

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03

Информационная безопасность
автоматизированных систем
Защищенные автоматизированные
системы управления

Специализация

ДИПЛОМНЫЙ ПРОЕКТ

на тему

АБОНЕНТСКОЕ УСТРОЙСТВО ПЕРЕДАЧИ РЕЧЕВОЙ ИНФОРМАЦИИ В
ТРАНКИНГОВЫХ СЕТЯХ СВЯЗИ СО ВСТРОЕННЫМ МОДУЛЕМ
КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ.

Студент		Сюняков Марат Ринатович
Руководитель		В.А. Миндалёв
Нормоконтролёр		А.Г. Фатеев
Рецензент	начальник сектора АО «ПНИЭИ»	А.Н. Зорин

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)

Заведующий кафедрой  С.Л. Зефи́ров

Работа защищена с отметкой удовлетворительно (протокол заседаний ГЭК
от 28.06.20 № 17)

Секретарь ГЭК  А.П. Иванов

Пенза 2020

Подпись  удостоверяю
Ведущий инженер  И.Л. Орлова



Оглавление

Введение.....	4
1 Обзор литературы.....	5
1.1 Описание назначение устройства.....	5
1.2 Описание транкинга.....	5
1.3 Описание каналов утечек информации.....	13
1.4 Способы защиты информации по каналам утечек информации.....	15
1.5 Методы закрытия речевых сигналов.....	15
2 Обобщенная структурная схема устройства.....	22
3 Описание технических характеристик взаимодействующего оборудования с транкинговой сетью связи.....	23
4 Аутентификация абонентов в стандарте TETRA.....	26
4.1 Описание аутентификации абонентов в стандарте TETRA....	26
4.2 Уязвимости аутентификации абонентов в стандарте TETRA.	28
5 Описание структурной схемы устройства.....	31
6 Описание функциональной схемы устройства.....	36
7 Выбор элементной базы.....	40
7.1 Выбор микрофона.....	40
7.2 Выбор динамика.....	40
7.3 Выбор кодека.....	40
7.4 Выбор микроконтроллера узла индикации и клавиатуры.....	42
7.5 Выбор радиомодуля.....	44
7.6 Выбор ИМС интерфейса.....	45
7.7 Выбор микрофонного усилителя	45
7.8 Выбор телефонного усилителя	46
8 Выбор элементной базы модуля криптографической защиты.....	47
8.1 Выбор микропроцессора обработки речевых сигналов.....	47

8.2	Выбор контроллера хранения ключей.....	49
8.3	Выбор FLASH-память.....	52
9	Описание метода шифрования цифровых сигналов.....	53
10	Описание технологии Bluetooth.....	59
10.1	Обзор технологии Bluetooth.....	59
10.2	Обзор топологии Bluetooth.....	60
11	Принципиальная схема модуля криптографической защиты.....	63
12	Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.....	64
12.1	Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации.....	64
12.2	Методы и средства физической культуры, снижающие их воздействие.....	68
	Заключение	70
	Список используемых источников.....	71
	Приложение А Схема электрическая структурная устройства передачи речевой информации.....	72
	Приложение Б Схема электрическая функциональная устройства передачи речевой информации.....	74
	Приложение В Схема электрическая принципиальная модуля криптографической защиты информации.....	76
	Приложение Г Протокол проверки ВКР в системе Антиплагиат.....	81

Введение

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, являющейся предметом собственности и подлежащей защите в соответствии с требованиями правовых документов или, устанавливаемых собственниками информации, несанкционированных и непреднамеренных на нее воздействий.[1]

Защита речевой информации является одним из составных частей в системе защиты информации. Особенностью защиты такой информации является то, что она взаимосвязана с источником речи и проявляется в виде волн.

Необходимость совершенствования средств защиты различных носителей информации является одной из главных задач любого объекта.

В данный момент существует большое количество систем и устройств связи, и очень трудно выбрать то, что требуется для решения задач при организации определенной деятельности.

Если рассматривать рынок радиостанций, то по большей части - это радиостанции обеспечивающие открытую передачу речи. Но такие радиостанции не безопасны. Существуют большое количество каналов утечек речевой информации. Поэтому силовые и правоохранительные структуры, службы общественной безопасности используют транкинговую связь для обеспечения связи абонентов между собой, со стационарными абонентами и абонентами телефонной сети, так как транкинговая связь включает в себя требования по обеспечению секретности переговоров и защиты от несанкционированного доступа к системе и, как правило, основными механизмами обеспечения безопасности связи является шифрование и аутентификация абонентов.

1 Обзор литературы

1.1 Описание назначения устройства

В данном дипломном проекте будут разрабатываться схемы устройства передачи речевой информации в транкинговой сети связи со встроенным модулем криптографической защиты информации (далее КЗИ). Из-за модуля криптографической защиты устройство может осуществлять шифрование информации, чтобы сохранить конфиденциальность разговора.

Устройство транкинговой связи используют для организации связи в РСЧС (единая государственная системы предупреждения и ликвидации чрезвычайных ситуаций), в органах внутренних дел Российской Федерации, в ФСБ, в системах корпоративной безопасности и прочих ведомственных организациях.

1.2 Описание транкинга

Транкинговая радиосистема - это цифровая двусторонняя радиосистема, которая использует цифровой канал управления для автоматического назначения частотных каналов группам пользователей. В традиционной полудуплексной системе сухопутной подвижной радиосвязи группа пользователей («разговорная группа») с портативными двусторонними радиостанциями связывается по одному общему радиоканалу, причем один пользователь одновременно разговаривает. Эти системы обычно имеют доступ к нескольким каналам, до 40 - 60, поэтому несколько групп в одной области могут общаться. В обычной (неуправляемой) системе выбор канала выполняется вручную; перед использованием группа должна решить, какой канал использовать, и вручную переключить все радиостанции на этот канал. Это неэффективное использование ограниченных ресурсов радиоканалов, потому что группа пользователей должна иметь исключительное использование своего канала независимо от того, насколько мало передачи они делают. Также

ничто не мешает нескольким группам в одной области выбирать один и тот же канал, что вызывает конфликты. Транкинговая радиосистема является усовершенствованной альтернативой, в которой процесс выбора канала выполняется автоматически.

Транкинг - это более автоматизированная и сложная радиосистема, но она обеспечивает преимущества, заключающиеся в меньшем вмешательстве пользователя в работу радио и большей спектральной эффективности при большом количестве пользователей. Вместо того, чтобы назначать радиоканал одной конкретной группе пользователей за раз, пользователи вместо этого назначаются логической группе, «разговорной группе». Когда какой-либо пользователь в этой группе хочет общаться с другим пользователем в разговорной группе, свободный радиоканал обнаруживается системой автоматически, и разговор происходит на этом канале. Многие несвязанные разговоры могут происходить на канале, используя в противном случае простой между разговорами. Каждый приемопередатчик содержит микропроцессор, который управляет процессом выбора канала. Канал управления координирует всю активность радиостанций в системе. Компьютер канала управления отправляет пакеты данных, чтобы одна разговорная группа могла общаться друг с другом независимо от частоты.

Основная цель этого типа системы - эффективность; многие люди могут вести много разговоров только на нескольких разных частотах. Транкинг используется многими правительственными организациями для обеспечения двусторонней связи с пожарными службами, полицией и другими муниципальными службами, которые совместно используют спектр, выделенный для города, округа или другого субъекта.

Транкинговая радиосистема является компьютерной сетью с коммутацией пакетов. Пользовательские радиостанции отправляют пакеты данных на компьютер, работающий на выделенной частоте, называемой каналом управления, для запроса связи в определенной разговорной группе. Контроллер

отправляет цифровой сигнал на все радиостанции, контролирующие эту разговорную группу, и инструктирует радиостанции автоматически переключаться на частоту, указанную системой для контроля за передачей. После того, как пользователь закончил говорить, пользовательские радиостанции возвращаются к мониторингу канала управления для дополнительных передач. Такое расположение позволяет нескольким группам пользователей обмениваться небольшим набором реальных радиочастот, не слыша разговоры друг друга. Транкинговые системы в основном сохраняют ограниченные радиочастоты, а также предоставляют пользователям другие расширенные функции.

В отличие от обычной радиостанции, которая назначает пользователям определенную частоту, магистральная система использует несколько частот, выделенных системе. Затем канал управления координирует систему, чтобы разговорные группы могли беспрепятственно делить эти частоты. Цель состоит в том, чтобы резко увеличить пропускную способность. Многие радиостанции сегодня рассматривают разговорные группы, как если бы они были частотами, поскольку они ведут себя так.

Концепция транкинга (совместного использования ресурсов) на самом деле довольно старая и взята из технологий и практики телефонной компании. Рассмотрены две телефонные станции центрального офиса, один в городе «А», а другой в соседнем городе «Б». Каждый из этих центральных офисов обладает теоретической способностью обрабатывать десять тысяч индивидуальных телефонных номеров. (Центральный офис «А», с префиксом «123», имеет 10 000 номеров с 123-0000 по 123-9999; центральный офис «Б», с префиксом «124», тоже самое.)

Если бы все 10 000 абонентов в «А» должны были одновременно вызывать 10 000 абонентов в «Б», то для соединения этих двух городов было бы необходимо иметь 10 000 линий (в терминах «магистральные линии» или

просто «транки»). Однако шансы на это невелики, так как количество одновременных телефонных звонков обычно намного ниже.

Эта концепция была просто применена к группам пользователей радиостанции, чтобы определить оптимальное количество каналов, необходимое в нормальных условиях для размещения определенного количества пользователей. В случае широко распространенной чрезвычайной ситуации, такой как сильное землетрясение, гораздо больше пользователей, чем обычно, будут пытаться получить доступ как к телефонной, так и к радиосистемам. В обоих случаях, после того как пропускная способность системы будет полностью использована, все последующие пользователи получают сигнал занятости.

В примере рассылки различным группам назначаются разные уровни приоритета системы, иногда с возможностью «упреждения», пытаясь обеспечить поддержание связи между критическими подразделениями.

Транкинговые радиосистемы отличаются от обычных радиосистем тем, что обычная радиосистема использует выделенный канал (частоту) для каждой отдельной группы пользователей, в то время как транкинговые радиосистемы используют набор каналов, которые доступны для очень многих разные группы пользователей.

Например, если полицейская связь сконфигурирована таким образом, что для разрешения отправки по всему городу на основе географических зон патрулирования требуется двенадцать обычных каналов, то в периоды медленной диспетчерской работы большая часть пропускной способности канала простаивает. В транкинговой системе полицейским подразделениям в данной географической области не назначается выделенный канал, а вместо этого они являются членами разговорной группы, имеющей право использовать общие ресурсы меньшего набора каналов.

Транкинговая радиосвязь использует преимущество вероятности того, что при любом данном количестве пользовательских блоков не каждому

потребуется одновременный доступ к каналу, поэтому требуется меньше дискретных радиоканалов. С другой стороны, при данном количестве радиоканалов может быть размещено гораздо большее количество групп пользователей. В примере полицейского управления эту дополнительную емкость можно было бы затем использовать для назначения отдельных разговорных групп в специализированные следственные группы, группы управления дорожным движением или группы специальных мероприятий, которые в противном случае не могли бы пользоваться индивидуальной частной связью.

Для пользователя транкинговая радиостанция выглядит как обычная радиостанция: для пользователя есть переключатель каналов, чтобы выбрать канал, который он хочет использовать. В действительности, однако, это не переключает частоты, как в обычном радио, но при изменении, это относится к внутренней программе программного обеспечения, которая заставляет принадлежность разговорной группы передаваться по каналу управления. Это идентифицирует конкретную радиостанцию для системного контроллера как члена определенной разговорной группы, и эта радиостанция будет затем включена в любые разговоры, в которых участвует эта разговорная группа.

Это также обеспечивает большую гибкость в использовании радио - одна и та же модель радио может использоваться для многих различных типов пользователей системы (например, полиция, общественные работы, контроль за животными и т.д.), просто изменяя программное обеспечение самой радиостанции.

Так как разговорные группы постоянно передают сигналы на разных частотах, транкинговые радиосистемы затрудняют слушателю сканера без запрограммированного сканера отслеживания соединительных линий следить за разговором.

Транкинговые радиотехнологии сегодня, как правило, разделились на три отдельных типа

Системы первого типа относительно примитивны в своей работе и отвечают только минимальным требованиям, которые должны быть определены как транкинговая радиосистема. Как правило, они не имеют улучшенных функций, таких как передача данных или осведомленность о регистрации. Они предоставят простые возможности транкинга только для голосовых вызовов. К таким системам относятся:

- SmarTrunk;
- Ericsson GE;
- Logic Trunked Radio;
- Motorola (Type 1, Type 2).

Системы второго типа обладают некоторыми характеристиками транкинговой радиосистемы высокого уровня, но не всеми функциями. Поэтому они подходят для небольших развертываний, где пользователи должны использовать всю доступную сеть (например, частную систему, охватывающую кампус или город). Из-за недостатка расширенных функций они обычно не подходят для критически важных развертываний, операций типа PAMR или несогласованных типов общих пользователей. Истинные протоколы DMR в конечном итоге предназначены для перехода в приведенный ниже список третьего типа, но сегодня нельзя классифицировать их как таковые из-за серьезных проблем взаимодействия, отсутствия развитого протокола и отсутствия четко определенных протокол пользовательского интерфейса. К системам этого типа относятся:

- OpenSky System;
- APCO Project 16;
- DMR ;
- NXDN;
- Hytera;

— Motorola (iDEN).

Некоторые транкинговые радиопротоколы имеют особые достоинства, поскольку они явно отличаются от других по следующим причинам:

— проверенная технология, используемая в многочисленных критически важных приложениях по всему миру;

— подвергается лишь незначительным изменениям, а не изменениям основных функций, и это должно происходить не менее нескольких лет;

— предназначен для критически важного применения;

— подходит для большого количества пользователей (свыше 500 различных типов групп пользователей);

— поддержка «подмножества» зон покрытия, при котором конкретный клиент может быть ограничен меньшей зоной покрытия;

— подтверждение вызова на уровне сети (а не сквозное обнаружение успеха / сбоя);

— бесперебойный роуминг, основанный на процедурах, управляемых с центрального контроллера, на основе гистерезиса RSSI или аналогичного;

— режимы отказа, определенные на уровне протокола;

— средства передачи данных;

— осведомленность о присутствии на уровне сети, которая задействует только те участки передатчика, которые необходимы для установления вызова;

— централизованное управление со степенью беспроводного управления терминалами (такими как блокирующие устройства);

— безопасность терминала на основе ESN или аналогичная;

— истинная и проверенная совместимость между производителями, продиктованная открытым стандартом;

— небольшая гибкость для пользовательских отклонений от стандарта, гарантируя, что все терминалы соответствуют стандарту;

— единый стандарт пользовательского терминала в отношении пользовательского интерфейса, тонов, схем набора.

