речи и цифровой информации предназначена для дуплексных, полудуплексных (F-24Д) и симплексных (E-24Д и E-24) радиоканалов метрового и дециметрового диапазонов, имеющих вход-выход в соответствии с международным стандартом С1-Н. Аппаратура обеспечивает засекречивание речи в условиях повышенного уровня шума и цифровой информации, поступающей от источника со скоростью 1200бит/с, передаваемой по УКВ-ДЦВ радио и проводным линиям связи.

1.6 Выводы по первой главе

Обзор существующих методов и средств защиты речевой информации показал:

1) Необходимость анализировать каналы утечки информации и прилагать конкретные мероприятия по борьбе с НСД;

2) Рассмотрены конкретные методы защиты речевой информации и предложены такие, которые включают организационно – технические, так и аппаратно – программные методы;

3) Анализ аппаратных методов показал, что наилучшими средствами защиты являются включение скремблеров высокой сложности;

4) Анализ средств защиты речевой информации показал, что наилучшим средством является аппаратура засекреченной речи F-24D, E-24D и E24.

2 Модели безопасности

Согласно требованиям большинства критериев оценки безопасности, система защиты должна иметь работу на основе определенных математических моделей, посредством которых должно быть теоретически доказано соблюдение системы защиты к требованиям политики безопасности набора. Алгоритм, который выполняет эту проверку, необходим для решения цели. Согласно цели увеличить информационную безопасность в телекоммуникационных сетях, мы рассмотрим существующие модели безопасности.

2.1 Формальные модели безопасности

Эти модели безопасности подобны аэродинамическим моделям самолетов и моделям плавучести судов – и те, и другие позволяют доказывать жизнеспособность системы и определять основные принципы ее архитектуры и технологических решений, используемых в ее строительстве. Главная цель создания политики безопасности [5] информационные системы и ее описания в форме формальной модели - определение условий, которые поведение системы, развитие критерия безопасности и выполнения формального доказательства соблюдения системы должно представить этому критерию в соблюдении установленных правил и ограничений. На практике это означает, что поскольку соответствующие зарегистрированные пользователи получат доступ к информации и будут в состоянии выполнить с ним только санкционированные действия.

Кроме того, формальные модели безопасности позволяют решать все еще много задач, возникающих во время дизайна, развития и сертификации о защищенных системах, поэтому их используют не только теоретики информационной безопасности, но также и другие специалисты, участвующие в процессе создания и операции защищенных информационных систем (производители, потребители, эксперты).

Производители защищенных информационных систем используют модели безопасности в следующих случаях:

- когда составляют формальную спецификацию политики безопасности разработанной системы;
- при выборе базовой архитектуры защищенной системы, определяя механизмы реализации средств защиты;
- в ходе анализа безопасности системы как эталонная модель;
- при подтверждении свойств разработанной системы формальным доказательством соблюдения политики безопасности.

У потребителей, составляя формальные модели безопасности, есть возможность сообщить производителям требования в точно определенной и последовательной форме, и также оценить соблюдение защищенных систем к требованиям.

Эксперты в квалификации во время анализа соответствия реализации политики безопасности в защищенных системах используют модели безопасности в качестве стандартов.

Эти рассматриваемые модели безопасности основаны на следующих базовых представлениях:

1) Система является совокупностью взаимодействующих сущностей – субъектов и объектов. Объекты могут быть представлены интуитивно в форме контейнеров, содержащих информацию, и рассматривать как программы переноса предметов, которые влияют на объекты различными способами. В таком представлении системной безопасности обработки информации, обеспечен решением проблемы управления доступом предметов к объектам согласно своду правил набора и ограничениям, которые формируют политику безопасности. Считается, что система безопасна, если предметы не имеют возможности нарушать правила политики безопасности. Нужно отметить, что общий подход для всех моделей - разделение ряда сущностей создания системы в большое число предметов и объектов, хотя определения понятий объект и предмет в различных моделях могут значительно отличаться.

2) Все взаимодействия в системе смоделированы учреждением отношений определенного типа между предметами и объектами. Набор типов отношений определен в форме ряда операций, какие предметы могут передать объекты.

3) Всеми операциями управляет монитор взаимодействий, и запрещают или решают согласно правилам политики безопасности.

4) Политика безопасности установлена в форме правил, согласно которым должны быть выполнены все взаимодействия между предметами и объектами. Взаимодействия, приводящие к нарушению этих правил, пересечены управляющими устройствами доступа и не могут быть выполнены.

5) Набор большого числа предметов, объектов и отношений между ними (установленные взаимодействия) определяет условие системы. Каждое состояние системы является либо безопасным, либо небезопасным в соответствии с предложенным в модели критерием безопасности.

6) Основной элемент модели безопасности - доказательство заявления (теорема), где система, которая находится в безопасном состоянии, не может перейти в небезопасное состояние в соблюдении всех установленных правил и ограничений.

Можно отличить два главных класса моделей политики безопасности: дискреционные (произвольные) и мандатные (нормативные). Мы рассмотрим самые широко распространенные модели: модель [5] Харрисона-Руззо-Ульмана и модель типизованной матрицы доступа, фундаментальную нормативную

модель безопасности Белла-ЛаПадулы, а также модели двух прикладных политик – ролевой политики и политики доменов и типов.

2.2 Дискреционная модель Харрисона-Руззо-Ульмина

Модель безопасности Харрисона-Руззо-Ульмина, которая является классической контролируемой моделью, реализует любое управление доступом субъектов к объектам и контроль распределения прав доступа.

В этой модели система обработки информации представлена в форме набора активных сущностей – субъектов (множествоS), которые обеспечивают доступ к информации, пассивных сущностей – объекты (множество O), содержащих защищенную информацию и заключительный набор прав доступа R = {r1 … r_n }, имея в виду полномочия на выполнении соответствующих действий (например, чтение, отчет, работа).

Причем для того, чтобы включить в область действия модели и отношения между субъектами, принято считать, что субъекты одновременно являются и объектами. Поведение системы смоделировано посредством понятия состояния: пространство условий системы сформировано декартовской работой наборов объектов, составляющих его, предметов и прав. Текущее состояние системы в этом пространстве определено тремя, состоящими из большого числа предметов, наборов объектов и матрицы прав доступа, описывающих плавные права доступа предметов к объектам. Линии матрицы соответствуют предметам и колонкам – к объектам, поскольку набор объектов включает большое число предметов, у матрицы вид прямоугольника. Любая клетка матрицы содержит ряд прав на предмет к объекту, принадлежащих к ряду прав доступа. Поведение системы вовремя смоделировано переходами между различными состояниями. Переход выполнен модификацией матрицы.

2.3 Мандатная модель Белла-ЛаПадулы

Мандатная модель управления доступом основана на правилах секретного документооборота, принятых в государственных и правительственных учреждениях многих стран. Основным положением политики Белла-ЛаПадулы [6]. Взятым ими из реальной жизни, является назначение всем участникам процесса обработки защищаемой информации и документам, в которых она содержится, специальной метки, например, секретно, совершенно секретно и т.д. получившей название уровня безопасности. Все уровни безопасности упорядочиваются с помощью установленного отношения доминирования, например, уровень, совершенно секретно считается более высоким чем уровень секретно, или доминирует над

ним. Контроль доступа осуществляется в зависимости от уровня безопасности взаимодействующих сторон на основании двух простых правил:

1) Уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.

2) Уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых ниже его собственного уровня безопасности.

Первое правило обеспечивает информационную безопасность, обработанную более порученными людьми (высокого уровня), от доступа от менее порученного (низкого уровня). Второе правило предотвращает утечку информации (сознательный или несознательный) от участников высокого уровня обработки информации к низкому уровню.

Таким образом, если в контролируемом управлении моделями доступом происходит инвестициями пользователей с полномочиями выполнить определенные операции по определенным объектам, мандатные модели управляют доступом неявным изображением – посредством назначения ко всем сущностям системы уровней безопасности, которые определяют все допустимые взаимодействия между ними. Следовательно, мандатное управление доступом не различает сущностей, которым присвоен одинаковый уровень безопасности, и на их взаимодействия ограничения отсутствуют. Поэтому в тех ситуациях, когда управление доступом требует более гибкий подход, мандатная модель применяется вместе с любым контролируемым, который используется для контроля взаимодействий между сущностями одного уровня и для установки дополнительных ограничений, усиливающих мандатную модель.

Система в модели безопасности Белла-ЛаПадулы, как в модели Харрисона-Руззо-Ульмана представляется в виде множеств субъектов S, объектов O (множество объектов включает множество субъектов, S и O) и прав доступа read (чтение) и write (запись). В мандатной модели рассматриваются только эти два вида доступа, и, хотя она может быть расширена введением дополнительных прав (например, правом на добавление информации, выполнение программ и т.д.), все они будут отображаться в базовые (чтение и запись). Использование столь жесткого подхода, не позволяющего осуществлять гибкое управление доступом, объясняется тем, что в мандатной модели контролируются не операции, осуществляемые субъектом над объектом, а потоки информации, которые могут быть только двух видов: либо от субъекта к объекту (запись), либо от объекта к субъекту (чтение).

В мандатной модели рассматривают только эти два типа доступа, и, хотя это может быть расширенное введение дополнительных прав (например, право для информационного дополнения, внедрения программ, и т.д.), все они будут показаны в основном (чтение и запись). Использование такого жесткого подхода, не позволяя осуществлять гибкий контроль над доступом, объяснено этим в мандатной модели операции, которые выполнены предметом по

объекту, и потоками информации, которые могут быть только двумя типами, от предмета, чтобы возразить (делают запись), или от объекта до подчиненного (чтение).

2.4 Ролевая политика безопасности

Ролевая политика безопасности [6] представляет значительно продвинутую модель Харрисона-Руззо-Ульмана, однако ее нельзя отнести ни к контролируемому, ни к мандатному, потому что контроль доступа в нем осуществлен и на основе матрицы прав доступа для ролей, и посредством правил, регулирующих цель ролей пользователям и их активации во время сессий. Поэтому ролевая модель представляет абсолютно специальный тип политики, основанный на компромиссе между гибкостью управления доступом, особенностью для контролируемых моделей, и жесткостью правил контроля доступа, врожденного от обязательных моделей.

В ролевой модели классическое понятие субъект замещается понятиями пользователь и роль. Пользователь - человек, который работает с системой и выполняет определенные официальные обязанности. Роль - абстрактная сущность, активно работающая в системе, с которой связан ограниченный, логический связанный набор полномочий, необходимых для внедрения определенной деятельности. Самым распространенным примером роли является присутствующий почти в каждой системе административный бюджет (например root для UNIX и Administrator для Windows NT), который обладает специальными полномочиями и может использоваться несколькими пользователями.

Ролевая политика широко распространена. Поскольку она, в отличие от других формальных политик, очень близка к реальной жизни. Ведь на самом деле работающие в системе пользователи действуют не от своего личного имени – они всегда осуществляют определенные служебные обязанности, т.е. выполняют некоторые роли, которые не связаны ни в коем случае с их индивидуальностью.

Поэтому довольно логично осуществить контроль над доступом и назначить полномочия не на настоящих пользователей. Такой подход к политике безопасности позволяет рассматривать подразделение обязанностей и полномочий между участниками прикладного информационного процесса с точки зрения ролевой политики личности пользователя, обеспечивающего доступ к информационным вопросам. Например, в реальной системе обработки информации могут работать системный администратор, менеджер баз данных и простые пользователи.

В такой ситуации ролевая политика позволяет распределять полномочия между этими ролями согласно их официальным обязанностям: роли администратора назначены специальными полномочиями, позволяющими его

управлять работой системы и управлять ее конфигурацией, роль менеджера баз данных позволяет осуществлять контроль над сервером БД, и права простых пользователей ограничены минимумом, необходимым для начала прикладных программ. Кроме того, количество ролей в системе не может соответствовать числу настоящих пользователей – один пользователь, если на нем лежат различные обязанности, требующие различные полномочия, может выполнить (в то же время или последовательно) некоторые роли, и некоторые пользователи могут использовать ту же самую роль, если они выполняют идентичную работу.

Использование ролевого стратегического контроля доступа осуществлено на двух стадиях: во-первых, для каждой роли назначен набор полномочий, представляющих ряд прав доступа к объектам и, во-вторых, каждому пользователю определен список ролей доступных ему. Полномочия назначаются ролям в соответствии с принципом наименьших привилегий, из которого следует, что каждый пользователь должен обладать только минимально необходимым для выполнения своей работы набором полномочий [7].

