МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

ИНСТИТУТ ЭНЕРГЕТИКИ И ЭЛЕКТРОТЕХНИКИ
(институт)
Промышленная электроника
(кафедра)
11.03.04 Электроника и наноэлектроника
(код и наименование направления подготовки, специальности)

БАКАЛАВРСКАЯ РАБОТА

на тему Устройство защиты речевых телефонных сообщений

Студент (ка)	А.О. Шпунтов	
	(И.О. Фамилия)	(личная подпись)
Руководитель	Г.Н. Абрамов	
	(И.О. Фамилия)	(личная подпись)
Консультанты		
	(И.О. Фамилия)	(личная подпись)
	(И.О. Фамилия)	(личная подпись)

Допустить к защите

Заведующий кафедрой к.т.н., доцент А.А. Шевцов _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)
«_____»_____20_____г.

Тольятти 2016

АННОТАЦИЯ

Объем 61с., 21 рис., 18 источников, таб.7,1 прил.

В настоящее время обладание достоверной информацией является составной частью конкуренции за рынки сбыта, а также в политической и экономической сферах. Обладание информацией законным образом в настоящее время является практически невозможным из-за использования системы защиты особо ценных сообщений от несанкционированного доступа сторонних лиц.

В бакалаврской работе разработан малогабаритный аналоговый скремблер - устройство для изменения телефонного речевого сообщения на передающей стороне и ее восстановление на приемной стороне с помощью определенных алгоритмов и ключей.

Устройство спроектировано на специализированных ИС и по ряду показателей превышает известные аналоги. Скремблер может обеспечивать защиту речи не только в телефонных линиях, но и при передаче по радиоканалу. Использование динамической смены комбинации кодов в процессе передачи по псевдослучайной последовательности существенно повышает защищенность (секретность) передаваемой информации, а синхронизация операций шифрования /дешифрования на передающей и приемной сторонах увеличивает разборчивость сообщения (речи).

Содержание

ВВЕДЕНИЕ

В мире реального бизнеса конкуренция ставит его участников в жесткие рамки и сводит их деятельность к принципу «победителей не судят».

В таких противоборствах на первое место выходит промышленный шпионаж как скрытая деятельность направленная на добывание, анализ и использование конфиденциальной информации о конкурентах, так как получение какой-нибудь достоверной информации о них законным путем является невозможным из-за использования ими систем защиты информации от противоправного доступа к ней сторонних лиц, в частности конкурентов.

Анализ различных способов получения информации о конкурентах указывает, что подслушивание телефонных переговоров очень часто служит эффективным методом несанкционированного доступа к конфиденциальной (секретной) информации. Действенным методом защиты телефонных сообщений (ТС) от несанкционированного доступа является их криптографическое преобразование. То есть чтобы при передачи скрыть от злоумышленников содержание передаваемого ТС, его необходимо изменить по определенным правилам. При этом изменение должно быть таким, чтобы восстановление исходного ТС санкционированным абонентом осуществлялось бы по тем же определенным правилам, что и на передающей стороне, а перехват ТС злоумышленниками был бы неэффективным в виду отсутствия у них знаний этих правил.

Криптографические преобразования обеспечивают посредством математических способов защиту передаваемых конфиденциальных ТС.

В отечественной практике широко используется ГОСТ 28147-89, который устанавливает единый алгоритм криптографического преобразования для систем обработки информации в сетях ЭВМ или в отдельных вычислительных комплексах. При этом алгоритм криптографического преобразования по своим возможностям не ограничивает степень секретности защищаемой информации.

1.Аналоговые способы и средства защиты речевых телефонных сообщений.

В настоящий момент индустрия производства средств телекоммуникаций стремится к тому, чтобы полностью перейти на производство цифрового оборудования. Но доля аналоговой техники на рынке все еще значительна. Кроме того, нужно учитывать и то, что многие отечественные организации на 90% используют аналоговые устройства. Так, силовые структуры, структуры безопасности, охраны и другие подобные им государственные учреждения широко применяют профессиональное оборудование с фазовой или частотной модуляцией. Эти радиосигналы являются аналоговыми и, соответственно, могут быть легко прослушаны. В таких ситуациях используют скремблер - одно из наиболее популярных устройств защиты радио и телефонных сообщений от прослушивания при использовании аналогового оборудования.

Скремблер - это малогабаритное устройство, предназначенное для изменения речевого сообщения при передаче и его восстановления при приеме с помощью определенных алгоритмов и ключей. В результате аналогового криптографических преобразований телефонных сообщений по кабелю или радиоканалу речь становится неузнаваемой и неразборчивой или превращается просто в низкочастотный шум (в зависимости от типа скремблера). Сложность устройства определяет уровень защищенности передаваемой информации.

Скремблеры для радио и телефонии производятся многими фирмами, среди них –Transcrypt International, Communico, MX COM, MIDIAN, Selectone, а также фирмы, производящие радиотерминалы.

Исходное ТС, которое может передаваться по радио- или проводному каналу электросвязи, принято называть открытым сообщением и обозначать как X(t). Такое сообщение подается в устройство криптографического шифрования, где и создается скрытое (зашифрованное) сообщение Y(t) посредством математической зависимости

$$Y(t) = F_k[X(t)],$$

здесь F_k и k – соответственно криптографическое преобразование и его ключ. Обобщенная структурная схема криптографических преобразующих устройств на рисунке 1.1.

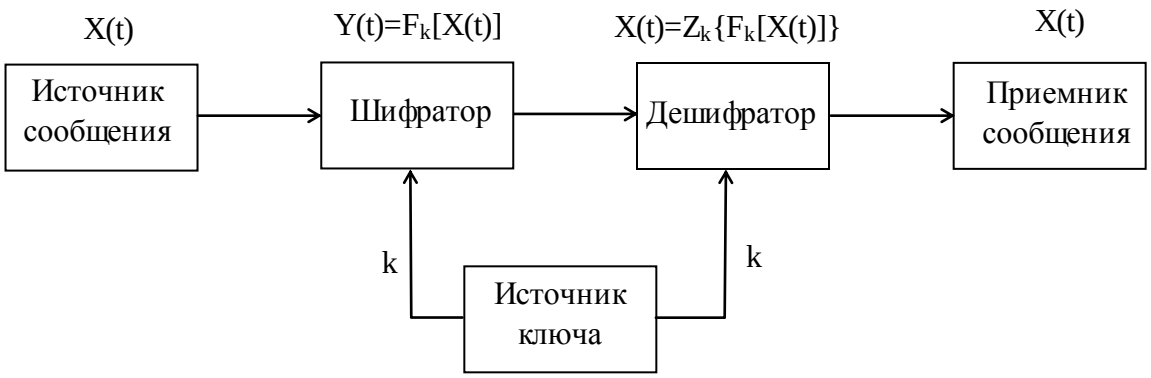

Рисунок 1.1 - Обобщенная схема крипто - преобразования.

В этом случае под ключом криптографического преобразования подразумевается некий параметр k, посредством которого производят выбор конкретного криптографического преобразования (крипто - преобразование) F_k. При этом чем больше мощность применяемых криптографического преобразования k, тем большему числу крипто -.преобразований подвергается телефонное сообщение X(t) и соответственно, тем больше неопределенность у злоумышленника в определении используемого в крипто - преобразования F_k.

Зашифрованное таким образом ТС Y(t) подвергается передачи по радио - или проводному каналу связи. Переданное ТС на приемной стороне расшифровывается (дешифрируется) и восстанавливается посредством математической зависимости

$$X(t) = Z_k[Y(t)] = Z_k\{F_k[X(t)]\},$$

где Z_k – является обратным по отношению к F_k преобразованием.

То есть обладание абонентами одинаковых ключей k и крипто - преобразований F_k, Z_k обеспечивает шифрование и дешифрование ТС.

Различные телефонные сообщения X(t) описываются длительностью и амплитудно - частотным спектром S(f), то есть ТС X(t) можно представлять равно во временной и частотной областях. Для обеспечения узнаваемости голоса абонента по тембру и разборчивость звуков достаточно использовать частотный диапазон от 300Гц до 3400Гц. Заметим, что такой частотной полосой пропускания обладают стандартные телефонные каналы всего мирового пространства.

Простым и поэтому наиболее распространенным способом аналогового крипто - преобразования речевых телефонных сообщений является разбиение сообщений X(t) на части и выдача этих частей в определенном порядке в канал связи и состоит в следующем. Длительность сообщения X(t) (рисунок 1.2) делится на определенные, равные по длительности временные интервалы (ВИ) T. Каждый такой ВИ дополнительно делится на более мелкие временные интервалы, но уже длительностью Δt . При этом значение $n = T/\Delta t$, как правило, выбирается из условия $n = m…10m$, где m - целое число, причем $m < 10$.

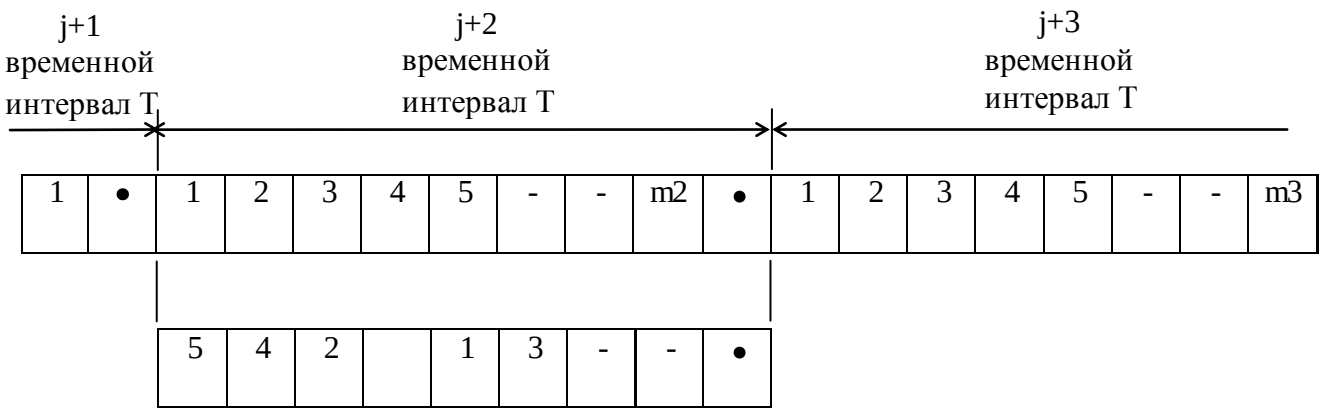

Рисунок 1.2 - Временные перестановки частей сообщения.

Части сообщения X(t) на ВИ Δt фиксируются в запоминающем устройстве, «перемешиваются» между собой по закону, установленном ключом крипто - преобразования k и уже в виде сигнала Y(t) направляется в канал связи.

На приемной стороне которого, где закон «перемешивания» известен, осуществляется «сшивка» открытого сообщения X(t). Преимуществам данного метода крипто - преобразования является его простота и возможность передачи зашифрованного ТС по стандартным телефонным каналам.

Однако рассмотренный метод обеспечивает только временную стойкость, так как открытое телефонное сообщение X(t) является непрерывным, то у злоумышленника после фиксации сообщения Y(t) и выделения ВИ длительностью Δt (это легко сделать в виду наличия в канале связи синхронизирующего сигнала) возникает возможность дешифрования сообщения Y(t), несмотря на отсутствие знаний о примененном ключе k.

Поэтому такой способ крипто - преобразования открытых ТС желательно применять в двух случаях, когда информация не строго ценная или когда ее ценность значительно устаревает через небольшой отрезок.

Значительно более высокую защиту от несанкционированного доступа обеспечивается при распространении рассмотренного метода на частотный спектр сообщения X(t). В таком варианте полоса пропускания телефонного канала ΔF разделяется посредством полосовых фильтров на n частотных полос шириной равной Δf, которые далее «перемешиваются» в соответствии с ключом крипто - преобразования k.

При этом «перемешивание» частотных полос производят со скоростью V циклов в секунду, таким образом перестановка полос длится всего 1/V с, а после чего она заменяется последующей.

Для повышения защиты от несанкционированного доступа после «перемешивания» частотных полос возможно производить инверсию частотного спектра сообщения Y(t).