Такой список требований диктует, что будет использоваться выделенный канал управления с центральным управлением.

MPT1327 была первой основной системой, отвечающей требованиям сети высокого уровня, и до сих пор является одним из самых успешных протоколов транкинговых радиосетей в мире.

DMR в настоящее время не фигурирует в этом списке из-за отсутствия доработанного стандарта (все еще находится в активной разработке), в настоящее время не отвечает требованиям к совместимости производителя, имеет значительные проблемы с блокировкой поставщика и не имеет четко определенного стандарта интерфейса пользовательского терминала.

Общий воздушный интерфейс NXDN был принят на собрании Международного союза электросвязи, состоявшемся в ноябре 2016 года, и был добавлен в отчет М.2014-3, опубликованный в феврале 2017 года. Он является открытым протоколом от нескольких поставщиков широко применяется в критически важных приложениях в Японии, США и континентальной Европе.

В третий тип входят следующие системы:

- MPT-1327;
- TETRA;
- APCO 25;
- TETRAPOOL;
- NXDN.

Транкинговая система включает в себя стационарное оборудование и абонентские станции. Абонентское устройство передачи речевой информации с модулем КЗИ подключается к абонентским радиостанциям. Основным элементом стационарного оборудования является базовая станция, которая включает в себя несколько ретрансляторов с соответствующим антенным

оборудованием и контроллер, который управляет работой базовой станции, коммутирует каналы ретрансляторов, обеспечивает выход на телефонную сеть общего пользования или другую сеть фиксированной связи. Структура транкинговой связи с использованием абонентского устройства приведена на рисунке 1.

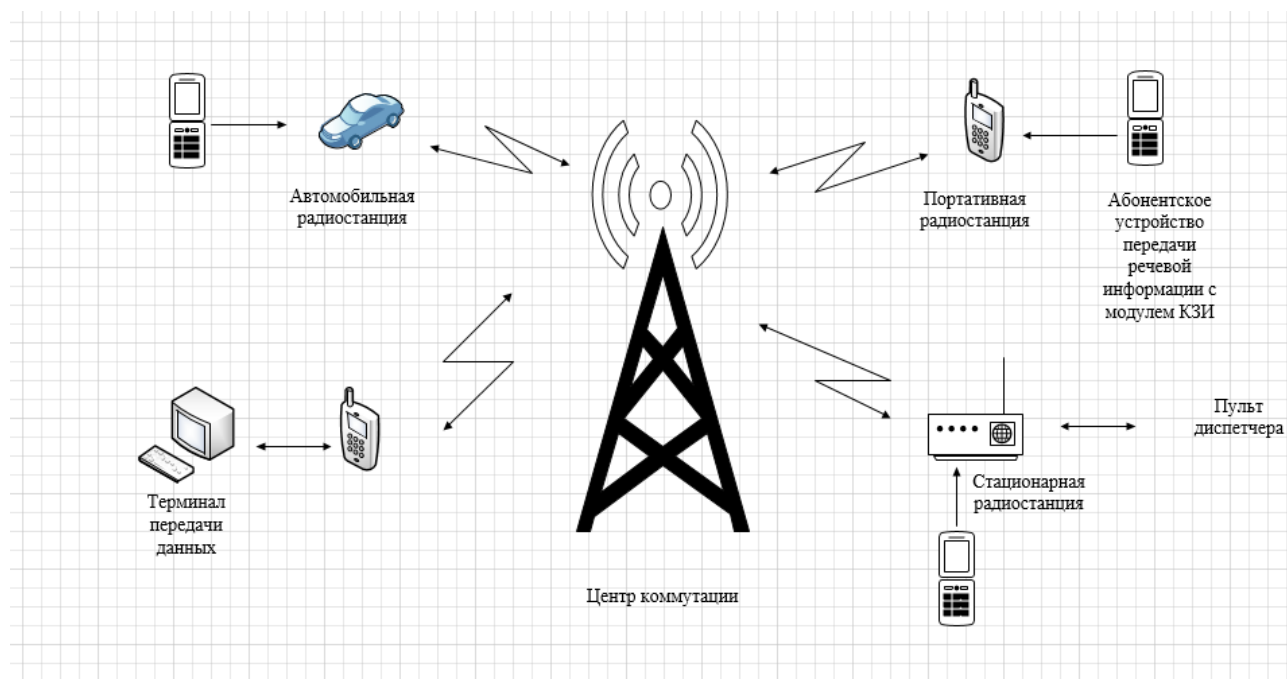


Рисунок 1 — Структура транкинговой связи

1.3 Описание каналов утечек информации

Различают следующие каналы утечки информации: акустовибрационные каналы, акустические каналы, электромагнитные каналы, лазерные каналы, акустоэлектрические каналы.

Перехват информации по прямому акустическому каналу утечки может осуществляться такими способами, как:

- запись речевой информации портативными средствами звукозаписи, скрытно установленными в выделенных помещениях;
- скрытая установка в выделенных помещениях закладных устройств с датчиками микрофонного типа, передающих информацию по радио, оптическим каналам, соединительным линиям вспомогательных технических

средств и систем;

- прослушивание разговоров направленными микрофонами, установленными в ближайших строениях или транспортных средствах.

Перехват информации по акустовибрационному каналу утечки осуществляется такими способами, как:

- скрытое прослушивание разговоров с использованием стетоскопов;
- скрытая установка закладных устройств с датчиками контактного типа, передающего информацию по радио или оптическим каналам.

Перехват информации по акустоэлектрическому каналу утечки осуществляется с помощью подключения специальных низкочастотных усилителей к соединительным линиям вспомогательных технических средств и систем, обладающих микрофонным эффектом и подключением аппаратуры высокочастотного навязывания к соединительным линиям вспомогательных технических средств и систем, обладающих микрофонным эффектом.

Перехват информации по лазерному каналу утечки осуществляется с помощью облучения оконных стекол помещения лазерными акустическими системами, установленными в ближайших строениях или транспортных средствах.

Перехват информации по электромагнитному каналу утечки осуществляется при помощи перехвата ПЭМИ на частотах работы высокочастотных генераторов, входящих в состав вспомогательных технических средств и систем, обладающих «микрофонным» эффектом, аппаратурой, установленной в ближайших строениях или транспортных средствах и с помощью высокочастотного облучения вспомогательных технических средств и систем, обладающих микрофонным эффектом, специальными генераторами, установленными в ближайших строениях или смежных помещениях.

1.4 Способы защиты информации по каналам утечек информации

С целью защиты информации от утечки по лазерному каналу рекомендуется располагать объект защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника, уменьшать освещенность объекта защиты, применять средства маскирования, имитации с целью защиты и введения в заблуждение злоумышленника, применять средства сокрытия объектов в виде аэрозольных завес и маскирующих сеток, красок, укрытий.

С целью защиты информации от утечки по акустическому каналу рекомендуется использование таких мер, как звукоизоляция, звукопоглощение и звукоподавление. Также стоит использовать генераторы шума.

В качестве методов защиты и ослабления электромагнитных полей может использоваться установка электрических фильтры, применение пассивных и активных экранирующих устройств и специальное размещение аппаратуры и оборудования.

С целью защиты информации от утечки по виброакустическому каналу рекомендуется использовать виброакустическую маскировку.

С целью защиты информации от утечки по акустоэлектрическому каналу рекомендуется использовать средства виброакустической и акустической защиты, ограничение сигналов малой амплитуды, отключение преобразователей сигналов.

1.5 Методы закрытия речевых сигналов

Скремблирование - это метод цифрового кодирования, который используется в современных схемах передачи данных и, в основном, может помочь в извлечении информации из принятых данных, улучшая синхронизацию между передатчиком и приемником. В цифровых системах часто встречаются длинные последовательности 1 и 0, что затрудняет

приемнику информацию о синхронизации. В результате устройство ввода рандомизирует данные, но получателю не удастся получить их в неизменном виде. Адаптивное выравнивание, восстановление тактового сигнала и вариации принятых данных - трудности, которые могут быть устранены, если битовая последовательность рандомизирована и это процедура, которую может гарантировать устройство скремблирования.

Техники скремблирования можно разделить на два класса: аддитивное скремблирование и мультипликативное скремблирование. В первом случае скремблеры имеют тенденцию использовать сложение по модулю 2 для преобразования потока входных данных и достижения синхронизации обоих концов с использованием слова синхронизации. Определенный шаблон помещается в начале каждого отправляемого кадра и может быть расшифрован только получателем. С другой стороны, мультипликативные скремблеры названы так, потому что они реализуют умножение между входным сигналом и передаточной функцией скремблера. Этот класс скремблирования также называется самосинхронизирующимся скремблированием, потому что им не нужно синхрослова для синхронизации

Скремблеры используются в различных приложениях. Например, в системах безопасности они могут безопасно шифровать данные и отправлять их в последовательность каналов. Таким образом, они не могут быть перехвачены на пути к приемнику и могут быть расшифрованы дескремблером, установленным на терминале. Основная цель скремблирующих устройств в системах передачи данных состоит в том, чтобы убедиться, что информация из данных, которые были получены от терминала, включает материал синхронизации, который помогает синхронизации обоих концов, таких как два модема.

Точность передачи данных очень высока, так как в противном случае это может привести к потере данных. Например, огромная неисправность сети может иметь место, учитывая скремблеры модема в инфраструктуре фондового

рынка страны, где данные должны быть представлены в режиме реального времени. Этот сбой может быть катастрофическим, учитывая тот факт, что данные передаются и принимаются со всего мира. Таким образом, безошибочная система связи необходима с достаточно точными приборами синхронизации, добавленными к ней. Это было бы легко выполнимо, если бы сети связи были просто построены, но в настоящее время подключаются многочисленные устройства, а большие наборы данных обрабатываются в сложных сетях связи, что затрудняет достижение или даже приближение к цели точечного контакта.

Скремблирование данных в основном использует фиксированные двоичные последовательности, которые в основном напоминают случайный сигнал. Обратная связь генерирует и предоставляет регистры сдвига с этими последовательностями, которые впоследствии используются сумматорами по модулю 2. Сдвиговый регистр состоит из триггеров, которые располагаются в определенном порядке, в котором они получают биты и постепенно направляют их на следующий триггер в каскадной формации. Соединения обратной связи на некоторых этапах включают в себя ответвления, в которых прослушиваемые сигналы добавляются по модулю 2 и возвращаются на первый триггер. Результат сдвигового регистра пройдет через тридцать одно состояние и затем с нуля будет повторять этот процесс ввода битов. Эта последовательность результатов может показаться случайной на первый взгляд, но принимая во внимание сдвиговый регистр, длину и ответвления, можно воспринимать точные биты передаваемой последовательности.

Парадигма отлично справляется с аддитивным скремблером, в котором используется входная битовая последовательность, чтобы соответствовать логическому добавлению по модулю 2 псевдослучайной последовательности.

Последовательность предоставляется генератором псевдослучайной последовательности и состоит из 5-битового ненулевого начального числа. Эта последовательность битов (s_1) передается в скремблер, который суммируется

по модулю 2 из положений 2 и 5 в регистре сдвига. Перед началом передачи данных биты сдвигаются на одну ступень вверх следующим образом: 5 переходов на канал, 4 перехода до 5, 3 смещается на 4, 2 смещается на 3, а 1 смещается на 2. После выполнения этой процедуры импортируется следующий бит последовательности, и этот процесс повторяется.

Когда передача данных (s_2') поступает в дескремблер, биты суммируются в суммы по модулю 2 на этапах 2 и 5, точно так же, как значения, указанные в первичной фазе скремблирования. Первый бит входящей последовательности получается из этой суммы, и содержимое в регистре сдвигается на одну ступень вверх следующим образом: 5 переходит к получателю, 4 переходит на 5, 3 переходит на 4, 2 переходит на 3 и 1 переходит на 2. Эта процедура затем повторяется.

Оглядываясь на начало парадигмы, следует отметить, что структура скремблера идентична структуре, которая расшифровывает данные исходящего кадра. Следовательно, любая оптимизация схемы скремблера должна быть реализована обоими способами, чтобы выполнить точное действие скремблирования и дескремблирования. Предположим, что выполняется успешное скремблирование и дескремблирование относительно этого s_1 равно s_2 .

Если еще глубже разобраться с действиями скремблера, то следует рассмотреть приведенный выше пример с учетом применения схемы. Основной характеристикой скремблирования является использование теории Галуа на полиномах, которая находит реализацию в вышеупомянутом примере в следующем уравнении:

$$s_2 = 1 + D^2s_2 + D^5s_2 \quad (1)$$

Где D - оператор единичной задержки, представляющий последовательность задержки на один бит. Таким образом, D^2s_2 и D^5s_2 относятся к эквивалентным битам скремблированной последовательности, которая передается в канал, как показано на рисунке 1, и между ними находится

двоичный оператор X-OR. Взяв все члены s_2 в одну сторону равенства, получается следующее уравнение:

$$[1 + D_2 + D_5] s_2 = s_1 \quad (2)$$

или, относительно процесса передачи:

$$s_2 = [1 / (1 + D_2 + D_5)] s_1 \quad (3)$$

Что касается подхода на основе уравнения дескремблера, то он отражается следующим образом:

$$s_3 = [1 + D_2 + D_5] s_2' \quad (4)$$

Все схемы в приближении глубины можно в общем случае представить в виде следующих уравнений:

$$s_2 = F(D) s_1 \quad (5)$$

а также

$$s_3 = G(D) s_2 \quad (6)$$

Которые в процедуре скремблирования и дескремблирования используются как:

$$F(D) G(D) = 1 \quad (7)$$

Таким образом, любые принимающие или передающие соединенные сдвиговые регистры, которые используют уравнение 7, подходят для использования в качестве пары скремблер и дескремблер.

Кроме того, теперь ясно, что данные могут быть скремблированы по многим причинам, но для того, чтобы терминал мог принять эти данные и преобразовать их в отличительный вид, необходимо устройство дескремблирования. Дескремблирование является противоположностью скремблирования, и его цель состоит в том, чтобы восстановить состояние данных сигнала в том виде, в котором они были первоначально переданы в связанный скремблер [дескремблер]. Дескремблирование выполняется посредством использования точных алгоритмов, которые были реализованы в начальном зашифрованном сигнале. Любое другое использование алгоритмов в

дескремблере не согласуется с полной процедурой скремблирования и дескремблирования.