Ролевая модель описывает систему в виде следующих множеств:

- U – множество пользователей;
- R – множество ролей;
- p – множество полномочий на доступ к объектам, представленное, например, в виде матрицы прав доступа;
- S – множество сеансов работы пользователей с системой.

Для перечисленных множеств определяются следующие отношения (рис.2.1).

PA – отображает множество полномочий на множество ролей;

UA – отображает множество пользователей на множество ролей;

USER - эта функция определяет пользователя который осуществляет этот сеанс работы;

ROLES - эта функция определяет набор ролей.

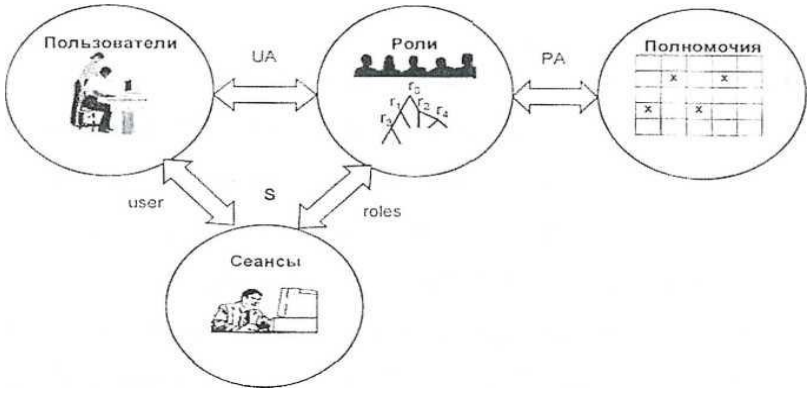


Рисунок 2.1 - Ролевая модель управления доступом

В качестве критерия безопасности [6] ролевой модели используется

следующее правило: система считается безопасной, если любой пользователь системы, работающий в сеансе S, может осуществлять действия, в рамках своих полномочий данных ему администратором.

Из формулировки критерия безопасности ролевой модели следует, что управление доступом осуществляется главным образом не с помощью назначения полномочий ролям, а путем задания отношения UA, назначающего роли пользователям, и функции roles, определяющей доступный в сеансе набор ролей. Поэтому многочисленные интерпретации ролевой модели различаются видом функций user, roles и permission, а также ограничениями, накладываемыми на отношения PA и UA.

Иерархическая организация ролей представляет собой наиболее распространенный тип ролевой модели поскольку она очень точно отражает установившееся в реальном мире отношение подчиненности между участниками процессов обработки информации и разделение между ними сфер ответственности. Роли в иерархии упорядочиваются по уровню предоставляемых полномочий. Чем выше роль находится в иерархии, тем больше с ней связано полномочий, поскольку считается, что если пользователю присвоена некоторая роль, то ему автоматически назначаются и все подчиненные им по иерархии роли. Иерархия ролей допускает множественное наследование.

2.5 Основные положения модели HRU

Модель HRU используется для анализа системы защиты, реализующей дискреционную политику безопасности, и ее основного элемента матрицы доступов. При этом система защиты представляется конечным автоматом, функционирующим согласно определенным правилам перехода.

Модель HRU была впервые предложена в 1971 г. В 1976 г. появилось формальное описание модели. Обозначим: O – множество объектов системы; S – множество субъектов системы (S и O); R – множество прав доступа субъектов к объектам, например права на чтение (read), на запись (write), владения (own); M матрица доступа, строки которой соответствуют субъектам, а столбцы объектам; M[s, o] и R – права доступа субъекта s к объекту o.

Отдельный автомат, построенный согласно положениям модели HRU, обычно называют системой. Функционирование системы рассматривается только с точки зрения изменений в матрице доступа.

2.6 Основные положения модели Take-Grant

Модель распространения прав доступа Take-Grant [6], предложенная в 1976 г., используется для анализа систем дискреционного разграничения доступа, в первую очередь для анализа путей распространения прав доступа в таких системах. Основные элементы модели используют колонки доступов и правило его преобразования. Цель состоит в том, чтобы дать ответ на вопрос возможности получения прав доступа предмет системы на объекте в состоянии, описанном количеством доступов. В настоящее время модель Take-Grant получила продолжение как расширенная модель Take-Grant, в которой рассматриваются пути возникновения информационных потоков в системах с дискреционным разграничением доступа.

Условие системы описано его подсчетом доступов. Системный переход из состояния в состояние определен операциями или правилами преобразования количества доступов. Рассмотренные модели HRU, Take-Grant, Белла-ЛаПадуллы могут быть использованы при построении и анализе детерминированных систем защиты, т е. систем, которые не включают элементов, имеющих вероятностную природу.

При исследовании систем, закономерности функционирования которых сложны или практически не поддаются описанию, целесообразно использовать элементы теории вероятностей. Можно нести глобальные компьютерные сети к числу таких систем, например Интернет, или современная мульти задача, многопользовательские сетевые операционные системы.

2.7 Автоматная модель системы защиты GM

Согласно описанию модели GM [5], система защиты представляется детерминированным автоматом, на вход которого поступает последовательность команд пользователей. Для каждого пользователя системы задана функция выходов, определяющая, что каждый из них «видит» на устройстве вывода в соответствующем состоянии системы.

В модели GM определяется понятие информационного невлияния или невмешательства. Если всех пользователей системы поделить на две группы – низкоуровневых и высокоуровневых, то информационное невмешательство есть требование независимости низкоуровневого вывода системы от ее высокоуровневого входа.

В модели GM информационное невмешательство, можно рассматривать как частный случай соответствующего понятия модели безопасности информационных потоков.

2.8 Выбор оптимальной модели безопасности

Любая политика безопасности обобщает набор норм и обработку регулирования правил информации, какая работа обеспечивает защиту против определенного набора угроз и делает необходимым условием из безопасности для существующей системы, которая в структуре может содержать различные средства информационной передачи и обработки. Данная система может состоять из локально- вычислительной сети (ЛВС), сети передачи данных (СПД), сотовой системы связи, спутниковой или транкинговой сети, а также комбинации всех перечисленных средств связи. Каждый из случаев будь, то применение на объекте любой из вышеупомянутых систем или комбинации этих систем, должен рассмотреть и находиться в работе на соответствующей математической модели безопасности. Как это было уже сказано выше согласно месту назначения, математические модели безопасности подобны аэродинамическим моделям самолетов, судов, и т.д., т.е. позволяет доказывать жизнеспособность системы, и также определяет основные принципы ее архитектуры и технологических решений, используемых в ее строительстве. Для выбора конкретной модели для конкретного случая необходимо понять все достоинства и недостатки всех вышеупомянутых моделей и выбрать самую оптимальную.

Рассмотрение начнем с дискреционной модели Харрисона-Руззо-Ульмана. Данная модель является классической и универсальной, что позволяет быть применимой ко многим существующим системам. Она не осуществляет жесткого контроля за доступом и не управляет правами доступа, что является ее главным недостатком. Применение данной модели должно ограничиваться небольшим объектом телекоммуникации, обладающей информацией малой и недолговременной секретности. Несмотря на свою невысокую сложность в реализации, она является также моделью с не очень гибкой системой управления, что создает дополнительные сложности в ее применимости.
Рассмотрев достоинства и недостатки можно сделать вывод, что модель Харрисона-Руззо-Ульмана не подходит к той системе которая лежит в основе заседания на магистерскую диссертацию.

Мандатная модель БеллаЛаПадулы, напротив, осуществляет жесткий четко регламентированный контроль за доступом субъектов к объектам и основан на правилах секретного документооборота, принятых в государственных и правительственных учреждениях многих стран. Данная модель является довольно сложной, но зато применима к объектам телекоммуникаций на которых содержится информация с грифом совершенно секретно и секретно, поэтому модель БеллаЛаПадулы и нашла широкое применение в правительственных учреждениях и агенствах. Если в дискреционных моделях управление доступом происходит путем наделения пользователей полномочиями осуществлять определенные операции над определенными объектами, то мандатные модели управляют доступом неявным

образом – с помощью назначения всем сущностям системы уровней безопасности, которые определяют все допустимые взаимодействия между ними. Главным достоинством является надежность данной модели и ее многопозиционность. Главным недостатком – сложность и узконаправленность реализации. В силу своей сложности в реализации и многоуровневых расчетов она также на подходит к нашей задачи.

Рассмотрев ролевую политику безопасности можно прийти к выводу, что она представляет собой существенно усовершенствованную модель Харрисона-Руззо-Ульмана, однако ее нельзя отнести ни к дискреционным, ни к мандатным, потому что управление доступом в ней осуществляется как и на основе матрицы прав доступа для ролей, так и с помощью правил регламентирующих значения ролей пользователем и их активацию во время сеанса. Можно отметить, что изменив основное строение модеои Харрисона-Руззо-Ульмана, она по сути является лишь усовершенствованной версией данной модели и обладает почти теми же свойствами, заметно лишь то что классическое понятие субъект замещается понятием пользователя. В ролевой политике управление доступом осуществляется в две стадии: во-первых, для каждой роли указывается набор полномочий представляющей набор прав доступа к объекту; во-вторых каждому пользователю назначается список доступных его ролей. Все это приводит к выводу о том, что данная модель применима в основном для объектов и систем оснащенных компьютерной сетью и трудно реализуется для комбинированных систем. В нашем случае необходимо, чтобы математическая модель учитывала защиту информации тональной частоты на любых терминалах, будь то транкинговые, сотовые или спутниковые системы связи.

Модель HRU является наиболее перспективной моделью т.к. используется для анализа системы защиты реализующей дискреционную политику безопасности и основана на элементе матрицы доступа. К сожалению данная модель тоже является применимой исключительно к объектам оснащенным компьютерной сетью. Нам она также не подходит.

Модель Take-Grant – это модель распространения прав доступа и систем дискреционного разграничения. В качестве основных элементов данной модели используется граф доступов и правила его преобразования. Цель данной модели состоит в том чтобы дать ответ на вопрос о возможности получения прав доступа субъектом системы на объект состоянии, описываемом графом доступов. Она к нашей системе также не применима вследствие направленности на локально-вычислительные сети.

Автоматная модель системы защиты GM, согласно описанию [5] представляется детерминированным автоматом. В модели GM также определяется понятие информационного невлияния или невмешательства. В силу двух этих аспектов модель стала абсолютно универсальной и нашла применение в широкой области объектов систем в состав которых входят как компьютерные сети, так и средства мобильной и стационарной связи. Данная модель не является особенно простой, но и в то же время не является сложной.

К достоинствам данной модели можно отнести ее применимость как к комбинированным системам так и к моно системам оснащенным каким-нибудь единственным телекоммуникационным средством. Главным недостатком модели GM является то, что ее нельзя использовать на режимных и секретных объектах. Так как последнего нам не требуется, а большинство достоинств отвечает запросам нашей системы, то именно автоматная модель GM мы возьмем за основу. Так из всего перечня моделей была выбрана автоматная модель GM.

2.9 Выводы по второй главе

Таким образом, во второй главе сделан:

1) Анализ всех формальных моделей безопасности.
2) Рассмотрены все достоинства и недостатки каждой математической модели безопасности в отдельности.
3) Выбрана абстрактная модель Гогена-Мезигера так как она дает четкое определение информационного не влияния и не вмешательства и применима к моно системам, к которым относится телекоммуникационная сеть.

3 Разработка критериев и требований по информационной безопасности

Для проектирования и разработки системы безопасности информации должны быть положены следующие положения [7]:

1) Анализ заданных требований на предмет перечня, структуры и динамики стоимости, информации подлежащей защите.

2) Выбор модели потенциального нарушителя.

3) Выявление максимально возможного количества каналов несанкционированного доступа к информации согласно выбранной модели потенциального нарушителя.

4) Анализ выявленных возможных каналов несанкционированного доступа (ВКНСД) и выбор готовых или разработка новых средств защиты, способных их перекрыть с заданной прочностью.

5) Качественная и количественная оценка прочности каждого из применяемых средств защиты.

6) Проверка возможности адаптации средств защиты в разрабатываемую систему.

7) Создание в разрабатываемой системе средств централизованного контроля и управления.