1.2. Скремблеры с частотной инверсией сигнала.

С учетом международных стандартов полоса частот для шифрования, называемая также телефонной полосой частот, соответствует диапазону (0,3…3,4) кГц.

Все, что находится за ее пределами, может игнорироваться без ухудшения разборчивости передаваемой речи.

Спад амплитудно - частотной характеристики (АЧХ) обусловлен тем, что наибольшая мощность сигнала находится в низкочастотной части спектра.

При методе *однократной частотной инверсии* ТС поступает в частотный инвертор спектра скремблера, где низкочастотные составляющие речевого сигнала преобразовываются в высокочастотные и наоборот. В результате инверсный сигнал занимает ту же полосу частот, что и исходный (рисунок 1.3).

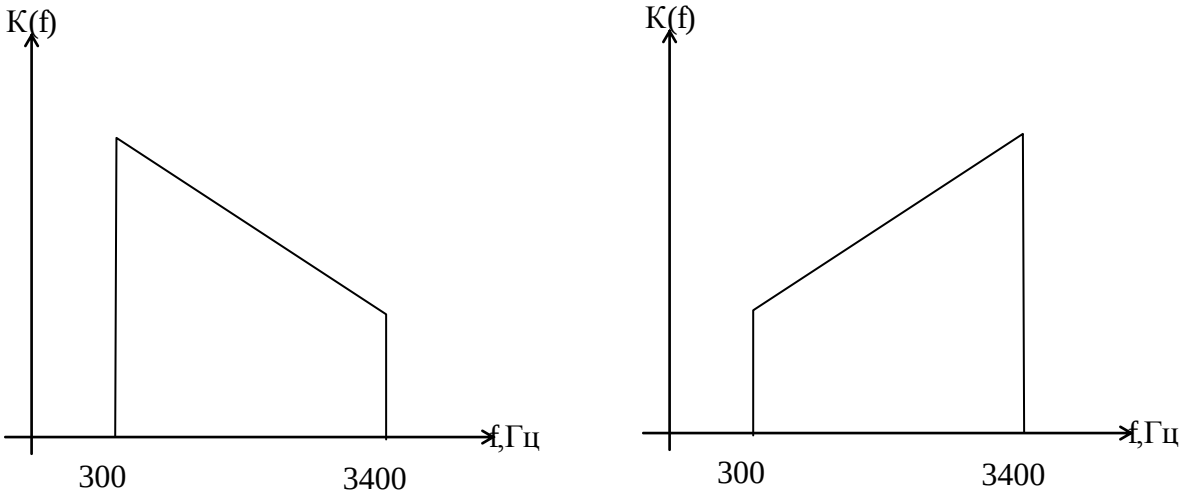

Рисунок 1.3 - Однократная частотная инверсия речевого спектра.

Разворот спектра в этом случае происходит относительно несущей частоты, которая может быть фиксированной в простых скремблерах или изменять свое значение во времени плавно или скачками в более сложных. Фиксированная частота или ее изменение является ключом системы. Обобщенная структурная схема шифратора речевого сигнала с однократной частотной инверсией приведена на рисунке 1.4.

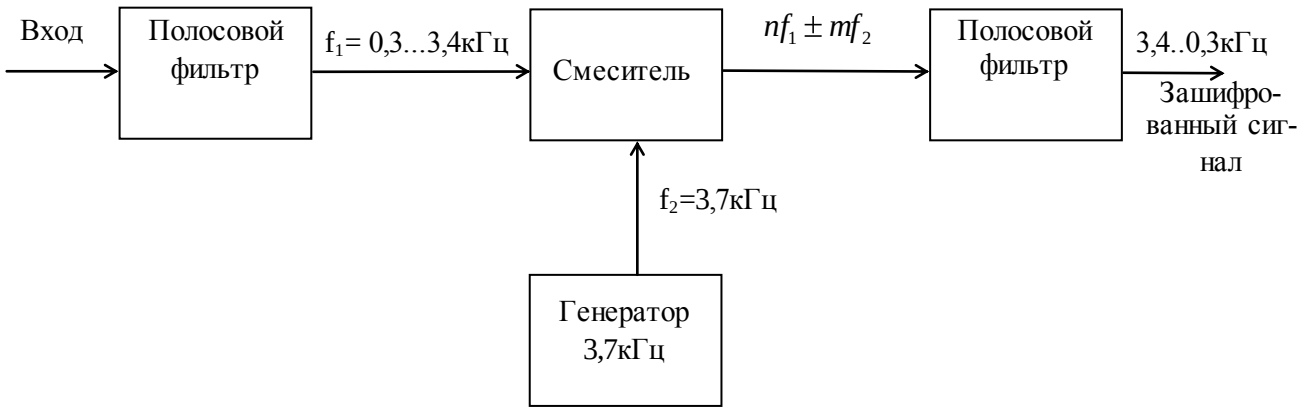

Рисунок 1.4 - Структурная схема шифратора с однократной частотной инверсией.

Шифруемый сигнал подвергается обработке в полосовом фильтре, чтобы в наибольшей степени подавить составляющие, не относящиеся к диапазону (0,3…3,4) кГц. Затем он смешивается с сигналом постоянной частоты, поступающим с максимально стабилизированного генератора.

Как правило, частота этого сигнала составляет порядка 3,7кГц.

На выходе смесителя присутствуют комбинационный набор входных частот $nf_1 \pm mf_2$, где $n,m = 0,1,2..\infty$. Активная НЧ фильтрация на выходе шифратора выделяет разностный сигнал $\Delta f = f_1 - f_2$, подавляя все более высокочастотные составляющие комбинированного сигнала.

Этот разностный сигнал и является зашифрованным сигналом. В итоге НЧ спектр входного сигнала инвертируется, что делает передаваемый речевой сигнал неразборчивым.

Для дешифрования такого сигнала достаточно изготовить практически идентичное устройство, структурная схема которого приведена на рисунке 1.5.

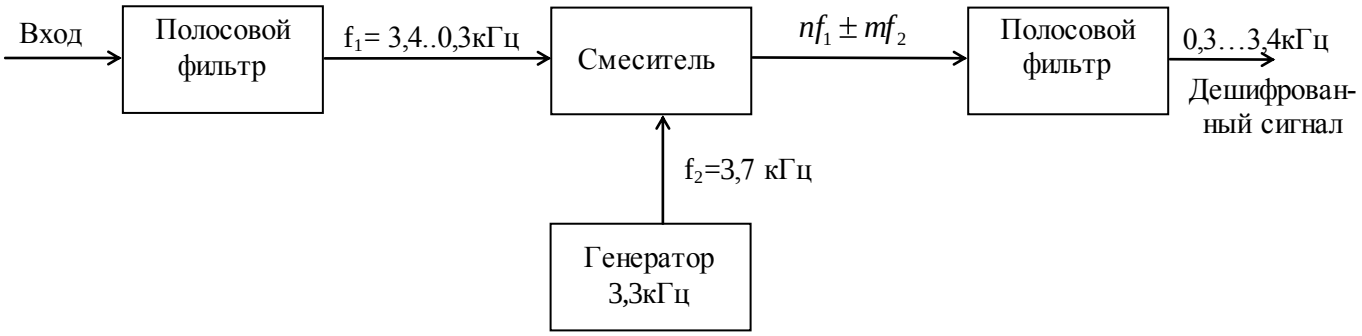

Рисунок 1.5 – Структурная схема дешифратора с однократной частотной инверсией.

Для подавления всех частот, не принадлежащих диапазону (0,5 – 3,4) кГц, зашифрованный сигнал проходит через полосовой фильтр. Затем он подводится к смесителю, аналогичному смесителю устройства для шифрования, куда поступает сигнал с постоянной частотой, максимально похожий на использованный при передаче.

Таким образом, на выходе опять получают комбинационный набор частот и отфильтровывают разностный сигнал. Этот сигнал является эквивалентом первоначально переданному сигналу.

Однократная частотная инверсия сигнала является простейшим видом аналогового скремблирования и обеспечивает самую низкую криптографическую стойкость. При закрытии телефонного сообщения посредством одиночной частотной инверсии несложно разобрать (пользуясь обычным приемником) почти до половины речевой информации в зависимости от темпа речи, темы разговоров.

Например, полностью прослушать такой сигнал можно, имея радиостанцию со встроенным инвертором частоты или специализированный радиоприемник-сканер (например, AR-16 японской фирмы AOR LTD).

Достоинством метода однократной инверсии является очень качественное восстановление зашифрованного (полученного из эфира) сигнала. Наиболее известные модели однократной инверсии - ST-20, ST-022 (Selectone), SC20-400 (Transcrypt International).Более эффективно защиту речевой информации обеспечивает *частотная инверсия двух и более поддиапазонов речевого спектра*. В этом случае полоса всего речевого спектра делится на частотные поддиапазоны (в большинстве случаев на два), которые затем инвертируются (рисунок 1.6). Ключом этой системы является частота разбиения спектра сигнала. Эти скремблеры, в отличие от моделей, использующих однократную частотную инверсию, несколько повышают уровень защищенности информации.

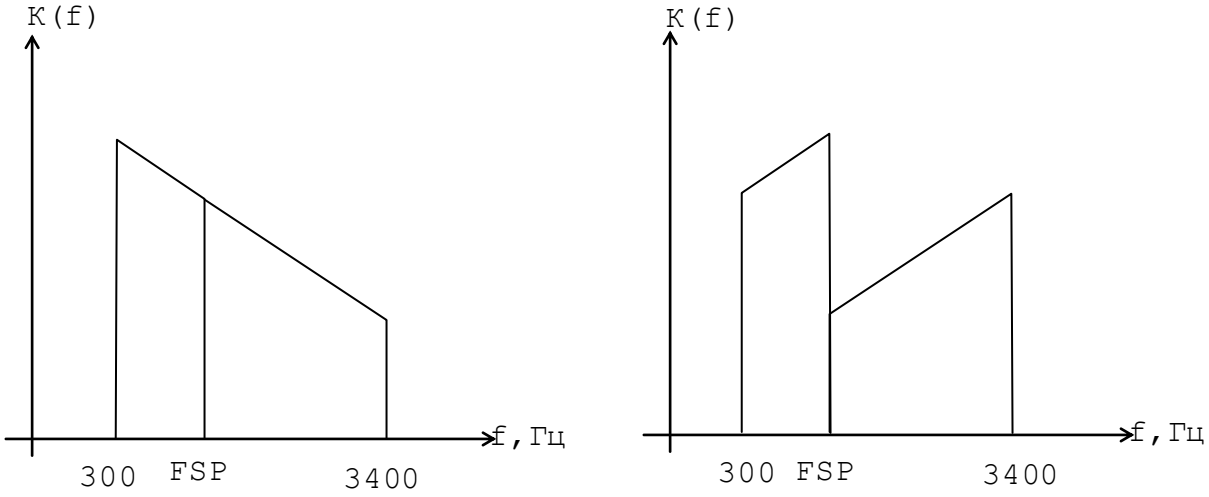

Рисунок 1.6 - Частотная инверсия двух диапазонов речевого спектра.

Структурная схема двухдиапазонной системы шифрования приведена на рисунок 1.7. Диапазон частот (300…3400) Гц искусственно разделен специальным фильтром на два поддиапазона: 300 - FSP и FSP - 3400. Под FSP понимается частота

разрыва (splitpoint). Каждый из полученных поддиапазонов смешивается с сигналом постоянной частоты, программируемой и характерной для каждого из них. Затем следует фильтр нижних частот, подавляющий все составляющие, кроме разностных (как в структурной схеме рисунок 1.4). Полученные сигналы после этого снова смешиваются и передаются.

Из структурной схемы, представленной на рисунке 1.8, видно, что при приеме используется похожий процесс: после полосового фильтра диапазон частот зашифрованного сигнала снова делится на два поддиапазона, идентичных полученным при передаче. Затем, сформированные таким образом две группы сигналов, независимо друг от друга смешиваются с постоянными частотами для восстановления исходных сигналов, которые после смешивания дают дешифрованный сигнал.