Самосинхронизирующаяся операция скремблирования действует в двух режимах. Первый режим называется запуском и работает с данными, которые помещаются в связанный скремблер и дескремблер. Этот конкретный источник информации аналогичным образом хранится на обоих концах. После предопределенного временного интервала первый режим завершается, а второй инициирует процедуру, в которой информация, которая хранится на обоих конечных устройствах, используется для формирования ключевых сигналов. Этот метод успешно работает с рандомизированными битами, используя логическое добавление задержанных цифр из исходной последовательности. В этом установившемся режиме ошибки не могут повлиять на данные, поскольку они уже загружены в устройства до начала дескремблирования.

В системах передачи данных, где скремблирование содержит передачи битового потока, может применяться улучшенный метод самосинхронизации. Управляемое скремблирование считается продолжением многокапитавного скремблирования, и его основной принцип основан на усовершенствованной методике кодирования, которая обеспечивает улучшенную передачу. Аналитически этот метод использует недостаток одного исходного бита, влияющего на многие другие частичные биты. Например, если 01001010001001010100101 является исходной последовательностью, шифрованная должна быть — 01000000001000000100000, которая является несбалансированной последовательностью, представляющей лишь несколько изменений. Наиболее значимый бит этой последовательности равен 0, но если для измененного фактора требуется, чтобы этот бит был равен 1, новая последовательность будет иметь вид: 11010110010111000010111.

Эта последовательность с изменением только одного бита, переносимого в процессе деления по модулю 2, явно показывает лучшие атрибуты передачи.

Управляемое скремблирование широко применяется в волоконно-оптической связи и обеспечивает сбалансированную, эффективную передачу с высокой плотностью перехода.

Поскольку количество оцифрованного контента быстро увеличивается, защита данных становится большой проблемой, такой же важной, как методы кодирования, реализованные для достижения желаемой безопасности. Скремблирование является широко известным и эффективным методом защиты, поскольку оно применяется в большинстве форм связи.

Шифрование - это формальное имя процесса скремблирования, которое применяет функцию, которая изменяет объем данных для защиты перед передачей. Современное шифрование включает в себя алгоритмы, основанные на сложных математических функциях, которые затрудняют или в некоторых случаях невозможно повернуть зашифрованные данные. Конфиденциальность - это, безусловно, необходимость в шифровании. Однако целостность также является большой проблемой, с которой успешно сталкивается шифрование данных. В течение долгого времени считалось, что функция, позволяющая свободно копировать и распространять контент, является выгодной, но кроме чтения данных можно легко изменить их осмысленным образом. Кроме того, скремблирование и шифрование данных являются основными компонентами протоколов, которые обеспечивают безопасность при выполнении системной, сетевой или коммуникационной задачи.[4]

В данном дипломной проекте было выбрано шифрование по алгоритму ГОСТ 28147-89 в режиме гаммирования.[6]

2 Обобщенная структурная схема устройства

Для защиты информации поможет применение радиоэкранирующих материалов, экранирование корпусов элементов, оптимальное построение системы электропитания, установка фильтров.

Для защиты информации от НСД может быть использована кнопка НСД.

При несанкционированном открытии крышки устройства, срабатывает кнопка НСД, при которой ключевая информация может быть стёрта.

Также в устройстве предусмотрена аутентификация оператора аппаратуры и администратора по предъявлению кода доступа и пароля администратора.

Для входа в систему, пользователем вводится код доступа.

Такая же процедура у администратора аппаратуры, для вызова служебного меню.

На рисунке 2 представлена обобщенная структурная схема устройствам

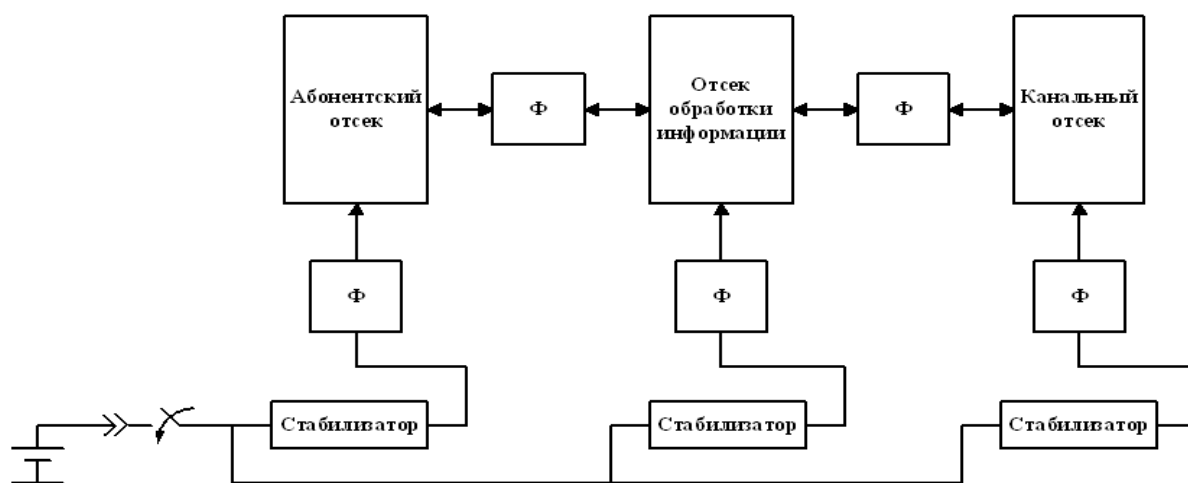


Рисунок 2 — Обобщенная структурная схема устройства

3 Описание технических характеристик взаимодействующего оборудования с транкинговой сетью связи

В качестве взаимодействующего оборудования была выбрана портативная радиостанция Motorola MTP3250.

Многофункциональный MTP3250 предоставляет полный пакет услуг TETRA в сочетании с дополнительной клавиатурой. Дополнительную универсальность обеспечивает возможность подключения Bluetooth для аксессуаров и устройств для совместной работы. Оно оптимизировано для превосходного качества звука и долговечности для использования во всех типах шумных и требовательных ситуаций, где безопасность пользователя имеет первостепенное значение. Этот терминал имеет новый боковой разъем для повышенной прочности. Обеспечение большей мощности увеличит дальность и производительность в здании, поэтому Motorola добавила опцию выходной мощности класса 3L. В сочетании с высокой чувствительностью приема, MTP3250 имеет возможность поддерживать связь в самых сложных ситуациях.

Портативная радиостанция Motorola MTP3250 TETRA обеспечивает высокую производительность и надежность, необходимые для повышения производительности труда и обеспечения безопасности пользователей. Используя лучшие функции двусторонней радиостанции общественной безопасности, MTP3250 был спроектирован для обеспечения громкой и четкой связи.

MTP3250 был разработан для прохождения ускоренного теста на срок службы, имитирующего более 5 лет использования; Эти тесты гарантируют, что они выдержат жесткие условия и обеспечат долговечность, что поможет снизить затраты на поддержку жизненного цикла.

Радиостанции серии MTP3000 оснащены технологией Bluetooth, которая гарантирует безопасное беспроводное соединение с другими устройствами, тем самым открывая множество новых функциональных возможностей для

пользователей. Решения, получаемые при подключении к другим устройствам, помогут улучшить безопасность и эффективность работы ваших сотрудников.

Основные возможности МТР3250:

- полнодуплексные индивидуальные, аварийные и телефонные вызовы в транкинговом режиме;
- полудуплексные индивидуальные, групповые и аварийные вызовы в транкинговом режиме;
- полудуплексные индивидуальные, групповые и аварийные вызовы в прямом режиме;
- идентификация вызывающего абонента;
- аутентификация по запросу инфраструктуры;
- аутентификация по обоюдному запросу терминалов;
- дистанционное выключение терминала;
- аутентификация пользователей;
- специальная кнопка экстренной связи;
- блокировка абонентских групп;
- установка номеров абонентских групп;
- передача звука и данных по Bluetooth.

Основные характеристики МТР3250 представлены в таблице 1.

Таблица 1 – Таблица технических характеристик устройства МТР3250

Размеры (ВхШхГ, мм)	124 x 53 x 33,5 (со стандартной аккумуляторной батареей)
Вес	280 г (радиостанция с аккумуляторной батареей 1650 мА/ч и антенной)

Продолжение таблицы 1

Эксплуатационные характеристики аккумуляторной батареи (батарея 1650 мА/ч класса 4)	Рабочий цикл 5/5/90 > 16 часов Рабочий цикл 5/35/60 > 12 часов
Аккумуляторная батарея	Литий-ионная 1650 мА/ч и 2150 мА/ч
Частотные диапазоны	412-417, 422-427, 457.4-459, 467.4-469 МГц
Передатчик	Мощностные режимы 3L (1,8 Вт) и 4 (1 Вт)

4 Аутентификация абонентов в стандарте TETRA

4.1 Описание аутентификации абонентов в стандарте TETRA

Под аутентификацией абонента обычно понимается механизм опознавания его подлинности. Процедуры аутентификации обычно используются для исключения несанкционированного использования ресурсов связи.

Была смоделирована система аутентификации TETRA, которая включает в себя три основные подсистемы: мобильные станции (MS) у пользователей, базовые станции (BS), в качестве сети радиодоступа и инфраструктуры коммутации и управления (SwMI), в качестве базовой сети, в которую входит центр аутентификации (AuC).

Протокол взаимной аутентификации, инициированной сетью SwMI представлен на рисунке 3.

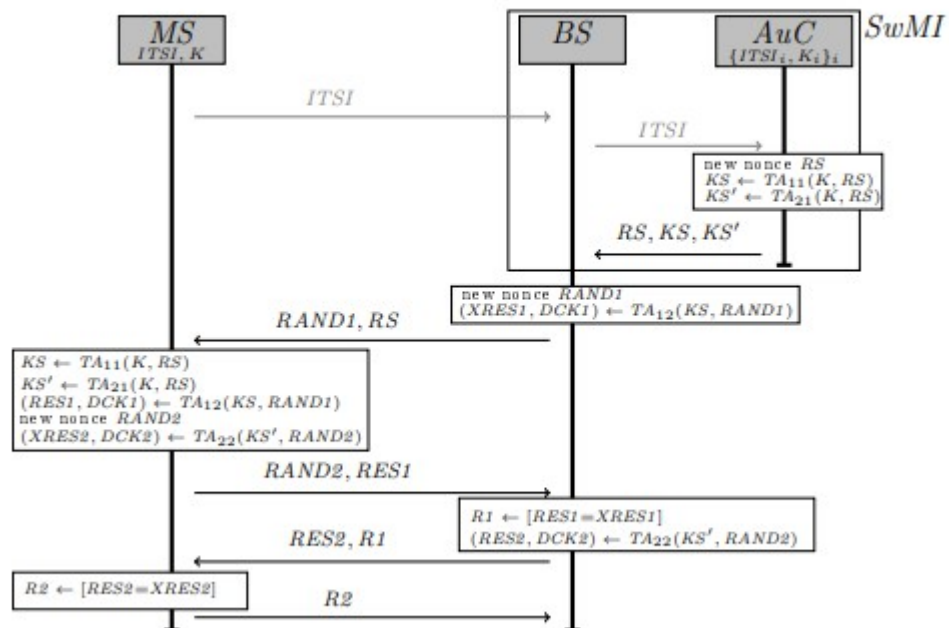


Рисунок 3 — Протокол взаимной аутентификации, инициированной сетью радиодоступа и инфраструктуры коммутации и управления

В этом протоколе используется взаимная аутентификация, инициированная сетью радиодоступа и инфраструктуры коммутации и управления. Мобильная станция и базовая станция согласовывают сеансовый ключ TB4 (DCK1, DCK2).

Мобильная станция определяется как физическое оконечное оборудование, идентифицированное с помощью TETRA.

Идентификация оборудования (TEI), уникальная для каждого устройства, и модуль идентификации абонента (SIM). SIM-карта сохраняет уникальную идентификацию пользователя TETRA и связанную с ней симметричный криптографический ключ в защищенной от несанкционированного доступа памяти и может выполнять криптографические примитивы, применяемые в протоколе аутентификации.

На рисунке 3 показана схема сообщений взаимной аутентификации TETRA. протокол, инициированный сетью радиодоступа и инфраструктуры коммутации и управления. После того, как центр аутентификации получает индивидуальный абонентский идентификатор TETRA (ITSI) мобильной станции, он выбирает ключ аутентификации пользователя K, в соответствии с его абонентский идентификатором.

Учитывая абонентский идентификатор, центр аутентификации затем генерирует случайное начальное RS и использование его с K для генерации пары сеансовых ключей KS и KS0 через алгоритмы TA11 и TA21 соответственно. KS, KS0 и RS перенаправляются в базовую станцию, которая генерирует случайное число RAND1 и вычисляет ожидаемый ответ XRES1 и полученный ключ шифрования DCK1 от KS и RAND1 под алгоритм TA12. Затем базовая станция отправляет RAND1 и RS в мобильную станцию. Мобильная станция затем также генерирует KS и KS0 и вычисляет ответ RES1 и DCK1, из которых RES1 отправляется обратно в базовую станцию. Пользователь также генерирует и отправляет случайное число RAND2 в

базовую станцию. Базовая станция сравнивает RES1 с XRES1 и, если два значения равны, устанавливает, что R1 – истинно.

Кроме того, базовая станция вычисляет ответ RES2 и полученный шифр DCK2 от KS0 и RAND2 по алгоритму TA22. Затем он возвращает RES2 и результат аутентификации R1 - истинно. Затем мобильная станция сравнивает RES2 с ожидаемым ответом XRES2, и, если они равны, мобильная станция в конечном итоге возвращает значение R2 - истинно. После этого обе стороны используют DCK1 и DCK2 для вычисления по алгоритму TB4 общего сеансового ключа DCK.[7]

4.2 Уязвимости аутентификации абонентов в стандарте TETRA

Был проанализирован протокол аутентификации TETRA в отношении так называемой модели безопасности DolevYao. В этой модели злоумышленник полностью контролирует сеть. Он может перехватить любое отправленное сообщение и разложить его. Нападающий может создавать и вставлять сообщения из информации, которую он узнал из перехваченных сообщений и из неограниченного числа свежих констант. Он может инициировать одновременное выполнение неограниченного числа протокольных сеансов.

Однако предполагается, что криптографические примитивы являются абсолютно безопасными. Злоумышленник может только узнать что-либо о нижележащем тексте данного зашифрованный текст, если он знает соответствующий ключ дешифрования. Там нет частичной информации об основных компонентах сообщения, например, о ключах или одноразовых номерах.