8) Количественная и качественная оценка прочности системы защиты информации с отдельными показателями по контролируемым и неконтролируемым ВКНСД.

Если использовать вероятностные величины при оценке прочности средств защиты на каналах передачи дискретной информации, то расчет прочности средств защиты производится по нижеследующим формулам для нескольких нарушителей [7]:

$$P_{сзн}=(1-P_{нр})(1-P_{обх1})(1-P_{обх2})\ldots\ldots(1-P_{обх\,к}) \qquad (3.1)$$

где $P_{сзн}$ – вероятность непреодоления преграды нарушителем;

$P_{нр}$ – вероятность преодоления преграды нарушителем;

$P_{обх}$ – вероятность обхода преграды нарушителем;

К – число путей обхода преграды.

Величину $P_{нр}$ можно определить по формуле:

$$P_{нр}=n/A^{S} \qquad (3.2)$$

где n – количество попыток подбора кода;

А – число символов в выбранном алфавите кода ключа;

S – длина кода ключа в количестве символов.

Когда время жизни информации $t_ж$ больше ожидаемого времени преодоления преграды нарушителем $t_н$ и вероятность обхода преграды нарушителем $P_{обх}>0$, то прочность защиты можно представить в виде:

$$P_{сзн}=(1-P_{нр})(1-P_{обх}) \quad (3.3)$$

Для случая старения информации:

$$P_{сзн}=1, \text{ если } t_ж \square t_н \text{ и } P_{обх}=0 \quad (3.4)$$

Условие прочности преграды с обнаружением и блокировкой НСД (несанкционированный доступ) можно представить в виде соотношения:

$$(T_Д+t_{ср}+t_{ом}+t_{бл})/(t_н) \square 1, \quad (3.5)$$

где $T_Д$ – период опроса датчиков;
$t_{ср}$ – время срабатывания тревожной сигнализации;
$t_{ом}$ – время определения места доступа;
$t_{бл}$ – время блокировки доступа.

Если обозначить сумму $(T_Д+t_{ср}+t_{ом}+t_{бл})$ через $T_{обл}$ – период обнаружения и блокировки несанкционированного доступа, то получится:

$$(T_{обл})/(t_н) \square 1, \quad (3.6)$$

В этом случае вероятность успеха нарушителя будет выражаться формулой:

$$P_{нр}=(T_Д-t_н)/(T_Д)=1- (t_н)(T_Д) \quad (3.7)$$

Тогда вероятность обнаружения несанкционированных действий будет равна [7]:

$$P_{обл}=1-P_{нр}=t_н/T_Д, \quad (3.8)$$

при $t_н>T_Д$ нарушитель будет обнаружен наверняка, т.е. $P_{обл}=1$, в случае $T_Д \square t_н \square T_{обл}$, вероятность успеха нарушителя будет равна:

$$P_{нр}=1-t_н/T_{обл}, \quad (3.9)$$

А вероятность обнаружения и блокировки несанкционированных действий нарушителя:

$$P_{обл}=t_н/ T_{обл}, \quad (3.10)$$

Для полного представления прочности преграды в виде автоматизированной системы обнаружения и блокировки НСД необходимо учитывать надежность ее функционирования и пути возможного обхода ее нарушителем.

Вероятность отказа системы при случайном потоке отказов определяется по формуле:

$$Q(t)=1-e^{-\lambda t}, \quad (3.11)$$

$$P_{отк}=1-Q \quad (3.12)$$

где λ – интенсивность отказов группы технических средств, составляющих систему обнаружения и блокировки НСД;

t – рассматриваемый интервал времени функционирования системы обнаружения и блокировки НСД.

С учетом возможного отказа системы контроля прочность преграды будет определяться по формуле:

$$P_{сзн\ К}=P_{обл}(1-P_{отк})(1-P_{обх1})(1- P_{обх2})…….(1- P_{обх\ J}) \quad (3.13)$$

где $P_{обл}$ – вероятность обнаружения и блокировки несанкционированных действий нарушителя;

J – число путей обхода преграды.

$P_{обл}$ и $P_{отк}$ определяются по формулам (3.10) и(3.12).

Т.е. прочность неконтролируемой преграды рассчитывается по формуле (3.1), а контролируемой по формуле (3.13).

Прочность защитной преграды [7] является достаточной, если ожидаемое время преодоления ее нарушителем больше времени жизни предмета защиты или больше времени обнаружения и блокировки его доступа при отсутствии путей скрытого обхода этой преграды.

В ответственных случаях при повышенных требованиях безопасности применяется многозвенная защита. Так, например, кроме системы контроля вскрытия аппаратуры, системы опознания и разграничения доступа, контролирующих доступ к периметру телекоммуникационной сети, имеются средства защиты от доступа к средствам отображения и документирования, побочному электромагнитному излучению и наводкам (ПЭМИН), система контроля доступа в помещение, охранной сигнализации и т.п.

В этом случае имеют место параллельные (сдублированные) преграды и защита носит многозвенный характер. Расчет прочности системы защиты информации можно проводить по следующим формулам:

а) при использовании неконтролируемых преград:

$$P_{сзн}= P_{сзн1}\ P_{сзн2}..... P_{сзн\ i}(1-P_{обх1})(1- P_{обх2})……(1- P_{обх\ J}), \quad (3.14)$$

где $P_{\text{сзн i}}$ – прочность n-ой преграды.

б) для прочности многозвенной защиты с контролируемыми преградами:

$$P_{\text{сзн К}} = P_{\text{сзн1}}\, P_{\text{сзн2}} \ldots\ldots\ldots P_{\text{сзн К n}}(1-P_{\text{обх1}})(1-P_{\text{обх2}})\ldots\ldots(1-P_{\text{обх J}}), \qquad (3.15)$$

Если все дополнительные преграды перекрывают то же количество или более возможных каналов НСД, то суммарная прочность дублированных преград будет определяться по формуле:

$$P_{\sum} = 1 - \prod_{i-1}^{m}(1 - P_i) \qquad (3.16)$$

где i=1, m – порядковый номер преграды;

m – количество дублирующих преград;

P_i –прочность i-ой преграды.

Анализ любой структуры телекоммуникационной сети показывает, что в ней наблюдается два вида возможных каналов НСД к информации сети:

- комплекс средств автоматизации;
- каналы связи.

Поскольку концепция построения средств защиты [7] рассмотрено выше, то остановимся кратко на концепции защиты информации в каналах связи. Принимая во внимание, что информация в сети постоянно обновляется, а также и то, что на каналах связи в отличие от элементов телекоммуникационной сети нарушитель ничем не рискует, особенно при пассивном перехвате информации, прочность защиты здесь должна быть особенно высокой. От активного вмешательства нарушителя в процесс обмена информацией между элементами системы должна быть применена система обнаружения и блокировки НСД. Но и при этом риск нарушителя по прежнему невысок, т.к. у него и в этом случае по причине сложности определения его места пребывания остается достаточно времени на то, чтобы отключиться и уничтожить свои следы.

Поэтому целесообразно строить защиту информации и сопровождающих ее служебных признаков на основе самой информации, а не на ресурсах самой телекоммуникационной сети. Для этого необходимо на основе специальных криптографических преобразований разрабатывать кодограммы сообщений, которыми должны обмениваться между собой элементы вычислительной сети. Целостность этой кодограммы и содержащейся в ней информации должны быть защищены от НСД.

Данная кодограмма должна содержать адрес получателя , заголовок, информацию отправителя, концевик, адрес отправителя, исходящий номер и время отправления. Для синхронизации приема и обработки кодограммы в нее включают признаки кадра. Кадр содержит информационное поле, а также заголовок и концевик, присваиваемый протоколом. Заголовок содержит следующую информацию, служащую для идентификации сообщения,

правильного приема кадров, восстановления и повторной передачи в случае ошибок и т.д. Концевик содержит проверочное поле, служащее для коррекции и исправления ошибок (при помехоустойчивом кодировании), внесенных каналом. Для обеспечения передачи блоков данных от передающей станции к приемной кодограмма должна содержать признаки маршрута.

Стойкость или прочность защитного механизма определяется стойкостью к подбору примененного секретного ключа в количестве времени, затрачиваемого нарушителем на эту работу. Если оно составляет величину, превышающую время жизни защищаемой информации, то прочность или вероятность этой преграды равна 1.

Можно предложить следующую группу средств для обеспечения безопасности информации:

1) средствами формирования цифровой подписи сообщений;
2) средства шифрования передаваемых данных;
3) средства обеспечения цифровой подписи служебных признаков передаваемой информации, включая адреса и маршруты сообщения, а также получения отправителем и посредником квитанции от получателя;
4) введение в систему передачи данных (СПД) маскирующих потоков сообщений при отсутствии активности в обмене информацией;
5) присвоение всем участникам обмена сообщениями переменных идентификаторов и создание в сети системы контроля и разграничения доступа с защитой цифровой подписью паролей от подмены их нарушителем.

Показатель прочности перечисленных средств защиты и будет в конечном итоге определять безопасность информации в канале связи.

Таким образом, телекоммуникационную сеть можно считать безопасной в смысле обработки информации [7], если в ней предусмотрена централизованная система управляемых и взаимосвязанных преград, перекрывающих с гарантированной прочностью заданное в соответствии с моделью потенциального нарушителя количество возможных каналов НСД и угроз, направленных на утрату или модификацию информации, а также несанкционированное ознакомление с ней посторонних лиц.

Также можно предложить следующие основные критерии качества алгоритмов криптографического закрытия сообщений:

1) скорость шифрования V_E;
2) скорость дешиврования V_D;
3) длина ключа k;
4) общее количество ключей n, в случае применения симметричных криптографических систем вычисляемое по формуле (3.17)

$$n=k! \tag{3.17}$$

где n – общее количество ключей, k – длина ключа;

5) безопасное время, которое определяется как математическое ожидание времени раскрытия криптографической системы методом прямого перебора ключей и вычисляется по формуле (3.18)

$$T_s = m_1\{T_c\} = \sum_{i=1}^{n} iT_D P_i = T_D \sum_{i=1}^{n} iP_i, \quad (3.18)$$

где T_s - безопасное время,

T_c - время раскрытия криптографической системы (дискретная случайная величина),

n– общее количество ключей,

T_D - время дешифрования при проверке одного ключа,

P_i - вероятность раскрытия криптографической системы при проверке i-го ключа.

Для случая одинаковых вероятностей раскрытия криптографической системы при проверке любого из ключей формула (3.17) преобразуется в формулу (3.19)

$$T_s=(n+1)T_p/2, \quad (3.19)$$

где T_s – безопасное время,

n – общее количество ключей,

T_p – время дешифрования при проверке одного ключа.

Скорость шифрования и скорость дешифрования, принятые как критерии качества алгоритмов криптографического закрытия сообщений, служат не только для оценки быстродействия этих алгоритмов. Они позволяют вычислить величину временной задержки, которую вносит алгоритм криптографического закрытия сообщений при передаче последних от источника сообщений к их получателю. Величина этой временной задержки может оказаться определяющей при выборе алгоритма криптографического закрытия сообщений.

Время безопасности является критерием качества в полном смысле этого понятия только при оценке криптостойкости алгоритмов криптографического закрытия сообщений допускающих всего один метод криптоанализа – метод прямого перебора ключей. Для остальных алгоритмов криптографического закрытия сообщений время безопасности может служить только приблизительной оценкой их криптостойкости.

3.1 Выводы по третьей главе

1) Показана, что любая система защиты должна строиться исходя из специальных критериев и требований по информационной безопасности.

2) Основными положениями при проектировании и разработки системы безопасности информации должны являться:

− анализ заданных требований на предмет перечня, структуры и динамики стоимости, информации подлежащей защите;

− выбор потенциальной модели нарушителя;

− выяснение максимально возможного количества каналов несанкционированного доступа;

− качественная оценка прочности каждого из применяемых средств защиты;

− количественная оценка прочности системы защиты информации.

3) Показано, что прочность защитной преграды является достаточной, если ожидаемое время преодоления ее нарушителем больше времени жизни предмета защиты.

4) Предложено рассчитывать прочность преграды для устройства по формуле:

$$P=1-П*(1-P_i);$$

где P_i – вероятность нарушения i-того звена защиты.