Для нормальной работы описанной системы необходимо, чтобы в блоках шифратора и дешифратора были идентичными следующие параметры:

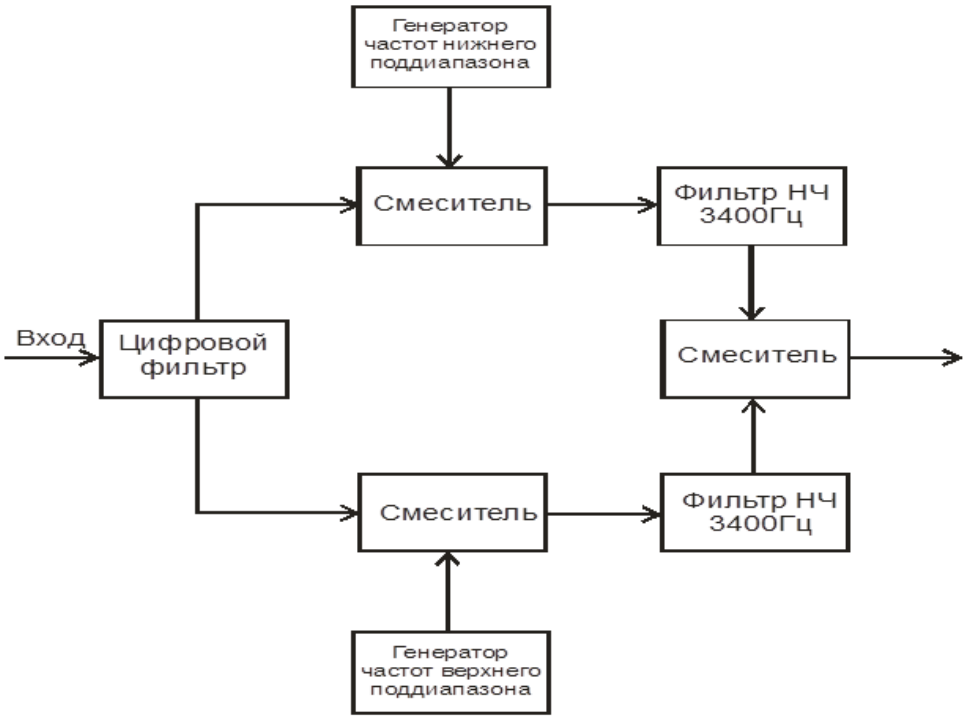

Рисунок 1.7 - Шифратор двухдиапазонной системы.

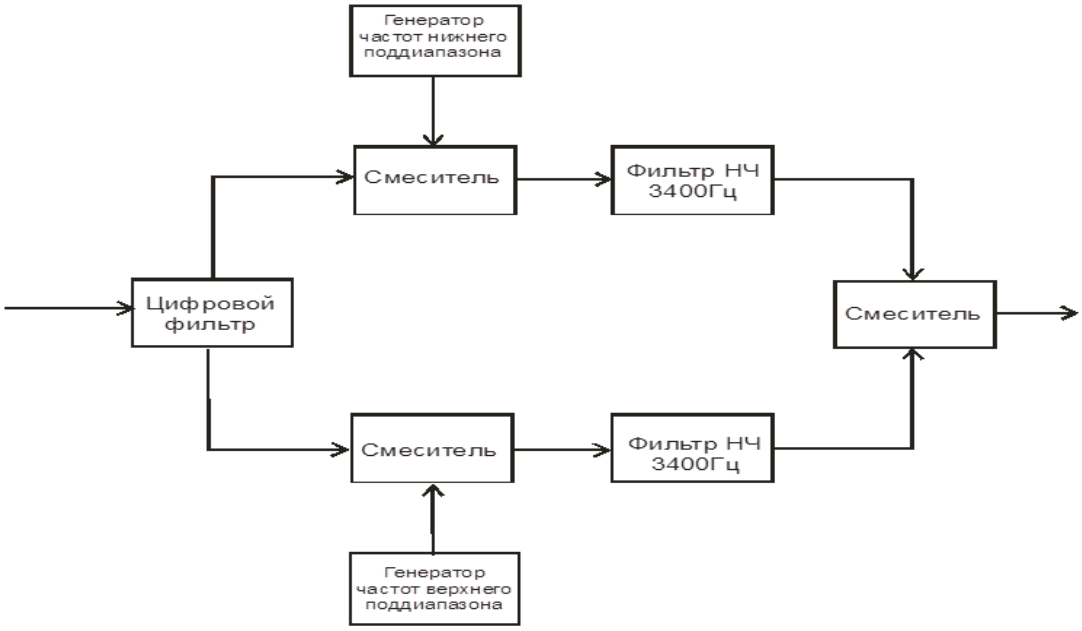

Рисунок 1.8 - Дешифратор двухдиапазонной системы.

- частота разрыва FSP;
- смешанная частота нижнего поддиапазона;
- смешанная частота верхнего поддиапазона.

Как показывает практика, защищенность двухдиапазонной системы от "пиратского" дешифрования значительно превышает данный показатель для систем с однократной частотной инверсией.

Для значительного повышения уровня закрытия информации применяют динамические скремблеры, которых параметры преобразования речевого сигнала изменяются во времени. Такие устройства требуют синхронизации передающих и приемных сторон. В зависимости от типа скремблера синхронизация может передаваться как в начале сообщения, так и во время его передачи.

Английская фирма Pentone представляет скремблер SCR1 с частотной инверсией двух поддиапазонов. Подобное устройство производит и отечественная компания "Квазар-Микро Радио" (модель KMR-1). Эти типы скремблеров могут быть как статическими, так и динамическими.

Качающаяся частотная инверсия - это непрерывное изменение несущей частоты речевого сигнала во время всего разговора. Несущая частота изменяется во времени по пилообразной траектории (рисунок 1.9,а).

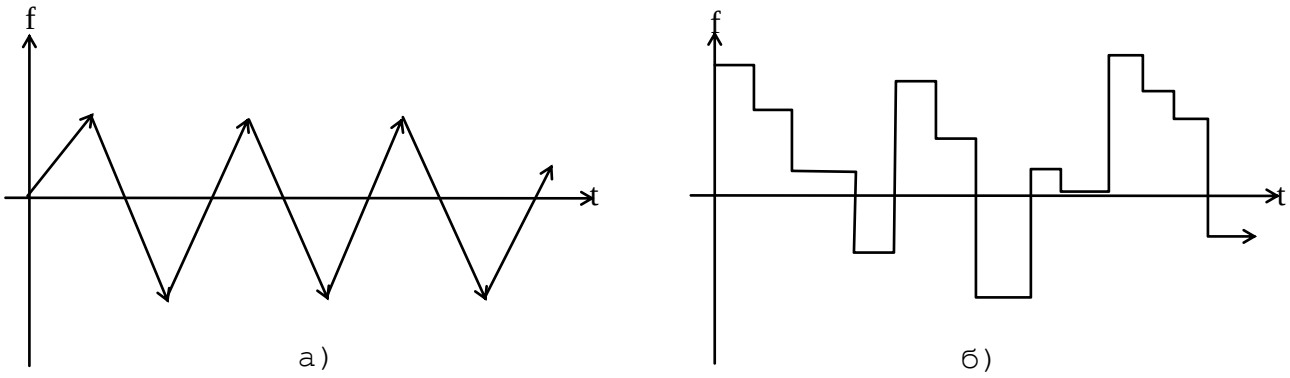

Рисунок 1.9 - Метод качающейся (а) и скачкообразной (б) инверсии речевого с-

В большинстве таких скремблеров синхронизация параметров изменения частоты присутствует на протяжении всего времени разговора. Так как эта синхронизация передается одновременно с речевым сигналом, то восстановленный сигнал получается не очень высокого качества. Однако при обычном прослушивании этот метод делает речь полностью неузнаваемой.

На рынке используют скремблеры как с медленным качающимся кодом-VPU-10A, VPU-10B (Midian), так и с быстрым-ST-25, ST-26 (Selectone), SC20-440, SC20-450 (Transcrypt International).

Метод *скачкообразного изменения частоты инверсии*. Частота в этом случае изменяется псевдослучайным образом, скачкообразно(рисунок 1.9,б). Закономерность изменения должна быть одинаковой как в шифрующем, так и в дешифрующем скремблере.

В большинстве таких устройств в передаваемом сигнале присутствует начальный синхронизирующий пакет, в котором содержится алгоритм изменения частоты инверсии для приемной стороны. В более сложных динамических скремблерах для повышения уровня защиты передаваемой информации такой алгоритм может меняться при каждом последующем установлении сеанса связи.

Речевой сигнал в случае использования этого типа скремблеров, в отличие от простого статического, теряет свою целостность. В зависимости от модели скрем-

блера частота инверсии может меняться от 1 до 1000 раз в секунду. Чем больше количество изменений в секунду, тем выше уровень защиты информации, но, как следствие, ниже качество восстановленного сигнала.

Недостаток большинства скремблеров со скачкообразным изменением частоты инверсии в том, что для передачи синхронизирующего пакета оператор вынужден в начальный момент делать паузу. В случае связи через ретранслятор радиостанция с таким скремблером не всегда может надежно соединяться (декодироваться) с другой радиостанцией. Дело в том, что в ретрансляторах существует так называемая прозрачность (нелинейность звуковых трактов), вследствие чего первоначальный пакет, проходя через тракты ретранслятора, может исказиться. Для повышения надежности такого соединения необходимо увеличить длительность передачи первоначального пакета (иногда до 1с), что может создавать определенные неудобства.

Синхронизирующий пакет сообщает закон изменения частоты инверсии для приемной стороны. Преимущество таких скремблеров заключается в том, что в случае достаточно быстрого изменения частоты инверсии (например, 800-1000 раз/с) они имеют относительно высокий уровень защиты передаваемой информации. Например, если скорость изменения составляет один раз в секунду, то 40-60% информации можно прослушать очень простым техническим методом. Широкую серию скремблеров, использующих скачкообразное изменение частоты инверсии,производит фирма Transcrypt International. Распространенные серии - 410 (изменение частоты инверсии 1 раз/с), 430 (300 раз/с), 460 (1000 раз/с), 480 (800 раз/с).

В качестве примера можно привести скремблер для радиотелефонии фирмы Consumer Microcircuits Limited (рисунок.1.10). Входной VSB фильтр устройства по команде микроконтроллера способен разделить "голосовой" диапазон частот (400…2700Гц) на различное число поддиапазонов (до 32). Причем точки разрыва могут изменяться с частотой от 4 до 60 раз в секунду ("rollingcode") по одному из 65000 уникальных ключей шифрования. Полученные частотные интервалы инвертируются и с помощью несущей частоты излучаются в эфир.

Более высокую криптостойкость обеспечивают скремблеры, использующие *цифровую технологию сигнальной обработки*. Это стало возможным благодаря применению сигнальных процессоров DSP (Digital Signal Processor).

Шифровальный модуль в цифровой форме записывает речевой сигналдля небольшого отрезка времени. Затем этот сигнал подразделяется на меньшие блоки, которые равны между собой по длительности.

Блоки в пределах временного отрезка перестраиваются в обратном порядке или по определенному правилу криптографического преобразования, отличающегося в каждом отдельном случае.

Правило перемешивания интервалов определяет ключ системы.

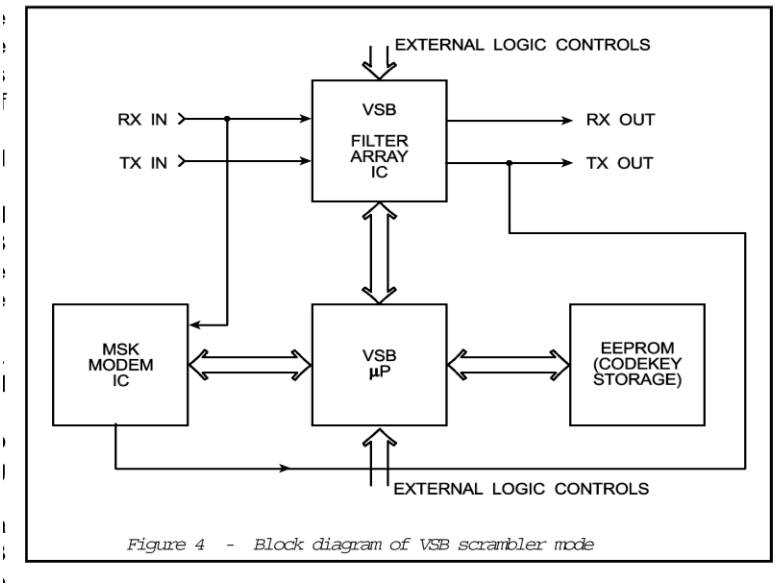

Рисунок 1.10 - Скремблер для радиотелефонии фирмы Consumer Microcircuits Ltd.