Было проанализировано, удовлетворяются ли следующие основные свойства аутентификации и секретности двухсторонних протоколов:

- слабое соглашение (протокол гарантирует слабое согласие стороне А, если для всех протокол уведомляет, что А завершается с предполагаемым партнером по связи В, если стороной В действительно был

выполнен прогон с предполагаемым партнером по коммуникации A);

— неинъективное соглашение (Протокол гарантирует, что неинъективное соглашение для стороны A, если A завершает с предполагаемой связью B, есть протокол, запущенный B с предполагаемым партнером A так, что содержание полученных сообщений в этих прогонах равно содержанию сообщения, отправленного соответствующим прогоном предполагаемого партнера);

— неинъективная синхронизация (Протокол гарантирует неинъективную синхронизацию для стороны A при определенном условии. Если для всех протоколов выполняется условие, что A завершает с намеченной связью партнера B, то есть протокол, запущенный B с предполагаемым партнером A так, что содержание полученных сообщений в этих прогонах равно содержанию сообщения, отправленного соответствующим прогоном предполагаемой связи партнера, и, кроме того, соответствующие действия отправки и получения выполняются в ожидаемом порядке);

— секретность данных (Протокол гарантирует секретность некоторых данных, которыми владеет сторона A. В конце завершеного прогона, например, ключ сеанса согласован).

Существует довольно очевидная слабость в изображенном протоколе аутентификации TETRA: биты подтверждения R1 и R2 не защищены целостностью.

Следовательно, злоумышленник, управляющий связью через радиointерфейс, может использовать эти биты по желанию. Кроме того, более тонким недостатком является то, что ответ RES1, отправленный мобильной станцией к сети радиодоступа и инфраструктуры коммутации и управления не привязана к случайному числу RAND2.

Учитывая это, предлагается использовать протокол аутентификации TETRA:

— добавление защиты целостности R2 путем добавления значения функции аутентификации сообщений TC 1 по R2 и одноразовый номер RAND2, и ключом которого является KS00 (то есть последнее сообщение, отправленное мобильной станцией, должно быть изменено с R2 на R2, TC 1 (R2, RAND2, KS00));

— добавление привязки RES1 и RAND2 путем добавления значения функции аутентификации сообщений TC 1 поверх RES1 и одноразового номера RAND2, ключом которого является KS00 (то есть вместо из RES1, RAND2 MS отправляет RES1, RAND2, TC 1 (RES1, RAND2, KS00)).

KS00 должен генерироваться мобильной станцией и центром аутентификации из RS и их долгосрочный ключ K с использованием функции деривации ключа, отличной от TA11 и TA21. Предлагаемые исправления учитывают сетевую инфраструктуру на практике, где мобильная станция изначально делится секретами только с центром аутентификации, но не с базовыми станциями. Предлагаемые исправления требуют введения дополнительная функция получения ключа (для генерации KS00, поэтому ни одна из KS, KS0, KS00 не является использованной для нескольких криптографических примитивов) и дополнительная функция TC 1 для аутентификации сообщений. Дополнительные сообщения не вводятся, и дополнительные вычислительные затраты могут быть неоправданными. При взаимной аутентификации отправка R1 является избыточной, поскольку это подразумевается при отправке запроса RAND2, что проверка на RES1 прошла. Точно так же нет необходимости отправлять R2, только результирующее значение TC 1 (R2, RAND2).

5 Описание структурной схемы устройства

Структурная схема устройства представлена в приложении А и в графической части дипломного проекта.

В состав структурной схемы входят следующие элементы:

- микрофон;
- динамик;
- микрофонный усилитель/телефонный усилитель;
- кодек;
- узел обработки речевой информации;
- узел шифрования и расшифрования;
- контроллер сопряжения;
- узел ввода ключевой информации;
- узел хранения ключевой информации;
- радиомодуль;
- модуль КЗИ;
- клавиатура;
- устройство индикации;
- стабилизатор;
- узлы фильтрации;
- блок питания;
- аккумулятор.

Устройство обрабатывает и передает данные в цифровом виде, поэтому звуковая информация, до того, как она будет промодулирована высокочастотным сигналом и передана по радиоканалу, должна быть преобразована в цифровой формат. Для преобразования аналогового сигнала в цифровой код и обратного преобразования цифрового кода в аналоговый сигнал, в структурной схеме устройства необходимо предусмотреть кодек.

Кодек предназначен для преобразования цифровых отсчётов передаваемого цифрового сигнала в аналоговый сигнал и его фильтрации, а также для обратного преобразования входного аналогового сигнала в отсчёты цифрового кода.

Для преобразования электрических колебаний звуковых частот в акустические колебания, в структурной схеме устройства необходимо предусмотреть электромагнитный излучатель звука (динамик).

В состав структурной схемы входит микрофонный усилитель предназначенный для усиления речевых сигналов.

Телефонный усилитель предназначен для усиления речевых сигналов до необходимого уровня, обеспечивающего хорошую слышимость удалённого абонента.

Для обработки, шифрования и расшифрования речевой информации, и управления узлами устройства в структурной схеме устройства следует предусмотреть узел обработки речевой информации. Узел обработки информации выполняет следующие функции: преобразование речевой информации в последовательный битовый поток в речепреобразующем устройстве (РПУ), управление узлами устройства в узле управления, шифрование информации в специальном блоке. Речепреобразующее устройство предназначено для обработки речевых сигналов в соответствии с алгоритмом дельта-модуляция. Речепреобразующее устройство осуществляет обработку оцифрованного сигнала программным способом. Хранения программы обработки оцифрованного сигнала, осуществляется в FLASH-памяти ЦПОСа. Специальный блок предназначен для шифрования и расшифрования речевой информации, передающейся в цифровом виде с устройства обработки речевой информации. Шифрование осуществляется по алгоритму ГОСТ 28147-89.[6] Шифрование осуществляется программным способом в соответствии с ключевыми документами, введенными в узле ввода, хранения КИ. Устройство управления в режиме передачи речевых сообщений осуществляет управление,

всеми узлами устройства, формируя необходимые команды, в соответствии с которым узлы принимают и передают информацию. Устройство управления осуществляет также приём и анализ сигналов состояния основных узлов устройства. Процесс установления соединения и ведение разговоров отображается на дисплейном модуле, команды для отображения формирует устройство управления и индикации.

Модуль КЗИ реализуется на ЦПОСе. ЦПОС предназначен для управления работой всех узлов устройства, приёма и анализа сигнала состояния основных узлов устройства, преобразования отсчётов речевых аналоговых сигналов, получаемых от аналого-цифрового преобразователя, и формирования кадров речепреобразования, обратного преобразования кадров речепреобразования по алгоритму дельта-модуляции со скоростью приёма/передачи информации 16 кбит/с, обработки кадров информации в соответствии с алгоритмом шифрования, обработки команд управления, поступивших от устройства индикации, и выдачи ответных управляющих команд.

Для ввода ключевой информации в специальный блок и её хранения в процессе работы следует предусмотреть узел ввода и хранения ключевой информации. Устройство ввода и хранения ключевой информации предназначено для ввода ключевых документов с ПЭВМ, подключаемой по стыку RS-232 и записи ключевых документов во внутреннюю FLASH-память микроконтроллера. Для ввода ключевой информации к соединителю подключается ПЭВМ и по командам, поступающих с устройства управления, осуществляется запись ключевой информации в FLASH – память микроконтроллера. Ввод ключевой информации производится по командам оператора с помощью клавиатуры, расположенной на лицевой панели устройства. Процесс ввода ключевых документов отображается на дисплее.

Для согласования скоростей работы и логических уровней сигналов, по которым осуществляется обмен информации между специальным блоком и приёмопередающим устройством, в структурной схеме устройства следует

предусмотреть контроллер сопряжения. Контроллер сопряжения предназначен для преобразования последовательного потока информации, принимаемой из радиомодуля в параллельный код, а также преобразования отсчётов информации из параллельного кода в последовательный и выдачи её в радиомодуль.

Для обеспечения всех необходимых номиналов напряжений питания, в структурной схеме устройства следует предусмотреть блок питания.

Для обеспечения стабильного напряжения, не зависящего от источника питания, структурной схеме устройства следует предусмотреть стабилизаторы напряжения.

Для подавления электромагнитных помех, нарушающих нормальную работу элементов устройства в структурной схеме следует предусмотреть фильтры.

Для передачи и приёма цифровой информации по радиоканалу в структурной схеме устройства следует предусмотреть радиомодуль. Радиомодуль представляет собой Bluetooth-модуль. Технология Bluetooth предназначена для беспроводной связи между собой различного оборудования и приборов в диапазоне не лицензируемых частот 2,4 ГГц.

Узел клавиатуры и индикации предназначен для формирования необходимых команд для специального блока, устройства обработки речевой информации и устройства сопряжения по командам, подаваемым с клавиатуры и отображения режимов работы устройства. Устройство индикации реализовано на микроконтроллере. Обработка команд управления осуществляется в соответствии с программой, записанной во внутреннюю FLASH- память микроконтроллера.

Устройство индикации необходимо для отображения текущего состояния аппаратуры, отображения состояния при вводе ключевой информации и отображения меню аппаратуры. Устройство индикации, представляет собой дисплейный модуль.

Для задания режимов работы, задания команд для обеспечения ввода ключевой информации, выбора абонентов и установления соединения в структурной схеме устройства необходимо предусмотреть кнопочную клавиатуру.

6 Описание функциональной схемы устройства

Функциональная схема устройства представлена в приложении Б и в графической части дипломного проекта.

Микрофон осуществляет преобразование акустических колебаний звуковых частот в электрические колебания.

Динамик осуществляет преобразование электрических колебаний звуковых частот в акустические колебания.

Микрофонный усилитель предназначен для усиления речевых сигналов, преобразованных микрофоном из акустических в электрические сигналы.

Кодек предназначен для преобразования цифровых отсчётов передаваемого цифрового сигнала в аналоговый сигнал и его фильтрации, а также для обратного преобразования входного аналогового сигнала отсчёты цифрового кода.

Телефонный усилитель выполняет функцию усилителя мощности.

Узел клавиатуры и индикации предназначен для формирования необходимых команд для специального блока и узла сопряжения по командам подаваемым с клавиатуры, а также для отображения режимов работы устройства.

Узел индикации обеспечивает отображение текущего состояния аппаратуры, отображение состояния при вводе ключевой информации и отображение меню аппаратуры.

Узел клавиатуры предназначен для выбора и задания режимов работы.

Стабилизатор предназначен для формирования напряжения, необходимого для работы элементов узла клавиатуры и индикации.

Стабилизатор предназначен для формирования напряжения, необходимого для работы элементов узла обработки речевой информации.

Выходное напряжение со стабилизатора подается в узел обработки речевой информации через фильтр.

Сигналы по информационным цепям между отсеками, проходят через фильтры.

Узел преобразования предназначен для приёма цифровых отсчётов, передаваемых от РПУ и преобразования их в параллельный код.

Узел управления в режиме передачи речевых сообщений осуществляет управление, всеми узлами устройства, формируя необходимые команды, в соответствии с которым узлы принимают и передают информацию.

Узел формирования 1 обеспечивает формирование из битового потока блока информации для обработки в узле шифратора.

Узел формирования 2 предназначен для формирования из блока информации, принятого от дешифратора, в битового потока.

Модуль КЗИ при начале работы выполняет программу пускового контроля. После проведения контроля модуль переходит к выполнению основной программы.

При установлении входящего соединения на аппаратуру поступает вызов от абонентских станций в каналный отсек и выдает по Bluetooth-радиоинтерфейсу команду «входящий вызов». Bluetooth модуль принимает данную команду и выдает ее в контроллер индикации, на дисплее устройства выводится сообщение о поступившем вызове. Процесс установления соединения и ведения переговоров отображается на дисплее устройства в соответствии с командами, формируемыми узлом клавиатуры и индикации.

Шифратор выполняет зашифрование блоков информации в режиме гаммирования, путем поразрядного суммирования по модулю 2 с гаммой шифра, в блоки зашифрованной информации.

Дешифратор выполняет расшифрование блоков информации, поступающих с узла анализа пакетов, в блоки информации для узла формирования 2.

Узел формирования пакетов предназначен для формирования из блоков шифрованной информации информационного пакета, предназначенного для передачи по радиоканалу.

Узел хранения КИ предназначен для хранения ключевой информации во внутренней памяти микроконтроллера, вводимой с узла ввода ключевой информации.

Узел ввода КИ предназначен для ввода в аппаратуру ключевой информации с помощью ПЭВМ.

Узел сопряжения с ПЭВМ предназначен для обеспечения обмена данными между ПЭВМ и аппаратурой по стыку RS-232.

Узел сброса ключевой информации предназначен для формирования сигнала установки и хранения ключевой информации в начальное состояние.

Стабилизатор предназначен для формирования напряжения необходимого для работы элементов модуля КЗИ.

Выходное напряжение со стабилизатора подается в отсек модуля КЗИ через фильтр.

Сигналы по информационным цепям между отсеками проходят через фильтры.

В контроллере сопряжения информация преобразуется в пакеты для передачи по Bluetooth-модулю. Контроллер сопряжения выдает сформированные пакеты в радиомодуль

Радиомодуль предназначен для передачи информационных пакетов по радиоканалу, в режиме передачи, и для приёма информационных пакетов в режиме приёма.

Коммутатор предназначен для выполнения переключения между приёмным и передающим трактами устройства, образуя режим «полудуплекс».

Стабилизатор предназначен для формирования напряжения, необходимого для работы элементов канального отсека.

Выходное напряжение со стабилизатора подается в канальный отсек через фильтр.

7 Выбор элементной базы устройства

7.1 Выбор микрофона

В телефонных аппаратах применяются электретные микрофоны. Микрофон расположен в абонентском отсеке. В качестве микрофона используем электретный микрофон CZN-15E, характеристики которого представлены в таблице 2.

Таблица 2 - Таблица технических характеристик CZN-15E

Чувствительность	от 42 до 62 мВ/Па
Частота	от 20 до 16000 Гц
Диапазон напряжения	от 1,5 В до 10 В
Стандартное рабочее напряжение	4,5 В
Потребляемый ток	Макс.0.5мА
Соотношение сигнал / шум	более 60 дБ

7.2 Выбор динамика

В качестве динамика в данном дипломном проекте используется электромагнитный излучатель звука ОВО – 25032G-01, характеристики которого приведены в таблице 3.

Таблица 3 - Таблица технических характеристик ОВО – 25032G-01

Полное сопротивление	32 Ом плюс минус 15% на 1.0 кГц
Чувствительность	72 плюс минус 3 дБ на 100мВ
Номинальная мощность	300 мВ
Полная мощность	500 мВ
Уровень звуковой отдачи	72 плюс минус 3 дБ
Резонансная частота	750 плюс минус 150 Гц
Частотный диапазон	От 450 до 12000 Гц

7.3 Выбор кодека

В данном дипломном проекте в качестве кодека был выбран W681310.

W681310 - это одноканальный кодек PCM общего назначения с возможностью выбора по выводам. Устройство соответствует спецификации ITU G.712. Он работает от одного источника питания 3 В и доступен в вариантах с 20-контактным SOG, SSOP и TSSOP. Выполняемые функции включают в себя оцифровку и реконструкцию речевых сигналов, а также фильтры ограничения полосы и сглаживания, необходимые для систем PCM. Производительность W681310 указана для промышленного температурного диапазона от минус 40 °С до плюс 85 °С.