5) Показано, что телекоммуникационную сеть можно считать безопасной в смысле обработки и передачи информации, если в ней предусмотрена централизованная система управляемых и взаимосвязанных преград, перекрывающих с гарантированной прочностью, заданное в соответствии с моделью потенциального нарушителя количество возможных каналов несанкционированного доступа НСД к информации.

4 Выбор оптимального варианта устройства защиты речевой информации

Проблема защиты речевой информации от подслушивания стала актуальной задачей [2]. Перехват разговоров может служить основанием для экономических преступлений, шантажа, имитации абонентов и т.д.

Устройства защиты речевой информации классифицируются по способу обработки сигналов на:

- аналоговые;
- цифровые;
- гибридные.

Аналоговые устройства не практичны из-за их громоздкости и ограниченных возможностей. К достоинствам аналоговых систем можно отнести простоту схемной реализации и дешевизну конструкции. Но за достоинствами идут недостатки и самый главный – низкий уровень секретности, что на данном этапе развития телекоммуникации не является приемлемым.

Цифровые системы требуют специальных сигнальных процессоров, которые осуществляют различные математические алгоритмы закрытия речи. Цифровые системы создают более высокий уровень секретности документа и дают возможность сохранности (от несанкционированного доступа) в течение длительного периода времени. Из-за сложности алгоритмов шифрования цифровые системы должны иметь в своем составе высокоскоростные скремблеры и дескремблеры, аналого-цифровые и цифро-аналоговые преобразователи, а также вокодеры исключающие избыточность речи построенные по принципу линейного предсказания. Все перечисленные компоненты делают цифровые устройства сложными с точки зрения схемной реализации и дорогостоящими, что делает их малоприменимыми к мобильным системам связи, но дающими высокую степень секретности, занимая при этом широкую полосу частот при передачи. Вследствие всего выше сказанного цифровые системы также редко применимы в средствах стационарной телефонной сети общего пользования.

Наиболее широкое распространение находят гибридные устройства защиты речевой информации [22]. Основная идея которых заключается в том, что входные и выходные сигналы у них являются аналоговыми, а весь процесс закрытия информации происходит в цифровом виде. Наличие аналогового сигнала позволяет использовать такие устройства на любых речевых трактах, будь то аналоговые или цифровые, в первом случае устройство просто монтируется после микрофона, осуществляя необходимые преобразования, в остальных случаях (цифровых каналах) выходной сигнал в цифровой форме

передавался в линию связи. Использование цифровых методов кодировки позволяет применять практически любые математические алгоритмы закрытия речи. Рассмотрев все достоинства и недостатки устройств защиты приходим к выводу что наиболее эффективными и малогабаритными являются устройства, построенные по гибридному принципу обработки данных. Этот принцип мы и будем использовать при дальнейшей разработке.

Средства защиты различают системы с преобразованием речи во временной или в частотной области, при этом используется маска и криптографические преобразования. Согласно алгоритмам преобразования во временной области, форматы речи или цифровые отсчеты переставляют местами во времени. Устройства такого типа широко распространены и часто называются скремблерами. Скремблеры в настоящее время находят широкое применение в средствах телекоммуникации за счет своей простоты и гарантийной стойкости от взлома. Скремблеры в свою очередь также делятся на группы. Так при частотном преобразовании речь разделяется на форматы, затем подвергаются линейным преобразованиям по определенному закону. Данный алгоритм не является на сегодняшний день универсальным, вследствие низкого уровня защиты.

Предлагаемое, в данной работе, устройство построено по гибридному принципу с уровнем защиты обеспечивающее временную стойкость. Как уже было сказано выше входные и выходные сигналы здесь аналоговые, а весь процесс закрытия информации происходит в цифровом виде внутри передатчика и приемника. Структурная схема данного устройства предложена на рис.4.1.

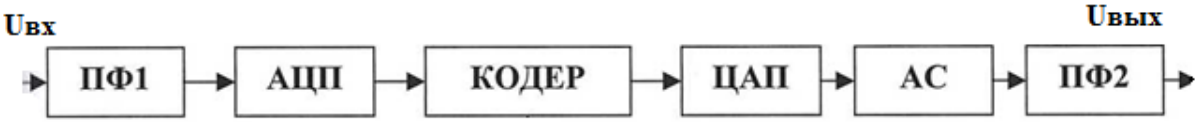


Рисунок 4.1 - Структурная схема устройства защиты речевой информации

Рассмотрим основное назначение каждого блока. Аналоговый сигнал поступает на вход полосового фильтра ПФ1, который ограничивает речевой спектр до стандартного значения 0,3 - 3,4 кГц. Фильтр является активным, т.е. собран с использованием операционных усилителей ОУ, но т.к. высокий коэффициент усиления обуславливает возникновение искажений необходимо его снижение, что и сделано включением в цепь отрицательной обратной связи ООС других операционных усилителей. Далее сигнал поступает на аналого-цифровой преобразователь АЦП, который переводит аналоговый сигнал в восьмиразрядный цифровой код, над которым впоследствии будет проходить процедура шифрования. После АЦП цифровой сигнал поступает на КОДЕР, который осуществляет процесс закрытия речи. Далее, уже закрытый речевой сигнал поступает на цифро-

аналоговый преобразователь ЦАП, который переводит цифровой восьми разрядный код в аналоговый сигнал. Следующим после ЦАП элементом является аналоговый скремблер АС, который в свою очередь стробирует определенную длительность аналогового сигнала и делает временную перестановку, увеличивая тем самым степень защиты. Завершает структурную схему полосовой фильтр ПФ2, который устраняет побочные продукты преобразования, приводя сигнал к стандартному значению 0,3-3,4 кГц. Следует также отметить, что данный полосовой фильтр снижает избыточность зашифрованного речевого сигнала, он также является активным – т.е. собран на операционных усилителях.

4.1 Разработка принципиальной схемы

4.1.1 Полосовые фильтры. В данной схеме целесообразно использовать активные фильтры, собранные на операционных усилителях ОУ, т.к. они помимо фильтрации осуществляют функцию усиления.

Активные фильтры можно использовать для реализации ФНЧ, ФВЧ, ПФ, ППФ. Известны различные конструкции активных фильтров, каждые из которых зависят от аппроксимации передаточной характеристики по функциям Баттерворта, Чебышева или другим. Некоторые свойства желательные для активного фильтра таковы:

1) малое число элементов, как активных, так и пассивных;
2) легкость регулировки;
3) малое влияние разброса параметров элементов по характеристике фильтра, в особенности значений емкостей конденсаторов;
4) отсутствие жестких требований к применяемому ОУ;
5) возможность создания высокодобротных фильтров;
6) нечувствительность характеристик фильтра по отношению к параметрам элементов и коэффициенту усиления ОУ.

По многим причинам последнее свойство является одним из наиболее важных. Фильтр, который требует соблюдение высокой точности значения параметров элементов, трудно настраивать, и по мере старения элементов настройка теряется; кроме того дополнительной неприятностью является требование использовать элементы с малым допуском значений параметров. В данном устройстве используется полосовой фильтр ПФ т.к. он должен пропускать лишь узкий диапазон тональной частоты 0,3 - 3,4 кГц. Существуют два основных метода по которым строятся ПФ:

1) метод переменных состояний;
2) фильтры на ИНУН (источник напряжения управляемый напряжением).

Схема фильтра на ИНУН обязана широкой популярностью в основном своей простоте и малому числу деталей, но эта схема страдает недостатком, а именно, высокой чувствительностью к изменениям значения параметров

элементов.

Фильтр, построенный на основе метода переменных состояний куда более сложен по сравнению с фильтрами на ИНУН, и он широко применяется благодаря повышенной устойчивости и легкости регулировки. Наиболее близким к фильтру, на основе метода переменных состояний, примыкает так называемый биквадратный фильтр, представленный на рис.4.2. [9]

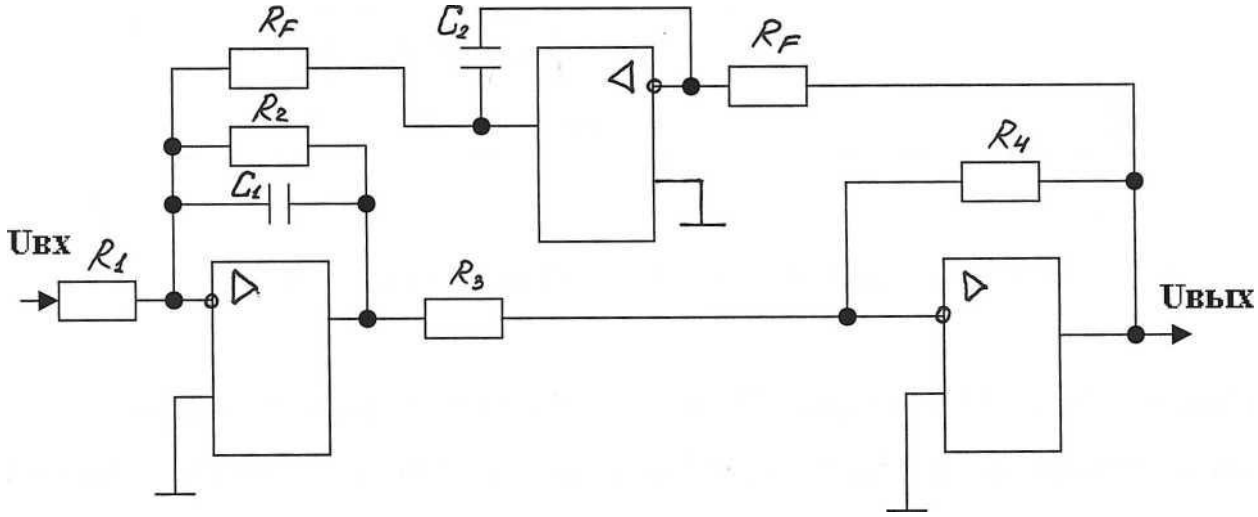


Рисунок 4.2 - Биквадратный фильтр

Данный фильтр обеспечивает 10 дБ коэффициента усиления и полосы пропускания - ПП 0,3 - 3,4 кГц. В этой схеме используются три ОУ ее можно сконструировать на основе метода переменных состояний. Замечательным свойством такого фильтра является возможность регулировки его частоты (с помощью R_F) при сохранении постоянной ширины полосы пропускания ПП.

Рассмотрим и другие модификации биквадратных фильтров.

Активный полосовой фильтр LM 358 (КР1040УД1), сдвоенный с внутренней частотной коррекцией см. рис. 4.3. Данный фильтр обеспечивает 2дБ коэффициента усиления и ПП 0,3 - 3,4 кГц.

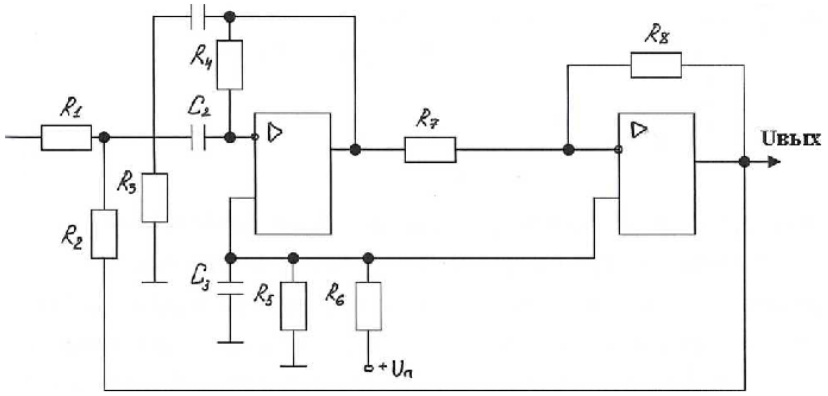


Рисунок 4.3 - Сдвоенный ПФ с внутренней частотной коррекцией

Активный биквадратный полосовой RC - фильтр LM124 (К1401УД2) - счетверенный ОУ с внутренней частотной коррекцией, но используется лишь три ОУ (представлен на рис.4.4). Предложенный фильтр обеспечивает коэффициент усиления равный 40дБ на ПП 0,8 - 2,8 кГц.