Естественно, что при использовании этого метода происходит некоторая задержка сигнала, зависящая от длительности интервалов (чем больше длительность интервалов, тем больше задержка сигнала и, соответственно, выше уровень защиты). Поскольку в большинстве случаев данные синхронизации посылаются непре-

рывно со звуковым сигналом, пользователь имеет возможность последующего соединения (его скремблер может декодировать даже в случае прерывания приема в начальный момент).

Несмотря на сложность шифрования, звуковые фильтры DSP - процессора обеспечивают высокое качество восстанавливаемого сигнала. Типичные модели скремблеров временного преобразования - ST-50, ST-51, ST-52 (Selectone).

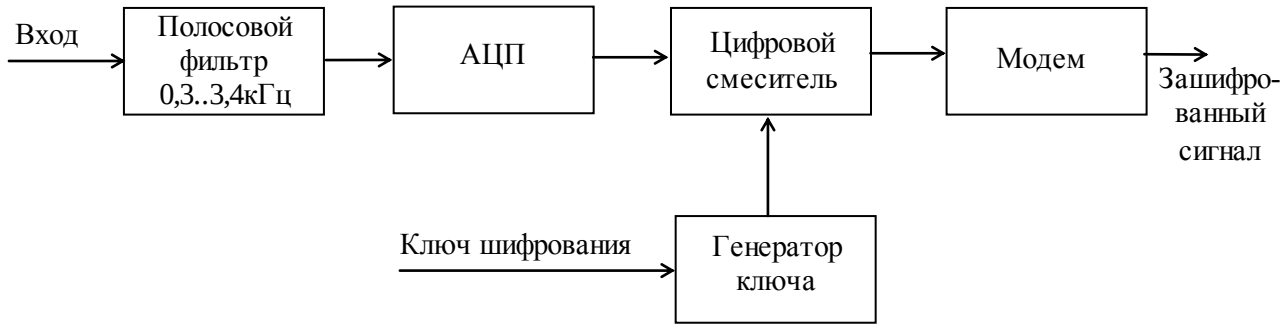

Рис.1.11 - Структурная схема шифратора (кодера) цифровой криптофонии.

Шифруемый сигнал после прохождения через полосовой фильтр подается на аналого-цифровой преобразователь АЦП. Выходящий из АЦП сигнал смешивается заданным или псевдослучайным (в зависимости от требуемого уровня обеспечения защиты) способом с ключом шифрования, который, в свою очередь, также может быть постоянным или переменным. Полученный сигнал с помощью модема передается по каналу связи.

Структурная схема дешифратора, основанного на этом принципе, представлена на рисунке 1.12.Полученный сигнал после обязательного прохождения через модем подается на цифровой дешифратор.

Дешифратор определяет, конструкционным или программным способом ключ был "подмешан" к сигналу, и обладает ключом для шифрования.

Если он является переменным, то достаточно иметь только так называемый начальный ключ, а затем вычислять его текущее значение.

При выполнении перечисленных условий на выходе модуля формируется цифровой сигнал. С помощью обычного ЦАП он преобразуется в аналоговый и после соответствующей обработки в полосовом фильтре получается исходный сигнал.

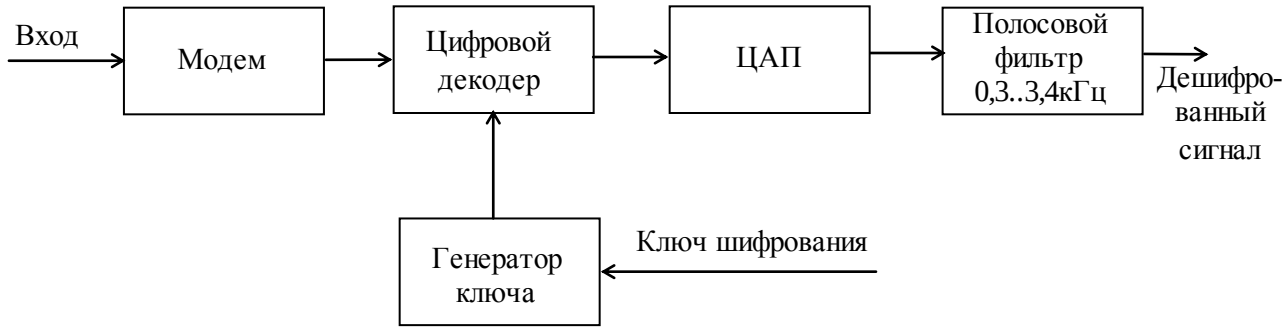

Рисунок 1.12 - Структурная схема дешифратора цифровой криптофонии.

Такой способ весьма устойчив против нежелательного дешифрования, особенно если используемый код состоит из достаточного числа битов (в наиболее надежных системах 64). Если ключ является переменным, степень защиты соответственно возрастает. Кроме того, передача в цифровом виде через модем создает для взломщика определенные трудности, поскольку невозможно определить идет ли шифрованная передача речевого сообщения или передается обычный цифровой поток данных.

В настоящее время наиболее известными криптографическими алгоритмами, обладающими гарантированной защитой передаваемых цифровых сообщений от несанкционированного доступа, являются американский стандарт шифрования данных DES (Data Encryption Standart).

Полностью цифровые скремблерысерии DES фирмы Transcrypt обеспечивают высший уровень криптостойкости для аналоговых радиостанций и телефонии. В этих устройствах низкочастотный сигнал вначале подвергается дискретизации (оцифровке), затем происходит кодирование согласно алгоритму DES.

Дальнейшим развитием стандарта DES является отечественный стандарт шифрования ГОСТ28147-89, который создавался с учетом мирового опыта, недостатков и нереализованных возможностей алгоритма DES.

Данный отечественный стандарт обязателен к применению для защиты, описываемых двоичными последовательностями.

Пименение в криптографическом алгоритме ГОСТ28147-89 ключа крипто - преобразования k длиной 256 символов обеспечивает высокую стойкость по сравнению с алгоритмом DES.

Это действительно так. Если злоумышленник при раскрытии передаваемого ТС применяет сплошное опробование ключей крипто - преобразования, а ключи из множества, мощность которого равна K, назначаются равновероятно, то вероятность $P_k(T)$ установления злоумышленником примененного ключа k за время T оценивается посредством выражения

$$P_k(T) = TW/K,$$

Здесь W- число опробований злоумышленником ключей крипто - преобразования за временную единицу.

В таблице 1 рассмотрены значения вероятности $P_k(T)$ для алгоритмов DES и ГОСТ28147-89 при $W = 10^9$ 1/с.

Таблица 1 Значения вероятности $P_k(T)$ при $W = 10^9$ 1/с

T	Алгоритм DES	Алгоритм ГОСТ28147-89
1 год	0,44	$2,72x10^{-61}$
2 года	0,88	$5,44x10^{-61}$
10 лет	1,0	$2,72x10^{-60}$

Из анализа данных таблицы 1, следует, что задавая $P_k = P_{k,тр}$, можно определить такие интервал времени T и алгоритм крипто - преобразования, при которых обеспечивается строгое соблюдение заданного требования.

Подводя итоги выше сказанному следует отметить, что достоинством применения вышерассмотренных алгоритмов крипто - преобразования цифровых ТС по сравнению со способами крипто - преобразования аналоговых ТС достаточно очевидны и состоит в обеспечении гарантированной стойкости передаваемых сообщений. Однако эта стойкость обеспечивается применением технически сложной и дорогой аппаратуры и отказа в большинстве случаев от стандартного телефонного канала связи. Покажем это.

В случае применении для передачи ТС импульсно – кодовой модуляции (ИКМ), для его восстановления на приемной стороне необходимо использовать по теореме Котельникова более 6800 мгновенных значений в секунду. Далее, если для преобразования этих мгновенных значений в код используются восьми разрядные аналого - цифровой (АЦП) и цифро - аналоговый преобразователи (ЦАП), то скорость передачи символов в канале связи должна быть равной 54,4 кбит/с.

Таким образом для передачи ТС необходимо основательно повысить полосу пропускания канала связи и построить шифратор (дешифратор) со скоростью крипто – преобразования равной 54,4 кбит/с.

В настоящее время на российском рынке гарантированно защищенных от несанкционированного доступа к передаваемым системам ТС очень и очень мало. При этом они обладают невысокой разборчивостью слогов и сложностью опознания абонента по голосовому тембру. В качестве примера таких систем можно привести систему. «Voice coder-2400», которая совместно с криптографическим алгоритмом ГОСТ28147-89 применяет и «устаревший» алгоритм кодирования параметров телефонного сообщения LPC-10.

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

Система размещается в корпусе телефонного аппарата "Panasonic KX-T2355/2365" и реализует наиболее современный алгоритм кодирования параметров телефонных сообщений CELP, что позволяет обеспечить высокое качество речи. Для защиты от несанкционированного доступа к передаваемым сообщениям используются криптографический алгоритм ГОСТ28147-89.

Электропитание системы осуществляется от сети 220В 50/60Гц или от источника постоянного тока напряжением в 9-12В, а потребляемая электрическая мощность не более 5Вт.

Системы цифровой криптофонии обладают великолепной устойчивостью против нежелательного декодирования. Однако цена их настолько высока, что к помощи дан-

ных систем прибегают только в тех устройствах, когда стоимость технического обеспечения не является главным критерием выбора.

Проведенный обзор показал, что для защиты коммерческой и личной информации аналоговые методы криптографии являются наиболее приемлемыми, так как имеют низкой стоимостью, а также то, что они могут применяться в самых распространенных в мире каналах связи. Однако следует учесть, что этот способ не должен использоваться при защите сведений, являющихся секретными в течение большого промежутка времени.

2.Обобщенная структурная схема устройства защиты речевых телефонных сообщений.

Как было показано выше, наиболее приемлемым вариантом реализации устройства защиты речевых сообщений (УЗРС) является использование двух диапазонной системы инверсии голосового спектра. При относительно невысоких аппаратурных затратах она обеспечивает достаточно высокую криптографическую стойкость (оценивается временем, необходимым для расшифровки информации).

Простейшие варианты таких систем разбивают полосу речевого сигнала на поддиапазоны с частотной инверсией сигнала в каждом поддиапазоне (рисунок 1.6). Инверсия обеспечивает преобразование речевого спектра, равносильное повороту частотной полосы речевого сигнала вокруг некой средней точки, являющейся ключом системы. Благодаря инверсии обеспечивается эффект преобразования низких частот в высокие, а высоких в низкие, при этом в качестве ключа системы выступает точка разбиения.

Дополнительное повышение уровня защиты ТС достигается изменением параметров преобразования сигнала во времени.

Такими ключевыми параметрами обычно выступают частота разбиения полосы сигнала и частоты инверсии в каждом из поддиапазонов (рисунок 1.10).

Уровень защиты при этом описывается числом градаций параметра сигнала и длиной ключа, то есть числом возможных комбинаций параметра и скоростью его изменения. В теоретическом смысле для перехвата злоумышленниками ТС в реальном времени в каналах связи, защищенных посредством скремблеров с параметрами преобразования, меняющимися во времени, следует использовать специальных технических средств, обеспечивающих вначале определение ключевой последовательности, а затем подстроиться под найденную ключевую последовательность.

Обобщенная структурная схема двух диапазонного УЗРС приведена на рисунок 1.13. Обычный аудиосигнал подается на вход полосового фильтра (300-3400) Гц для фильтрации спектральных составляющих речи, не попадающих в полосу частот, соответствующую требованиям международных стандартов по телефонии. Устройство шифрования проводит необходимые частотные преобразования речевого спектра для обеспечения заданной криптографической стойкости передаваемого сообщения.

Фильтр низких частот на выходе шифратора срезает комбинационные частоты и обеспечивает соответствие зашифрованного сигнала требованиям канала связи.

В случае приема зашифрованного сообщения сигнал поступает на дешифратор, производящий частотные преобразования в обратном порядке.