W681310 включает в себя ссылку на чипе точность напряжения и дополнительный усилитель мощности, способный управлять нагрузками дифференцированно до уровня 3,544 В от пика до пика. Аналоговая секция является полностью дифференциальной, что снижает уровень шума и улучшает коэффициент подавления питания. Протокол передачи данных поддерживает как длинную, так и короткую синхронную связь для приложений PCM, а также связь IDL и GCI для приложений ISDN. W681310 поддерживает восемь основных тактовых частот от 256 кГц до 4,800 МГц, а встроенный предварительный масштаб автоматически определяет коэффициент деления для требуемой внутренней тактовой частоты.

Характеристики W681310:

- один плюс 3В источник питания (от 2,7 до 5,25 В);
- типичная рассеиваемая мощность 10 мВт, режим выключения питания 0,5 мВт;
- полностью дифференциальная аналоговая схема
- точность на кристалле 0,886 В для TLP -5 дБм при 600 Ом;
- двухтактные усилители мощности с внешней регулировкой усиления с нагрузкой 300 Ом;
- восемь тактовых частот от 256 кГц до 4800 МГц;

- выбираемый по пин-кодам компандинг по Law-Law и A-Law (в соответствии с ITU G.711);
- фильтрация кодеков А / D и D / А в соответствии с ITU G.712;
- диапазон промышленных температур (от минус 40 °С до плюс 85 °С);
- пакеты: 20-контактный SOG (SOP), SSOP и TSSOP.

7.4 Выбор микроконтроллера узла индикации и клавиатуры

Так как узел управления выполняет управление всеми узлами, осуществляя выбор режима работы проектируемого устройства и обеспечивает вывод необходимой информации на индикаторе, то необходимо выбрать узел, который может обеспечить выполнение всех функций узла управления. Для применения в качестве устройства управления в данном случае, лучше всего подходит микроконтроллер.

В данном дипломном проекте был выбран STM32L471R.

Характеристики STM32L471R:

- источник питания от 1,71 до 3,6 В;
- от минус 40 °С до плюс 125 °С в диапазоне температур;
- 300 нА в режиме VBAT: питание для RTC и 32х32-битных резервных регистров;
- режим отключения 30 нА (5 выводов для пробуждения);
- режим ожидания 120 нА (5 выводов для пробуждения);
- 420 нА в режиме ожидания с RTC;
- 1,1 мкА в режиме Stop 2, 1,4 мкА в режиме Stop 2 с RTC;
- режим работы 100 мкА / МГц;
- пакетный режим сбора данных (BAM);
- 4 мкс пробуждения из режима остановки;

— сброс из-за отключения (BOR) во всех режимах, кроме выключения;

— 32-разрядный процессор ARM® Cortex®-M4 с FPU, адаптивный ускоритель в реальном времени, обеспечивающий выполнение в состоянии ожидания 0 из флэш-памяти, частота до 80 МГц, MPU, 100DMIPS / 1.25DMIPS / МГц (Dhrystone 2.1) и инструкции DSP;

— кварцевый генератор от 4 до 48 МГц;

— кварцевый генератор 32 кГц для RTC (LSE);

— внутренняя 16 МГц заводская настройка RC (плюс минус 1%);

— внутренний маломощный 32 кГц RC (плюс минус 5%);

— внутренний многоскоростной генератор от 100 кГц до 48 МГц с автоматической подстройкой LSE (точность выше плюс минус 0,25%);

— 3 PLL для системных часов, аудио, АЦП;

— RTC с календарем, сигналами тревоги и калибровкой;

— до 24 емкостных сенсорных каналов: поддержка сенсорных кнопок, линейных и поворотных сенсорных датчиков;

— таймеры: 2 x 16-битного расширенного управления двигателем, 2 x 32-битных и 5 x 16-битных общего назначения, 2x16-битные базовые, 2x маломощных 16-битных таймера (доступны в режиме Stop);

— до 114 быстрых входов / выходов, большинство с допуском 5 В, до 14 входов / выходов с независимым питанием до 1,08 В.

В качестве индикатора был выбран OLED-индикатор WEO012864H.

Технические характеристики WEO012864H:

— диагональ видимой части — 2.42 дюйма;

— тип дисплея — OLED;

— режим — графический;

— разрешение 128x64;

- тип встроенного контроллера — SSD1309ZC;
- особенности — COG;
- напряжение питания — от 2,8 В до 3,3 В;
- размер — 60,5x37x2,15 мм;
- рабочая температура — от минус 40 °С до плюс 80 °С.

7.5 Выбор радиомодуля

Для данного дипломного проекта был выбран Bluetooth-модуль BLE (dual model) Bee V1.0.

Этот модуль применяется, в основном, для телефонов и КПК, где приемопередатчик работает под управлением процессора устройства, которое, в том числе, отвечает за формирование протокола передачи.

Особенности данного модуля:

- Bluetooth спецификация V4.0 и BLE;
- UART прием и передача: max 512 байт;
- прием/передача данных устройство-модуль в режиме SPP: 90 байт за пакет;
- прием/передача данных устройство-модуль в режиме BLE: 20 байт за пакет;
- два режима передачи данных: сбалансированный режим и высокоскоростной режим;
- рабочая частота: 2.4 ГГц полоса ISM;
- метод модуляции: GFSK (гауссово частотная манипуляция);
- мощность: 23дБм
- скорость асинхронная и синхронная: 3К байт;
- безопасность: аутентификация и шифрование;
- службы: Slave SPP, Peripheral BLE, UUID FFE0, FFE1;

- питание: плюс 3.3В 50мА;
- диапазон работы: в режиме SPP 30 метров, в режиме BLE 60 метров;
- потребляемый ток: в режиме SPP 13.5мА, в режиме BLE 9.5мА.

7.6 Выбор ИМС интерфейса RS-232

Устройство ввода и хранения ключевой информации предназначено для ввода ключевых документов с ПЭВМ, подключаемых по стыку RS-232.

В качестве ИМС интерфейса RS-232 был выбран продукт SP3243EB.

SP3243EB - это приемопередающие решения RS-232, предназначенные для портативные приложения, такие как ноутбуки и карманные компьютеры.

SP3243EB использует внутренний высокоэффективный источник питания с подкачкой заряда, для которого требуется только конденсаторы 0,1 мкФ в режиме 3,3 В. Этот зарядный насос и архитектура драйвера Sipex позволяет SP3243EB для обеспечения совместимой производительности RS-232 от одного источника питания в диапазоне от 3,0 В до 5,5 В.

Основные характеристики SP3243EB указаны в таблице 4.

Таблица 4 - Основные характеристики SP3243EB

Источник питания	Драйверы RS-232	Приемники RS-232	Конденсаторы
3,0 В до 5,5 В	3	5	4

7.7 Выбор микрофонного усилителя

Микрофонный усилитель предназначен для фильтрации сигнала, поступающего с микрофона.

В качестве микрофонного усилителя был выбран MAX4252 из-за своих габаритов и стабильных параметров.

Характеристики указаны в таблице 5.

Таблица 5 — Характеристики МАХ4252

Номинальное напряжение источников питания	от 2,4 В до 5,5 В
Максимальный потребляемый ток	1 мА
Коэффициент усиления по постоянному напряжению	100 дБ
Выходное сопротивление	140 Ом
Граничная частота усиления	3 МГц

7.8 Выбор телефонного усилителя

Телефонный усилитель предназначен для усиления сигнала звуковой частоты.

В качестве телефонного усилителя был выбран ТРА301.

Основные характеристики указаны в таблице 6.

Таблица 6 — Характеристики ТРА301

входное напряжение	от 0 В до 5,5 В
выходная мощность	350 мВт
диапазон рабочих температур	минус 20 °С до плюс 70 °С
коэффициент усиления	10
выходное напряжение шума	15мкВ
напряжение питания	от 2,5 В до 5,5 В

8 Выбор элементной базы модуля криптографической защиты информации

8.1 Выбор микропроцессора обработки речевых сигналов

Устройство обработки речевой информации реализовано на цифровом процессоре обработки сигналов. Для обеспечения полудуплексного режима работы проектируемого устройства и обработки оцифрованного речевого сигнала в реальном масштабе времени, необходим специализированный процессор обработки сигналов. Если обработку будет производить универсальный микропроцессор, то он не сможет работать в реальном масштабе времени. Поэтому нужно использовать специализированный цифровой процессор обработки сигналов (ЦПОС).

В данном дипломном проекте был выбран ЦПОС TMS320C5517.

Это устройство входит в семейство продуктов цифрового сигнального процессора (DSP) TIC5000™ и предназначено для низкого потребления активной и резервной энергии.

Устройство основано на ядре процессора ЦП поколения TMS320C55x. Архитектура C55x DSP обеспечивает высокую производительность и низкое энергопотребление за счет увеличения параллелизма и общего внимания к экономии энергии. ЦП поддерживает структуру внутренней шины, которая состоит из одной программной шины, одной 32-разрядной шины чтения данных и двух 16-разрядных шин чтения данных, двух 16-разрядных шин записи данных и дополнительных шин, предназначенных для периферийных устройств и операций прямого доступа к памяти. Эти шины обеспечивают возможность до четырех 16-битных операций чтения данных и двух 16-битных операций записи данных за один цикл. Устройство также включает в себя четыре контроллера DMA, каждый из которых имеет 4 канала, обеспечивая перемещение данных для 16 независимых контекстов канала без вмешательства ЦП.

Каждый контроллер DMA может выполнять одну 32-битную передачу данных за цикл параллельно и независимо от активности процессора.

ЦП C55x обеспечивает два блока с многократным накоплением (MAC), каждый из которых способен к 17-битному $\times$ 17-битному умножению и 32-битному сложению за один цикл. Центральный 40-разрядный арифметико-логический блок (АЛУ) поддерживается дополнительным 16-разрядным АЛУ. Использование АЛУ находится под контролем набора команд, что позволяет оптимизировать параллельную активность и энергопотребление. Этими ресурсами управляют в адресном блоке (AU) и блоке данных (DU) ЦПУ C55x.

ЦП C55x поддерживает набор команд с переменной шириной байта для улучшения плотности кода. Блок команд (IU) выполняет 32-битные выборки программ из внутренней или внешней памяти и ставит в очередь инструкции для блока программы (PU). PU декодирует инструкции, направляет задачи на ресурсы AU и DU и управляет полностью защищенным конвейером. Возможность прогнозирующего ветвления позволяет избежать сбросов конвейера при выполнении условных инструкций.

GPIO (интерфейс ввода/вывода общего назначения) функционирует вместе с 10-разрядным АЦП SAR, чтобы обеспечить достаточное количество контактов для состояния, прерываний и битового ввода-вывода для клавиатур и мультимедийных интерфейсов. Последовательный носитель поддерживается через две мультимедийные платы и защищенные цифровые (MMC и SD) периферийные устройства, три модуля Inter-IC Sound (шина I2S), один интерфейс последовательного порта (SPI) с возможностью выбора до четырех микросхем, один ведущий и ведомый многоканальные последовательные порты. Интерфейс (McSPI) с возможностью выбора до трех микросхем, одним многоканальным последовательным портом (McBSP), одним интерфейсом ICM и несколькими подчиненными устройствами и универсальным асинхронным интерфейсом приемник / передатчик (UART)

Комплект периферийных устройств устройства включает в себя интерфейс внешней памяти (EMIF), который обеспечивает бесклеевой доступ к асинхронной памяти, такой как EPROM, NOR, NAND и SRAM, а также к высокоскоростной памяти высокой плотности, такой как синхронная динамическая память с произвольным доступом (SDRAM) и мобильный SDRAM (mSDRAM).

Дополнительные периферийные устройства включают настраиваемый 16-разрядный универсальный интерфейс хост-порта (UHPI), только режим устройства высокоскоростной универсальной последовательной шины (USB2.0), часы реального времени (RTC), три таймера общего назначения с одним настраиваемым в качестве сторожевого таймера и генератора тактовых импульсов с аналоговой фазовой автоподстройкой частоты (APLL).

8.2 Выбор контроллера хранения ключей

В данном дипломной проекте в качестве контроллера хранения ключей был выбран STM32L496.

STMicroelectronics STM32L4 32-битный MCU + FPU - это сверхмощные микроконтроллеры на основе высокопроизводительного 32-битного RISC-ядра ARM® Cortex®-M4, работающие на частоте до 80 МГц. Ядро Cortex-M4 имеет одинарную точность с плавающей запятой (FPU), которая поддерживает все инструкции обработки данных ARM с одинарной точностью и типы данных. Он также реализует полный набор инструкций DSP и блок защиты памяти (MPU), который повышает безопасность приложений.

Микроконтроллер STM32L4 основан на новой сверхмощной платформе с FlexPowerControl. Это расширяет гибкость для достижения оптимального энергопотребления

Технические характеристики STM32L496:

— диапазон температур от минус 40 °C до плюс 125 °C;

- 300 нА в режиме VBAT, питание для RTC и 32х32-битных резервных регистров (4 нА без RTC);
- режим отключения 30 нА (5 выводов для пробуждения);
- режим ожидания 120 нА (5 выводов для пробуждения);
- режим ожидания 420 нА с RTC;
- режим 1,1 мкА Stop 2, 1,4 мкА Stop 2 с RTC;
- режим работы 100 мкА / МГц;
- пакетный режим сбора данных (BAM);
- 4 мкс пробуждения из режима остановки 1, 5 мкс из режима остановки 2;
- отключение сброса (BOR) во всех режимах, кроме выключения;
- матрица межсоединений;
- 32-разрядный процессор Cortex-M4 с процессором FPU, адаптивный ускоритель реального времени (ART Accelerator), позволяющий выполнять в режиме ожидания 0 из флэш-памяти, частота до 80 МГц, MPU, 100DMIPS / 1.25DMIPS / МГц (Dhrystone 2.1)) и инструкции DSP;
- источники часов;
- кварцевый генератор от 4 до 48 МГц;
- кварцевый генератор 32 кГц для RTC (LSE);
- внутренняя 16 МГц заводская настройка RC (плюс/минус 1%);
- внутренний маломощный 32 кГц RC (плюс/минус 5%);
- внутренний многоскоростной генератор от 100 кГц до 48 МГц с автоматической подстройкой LSE (точность выше плюс/минус 0,25%);
- 3 PLL для системных часов, USB, аудио, АЦП;
- IoT и портативные измерения;

- RTC с календарем HW, сигналами тревоги и калибровкой;
- ЖК-дисплей 8×40 или 4×44 с повышающим преобразователем;
- 16х таймеры: 2х16-битное расширенное управление двигателем, 2х32-битные и 5х16-битные общего назначения, 2х16-битные базовые, 2х маломощные 16-битные таймеры (доступны в режиме Stop), 2х сторожевые таймеры, таймер SysTick;
- до 24 емкостных сенсорных каналов: поддержка сенсорных кнопок, линейных и поворотных сенсорных датчиков;
- до 114 быстрых входов / выходов, наиболее устойчивых к 5 В, до 14 входов/выходов с независимым питанием до 1,08 В;
- FLASH-память до 2 МБ, 2 банка для чтения во время записи, защита проприетарного кода;
- SRAM до 640 КБ, включая 32 КБ с проверкой четности оборудования;
- интерфейс внешней памяти для статической памяти с поддержкой памяти SRAM, PSRAM, NOR и NAND;
- интерфейс памяти Quad SPI;
- 4 цифровых фильтра для сигма-дельта модулятора;
- 3×12-битный АЦП 5 Мбит/с, до 16 бит с аппаратной избыточной дискретизацией, 200 мкА/Мбит/с;
- 2х12-битный ЦАП, маломощный сэмпл и удержание;
- 2х операционные усилители со встроенным PGA;
- 2х сверхмощных компаратора;
- промышленный контроль;
- 14-канальный контроллер DMA;
- истинный генератор случайных чисел;

— блок вычисления CRC, 96-битный уникальный идентификатор.