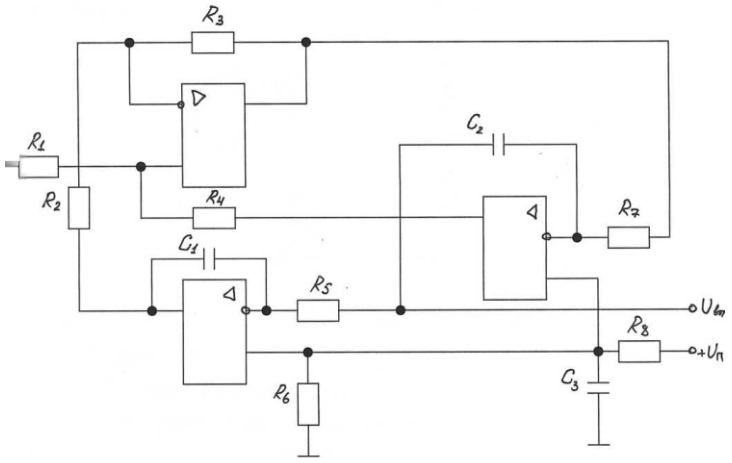


Рисунок 4.4 - Полосовой RC - фильтр с внутренней частотной коррекцией

В предложенном устройстве выберем фильтр LM358 (КР1040УД1) т.к. он обладает более широкой полосой пропускания 0,3 - 3,4 кГц и невысоким коэффициентом усиления 2дБ, что полностью удовлетворяет нашим требованиям. Данный фильтр полностью перекрывает наш диапазон 0,3 - 3,4 кГц, а малый коэффициент усиления не приводит к искажениям.

4.1.2 Аналого-цифровой преобразователь. В качестве аналого-цифрового преобразователя выбрана микросхема К572ПВ3 [9]. Она представляет собой восьми разрядный АЦП, работающий по принципу последовательного приближения. Скорость АЦП последовательного приближения выше чем у АЦП последовательного счета, что дает ему большие преимущества. Микросхема работает от одного источника питания, в ней может использоваться как внутренний, так и внешний тактовый генератор. В большинстве случаев схема используется с внешним генератором, как показано ниже на рис. 4.5.

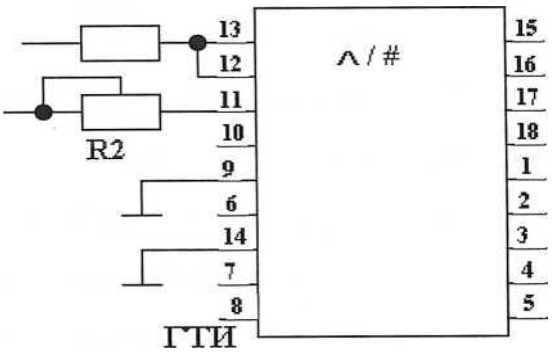


Рисунок 4.5 - АЦП последовательного приближения

Назначение выводов:

1-3 - цифровые выходы 4-2;

4 - цифровой выход 1 (младший разряд);

5 - выход состояния BUSY;

6 - вход управления RD;

7 - вход упрвления CS;

8 - вход тактирования;

9 - цифровая земля;

10 - напряжение источника питания;

11 - опорное напряжение;

12 - вход смещения характеристики;

13 - аналоговый вход;

14 - аналоговая земля;

15 - цифровой выход 8 (старший разряд)

16-18 - цифровые выходы 7 -5.

Резисторы R1 и R2 служат для компенсации абсолютной погрешности, внешний генератор может подключаться к выводу 8. Выводы микросхемы 1-5, 15-18 можно нагружать на ТТЛ ИС, что нам и необходимо в предложенной схеме, т.е. данные выводы являются цифровыми выходами АЦП.

Основные параметры преобразователя при $U_{ИП}$=5В, $U_{ОП}$=-10В:

- нелинейность $\delta_л$=±0,5 ед. МР;
- дифференциальная нелинейность $\delta_{ЛД}$=±0,75 ед. МР;
- абсолютная погрешность преобразования $\delta_{ПШ}$=±3 ед. МР;
- время преобразования $t_{ПРБ}$=7,5 мкс;
- потребляемый ток $I_{пот}\leq$1 мА;
- тактовая частота 0,4…1,5 МГц;
- $U_{ОП}$=-(19,8,,,10,5) В.

4.1.3 Цифро–аналоговый преобразователь. Цифро-аналоговые преобразователи ЦАП служат для преобразования информации из цифровой формы в аналоговую. В нашем устройстве в качестве ЦАП выбрана микросхема К1108ПА2 [9]. Она представляет собой восьми разрядный

преобразователь двоичного кода в напряжение. Данный ЦАП является функционально законченным устройством, включающим:

- восьмиразрядный преобразователь код-ток;
- входной регистр для хранения данных;
- выходной операционный усилитель ОУ;
- источник опорного напряжения;
- устройство управления регистром;
- устройство согласования и обеспечения режимов работы ЦАП.

Микросхема может сопрягаться с микропроцессорами.

Основные параметры ЦАП при $U_{ИП1}$=5В, $U_{ИП2}$=-6В:

- нелинейность $\delta_л$=±0,28%;
- дифференциальная нелинейность $\delta_{ЛД}$=±0,2%;
- абсолютная погрешность $\delta_{ПШ}$=±1,5%;
- максимальное выходное напряжение $U_{вых\ max}$=2,5В;
- потребляемый ток $I_{пот}$=(от 2-х источников)≤100мА;
- время установления выходного напряжения $t_{уст}$ = 1,5 мкс.

Схема включения микросхемы ЦАП К1108ПА2 представлена на рис.4.6.

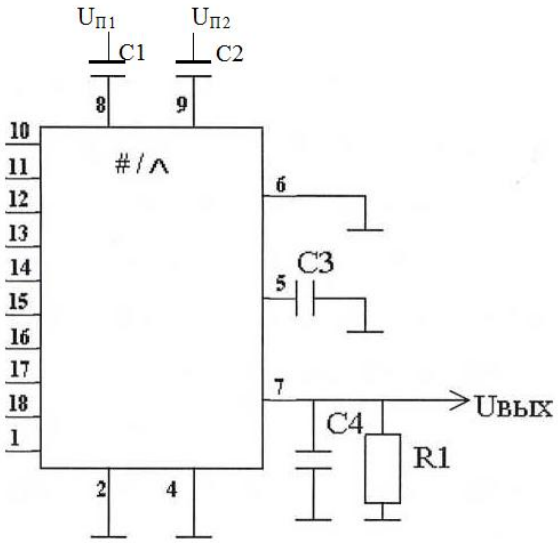


Рисунок 4.6 - Типовая схема включения ЦАП

1 - назначение выводов: - выбор кристалла $\overline{CS}$;
2 - цифровая земля;
4 - аналоговая земля;
5 - коррекция ОУ;
6 - смещение нуля;
7 - выход;
8 - источник напряжения Un1;

9 - источник напряжения Un2;

10-17 - цифровые выходы;

18 - запись $\overline{CE}$;

3 - не используется.

Управление и запись информации в регистр хранения осуществляется путём подачи сигналов на выводы 1 и 18. При образовании входных данных без хранения в регистре выводы 1, 18 заземляются. Режим хранения обеспечивается при напряжениях высокого уровня на указанных выводах. Микросхема может работать в одно- и двуполярном режимах. Включение микросхемы ЦАП в однополярном режиме осуществляется простым заземлением вывода 6. Для перевода в двуполярный режим необходимо заземлить вывод 6 через емкость 0,1 мкФ.

Для данной микросхемы ЦАП существует следующая последовательность подачи напряжения: потенциал земли, $U_{ИП1}$, $U_{ИП2}$, напряжение на цифровые входы. Порядок снятия – обратный. Можно одновременно подавать и снимать указанные напряжения. Длительность импульсов при записи информации не менее 50 нс. Максимальная емкость нагрузки микросхемы 50 пФ.

Предложенная микросхема цифро-аналогового преобразователя полностью удовлетворяет предложенным требованиям. Кроме всего прочего следует отметить, что данный ЦАП обладает дополнительными полезными свойствами такими как: возможность работы любом режиме (однополярный или двуполярный), наличие регистра для хранения данных позволяет, в свою очередь, усложнять степень кодировки не используя дополнительных регистров хранения.

4.1.4 Буферный регистр. Рассмотрев полосовые фильтры, находящиеся на входе и выходе устройства, а также аналого-цифровые и цифро-аналоговые преобразователи можно перейти к более детальному изучению самого аппарата закрытия речи.

Как уже было сказано выше аналоговый сигнал пройдя через полосовой фильтр ПФ1 попадает на АЦП, который в свою очередь посредством последовательного приближения переводит наш речевой сигнал в цифровой восьмиразрядный код. Тут возникает небольшая проблема. Аналоговый сигнал с выхода микрофона попадает на ПФ1, а затем и на АЦП и все это происходит непрерывно, что в принципе может нарушить синхронизацию всей системы в целом. Для устранения этого недостатка необходимо вмонтировать в схему буферный регистр.

Главное назначение микросхемы буферного регистра будет заключаться в парциальной подаче цифрового информационного потока с определённым интервалом для последующей обработки. Таким образом, цифровой информационный сигнал, проходя через буферный регистр, делится на небольшие пакеты, которые появляются на выходе регистра

через равные промежутки времени, что улучшает процесс дальнейшей обработки.

Буферный регистр обладает ещё одним немаловажным свойством - он усиливает информационный сигнал по уровню, что также немаловажно.

В качестве буферного регистра выбрана микросхема К589ИР12 [9] изображённая на рис.4.7.

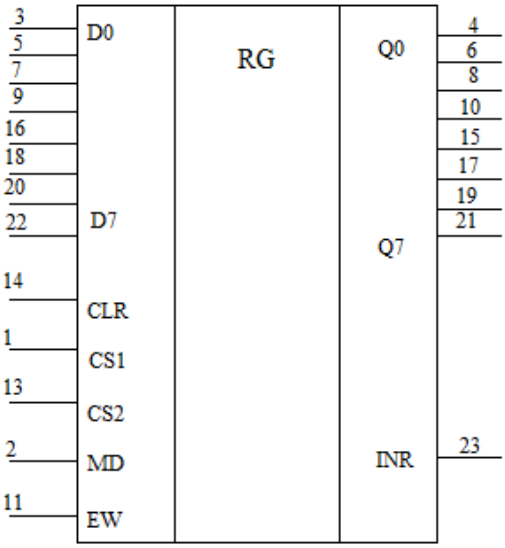


Рисунок 4.7 - Графическое изображение регистра К589ИР12

Данная интегральная схема представляет из себя многорежимный буферный регистр. Напряжение источника питания U_{nHT} = 5 В ± 5%, диапазон рабочих температур t_p = -10 +70°С.

Назначение выводов:

1 - вход выбора кристалла CS1;

2 - вход выбора режима MD;

11 - вход строба EW;

12 - общий GND;

13 - вход выбора кристалла CS2;

14 - вход установки нуля CLR;

23 - вход запроса прерывания INR;

24 - питание U_{CC};

3,5,7,9,16,18,20,22 - информационные входы DO……D7;

4,6,8,10,15,17,19,21 - информационные выходы Q0……. Q7.

4.1.5 Кодер. Буферный регистр, описанный выше, не принимает непосредственного участия в закрытие речи, т.е. в процессе кодирования, но формирует цифровой информационный поток для осуществления многоступенчатого алгоритма защиты. Непосредственно роль кодера осуществляют:

– инвертор;
– генератор тактируемых импульсов ГТИ.

Рассмотрим по подробнее назначение каждого из перечисленных элементов.

Сформированный восьмиразрядный информационный поток с выхода буферного регистра попадает на блок кодера. Здесь, в первую очередь для меньшей узнаваемости информационного сигнала, инвертируются его нечётные разряды, т.е. 1,3,5 и 7, для этого используется элемент логики НЕ, изображённый на рис.4.8. и представляет собой блок микросхемы К555ЛН1 [9], которая представляет собой шесть элементов НЕ.

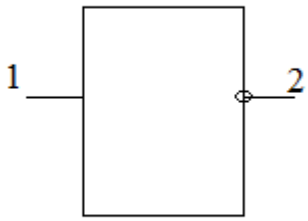


Рисунок 4.8 - Типовая схема включения К555ЛН1

Назначение выводов:
1, 3, 5, 9, 11, 13 - информационные входы микросхемы;
2, 4, 6, 8, 10, 12 - информационные выходы;
7 - общий.

Из шести элементов логики задействуются, соответственно, только два. Далее сигналы с выходов инвертора снова объединяются с чётными неинвертированными разрядами.