Фильтр НЧ устраняет нежелательные комбинационные частоты, а усилитель обеспечивает требуемые уровень и мощность дешифрованного аудиосигнала.

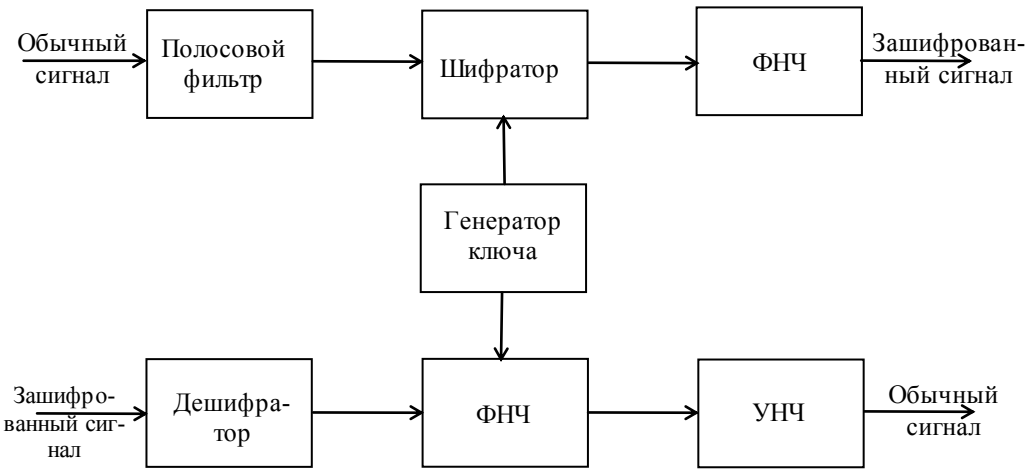

Рисунок 1.13 - Обобщенная структурная схема двух диапазонного УЗРТС.

Идентичность проводимых частотных преобразований обеспечивается с помощью специального генератора ключа, задающего последовательность частот разбиения спектра и частот инверсии в каждом частотном поддиапазоне.

Вполне очевидно, что другая сторона, участвующая в разговоре, должна иметь совершенно аналогичное устройство. Для правильной и устойчивой работы УЗРС необходима тщательная синхронизация операций шифрования и дешифрирования в каждом устройстве.

2.1 Выбор интегральной схемы скремблера.

Для обеспечения минимальных габаритов и стоимости разрабатываемого УЗРТС был проведен Интернет – поиск ИС, обеспечивающих заданные частотные преобразования речевого спектра. Поиск показал, что одним из лидеров в производстве недорогих аналоговых ИС скремблеров является английская фирма CML (Consumer Microcircuits Limited). Фирма выпускает довольно большое количество ИС скремблеров с частотной инверсией (серии FX, CMX и MX), в том числе и устройства динамического типа (Split - Band Scrambling Furnishes Voice Security).

Микросхемы скремблеров фирмы CML (CML/products/datasheets)отличаются способами инверсии частотного спектра, количеством частот разрыва FSP при разбиении на поддиапазоны, частотами инверсии спектра внутри поддиапазонов, спо-

собом и алгоритмами смены указанных частот. Фильтры, используемые в ИС, обеспечивают соответствие передаваемого спектра сигнала стандартам различных каналов связи. Кроме этого, ИС отличаются набором сервисных функций и, естественно, ценой.

Проведенный анализ ИС скремблеров фирмы CML позволил выбрать микросхему VSB (VariableSplitBand) скремблера FX224 как наиболее подходящую для решения поставленной задачи.FX244 включает в себя все элементы, необходимые для построения шифратора - дешифратора УЗРС, согласно структурным схемам, приведенным на рисунках 1.7 и 1.8. Микросхема реализована по КМОП технологии и обеспечивает весьма низкое энергопотребление устройства. Упрощенная функциональная схема внутренней конфигурации ИС FX244 (рисунке 1.14) содержит как логическую часть, состоящую из тактового генератора частотой 1МГц, памяти ROM и схемы выбора из 32 комбинаций трех частот, так и аналоговую, в составенескольких фильтров НЧ и ВЧ на переключаемыхконденсаторах. Микросхема обеспечивает работу в обычном режиме "Clear" или в режиме шифрования "Scramble". В зависимости от установленного алгоритма работы возможна статическая или динамическая инверсия частотного спектра.

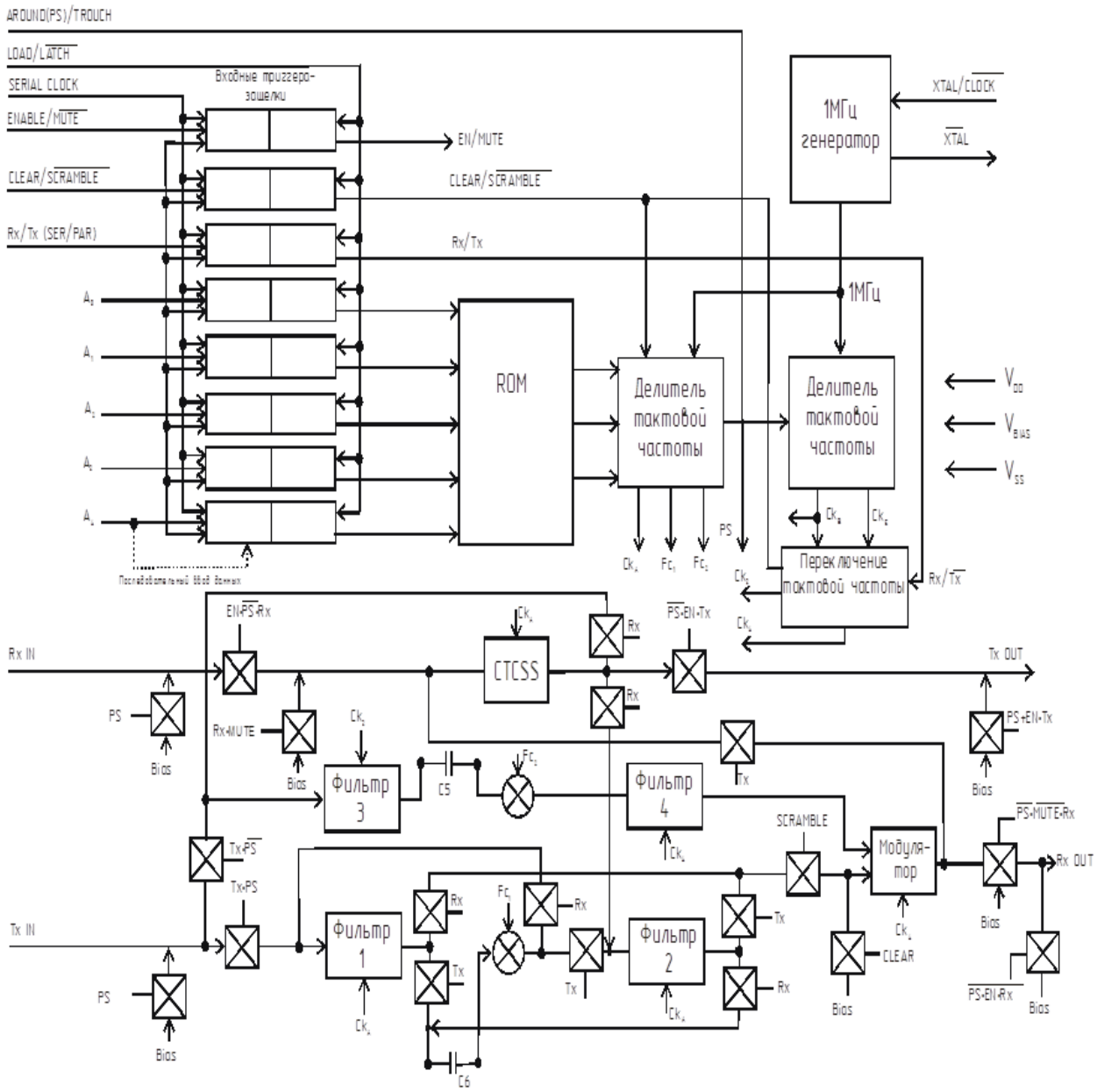

Рисунок - 1.14 - Функциональная схема ИС скремблера FX224.

Интегральная схема FX224 имеет отдельные входы приема - передачи (Rx/Tx), что обеспечивает полудуплексный режим работы УЗРС.

Для подавления взаимовлияния входов Rx/Tx используется специальный ВЧ фильтр CTCSS (Continuous Tone Con - trolled Squelch System), автоматически подключаемый к входу в режиме Rx и к выходу в режиме Tx.

Шифрование (scrambling) голосового аудиосигнала в ИС происходит за счет разбиения речевого спектра с помощью фильтра на "верхний" (high) и "нижний"(low) поддиапазоны, с дальнейшей инверсией каждого поддиапазона относительно отдельной частоты инверсии (frequency invert).

Полученный в результате этого суммарный сигнал и является зашифрованным сообщением.

Операция дешифрования (de-scrambling) происходит в обратном порядке теми же методами.

Использование FX224 обеспечивает 32 различных комбинации частот разрыва спектра FSP (Split Point)и частот инверсии нижнего f_{c1} и верхнего f_{c2} поддиапазонов, предварительно занесенных в память (ROM) микросхемы (таблица 1.1).

Генерация последовательности этих комбинаций обеспечивается 5 - битовым кодом, подаваемым на входы (A0…A4) интегральной схемы.

Код последовательности может быть фиксированным (статический скремблер) или каким-либо образом меняться извне (rollingcode в динамическом скремблере).

Синхронизация операций шифрования/дешифрования осуществляется либо передачей данных при смене комбинации частот инверсии, либо специальным тоновым сигналом вне полосы речевого спектра.

Тактирование схемы FX224 и работа фильтров на переключаемых конденсаторах обеспечивается встроенным 1МГц генератором или через специальный вход синхронизации XTL/CLC.

Таблица 1.1

Адреса и значения частот инверсии речевого спектра

ROM адрес A4-A0	FSP, Гц	f_{c1}, Гц	f_{c2}, Гц	ROM адрес A4-A0	FSP, Гц	f_{c1}, Гц	f_{c2}, Гц
00000	2800	3105	6172	10000	1135	1436	4504
00001	2625	2923	6024	10001	1050	1351	4424
00010	2470	2777	5813	10010	976	1278	4347
00011	2333	2631	5681	10011	913	1213	4310
00100	2210	2512	5555	10100	857	1157	4273
00101	2100	2403	5494	10101	792	1094	4166
00110	2000	2304	5376	10110	736	1037	4132
00111	1909	2212	5263	10111	688	988	4065
01000	1826	2127	5208	11000	636	936	4032
01001	1750	2049	5102	11001	591	891	3968
01010	1680	1984	5050	11010	552	853	3937
01011	1555	1858	4950	11011	512	813	3906
01100	1448	1748	4807	11100	471	772	3846
01101	1354	1655	4716	11101	428	728	3816
01110	1272	1572	4629	11110	388	688	3787
01111	1200	1501	4587	11111	350	650	3731

3. Функциональная схема устройства защиты речевых телефонных сообщений.

Полная функциональная схема разработанного УЗРТС приведена на рисунке 1.15. Схема обеспечивает выполнение следующих функций в полудуплексном режиме работы:

- формирование обычного или шифрованного (clear/scramble) аудиосигнала,
- прием и дешифрование (в случае необходимости) аудиосигнала,
- генерацию псевдослучайной последовательности 3-х частотной комбинации речевого спектра (32 комбинации) с реализацией 6 вариантов числа изменений этих комбинаций в секунду (5раз\сек, 1раз\сек, 1 раз в 3 сек и т.д),
- формирование фиксированного или динамического кода последовательности комбинаций частот,
- синхронизацию операций шифрования \ дешифрования на передающей и приемной стороне.

При работе в обычном режиме (Clearmode) входной аудиосигнал приводится к заданному уровню с помощью регулируемого усилителя - нормализатора.

Для обеспечения качественной инверсии речевого спектра необходимо удалить все высокочастотные составляющие аудиосигнала, в том числе возможные выбросы и всплески напряжения. Это осуществляется амплитудным ограничителем входного сигнала и полосовым фильтром (300…3400) Гц (эта полоса частот определена международными стандартами по телефонии).