8.3 Выбор FLASH-памяти

В качестве FLASH-памяти была выбрана микросхема S29AL032D, которая имеет ёмкость 32 Mbit 2M x 16 – bit со временем выборки 80 нс и напряжением питания 3,3 В. FLASH память предназначена для хранения программы работы ЦПОС. При включении аппаратуры и установке режимов работы программа в соответствии которой работает аппаратура переписывается из флэш памяти во внутреннее оперативно запоминающее устройство ЦПОС. Обладает четырьмя режимами низкой потребляемой мощности. Такой большой объём памяти объясняется сложными алгоритмами обработки речевой информации при её сжатии и шифровании. Эта ИМС имеет высокую скорость обмена информацией и относительно низкую потребляемую мощность.

При сложении и циклическом сдвиге двоичных векторов старшими разрядами считаются разряды накопителей с большими номерами.

При записи ключа ($W_1, W_2, \dots, W_{256}$), $W_q \in \{0,1\}$, q равно $i \div 256$, а КЗУ значение W_1 вводится в 1-й разряд накопителя X_0 , значение W_2 вводится во 2-й разряд накопителя X_0 , ..., значение W_{32} вводится в 32-й разряд накопителя X_0 ; значение W_{33} вводится в 1-й разряд накопителя X_1 , значение W_{34} вводится во 2-й разряд накопителя X_1 , ..., значение W_{64} вводится в 32-й разряд накопителя X_1 ; значение W_{65} вводится в 1-й разряд накопителя X_2 и т.д., значение W_{256} вводится в 32-й разряд накопителя X_7 .

При перезаписи информации содержимое p -го разряда одного накопителя (сумматора) переписывается в p -й разряд другого накопителя (сумматора).

Значение постоянной заполнения C_1 (константа) накопителя N_6 приведено в таблице 7.

Таблица 7 – Значение постоянной C_1 накопителя N_6

Разряд накопителя N_6	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
Значение разряда	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
Разряд накопителя N_6	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Значение разряда	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0

Значение постоянной заполнения C_2 (константа) накопителя N_5 приведено в таблице 8.

Ключи, определяющие заполнения КЗУ и таблиц блока подстановки K , являются секретными элементами и поставляются в установленном порядке.

Заполнение таблиц блока подстановки K является долговременным ключевым элементом, общим для сети ЭВМ.

Организация различных видов связи достигается построением соответствующей ключевой системы.

При этом может быть использована возможность выработки ключей (заполнения КЗУ) в режиме простой замены и зашифрования их в режиме простой замены с обеспечением имитозащиты для передачи по каналам связи или хранения в памяти ЭВМ

Таблица 8 - Значение постоянной С2 накопителя N5

Разряд накопителя N6	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
Значение разряда	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
Разряд накопителя N6	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Значение разряда	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1

В криптосхеме предусмотрены четыре вида работы:

- зашифрование (расшифрование) данных в режиме простой замены;
- зашифрование (расшифрование) данных в режиме гаммирования;
- зашифрование (расшифрование) данных в режиме гаммирования с обратной связью;
- режим выработки имитовставки.

В качестве режима работы алгоритма шифрования был выбран режим гаммирования. Криптосхема, реализующая алгоритм зашифрования в режиме гаммирования, должна иметь вид, приведенный на рисунке 6.

Открытые данные, разбитые на 64-разрядные блоки $T_0(1)$, $T_0(2)$, ..., $T_0(M-1)$, $T_0(M)$, зашифровываются в режиме гаммирования путем поразрядного суммирования по модулю 2 в сумматоре СМ5 с гаммой шифра Гш, которая вырабатывается блоками по 64 бита.

$$\text{Гш}=(\text{Гш}(1), \text{Гш}(2), \dots, \text{Гш}(M-1), \text{Гш}(M)) \quad (8)$$

где M – определяется объемом шифруемых данных.

переписывается в 32-разрядные накопители N3 и N4 так, что заполнение N1 переписывается в N3, а заполнение N2 переписывается в N4.

Заполнение накопителя N4 суммируется по модулю $(2^{32}-1)$ в сумматоре CM4 с 32-разрядной константой C1 из накопителя N6, результат записывается в N4.

Заполнение накопителя N3 суммируется по модулю 232 в сумматоре CM3 с 32-разрядной константой C2 из накопителя N5, результат записывается в N3.

Заполнение N3 переписывается в N1, а заполнение N4 переписывается в N2, при этом заполнение N3, N4 сохраняется.

Заполнение N1 и N2 зашифровывается в режиме простой замены в соответствии с требованиями пункта 3.1 ГОСТ 28147-89.[6] Полученное в результате зашифрования заполнение N1, N2 образует первый 64-разрядный блок гаммы шифра $\Gamma_{ш}(1)$, который суммируется поразрядно по модулю 2 в сумматоре CM5 с первым 64-разрядным блоком открытых данных $T_0(1)$ равно $(t_1(1), t_2(1), \dots, t_{63}(1), t_{64}(1))$. В результате суммирования получается 64-разрядный блок зашифрованных данных $T_{ш}(1)$ равно $(\tau_1(1), \tau_2(1), \dots, \tau_{63}(1), \tau_{64}(1))$.

Значение $\tau_1(1)$ блока $T_{ш}(1)$ является результатом суммирования по модулю 2 в CM5 значения $t_1(1)$ из блока $T_0(1)$ со значением 1-го разряда N1, значение $\tau_2(1)$ блока $T_{ш}(1)$ является результатом суммирования по модулю 2 в CM5 значения $t_2(1)$ из блока $T_0(1)$ со значением 2-го разряда N1 и т.д., значение $\tau_{64}(1)$ блока $T_{ш}(1)$ является результатом суммирования по модулю 2 в CM5 значения $t_{64}(1)$ из блока $T_0(1)$ со значением 32-го разряда N2.

Для получения следующего 64-разрядного блока гаммы шифра $\Gamma_{ш}(2)$ заполнение N4 суммируется по модулю $(2^{32}-1)$ в сумматоре CM4 с константой C1 из N6, заполнение N3 суммируется по модулю 232 в сумматоре CM3 с константой C2 из N5. Новое заполнение N3 переписывается в N1, а новое заполнение N4 переписывается в N2, при этом заполнение N3 и N4 сохраняется.

Полученное в результате зашифрования заполнение $N1$, $N2$ образует второй 64-разрядный блок гаммы шифра $\Gamma_{ш}(2)$, который суммируется поразрядно по модулю 2 в сумматоре $СМ5$ со вторым блоком открытых данных $T0(2)$. Аналогично вырабатываются блоки гаммы шифра $\Gamma_{ш}(3)$, $\Gamma_{ш}(4)$..., $\Gamma_{ш}(M)$ и зашифровываются блоки открытых данных $T0(3)$, $T0(4)$..., $T0(M)$. Если длина последнего M -го блока открытых данных $T0(M)$ меньше 64 бит, то из последнего M -го блока гаммы шифра $\Gamma_{ш}(M)$ для зашифрования используется только соответствующее число разрядов гаммы шифра, остальные разряды отбрасываются.

В канал связи или память ЭВМ передаются синхропосылка S и блоки зашифрованных данных $T_{ш}(1)$, $T_{ш}(2)$..., $T_{ш}(M)$.

При расшифровании криптограмма имеет тот же вид, что и при зашифровании. В КЗУ вводятся 256 бит ключа, с помощью которого осуществлялось зашифрование данных $T0(1)$, $T0(2)$..., $T0(M)$ при этом $T0(M)$ может содержать меньше 64 разрядов.

10.1 Обзор технологии Bluetooth

Радиочастотный приемопередатчик Bluetooth работает в нелицензированном диапазоне ISM с центром в 2,4 гигагерца (тот же диапазон частот, который используется микроволнами и Wi-Fi). В базовой системе используется приемопередатчик со скачкообразной перестройкой частоты для борьбы с помехами и замираниями.

Устройства Bluetooth управляются с использованием топологии RF, известной как «топология звезды». Группа устройств, синхронизируемых таким образом, формирует пикосеть, которая может содержать одного главного и до семи активных подчиненных устройств с дополнительными подчиненными устройствами, которые не принимают активного участия в сети. Данное устройство также может быть частью одной или нескольких пикосетей, либо как ведущее устройство, либо как подчиненное устройство. В пикосети физический радиоканал совместно используется группой устройств, которые синхронизированы с общим тактовым сигналом и скачкообразной перестройкой частоты.

Устройства в пикосети используют определенный шаблон скачкообразной перестройки частоты, который алгоритмически определяется ведущим устройством. Основной шаблон скачкообразной перестройки представляет собой псевдослучайное упорядочение 79 частот в диапазоне ISM. Шаблон скачкообразной перестройки может быть адаптирован для исключения части частот, которые используются мешающими устройствами. Адаптивная технология скачкообразной перестройки улучшает сосуществование технологии Bluetooth со статическими системами ISM, такими как сети Wi-Fi, когда они расположены вблизи пикосети.

Физический канал (или беспроводной канал) подразделяется на единицы времени, известные как временные интервалы. Данные передаются между

устройствами с поддержкой Bluetooth в пакетах, которые расположены в этих слотах. Переключение частоты происходит между передачей или приемом пакетов, поэтому пакеты, составляющие одну передачу, могут отправляться на разных частотах в пределах полосы ISM.

Физический канал также используется в качестве транспорта для одного или нескольких логических каналов, которые поддерживают синхронный и асинхронный трафик, а также широковещательный трафик. Каждый тип ссылки имеет конкретное использование. Например, синхронный трафик используется для переноса аудиоданных без помощи рук, в то время как асинхронный трафик может переносить другие формы данных, которые могут выдерживать большую изменчивость во времени доставки, например, печать файла или синхронизация календаря между телефоном и компьютером.

Одной из сложностей, часто связанных с беспроводной технологией, является процесс подключения беспроводных устройств. Пользователи привыкли к процессу подключения проводных устройств, подключив один конец кабеля к одному устройству, а другой конец к дополнительному устройству.

Технология Bluetooth использует принципы устройства «запрос» и «запрос сканирования». Сканирующие устройства прослушивают на известных частотах устройства, которые активно запрашивают. Когда запрос получен, сканирующее устройство отправляет ответ с информацией, необходимой запрашивающему устройству, чтобы определить и отобразить природу устройства, которое распознало его сигнал.

10.2 Обзор топологии Bluetooth

Все устройства сети делятся на ведущие (master) и подчиненные (slave).

Обмен информацией может осуществляться только между ведущим и подчинённым устройствами. Каждое устройство может быть и ведущим, и подчинённым.

Пикосеть:

- в одной пикосети существует только одно ведущее устройство, все остальные – подчинённые;
- максимальное количество устройств одной пикосети, одновременно участвующих в передаче информации, – не более 8;
- общее количество устройств, подключенных к ведущему устройству одной пикосети не ограничено;
- в каждый момент времени обмен данными может идти только между двумя устройствами в одном направлении.

Рассеянная сеть:

- образуется путём перекрытия отдельных пикосетей;
- каждое устройство одной пикосети может входить в другую пикосеть как в качестве подчинённого, так и в качестве ведущего.

Стек протоколов изображен на рисунке 7.

- AT – префикс модема;
- IP – протокол Internet;
- OBEX протокол объектного обмена;
- PPP – протокол двухточечного соединения;
- RFCOMM – протокол замещения кабеля;
- SDP – протокол обнаружения службы;
- TCP – протокол управления передачей;
- TCS BIN – бинарная спецификация управления телефонией;
- UDP – протокол пользовательских дейтаграмм;
- vCal – виртуальный календарь;
- vCard – виртуальная карта;
- WAE – среда беспроводных приложений;

— WAP – протокол беспроводных приложений.

Стек протоколов Bluetooth

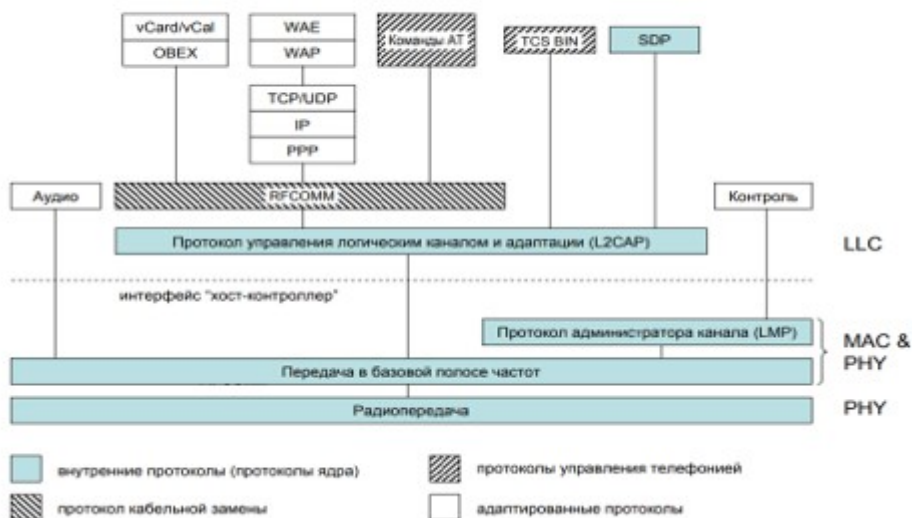


Рисунок 7 — Стек протоколов Bluetooth

Модели использования представлены на рисунке 8.