Для синхронизации всего кодера используется генератор тактируемых импульсов ГТИ с кварцевой стабилизацией частоты. Он представляет собой кварцевый генератор, частота которого рассчитывается по специальной формуле, и трёх элементов И - НЕ. Схема данного генератора приведена на рис.4.9. В качестве элементов И - НЕ используем микросхему К555ЛА3 [9], которая представляет собой четыре элемента 2И - НЕ, в нашем случае мы используем лишь три элемента. Типовая схема включения микросхемы К555ЛА3 представлена на рис.4.10.

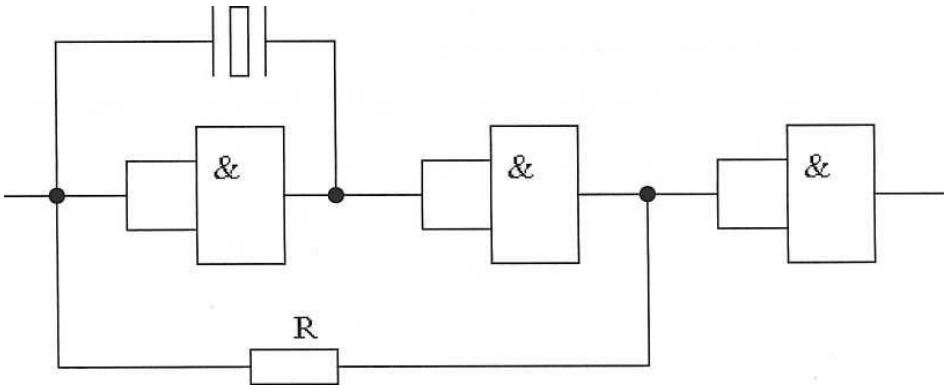


Рисунок 4.9 - Генератор тактируемых импульсов на ИМС К555ЛА3

Расчет частоты генератора производится по формуле Ғ = 1/ (3 * R* C), резистор R у нас постоянен и равняется 1 кОм. В качестве емкости выступает кварц, который подбирается согласно необходимой частоте.

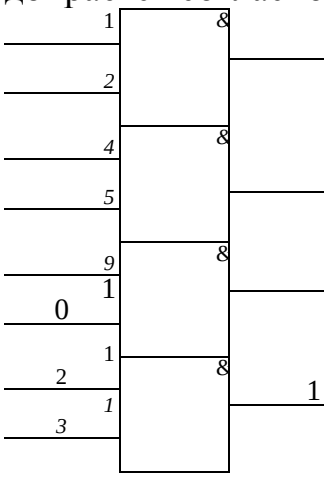


Рисунок 4.10 - Графическое изображение микросхемы К555Л1А3

Назначение выводов:
1, 2, 4, 5, 9, 10, 12, 13 - информационные входы;
3, 6, 8, 11 - информационные выходы;
7 - общий.

На этом обработка информации в кодере завершается и закрытый сигнал из цифрового вида, при помощи цифро-аналогового преобразователя, переводится в аналоговый сигнал. Далее зашифрованный аналоговый сигнал поступает на аналоговый скремблер.

4.1.6 Аналоговый скремблер. Дополняет процесс кодирования аналоговый скремблер, который представляет собой микросхему изображенную на рис. 4.11.

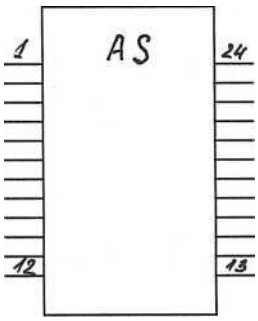


Рисунок 4.11 - Графическое изображение скремблера на ИМС 1146ФП4

Микросхема 1146ФП4 представляет собой программируемый шифратор речевых сигналов, работающий в диапазоне частот 0,3 - 3,4 кГц. Шифрование осуществляется путем разделения частотного диапазона на два поддиапазона, (точка разделения программируется) и разворотом спектра сигнала в каждом из поддиапазонов вокруг их средних частот.

Назначение выводов:

U_{dd} - напряжение питания +5В - 24;

LFO - вход фильтра нижнего частотного диапазона - 23;

T_XIN - вход чистого звукового сигнала передающего канала - 22;

LBMI - вход балансного модулятора нижнего частотного диапазона - 21;

HBMI - вход балансного модулятора верхнего частотного диапазона - 20;

HFO - выход входного фильтра верхнего частотного диапазона - 19;

R_XIN - вход шифрованного звукового сигнала приемного канала - 18;

U_{BIAS} - номинальное напряжение Udd / 2 - 17;

T_xOUT - выход 16;

R_xOUT - выход дешифрованного звукового сигнала приемного канала - 15;

U_{SS} - общий минус - 13;

XTAL/CLK – вход инвертора тактового генератора – 1;

XTAL – выход инвертора тактового генератора – 2;

A4 – A0 – входы программирования – 3 – 7;

P_X/T_X – переключение режима передачи/приема – 8;

CLR/SCR – переключение режима шифрования – 9;

EN/MUTE – блокировка сигнальных каналов – 11;

LOAD/LATCH – стробирование ввода данных программирования – 12;

PDN – включение режима энергосбережения – 13.

4.2 Работа схемы

На основе разработанной структурной схемы выбрана элементная база для всех блоков и построена принципиальная схема системы защиты информации представленная на рисунке 4.12.

В разработанной схеме применена многоступенчатая система защиты. Рассмотрим подробно прохождение сигнала с входа системы на выход и преобразование в цифровом виде.

Аналоговый сигнал поступает на активный полосовой фильтр ПФ1 собранный на операционных усилителях D5, D6, в задачу которого входит ограничение полосы частот речевого сигнала до значения 0,3-3 кГц. Кроме всего прочего активный фильтр обладает коэффициентом усиления, который составляет 2дБ, что также является достоинством. Пройдя через фильтр, аналоговый сигнал уже без побочных составляющих попадает на микросхему аналого-цифрового преобразователя D9, представляющего собой АЦП последовательного счета. Основная задача данной микросхемы заключается в переводе информационного аналогового сигнала в цифровой восьмиразрядный код. Далее кодированный сигнал поступает на информационные входы D1-D8 буферного регистра D10. Основное назначение данного регистра заключается в том , что он формирует из общей последовательности цифровых входов небольшие пакеты определенной длительности, осуществляя таким образом парциальную подачу цифровой информации для шифрования, способствуя тем самым лучшей дальнейшей обработки. После буферного регистра происходит первый этап шифрования, который заключается в следующем – при помощи инвертора, собранного на микросхеме типа D11, инвертируются четные разряды цифровой последовательности, которые в последствии опять занимают свое место в восьми разрядной выборке.

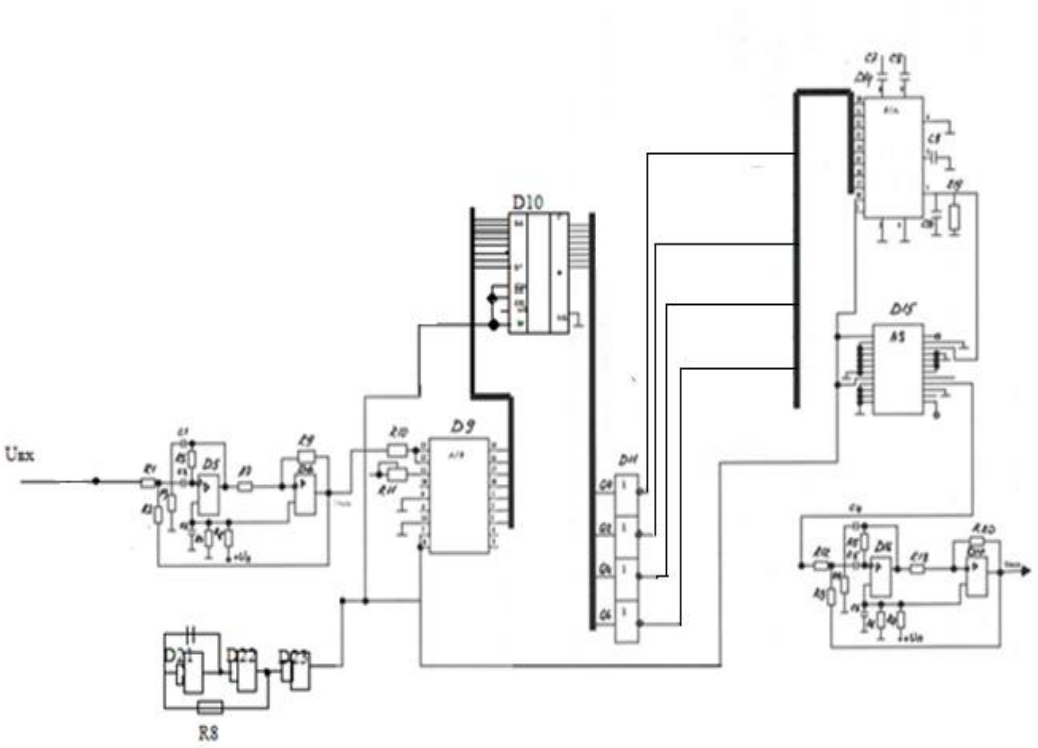


Рисунок 4.12 - Принципиальная схема устройства защиты речевой информации

После инвертора закрытый цифровой речевой сигнал поступает на цифро-аналоговый преобразователь, в задачу которого входит преобразование цифровой последовательности в аналоговый сигнал.

Для более высокой степени защиты на выходе ЦАП устанавливается микросхема аналогового скремблера (АС). Данная микросхема осуществляет временную перестановку аналогового сигнала, выбирается определенная длительность сигнала и стробирующим импульсом делится на две части, после чего они меняются местами.

Полностью закрытый речевой аналоговый сигнал поступает на активный полосовой фильтр ПФ2, который ограничивает его полосу частот до значения 0,3-3,4 кГц, устраняя таким образом избыточность сигнала. При ослаблении сигнала используется усилитель перед выходом сигнала в канал.

Для нормального функционирования всего устройства в целом необходима жесткая синхронизация, для чего в схеме имеется генератор тактируемых импульсов ГТИ с кварцевой стабилизацией частоты. Данный ГТИ обеспечивает жесткую синхронизацию за счет наличия кварца и не происходит сдвига частоты.

Для проверки достоверности работы модели схемы защиты речевой информации, имеющий аналоговый вид, разработана модель на пакете программ SystemView. Она позволяет оценить результаты эксперимента и дает визуальную информацию форм сигналов данного устройства. Разработанная модель представлена на рисунке 4.13.