Скремблер на ИС FX224 осуществляет частотную инверсию аудиосигнала с помощью меняющегося кода (rolling code), формируемого генератором псевдослучайной последовательности (PRCG- Pseudo-Random Code Generator). Шифрованный сигнал поступает на специальный фильтр НЧ для согласования частотного спектра выходного сигнала с требованиями стандартов различных систем радиосвязи (в том числе и сотовой связи). Цепи дешифрации на второй ИС FX224 используют идентичную псевдослучайную последовательность при обработке принятого инвертированного аудиосигнала.

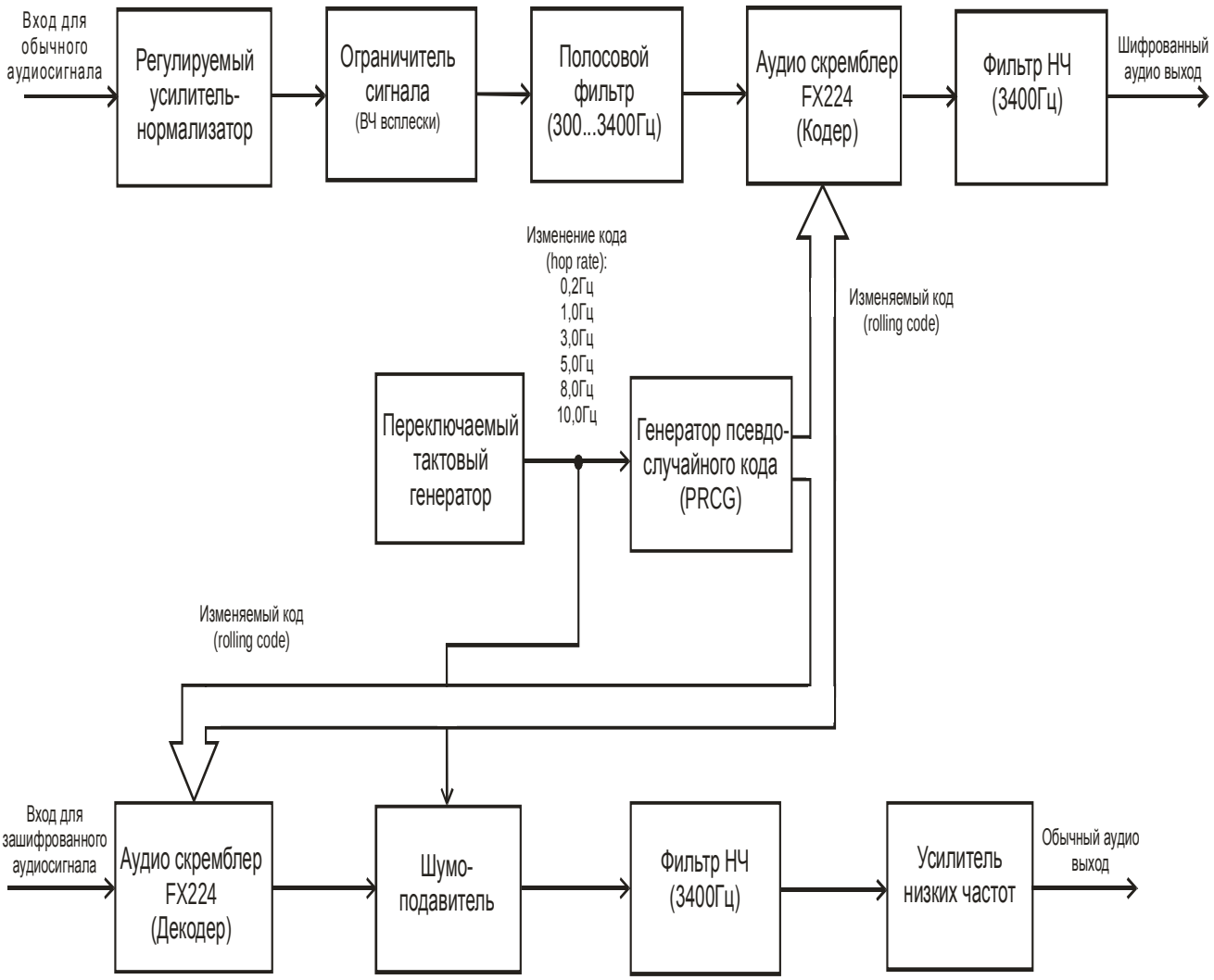

Рисунок 1.15 - Функциональная схема разработанного устройства защиты речевых сообщений (УЗРТС).

В технической документации фирмы CML отмечена проблема, возникающая при реализации динамических скремблеров.

При смене кода очередной комбинации частот (FSP, f_{c1} и f_{c2}) появляются паразитные шумовые всплески сигнала, связанные с переходными процессами в фильтрах устройства.

Для устранения этого эффекта используется схема шумоподавителя, формирующая специальный стробирующий импульс (noiseblankingpulse). При работе в обычном режиме (Clearmode) этот импульс не формируется.

Фильтр низких частот подавляет комбинационные ВЧ составляющие, а усилитель НЧ обеспечивает требуемые уровень и мощность дешифрованного аудиосигнала.

Генератор псевдослучайного кода формирует 5-битовую 31-шаговую последовательность смены комбинации частот (FSP,f_{c1} и f_{c2}).

Смена комбинаций может происходить с частотой от 0,2Гц до 10Гц за счет изменения частоты переключаемого тактового генератора.

Сама последовательность может быть задана различными способами, например, число - импульсным генератором, регистром сдвига с обратной связью и пр.

4. Электрические схемы отдельных узлов устройства защиты речевых телефонных сообщений.

4.1. Принципиальная схема усилителя - нормализатора.

Согласно известным данным, номинальное входное напряжение для ИС скремблера FX224 составляет 300мВ среднеквадратического значения (rms). Указанное значение в обычном режиме (Clearmode) обеспечивается усилителем-нормализатором (рисунок 1.16), в состав которого входит буферный повторитель напряжения DA1 и регулируемый усилитель DA2 с переменным резистором R4 в цепи его ООС.

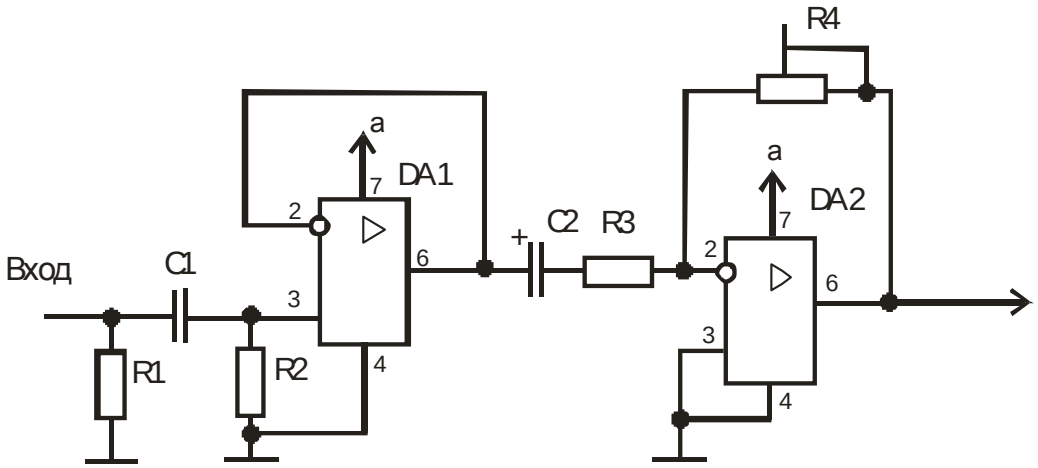

Рисунок 1.16 - Схема усилителя - нормализатора УЗРТС.

Так как к данной части схемы особых требований не предъявляется для построения нормализатора использованы операционные усилители широкого применения LM741 NationalSemiconductor.

4.2. Электрическая схема шифратора.

Для получения полосы частот соответствующей международным стандартам по телефонии (300…3400) Гц использован аудиофильтр на переключаемых конденсаторах FX306P фирмы CML. Структурная схема приведена на рисунке 1.17.

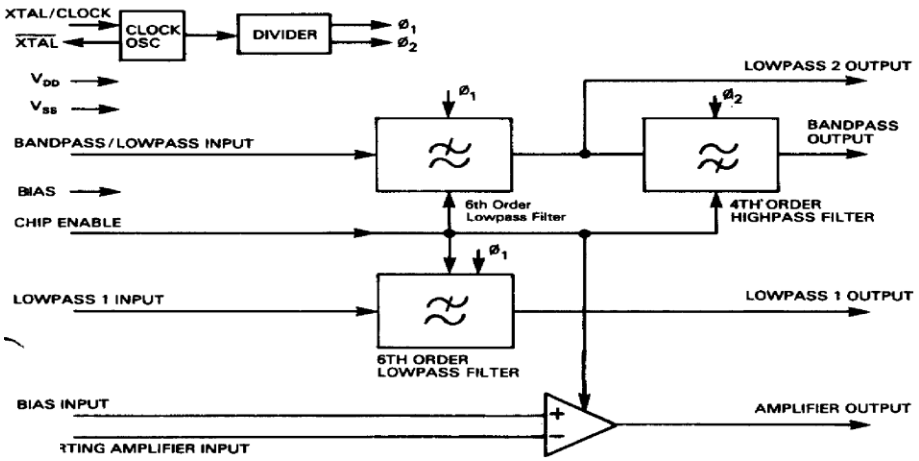

Рисунок 1.17 - Структурная схема аудиофильтраFX306P фирмы CML.

Как видно из рисунка схема фильтра содержит три канала:

1- фильтр НЧ 6-го порядка с полосой 3400Гц,

2- полосовой фильтр (300…3400)Гц (ФНЧ аналогичный 1 в сочетании с фильтром ВЧ 4-го порядка),

3- независимый инвертирующий усилитель.

Управление фильтрами осуществляется от внутреннего тактового генератора 1МГц через делитель частоты с переменным коэффициентом деления. Альтернативным вариантом является использование внешнего тактового генератора через вход XT/CLC (Xtal / Clock). Характеристики фильтра по заявлению фирмы CML полностью соответствуют весьма жестким требованиям (Specification) аналоговой сотовой связи стандартов NMT, TASK и AMPS.

Схема включения (рисунок 1.18) ИС FX224 в режиме шифрования (Scramble) не имеет особенностей и рекомендована фирмой производителем CML.

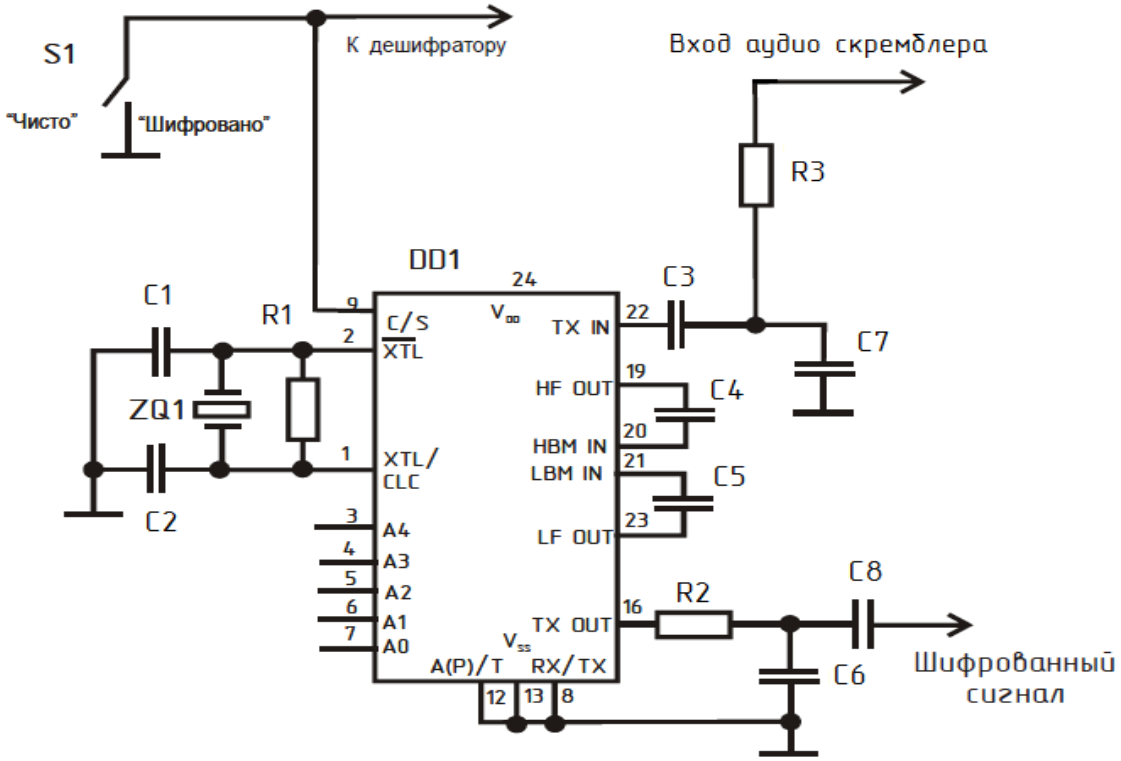

Рисунок 1.18 - Шифратор разработанного УЗРС.