Модели использования

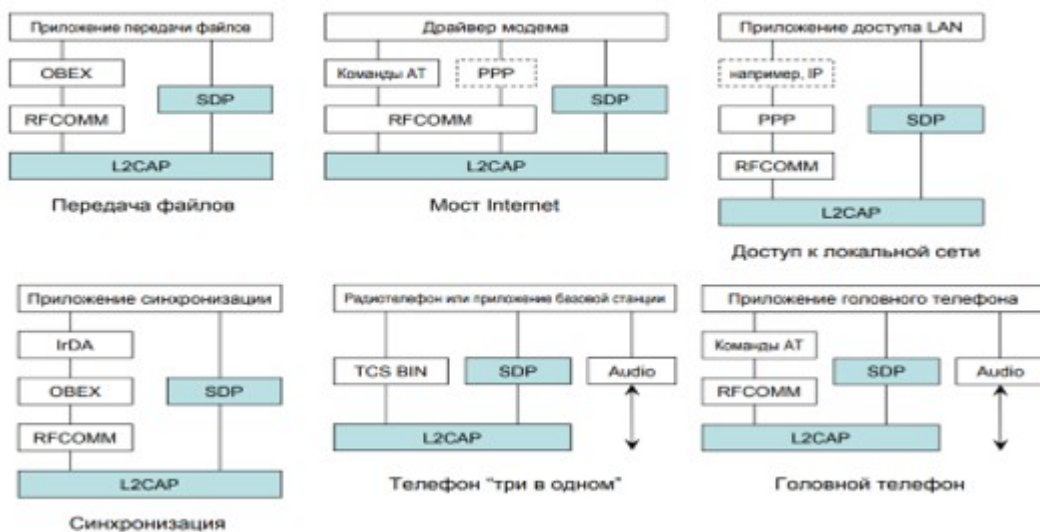


Рисунок 8 — Модели использования Bluetooth

11 Принципиальная схема модуля криптографическое защиты информации

Принципиальная схема модуля криптографической защиты информации представлена в приложении В и в графической части дипломного проекта.

На 1 листе изображен цифровой процессор обработки сигналов TMS320c5517.

На 2 листе изображен контроллер хранения ключевой информации в данном модуле.

На 3 листе изображен узел ПЛИС, а именно узел формирования.

На 4 листе изображено питание модуля.

12 Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

12.1 Вредные психофизиологические факторы, влияющие на нервную систему специалиста по защите информации

Существует много различных вредоносных производственных факторов и, что немаловажно, один и тот же фактор по специфике может по-разному сказываться на здоровье человека и относиться к разным группам.

Постоянное напряжение, эмоциональные перегрузки неизбежно приводят к стрессам, которые можно визуально определить по признакам поведения сотрудника.

Признаки стресса у персонала, как правило, включают в себя раздражительность, другие признаки психического истощения, а порой даже чрезмерное употребление алкоголя, наркотиков или курение.

Нервно-психические перегрузки имеют несколько видов:

- умственное перенапряжение;
- перенапряжение анализаторов;
- монотонность труда;
- эмоциональные перегрузки.

Умственное перенапряжение может возникнуть по ряду разных причин. К примеру, погружение в рабочий процесс «с головой». Чередование умственной и физической нагрузки переносится гораздо легче, чем каждая из них по отдельности. Оптимальнее и эффективнее для здоровья после каждого часа напряженной умственной работы делать десятиминутный перерыв.

Часто в ежедневной погоне за временем человек совершает одну очень серьезную ошибку: «заставляет» мозг работать сразу же после утреннего пробуждения, а «отдыхать» позволяет только в момент сна, что, конечно же, в

корне неправильно. Нагрузка на мозг в течение дня должна распределяться, в противном случае переутомление неизбежно. Утомленный мозг будет делать все больше и больше ошибок, на устранение которых понадобятся дополнительные ресурсы (время, силы и т.д.). Предотвратить появление переутомления можно очень легко – достаточно периодически отвлекаться от мыслительного процесса и устраивать, скажем, 10-ти минутные прогулки на воздухе в течение дня.

Ни для кого не секрет, что интеллектуальная нагрузка вне зависимости от её объемов, действует на сравнительно незначительную часть нервных клеток коры головного мозга человека. Предположим, что человек устал, длительное время составляя сводную таблицу, однако, это не значит, что так чувствует себя весь его организм. В этом случае полезно переключить внимание на другое занятие, к примеру, почитать художественную книгу, и уставший участок коры головного мозга вернется к состоянию покоя, а в это время заработает другая часть мозга. Спустя некоторое время усталость проходит и можно снова вернуться к работе с таблицей.

Чтобы не переутомлять таким образом мозг, полезно каждодневно составлять своеобразное расписание умственного труда, в котором бы чередовалась напряженная умственная деятельность с занятиями другого характера: рисованием, музыкой, чтением художественных книг и др. Подобные занятия способствуют снятию нервно-психического напряжения. Но все же, эффективность умственного труда лучше всего повышают активные движения, физические упражнения и труд.

Современные исследования многих ученых подтвердили очевидную рациональность такого чередования занятий в связи с тем, что наш организм - целостная система. Напрягая мышцы тела, человек повышает тем самым готовность к работе нервной системы, а она, в свою очередь, активизирует деятельность мозга. Так, выполняя физическую работу, гимнастические упражнения, занимаясь ходьбой, бегая, играя в спортивные игры, то есть,

рационально сочетая напряжение мышц с последующим их расслаблением, можно длительное время успешно поддерживать высокую работоспособность своего интеллекта.

Центральная нервная система получает информацию от внешнего мира, внешней среды с помощью чувствительных аппаратов, воспринимающих сигналы. Такие аппараты имеют название – анализаторы – благодаря академику И.П. Павлову.

Их основная характеристика – высокая чувствительность, хотя не любой раздражитель, действующий на анализатор, вызывает ощущение. Чтобы ощущение проявилось, необходима определенная интенсивность раздражителя. Всякое воздействие, превышающее предел интенсивности, вызывает боль и нарушение деятельности анализаторов.

В центральную нервную систему в процессе труда поступает большой объем информации. Мозг ее «перерабатывает» и «распределяет» по степени важности. Самыми важными являются сигналы, имеющие значение для жизнедеятельности всего организма. После этого воспринимаются сигналы, которые имеют значение только для отдельных систем и органов.

Основная задача правильного проектирования технологического процесса – не допустить перенапряжения анализаторов, которое может привести к стрессам.

Монотонность означает однообразное систематическое повторение каких-либо рабочих операций. Опасность монотонности заключается в снижении внимания к процессу производства, быстрой утомляемости и снижении интереса к трудовому процессу, что, в свою очередь, сильно влияет на безопасность труда в целом. Одной из форм, предрасполагающей к формированию монотонности, является автоматизм – деятельность, осуществляемая без непосредственного участия сознания. Автоматизм формируется в результате нескольких факторов: многолетнего опыта деятельности, рутинности работы, отсутствия вовлеченности в трудовой

процесс и интереса к нему, воображения и творческого подхода, физических перегрузок. Особое значение это имеет на сложных производствах или производствах с вредными условиями труда, где аккуратность и внимание имеют решающее значение. Монотонность сопровождается скукой и, так называемой, апатией к выполнению трудовой деятельности. Но при этом почти невозможно с точностью определить, что выполнение именно определенных действий является монотонным и скучным занятием. Каждый человек сам для себя определяет род своей деятельности и дает ей свою объективную оценку. К примеру, один сотрудник, работающий у станка, считает свою работу монотонной и скучной, а его коллега, наоборот, находит ее очень даже интересной. Большинство людей, занимающихся динамичной, активной работой, которую никак нельзя назвать монотонной, считают ее скучной и неинтересной. И в подобных случаях многое зависит от мотивации сотрудников. Поэтому решающее значение имеет четкое соблюдение техники безопасности труда, контроля за трудовым процессом и чередование периодов труда и отдыха, а самым лучшим способом борьбы со скукой является расширение круга обязанностей, усложнение работы или обогащение ее такими функциями и обязанностями, которые способны сыграть роль стимулов и мотивации для того или иного сотрудника.[5]

Эмоциональные перегрузки обычно обусловлены спецификой трудовой деятельности, а именно:

- высочайшим уровнем ответственности;
- необходимостью ежедневного интенсивной коммуникации с десятками (или даже сотнями) людей;
- чрезвычайно высокой с точки зрения опасности для здоровья продолжительности рабочего дня;
- непродуманностью организации рабочих мест;
- регулярным участием в конфликтных ситуациях.

Для профилактики эмоциональных расстройств, связанными с причинами, описанными выше, необходимо:

- стараться не сдерживать свои эмоции (выход накопившемуся негативу может дать активный отдых, спорт, физические нагрузки);
- высыпаться и рационально регулярно питаться;
- дозировать труд (не пытаться выполнить месячный объем работы за два дня, даже при материальной заинтересованности во избежание нанесения порой непоправимого ущерба здоровью);
- устраивать отдых в свободные от работы дни и ежегодно (лучше не один, а два раза в год) ездить в отпуск;
- отбросив стеснения обращаться за помощью к психологу в случае обнаружения эмоционального дискомфорта.

12.2 Методы и средства физической культуры, снижающие их воздействие

К профилактическим мероприятиям относятся проведение производственной гимнастики, утренние зарядки, занятие физкультурой и спортом и другие физические упражнения.

Положительными эмоциями, значительно продлевающих период стойкой трудоспособности, являются уверенность, спокойствие, бодрость духа.

Продлить стойкую трудоспособность возможно за счет:

- оптимального уровня напряжения психофизиологических функций;
- комфортных условий труда;
- правильного совмещения режимов труда и отдыха;
- проведения непродолжительных физкультурных пауз и эмоциональной разгрузки;
- использования специальных психофармакологических средств или тонизирующих напитков;

— информирования (с положительной точки зрения) человека о результатах его деятельности;

— наблюдения и контроля за его работой.

Помимо высокой трудоспособности, комфортные условия способны обеспечить хорошее самочувствие, при этом не возникают опасные напряжения компенсаторных систем организма, а здоровье человека не ухудшается довольно продолжительное время.

Не секрет, что на трудоспособность и производительность труда, на жизнедеятельность в целом огромное влияние оказывает отдых. Отдых бывает двух видов – активный и пассивный.

Активный отдых – это занятие спортом, туристические поездки, походы в лес, путешествия, плавание в бассейне, активные игры на свежем воздухе, гимнастика и т.п. Именно активный отдых способствует повышению трудоспособности, улучшению психического состояния личности и, соответственно, настроения человека.

Пассивный отдых – это, к примеру, просмотр сериалов, прослушивание музыки сидя, лежа, чтение книг, рисование, собирание пазлов и т.п. Особым, но неотъемлемым видом такого отдыха является сон.

Безусловно, беспокойные ночи, неприятные сновидения с переживанием ужасов, опасностей, страха – все это негативно влияет на состояние человека, и, соответственно, на различные активности его жизнедеятельности.

Заключение

В результате выполнения ВКР были разработаны структурная, функциональная схема устройства передачи речевой информации и принципиальная схема модуля криптографической защиты информации.

В ходе дипломного проектирования был сделан выбор элементной базы для устройства речевой информации и модуля криптографической защиты информации.

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены в полном объеме.

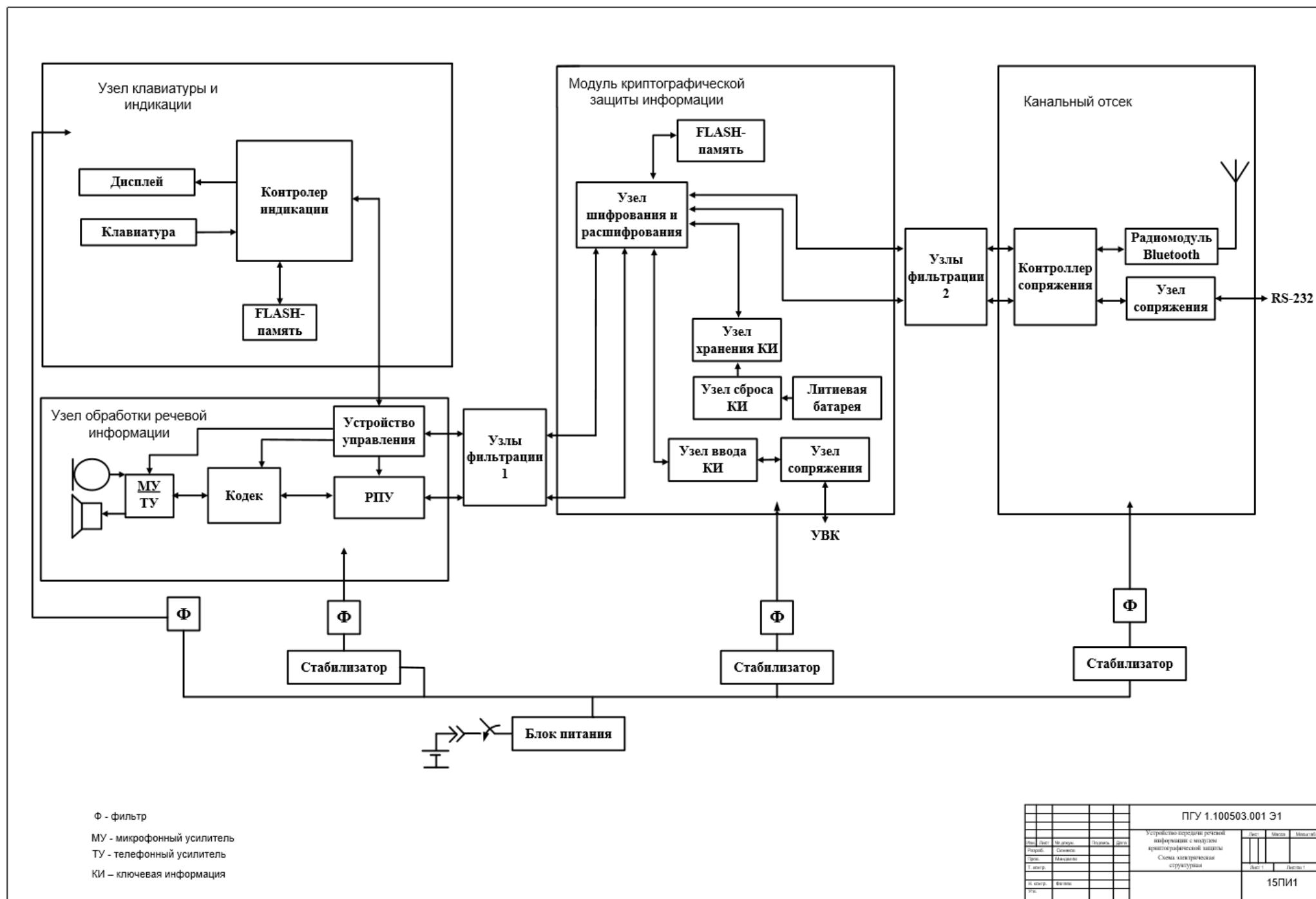
Была проведена проверка отчета на оригинальность в системе «Антиплагиат.ВУЗ». Результат проверки представлен в приложении Г на рисунке Г.1.