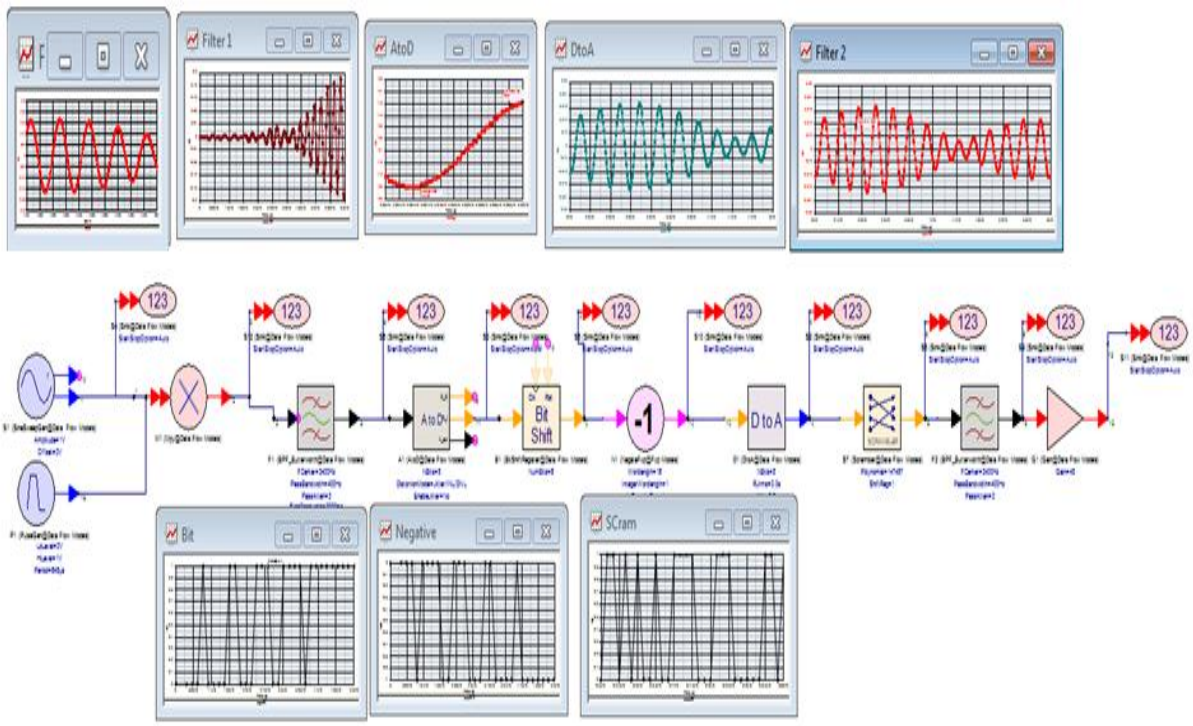
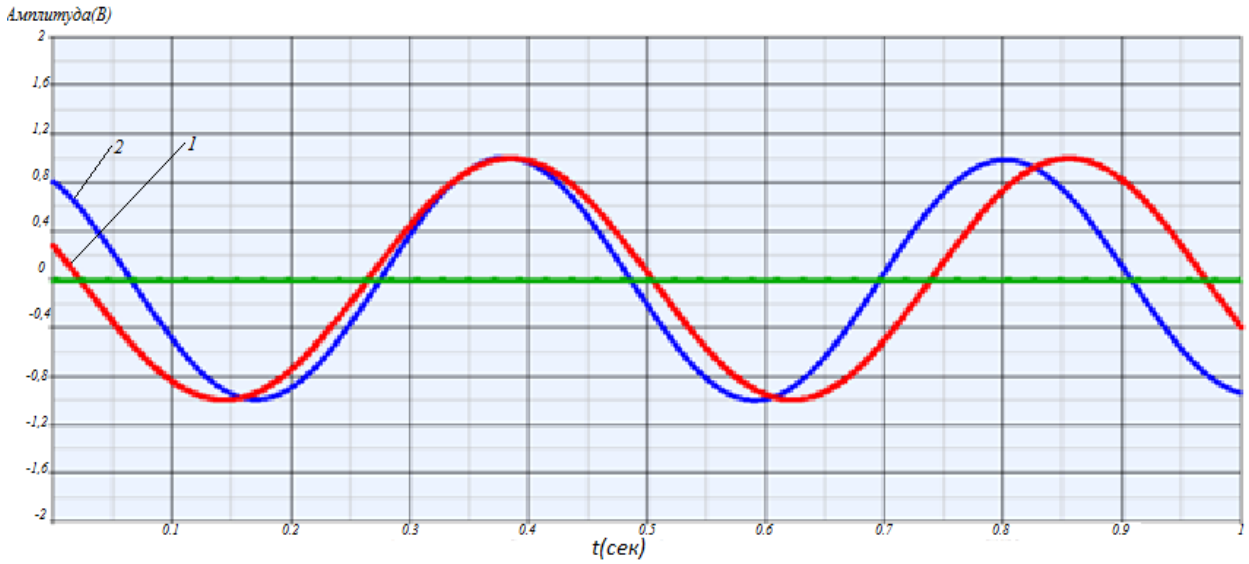


Рисунок 4.13 - Модель схемы в пакете SystemView

На рисунке 4.14 представлены исходный и результирующий сигналы модели системы защиты информации.



1-Результирующий сигнал, 2-Исходный сигнал

Рисунок 4.14 – Исходный и результирующий сигналы смоделированной системы

Из рисунка видно, что сигнал на выходе отличается по фазе.

4.3 Процесс дешифрации сигнала на приемном конце

Дешифрация сигнала на приемном конце происходит обратно процессу шифрования. Закрытый речевой сигнал первоначально поступает на полосовой фильтр для ограничения полосы частот до стандартного значения 0,3-3,4 кГц. Далее аналоговый информационный сигнал проходит через микросхему аналогового скремблера, который осуществляет первый этап декодирования, делая частотную перестановку полученного сигнала.

После первого этапа преобразования сигнал поступает на аналого-цифровой преобразователь с целью перевода его в цифровую форму. После АЦП сигнал попадает на декодер, который складывает по модулю два полученный сигнал с псевдослучайной последовательностью образованной микросхемой ПЗУ, в памяти, которого записано 1024 восьмиразрядных слов, этим осуществляется второй этап декодирования.

Завершает процесс дешифрации четыре элемента НЕ, в задачу которого входит инвертирование нечетных разрядов полученной восьмиразрядной

выборки. После всех преобразований раскодированный цифровой сигнал поступает на микросхему ЦАП, которая преобразует его в аналоговую форму.

На выходе данного устройства стоит полосовой фильтр, который отбраковывает побочные продукты преобразования, ограничивая тем самым спектр до значения 0,3-3,4 кГц, усиливая при этом сигнал необходимого уровня.

4.4 Спецификация

Т а б л и ц а 4.1 – Спецификация

Условное обозначение	Сериал, номинал	Количество	Замечания
Резисторы			
R2, R3, R13, R14	620 кОм	4	
R1, R4, R12, R15	300 кОм	4	
R9, R19	120 кОм	2	
R5, R6, R16, R18	100 кОм	4	
R7, R17	30 кОм	2	
R8, R10, R14	1 кОм	3	
Конденсаторы			
C4, C5	20 мкФ	2	
C6,C7	0,1 мкФ	2	
C1, C2, C8, C9	0,01 нФ	4	
C3, C10	10 нФ	2	
Логика			
D1	К555ЛИ6	1	
D7	К555ЛА3	1	
D11	К555ЛН1	1	
D12, D13	К555Л	2	

	П5		
Счетчики			
D2, D3, D4	К555ИЕ7	3	
Операционные усилители			
D5, D6, D16, D17	КР1040УД1	4	
АЦП			
D9	К572ПВ3	1	
ЦАП			
D14	К1108ПА2	1	
Буферный регистр			
D10	К589ИР12	1	
ПЗУ			
D8	К573РФ1	1	
Кварц			
		1	

4.5 Выводы по четвертой главе

1) Выбираем оптимальную структурную схему устройства защиты, подчиняющуюся выбранной автоматной модели безопасности GM и отвечающую критериям защиты.

2) Сделан подбор элементной базы с последующим созданием принципиальной схемы.

3) Разработанное устройство обеспечивает трехуровневую защиту речевой информации по заданному алгоритму, который представляет собой выборочную инверсию исходной восьмиразрядной выборки с последующим суммированием по модулю два с псевдослучайной последовательностью. И в дальнейшем аналоговый скремблер осуществляет частотную перестановку сигнала.

По завершении проектирования устройства нарисована полная принципиальная схема, разработана модель на пакете программ SystemView и составлена спецификация. Конечным этапом разработки приведено описание работы схемы и принцип дешифрации сигнала на приемном конце.

5 Расчет надежности

5.1.Понятие надежности

Под надежностью системы [8] понимают ее способность выполнять определенные задачи в определенных условиях эксплуатации в течении определенного срока т.е. при наличии установленных параметров функционирования X1, X1, X2…..система должна сохранять во времени эти параметры в пределах X_i - заданных техническими требованиями, при соответствующих режимах и условиях эксплуатации, хранения и транспортировки. Из определения надежности очевидно, что основными составляющими надежности являются три элемента: выполнение системой заданных функций; время, в течении которого должно быть обеспечено выполнение этих функций; условия эксплуатации, хранения и транспортировки.

Выполнение заданных функций зависит от работоспособности системы и события, заключающего в утрате работоспособности, т.е. отказе системы. Утрата работоспособности системы может заключаться в уходе одного либо нескольких параметров, установленных в качестве критериев годности системы, за пределы заданных норм.

Применительно к ИМС и БИС, отказ – это устойчивое нарушение работоспособности ИМС из-за необратимого физического дефекта.

Основными свойствами характеризующими надежность системы, устройства, являются:

− безотказность – сохранение работоспособности в течении требуемого времени ;

– долговечность – сохранение работоспособности до полного износа при соблюдении установленных для системы, устройства правил технического обслуживания;

– сохраняемость – сохранение показателя безотказности и долговечности в течении и после хранения и транспортировки;

– ремонтопригодность – приспособленность системы, изделия к обнаружению, устранению и предупреждению отказов.

Ремонтируемым, т.е. восстанавливаемым системам, изделиям, присуще все четыре свойства, а большинству ИМС и БИС только три первых, т.к. восстановление ИМС и БИС возможно только на завершающих стадиях их изготовления. Для ИМС понятие безотказности и долговечности совпадают т.к. при наступлении первого отказа к них нарушается и безотказность и исчерпывается долговечность. Т.е. основными свойствами определяющими надежность ИМС и БИС, являются безотказность и сохраняемость.

Количественно выразить свойства радиоэлектронного узла, блока, системы во времени в неизменном совокупность параметров в каких либо единицах не возможно. Поэтому для количественной оценки надежности радиоэлектронной аппаратуры (РЭА) применяют вероятностные величины.

Критерии надежности [8] – это признак, мерило, по которому оценивается надежность различных изделий.

Количественно безотказность оценивается такими показателями, как вероятность безотказной работы, интенсивность отказов и средняя наработка до отказа (среднее время безотказной работы).

Долговечность оценивается ресурсом и сроком службы.

Ремонтопригодность характеризует вероятность восстановления, интенсивность восстановления, среднее время восстановления, коэффициенты готовности, простая оперативная готовность.

Экспериментальные исследования безотказности большого числа компонентов и систем радиоэлектронной аппаратуры (РЭА) дали возможность определить общую зависимость интенсивности отказов от времени.

Предложено три периода отказов:

– начальный период отказов (время приработки элементов и технологических отказов);

– период случайных отказов (время нормальной работы);

– период износа (старения).

Выберем второй период т.е. время нормальной работы. Для нормального периода эксплуатации РЭА имеет место экспоненциальный закон распределения отказов во времени без учета сбоев в системе.

При оценке надежности любой радиотехнической системы необходимо составить структурно - логическую схему соединения всех элементов по надежности этой системы. В нашей схеме выход одного элемента из строя приведет к нарушению работоспособности всей системы. Поэтому структурно - логическая схема нашего устройства представляет из себя

последовательное соединение всех элементов схемы по надежности в этом случае интенсивность отказа всего устройства представляет из себя сумму интенсивности отказов всех элементов см. рис. 5.1.

Рисунок 5.1 - Структурно - логическая схема по надежности разрабатываемой системы

В этом случае, если Pi(t) - вероятность безотказной работы одного элемента и $\lambda_{ij} = \lambda_n = \lambda$ и имеется n последовательно по надежности соединенных элементов. Таким образом в случае экспоненциального закона распределения отказов :

$$Рсист(1)=e^{-\lambda общt}, \quad (5,1)$$

$$\lambda_{общ}=\sum\lambda_i, \quad (5,2)$$

$$Тср.сис = 1 / \lambda_{общ} \quad (5,3)$$

5.2 Расчет надежности устройства

Согласно принципиальной схеме наше устройство состоит из навесных элементов и микросхем. Найдем интенсивности отказов навесных элементов и МС.

1) Расчет интенсивности отказов навесных элементов

-для резисторов:

Выбираем резисторы МЛТ 0,25 их интенсивность отказов согласно [8] равна $0,04*10^{-5}$ 1/час их общее количество 19, следовательно:

$\lambda_{рез}=19*0,04*10^{-5}=0,76*10^{-5}$ 1/час.

-для конденсаторов:

Общее количество 10 шт. Два из них электролитических – КЭГ

$\lambda кон1=0,39*10^{-5}$ 1/час, и восемь КБМ $\lambda кон2=0,35*10^{-5}$ 1/час.

$\lambda кон=2*0,39*10^{-5}+8*0,35*10^{-5}=3,58*10^{-5}$ 1/час.

-кварц (селеновый диод) $0,5*10^{-5}$ 1/час [8]

Общая интенсивность отказов всех навесных элементов.

$\lambda общ.нав.= \lambda рез+\lambda кон+\lambda кварц$

$\lambda общ.нав.=(0,76+3,58+0,5)*10^{-5}=4,84*10^{-5}$ 1/час.

2) Расчет интенсивности отказов ИМС [8].