Управление ИС осуществляется по входам (A0…A4) от генератора псевдослучайного изменяющегося кода (rollingcode), задающего последовательность изменяемых частот инверсии речевого спектра.

Схема включения ИС DD4 FX224 в режиме дешифрации (de-scramble) является типовой и каких-либо отклонений по отношению к рекомендациям фирмы-производителя CML не имеет.

Дешифрованный сигнал с выхода RxOUT (к.15) ИС DD4 через аналоговый переключатель DD9 поступает на вход ИС DD10 второго фильтра FX316J фирмы CML.

Фильтр FX316 (рисунок 1.19) представляет собой ИС с весьма низким энергопотреблением, созданную по КМОП технологии на базе переключаемых конденсаторов.

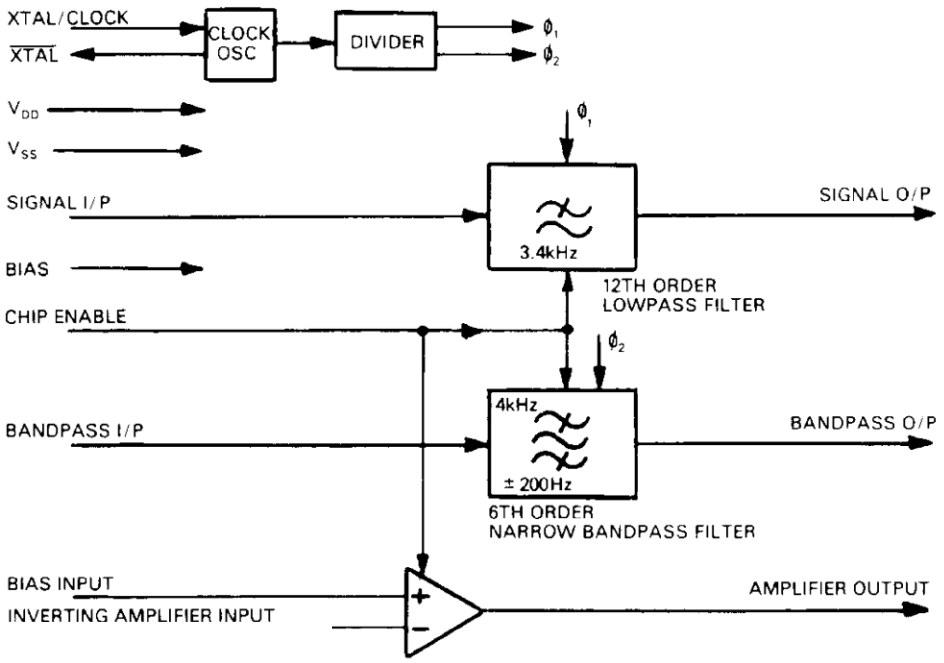

Рисунок 1.19 - Функциональная схема аудиофильтра FX316 фирмы CML.

В состав ИС входят:

1- фильтр НЧ 12-го порядка с частотой среза 3,4кГц и весьма низкими искажениями,

2- полосовой фильтр 6-го порядка на частоту 4±0,2 кГц,

3- независимый инвертирующий усилитель.

Фильтр полностью соответствует стандартам аналоговой сотовой связи NMT450, NMT900 и т.п. С помощью фильтра НЧ (12-го порядка!) этой ИС происходит достаточно эффективная фильтрация комбинационных и шумовых составляющих выходного аудиосигнала.

Встроенные генератор на частоту 1МГц (Xtal) и делитель частоты обеспечивают необходимые сигналы для работы НЧ и ПФ фильтров.

Альтернативным вариантом является использование внешнего тактового генератора через вход XT/CLC (Xtal/Clock).

Как уже указывалось выше, при смене комбинации частот (FSP,f_{c1} и f_{c2}) в динамических скремблерах появляются паразитные шумовые всплески сигнала, связанные с переходными процессами в фильтрах устройства.

Для устранения этого эффекта в разработанном УЗРС используется схема шумоподавителя на микросхемах DD5, (DD7…DD9), формирующая специальный стробирующий импульс (noiseblankingpulse).

Стробирующий импульс на время переходных процессов переключает выход аналогового ключа DD9 между дешифратором FX224 (DD4) и некоторым уровнем постоянного напряжения на время смены кодовой комбинации. Это время регулируется с помощью резистора R25 во времязадающей цепи таймера DD5. Уровень постоянного напряжения порядка 60мВ формируется в цепи смещения (V_{bias}) дешифратора DD4 и может быть изменении резистором R22.

В обычном режиме (Clear) за счет внутреннего резистора на входе C/S (к.9) шифратора DD1 на вход инвертора DD7.1 подается сигнал запрета формирования стробирующего импульса схемы шумоподавителя.

4.3.Функциональная и принципиальные схемы генератора псевдослучайной двоичной последовательности.

Сочетание цифровых и аналоговых методов позволяет довольно просто формировать псевдослучайные двоичные последовательности (ПСДП). Они имеют достаточно высокие статистические свойства.

Кроме очевидного использования в аналоговых и цифровых генераторах шума, ПСДП применяются для шифровки данных или сообщений. При этом ключ для дешифровки на приемной стороне выполняется посредством такого же генератора ПСДП, что и на передающей стороне.

ПСДП применяются и в кодах с обнаружением и исправлением ошибок, так как обеспечивают формирование блоков данных, в которых правильные сообщения становятся разделенными значительным расстоянием Хемминга [9].

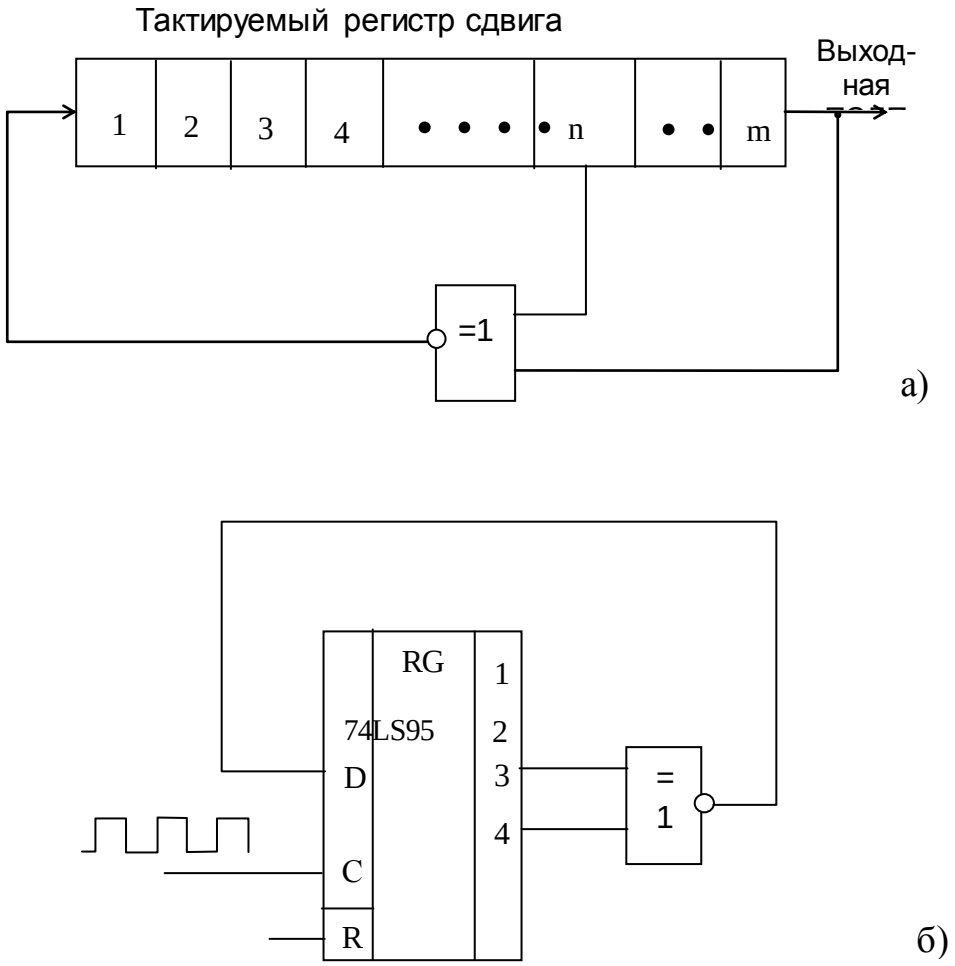

Рисунок 1.20 - Генератор псевдослучайной двоичной последовательности.

Наиболее распространенным и относительно простым генератором псевдослучайной двоичной последовательности (ГПСДП) является регистр сдвига с обратной связью ОС (рисунок 1.20,а).

Регистр сдвига, длинной m бит, синхронизируется фиксированной частотой f_o, а посредством логического элемента «исключающее ИЛИ» на его вход подается последовательный сигнал, являющей собой логическую сумму по модулю 2 n - го и последнего (m - го) разрядов регистра.

Такое выполнение регистра обеспечивает совокупностью состояний, которая в свою очередь устанавливается комбинациями битов в регистре после каждого тактового импульса. Причем комбинация повторяется через каждые К тактовых импульсов, обеспечивая цикличность работы генератора с периодом равным К.

Количество все возможных состояний m - разрядного регистра равно $K = 2^m$, то есть соответствует количеству двоичных комбинаций из m бит.

Однако, учитывая, что состояние регистра все "0" является запрещенным, число комбинаций будет равно

$$2^m - 1.$$

Получение последовательностей максимальной длины возможно лишь при правильном выборе значений m и n [10].

В качестве примера ниже приведена ПСДП 4 - разрядного регистра с обратной связью (рисунок 1.20,б)

1111	0100	1011
0111	0010	0101
0011	1001	1010
0001	1100	1101
1000	0110	1110

В данном случае имеется 15 различных состояний

$$(2^m - 1),$$

перебрав которые, последовательность формируется вновь и обладает наибольшей длиной.

Регистры сдвига максимальной длины выполняются и с применением и более двух точек для подключения ОС посредством логического элемента «исключающее ИЛИ», суммируя их по модулю два несколько битов.

Ниже приведена таблица 1.2 значений m, вплоть до 33, для построения генератора ПСДП которых достаточно двух точек соединения обратной связи, другими словами ОС берется с n - ой и m - ой ячейк.

При этом численные значения n и циклической длины, обеспечиваются числом периодов тактовой частоты.

Таблица 1.2

Число возможных состояний генератора ПСДП

m	n	Длина	m	n	Длина
3	2	7	18	11	262143
4	3	15	20	17	1048575
5	3	31	21	19	2097151
6	5	63	22	21	4194303
7	6	127	23	18	8388607
9	5	511	25	22	33554431
10	7	1023	28	25	268435455
11	9	2047	29	27	536870911
15	14	32767	31	28	2147483647
17	14	131071	33	20	8589934591

В ряде случаев n может иметь более одного значения; в любом случае вместо n можно взять m - n. То есть для схемы приведенной на рисунка 1.20,б возможно использовать точки подключения ОС при n = 1 и m = 4. Длина регистра обычно кратна 8. В этом случае требуется более двух точек подключения ОС.