Список используемых источников

- 1 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
- 2 Цифровые системы передачи : учебное пособие для вузов. Крухмалев В.В., Гордиенко В.Н. – Горячая линия – М: Телеком, 2007 г. – 78 с.
- 3 Цифровая обработка и передача речи. Шелюхин О.И. – М: Радиосвязь, 2002г.
- 4 Dumitru B.. Advances in Wavelet Theory and Their Applications in Engineering, Physics and Technology. Babylon, IN-TECH Publ., 2012. 643 p. DOI: 10.5772/37350
- 5 Психология труда : конспект лекций. Боронова Г.Х., Прусова Н.В. – Эксмо, 2008 г. – 160 с.
- 6 ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
- 7 Dunlop J., Girma D., Irvine J. Digital Mobile Communications and the Tetra System. Wiley Publ., 1999. 436 p. DOI:10.1002/9781118832585

Приложение А
(обязательное)

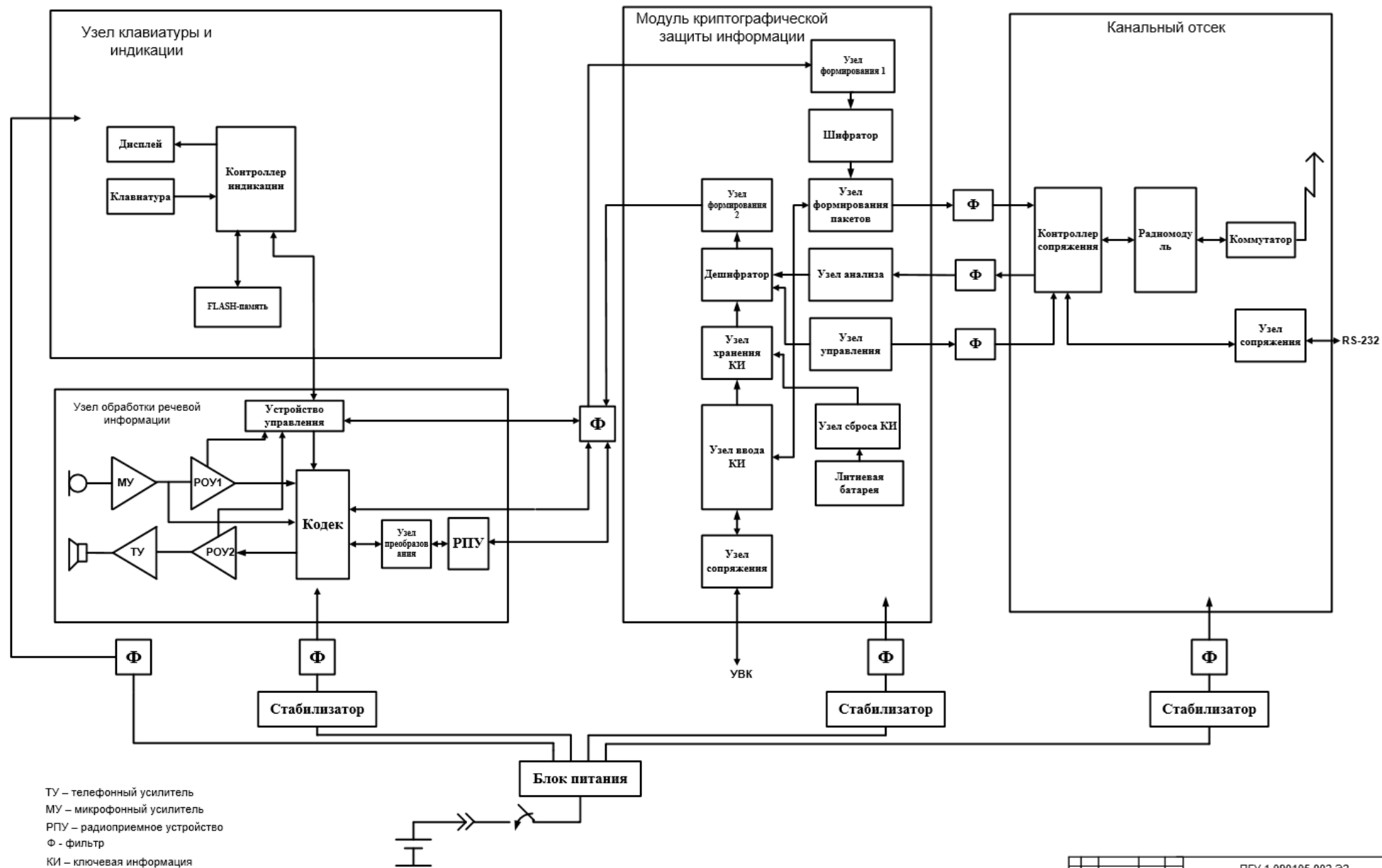
Схема электрическая структурная устройства передачи речевой информации



Приложение Б

(обязательное)

Схема электрическая функциональная устройства передачи речевой
информации



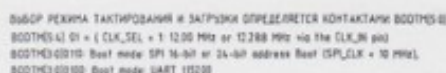
ТУ – телефонный усилитель
МУ – микрофонный усилитель
РПУ – радиоприемное устройство
 Φ – фильтр
КИ – ключевая информация
РОУ – регулируемый операционный усилитель

ПГУ 1.090105.002 Э2									
Устройство передачи речевой информации с модулем криптографической защиты									
Схема электрическая структурная									
Изм.	Дет.	Исполн.	Провер.	Дет.	Изм.	Дет.	Исполн.	Провер.	Дет.
Рис.	Содерж.	Содерж.	Содерж.	Содерж.	Рис.	Содерж.	Содерж.	Содерж.	Содерж.
Т. экз.	Максимум	Максимум	Максимум	Максимум	Т. экз.	Максимум	Максимум	Максимум	Максимум
В. экз.	Максимум	Максимум	Максимум	Максимум	В. экз.	Максимум	Максимум	Максимум	Максимум
Изм.	Дет.	Исполн.	Провер.	Дет.	Изм.	Дет.	Исполн.	Провер.	Дет.
								15ПИ1	

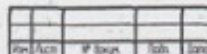
Приложение В

(обязательное)

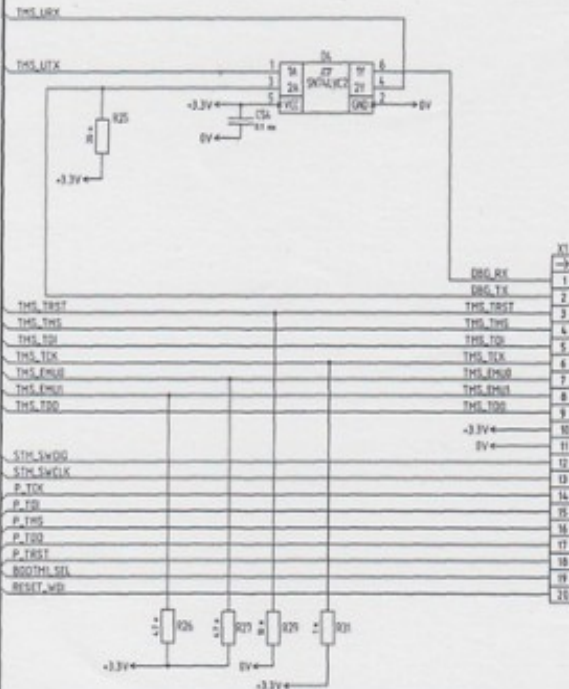
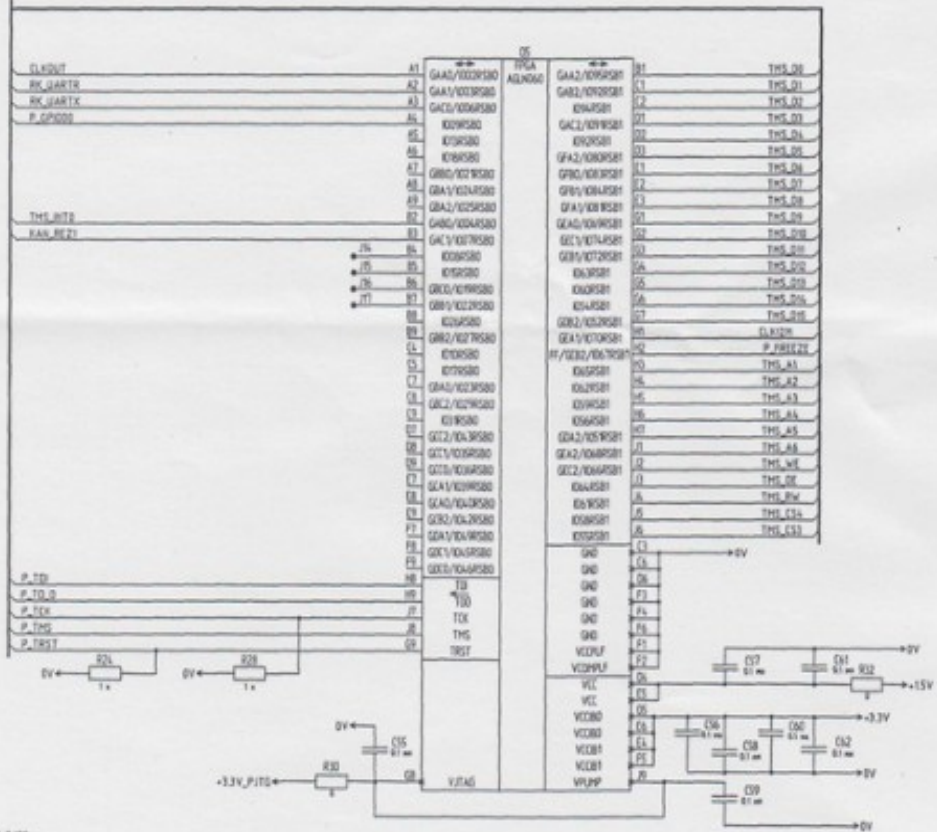
Схема электрическая принципиальная модуля криптографической защиты информации



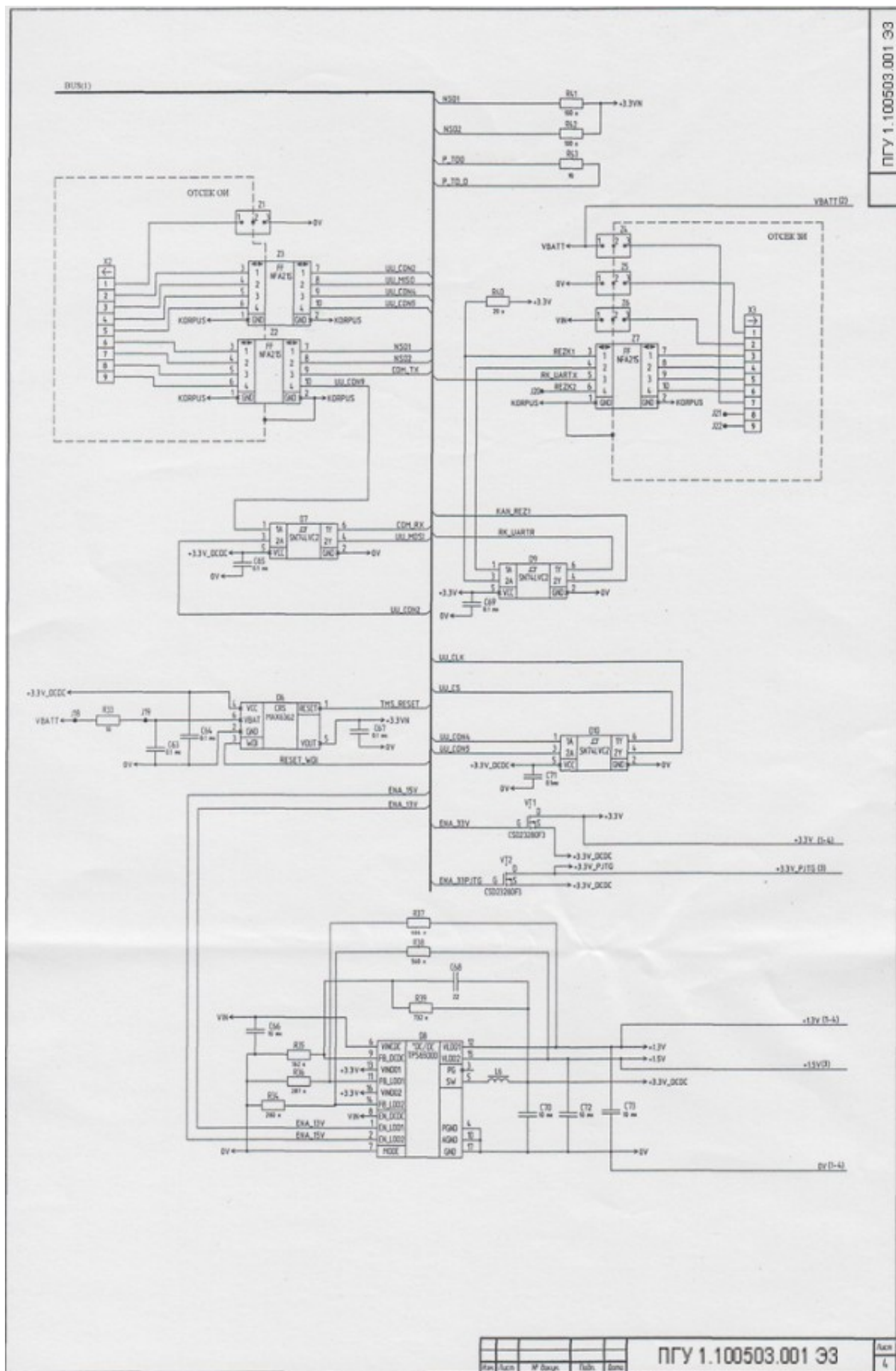
						ПГУ 1.100503.001 ЭЗ			
Изм./Лист	№ докум.	Дата	Лист	Листов		Модуль КЗИ Схема электрическая принципиальная			
Исполн.	Сметин					Авт.	Прош.	Провер.	
Долж.	Механик								
Город						Акт	Акт	А	
Изд.	Изм. 10								



BUS(1)



+3.3V_P170 (4) → +3.3V_P170
+1.5 V (4) → +1.5 V
+3.3V (4) → +3.3V
+1.5 V (4) → +1.5 V
0 V (4) → 0 V



Приложение Е

Протокол проверки ВКР в системе Антиплагиат

Рисунок Е.1 — отчет о проверке на оригинальность