-логические элементы:

у нас 8 ячеек ИЛИ => $\lambda=8*23,12*10^{-8}=184,96*10^{-8}$ 1/час

у нас 4 ячейки И => $\lambda=4*8,24*10^{-8}=32,96*10^{-8}$ 1/час

у нас 4 ячейки НЕ => $\lambda=4*8,24*10^{-8}=32,96*10^{-8}$ 1/час

λобщ.лог= λи+ λили+ λне

λобщ.лог=(184,96+32,96+32,96)$*10^{-8}=250,88*10^{-8}$ 1/час

-регистры и счетчики:

отнесем их к ИМС первой степени интеграции интенсивность их отказов равна $4,27*10^{-6}$ 1/час [8].

λрег.сч.=$4*4,27*10^{-6}=17,08*10^{-6}$ 1/час.

-АЦП и ЦАП. Эти ИМС отнесем к третьей степени интеграции, интенсивность их отказов равна:

λцап.ацп=$2*35,28*10^{-6}=70,56*10^{-6}$ 1/час.

-Аналоговый скремблер отнесем к третьей степени интеграции

λа.с.=$35,28*10^{-6}$ 1/час.

-ПЗУ интенсивность отказов будет равна [8]:

λпзу=$81,2*10^{-6}$ 1/час.

-ОУ отнесем их к ИМС первой степени интеграции для которых интенсивность отказов будет равна [8]:

λоу=$4*4,27*10^{-6}=17,08*10^{-6}$ 1/час.

λобщ.имс= λобщ.лог+ λрег.сч.+ λацп.цап+ λас+ λпзу+ λоу

λобщ.имс=(2,5+17,08+70,56+35,28+81,2+17,08)$*10^{-6}=223,7*10^{-6}$ 1/час.

3) Интенсивность отказов паяных соединений равно

λсоед=$0,1*10^{-8}$ 1/час.

для нашего случая (количество паяных соединений 200)

λсоед=$0,1*10^{-8}*200=20*10^{-8}$ 1/час.

– Общая интенсивность отказов:

λобщ.= λнавес+ λимс+ λсоед.

λобщ.=$48,4*10^{-6}+223,7*10^{-6}+0,2*10^{-6}=272,3*10^{-6}$ 1/час.

– Вероятность безотказной работы:

$P(t)=e^{-\lambda t}$; при t=720 час

$P(t)=e^{-272,3*10\wedge(-6)*720}=0.82$.

В следствии того, что вероятность безотказной работы не получилась максимальной, а также для устранения сбоев в самой системе используем мажоритарное резервирование.

– Среднее наработка на отказ:

$T_0=1/\lambda$общ.=$1/272,3*10^{-6}=37*10^3$ час.

– Среднее время восстановления:

Тср.в.=5мин.=0,08 час

Тср.в.=1/μ=> μ=1/Тср.в.=1/0,08=12 1/час.

– Коэффициент готовности:

Кг=T_0/(T_0+Тср.в.)= μ/(μ+ λобщ.)

Кг=$12/(12+272,3*10^{-6})=0,9997$

– Коэффициент оперативной готовности:

Ког= μ/(μ+ λобщ.)* $e^{-\lambda t}$; Ког=P(t)*Кг.
Ког=0,9997*0,82=0,819.

Заключение

Основной задачей данной магистерской диссертацией было проведение анализа по методам защиты информации, средствам защиты, выбор оптимального метода и средства, а также практическое их исполнение. Также был сделан обзор существующих средств защиты речевой информации предлагаемых на сегодняшнем рынке, и проделана классификация на группы: средства контроля, простейшие средства защиты, средства защиты средней сложности, а также средства защиты высокой сложности.

В связи с тем, что на сетях телекоммуникации, на приемных и передающих участках имеет место речевой сигнал, что наиболее уязвимым местом по несанкционированному доступу является канал тональной частоты.

При этом средства несанкционированного доступа к речевой информации по своей изощренности намного превышают средства защиты и контроля в этих каналах. Поэтому необходимо заниматься защитой именно в речевых системах передачи информации, чтобы установить паритет, ведь в компьютерных сетях эта проблема практически решена применением аппаратных и программных мер защиты.

Первая глава посвящена обзору основных каналов утечки информации, по которым злоумышленники осуществляют несанкционированное получение информации частного и коммерческого характера. Также был сделан обзор основных приемов сбора акустической (телефонной) информации, классифицируя их по диапазону используемых частот, долговременности работы, дистанции передачи, виду используемой модуляции.

Рассмотрены основные достоинства и недостатки этих двух методов. На основе проведенного анализа методов защиты информации от несанкционированного доступа был сделан вывод, что 70% защиты (по своей

эффективности) обеспечивают программные и аппаратно-программные методы так как именно они обеспечивают закрытие канала связи, в то время как организационные методы обеспечивают лишь контроль за помещениями экранировку помещения и т.д.

Рассмотрев методы защиты информации, был проведен обзор существующих на сегодняшний день средств защиты речевой информации, подразделяя их на:

- шифровальные и криптографические средства защиты;
- средства защиты информации от ее утечки по побочным каналам;
- средства защиты информации при ее пересылке или транспортировке.

Также был сделан обзор сегодняшнего рынка средств защиты речевой информации. По итогам первой главы были написаны выводы, в которых предлагались основные принципы защиты информации:

- необходимо анализировать каналы утечки информации и прилагать конкретные мероприятия по борьбе с несанкционированным доступом;
- наилучшими средствами защиты являются включение скремблеров высокой сложности;
- наилучшим средством среди рассмотренных устройств является аппаратура засекреченной речи F-24D, E-24D и E24.

Любая современная телекоммуникационная сеть в основе своего проектирования не может обходиться без математической модели. Точно также проектируя систему защиты необходимо рассматривать модеои безопасности. Согласно требованиям большинства критериев оценки безопасности, системы защиты должны строиться на основе математических моделей, с помощью которых должно быть теоретически обосновано соответствие системы защиты требованиям заданной политике безопасности. Во второй главе были рассмотрены основные классические модели безопасности по которым строятся большинство современных систем защиты на объектах телекоммуникаций. Среди перечисленного ряда моделей была выбрана наиболее подходящая модель, которая по всем своим параметрам удовлетворяет необходимым условиям защиты речевого сигнала, а не разграничивает доступ и определяет потоки как это предлагается в остальных моделях. По второй главе написаны выводы, где расписываются все достоинства и недостатки предложенных моделей и обосновывается принцип выбора модели GM.

В третьей главе была проведена разработка критериев и требований по информационной безопасности. В основе данной разработки лежит анализ заданных требований на предмет перечня, структуры и динамики стоимости информации подлежащей защите, а также выбор моделей потенциального нарушителя и выявления максимально возможного количества каналов несанкционированного доступа к информации. На основе данного анализа вычисляются основные вероятностные величины, которые служат основным элементом стоящим на втором месте по важности, после математических моделей, при проектировании системы защиты. По итогам третьей главы

написаны выводы, в которых производится краткий обзор формул используемых при расчете критериев надежности основными из которых являются прочность преграды:

$$P=1-П*(1-P_i);$$

и вероятность отказа системы при случайном потоке отказов:

$$Q(t)1-e^{-\lambda t};$$

На основе проделанной теоретической работы в предыдущих трех главах разработан алгоритм закрытия информации. Разработка устройства начинается с выбора структурной схемы устройства защиты и основного способа обработки, кодирование информации. По способу защиты существует три типа устройств: аналоговые, цифровые и гибридные, проведя рассмотрение каждого из них в отдельности, в качестве оптимального выбирается устройство, построенное по гибридному принципу, где используется шифрование и скремблирование. После выбора структурной схемы разработана принципиальная схема с полным выбором всей элементной базы. Таким образом, в результате всего проектирования получено устройство, построенное по гибридному принципу кодирования информации с тремя уровнями шифрования, работающее в стандартном диапазоне тональной частоты 0,3-3,4 кГц. Гибридная схема реализации подразумевает под собой цифровое кодирование с возможностью внедрения устройства в аналоговые каналы связи. Адаптированность к аналоговым системам передачи осуществляется за счет применения на входе и выходе устройства аналого-цифровых и цифро-аналоговых преобразователей. Полностью описана работа устройства и разработана модель на пакете программ SystemView. Кроме этого, выполнена спецификация. По итогам четвертой главы написаны выводы, в которых формулируются основные принципы устройств данного типа, обосновывается выбор элементов, а также рассматривается принцип трехступенчатого кодирования и обосновывается мотивация выбора трех ступеней.

Для оценки качественных показателей устройства защиты речевой информации выполнен расчет надежности.

Приведены расчеты основных параметров надежности:

- вероятность безотказной работы;
- средняя наработка на отказ;
- среднее время восстановления;
- коэффициент готовности;
- коэффициент оперативной готовности.

По данным расчета надежности, его численных значений можно судить о надежности всего устройства в целом. Следует отметить, что данное устройство с использованием микросхем 555 серии обеспечивает непрерывную работу без ухудшения параметров шифрования в течении 8000 часов, что

вполне совпадает с нормами на данное устройство выпускаемыми другими фирмами производителями. Надежностные характеристики помимо всего прочего помогают установить степень гарантийной работы схемы, что является не маловажным критерием на сегодняшний день.

Список литературы

1 Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонных каналах. - М.: Энергоатомиздат, 2006.

2 Петраков А.В. Основы практической защиты информации. – М.: Радио и связь,1999.

3 Калинцев Ю.К. Конфиденциальность и защита информации. – М.: МТУСИ,2007.

4 http://daily.sec.ru/%&Ovr0/dailypblshow.cfm?rid=13&pid=4819&pos=1&stp=50

5 http://www.dp5.ru/0_Bibl_SD/No_Publish/catalog/doc/book_www.dp5.ru_000119.doc

6 Казарин О.В., Лагутин В.С., Петраков А.В. Защита достоверных цифровых электрорадиосообщений. – МТУСИ,1997.

7 Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком 2000.

8 http://topreferat.znate.ru/docs/index-8060.html?page=34

9 Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь 2000.

10 Раджабов Т.Д., Васильева М.Г., Абдуазизов А.А. Отчет о научно-исследовательской работе: Исследование и разработка методов обеспечения информационной безопасности почты и телекоммуникаций Республики Узбекистан. – Т.: ТЭИС,1998.

11 Васильева М.Г., Абдуазизов А.А. Оценка надежности радиоэлектронной аппаратуры и интегральных микросхем. – Т.: ТЭИС,1997.

12 Тарабрин Б.В. Интегральные микросхемы справочник. – М.: Энергоатомиздат,1995.

13 Агаханян Т.М. Интегральные микросхемы справочник. – М.: Энергоатомиздат,1993.

14 Мельников Ю.Н. Достоверность информации в сложных системах. - М.: Сов. радио, 1993.

15 Хоффман Л.Дж. Современные методы защиты информации: Пер. с англ. – М.: Сов. радио,1990.

16 Ухлинов Л.М. принципы построения системы управления безопасностью данных в информационно-вычислительныхсетях. – Автоматика и вычислительная техника, 1990, №4.

17 Шеннон К. Теория связи в секретных системах. – В кн.: Работы по теории информации и кибернетике: Пер. с англ. М.: ИЛ,1963.

18 Основы обеспечения безопасности данных в компьютерных системах и сетях. Часть I. Методы, средства и механизмы защиты данных/А.А. Большаков, А.Б. Пеиряев, В.В. Платонов, Л.М. Ухлинов. – С-Пб.:ВИККА им. А.Ф.Можайского,1995.

19 National Bureau of Standards, Data encryption Standard, Federal Information Processing Standard Publication 46, (NTIS NBS-FIPS PUB 46), January 2007.

20 ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

21 Аспис И.Л., Федоренко С.В., Шабунов К.Б. Краткий обзор криптосистем с открытым ключом. – Защита информации «Конфидент», 1994, №2.

22 Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ,2007.

23 Ватолин В.С., Ляшев С.Г. Защита программных средств от несанкционированного использования. – Зарубежная радиоэлектроника, 1989, №12.

24 Громаков Ю.А. Стандарты и системы подвижной радиосвязи. – М.: Радио и связь, 1996.

25 Шахов В.Г.,/Фомин В.В. Защищенная от перехвата система радиотелефонных переговоров. – Автоматика, телемеханика и связь, 1997, №7.