Последовательности наибольшей длины обладают следующими свойствами:

- в одном полном цикле (К тактовых импульсов) число "1" на одну превышает число "0";

- в каждом цикле половину всех единиц составляют "одиночные", четвертую часть - "двойные" (т.е. две подряд), восьмую часть – тройные и т.д.;

Приведенные в [9-12] схемы генераторов обладают более высокими сервисными характеристиками, однако по принципу реализации ПСДП мало отличаются от рассмотренных выше.

Основным недостатком рассмотренных генераторов является тот факт, что они строятся на базе стандартных детерминированных логических элементов (регистров сдвига). Поэтому генерируемые ими ПСДП являются периодически повторяющимися и предсказуемыми.

Применение средств микропроцессорной техники принципиально дело не меняет, т.к. в данном случае аппаратная предсказуемость генераторов заменяется на программную. Достаточно просканировать (2-3) последовательных значения кода, чтобы с высокой степенью надежности предсказать следующие кодовые комбинации и таким образом дешифровать принятый сигнал. Широкое распространение мощных и быстродействующих портативных компьютеров и их компонентов является в данномслучае неблагоприятным фактором.

На рисунке 1.21 приведена схема генератора псевдослучайной последовательности, собранного на микросхемах DD1 и DD2.

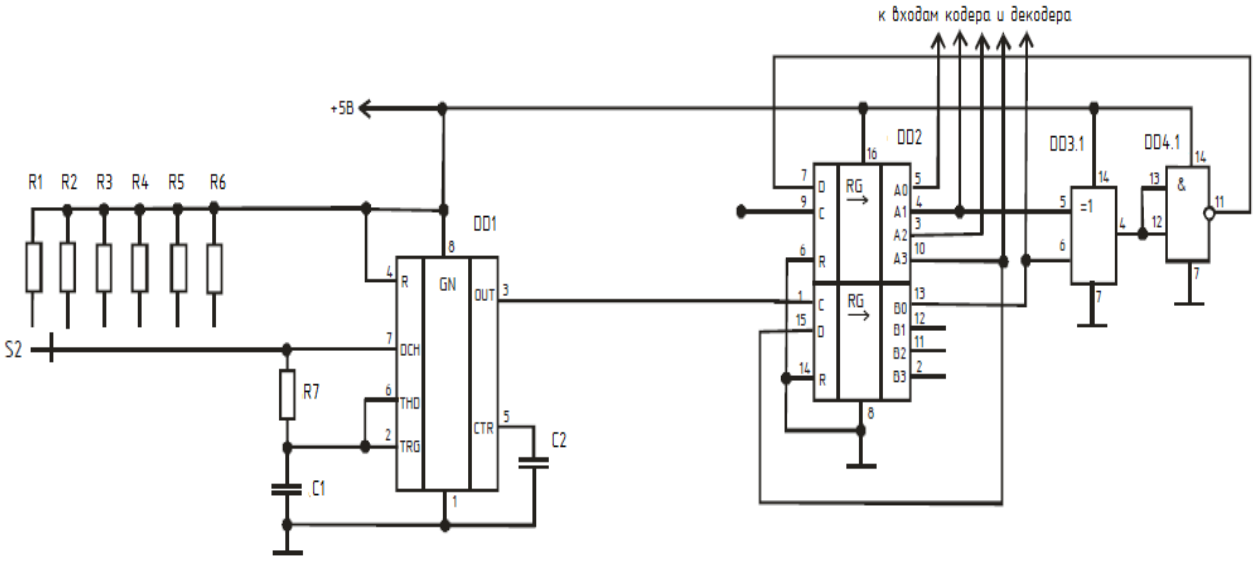

Рисунок 1.21 - Схема генератора псевдослучайной двоичной последовательности (ГПСДП).

Так как в памяти ROM микросхемы скремблера FX224 "прошиты" только 32 комбинации, а выбор их ведется с помощью 5-ти битового кода, для реализации

генератора была использована ИС DD2 регистра сдвига (2х4 разрядного) CD4015BC Fairchild Semiconductor.

В обратной связи регистра на элементах микросхем HD14070B Hitachi и CD4011BC Fairchild Semiconductor реализована схема "исключающее ИЛИ-НЕ". Изменяя точку подключения этого элемента к входам регистра можно удлинять или изменять кодовую последовательность для сменычастот инверсии сигнала.

Задающий генератор на ИС DD2 реализован на широко распространенной ИС (таймере NE555 National Semiconductor) в типовом ее включении. Выбором времязадающих резисторов R1 ÷ R6 возможно изменение частоты смены комбинаций частот инверсии спектра. Для выбранных значений резисторов они соответственно составят: 0,2-1; 0-3; 0-5;0-8,0-10,0 Гц.

Как уже указывалось выше, при работе в динамическом режиме (rollingcode) для правильной работы узлов шифрования/дешифрования (скремблеров FX224) необходима передача специальных синхронизирующих импульсов. Для выполнения этой функции в ИС скремблеров имеется специальный вход Enable/Mute (к.10).

По условию работы ИС вся необходимая информация будет передана в течение периода синхронизации, если на указанном входе будет присутствовать уровень логической "1". С учетом того, что данный вывод имеет внутренний резистор 1МОм, соединенный с шиной питания (pullup resistor) неприсоединение его к нулевой шине обеспечит заданный режим работы ИС скремблеров.

5. Экономический раздел

5.1.Экономическая эффективность разработанного устройства защиты речевых телефонных сообщений.

Выбор и обоснование базового варианта. Определение показателей экономической эффективности разработанного УЗРС базируется на сравнении его с базовым вариантом, адекватность которому является важнейшим фактором для определения количественных значений показателей эффективности. Следовательно, вопрос правильного выбора базового варианта имеет существенное значение для объективной оценки нового технического решения**.**

При выборе базы для сравнения необходимо руководствоваться двумя основными правилами:

- это может быть устройство, выполняющее те же основные функции, что и разработанное;

- должно быть выбрано современное и наиболее эффективное устройство. Только в этом случае, если показатели разработанного устройства выше, производство будет целесообразным.

На основе аналитического обзора Интернет- сайтов ведущих производителей бытовой РЭА, можно сделать вывод, что наиболее подходящим в качестве базового объекта является выпускаемый ОАО "Утес" (Ульяновский приборостроительный завод- www.utyos.ru) скремблер для трансиверов Q-MAC HF-90 (бескорпусной аналог скремблера "Орех-4130F" фирмы Анкад, г. Киев). Устройство Q-MAC HF-90 обеспечивает приемлемый уровень защиты речи, на основе переменной инверсии участков частотного спектра речи. Блок скремблера вставляется в корпус микрофона/динамика и обеспечивает скремблирование сигнала речи, прежде чем он будет направлен в передатчик, и восстановление сигнала речи при приеме, прежде чем он будет направлен в динамик, расположенный в корпусе микрофона.

Через щель на корпусе микрофона поворотом отверткой можно выбрать один из 16 используемых кодов. Переключатель на боковой стенке микрофона позволяет выбирать режимы работы со скремблированием или без него.

При подключении микрофона к трансиверу включается заранее выбранный код. Оба трансивера, участвующие в сеансе связи, должны иметь одно и то же положение переключателя кодов.

Сравнительный анализ базового и разработанного устройств показывает, что разработанное УЗРТС обладает следующими преимуществами:

- более широкими функциональными возможностями, т.к. обеспечивает защиту речи не только при передаче по радиоканалу, но и по телефонной линии;
- использование динамической смены комбинации кодов в процессе передачи по псевдослучайной последовательности существенно повышает защищенность (секретность) передаваемой информации;
-возможность изменения частоты смены 3-х частотной комбинации речевого спектра (6 вариантов) так же увеличивает секретность передаваемой информации;
- за счет синхронизации операций шифрования\дешифрования на передающей и приемной стороне повышается разборчивость речи.

Схемотехника разработанного УЗРТС реализована на современных специализированных ИС (допускающих SMD монтаж) и содержит современные малогабаритные радиокомпоненты.

На основании проведенных расчетов разработанного УЗРТС и паспортных данных на скремблер Q-MAC HF-90 можно составить сводную аналитическую таблицу (таблица 5.1) со сравнительными характеристиками технических и экономических показателей базового и разработанного устройств.

Это позволит комплексно оценить качество и эффективность разработанного УЗРТС.

Таблица 5.1

Основные технико-экономические показатели УЗРТС

Наименование Показателя	Количественное значение		Оценка
	Базовый вариант	Разработанный вариант	
1 Показатели технического уровня			
1 Число частот комбинации инверсии спектра	1	3	+
2 Число кодовых комбинаций инверсии спектра	16	32	+
3 Код последовательности комбинации частот	фиксированный	динамический	+
4 Синхронизация операций шифрации\дешифрации	да	да	0
5 Возможность шифрования по алгоритмам IDEA, ГОСТ, DES	да	нет	-
6 Вес и габариты, кг (длина х шир.)	0,36 125х71мм	0,2 75х60	+ +
7 Наработка на отказ, ч	18 тыс.	21 тыс.	+
2 Экономические показатели			
8 Трудоемкость изготовления, час.	6,34	2,36	+
9 Себестоимость изготовления, руб.	2345	1342	+
10 Оптовая цена, руб.	3050	1744	+

Снижение трудоемкости разработанного УЗРТС по сравнению со скремблер Q-MAC HF-90обусловлено использованием специализированных БИС большой степени интеграции и практическим отсутствием механических элементов конструкции. Приведенные в таблице 5.1 данные показывают, что разработанное УЗРС по основным показателям превосходит базовый образец. Это значит, что выпуск разработанного устройства будет эффективным.

Расчет экономической эффективности.Для расчета затрат на производство необходимо выбрать завод-изготовитель, условия и технологическая

оснащенность которого позволяют организовать выпуск разработанного УЗР ТС. На основании затрат на производство в выбранном цехе завода-изготовителя рассчитаем себестоимость и оптовую цену изделия.

На различных стадиях проектирования в зависимости от полноты исходной информации себестоимость изготовления может быть определена различными методами: по удельным весам, по типовой структуре производственных затрат, путем калькулирования и др.

Расчет себестоимости изделия путем калькулирования позволяет провести наиболее точный расчет цены УЗРС. Сущность данного метода заключается в последовательном расчете статей калькуляции.

Как уже указывалось, базовое изделие выпускается на ЗАО "Утес" (цех №12 Ульяновского приборостроительного завода). Спроектированное изделие ориентировочно так же будет размещено в этом цехе. Структура производства соответствует мелкосерийному производству.

Расчет себестоимости будем проводить исходя из сложившихся затрат по данному производству. Исходные данные для расчета:

1. Зарплата дополнительная $З_{доп}$ 10% от $З_{осн.}$
3. Расходы на содержание и эксплуатацию оборудования $У_{СО}$ 22,2% от $З_{осн}$
4. Отчисления в соц.страх $О_{сс}$ 35,6% от($З_{осн}$+$З_{доп}$)
5. Накладные общезаводские расходы $Н_{оз}$ 118,7% от $З_{осн}$
6. Накладные общецеховые расходы $Н_{оц}$ 78% от $З_{осн}$
7. Внепроизводственные расходы 6% от $С_{пр}$
8. Рентабельность 30% от $С_{п}$

Затраты по статье "Материалы основные" (таблица 5.2).

Количество паек, общий расход материалов взяты из приведенных ниже материалов по технологии изготовления и сборки УЗРС. Стоимость материалов взята из "Ведомости материальных затрат на изделия" по ЗАО "Утес" на 2004 год.При

составлении таблицы необходимо учесть нормативный расход материалов на 1 пайку:

Припой ПОС-61 ГОСТ 21193-76 0,00007 кг

Флюс ФСК ОСТ 470.033.200 0,00003 кг

Спиртово - бензиновая смесь 5977-72 ТУ 0,00001 кг

Таблица 5.2

Расчет затрат по статье "Материалы"

Наименование материалов	ГОСТ, ОСТ, ТУ	Кол-во паек, шт.	Норма на 1 пайку, кг	Цена за 1 кг, руб.	Вес, кг	Стоимость, руб.
Припой ПОС-61	21193-76	309	0,00007	290,0	0,0216	6,27
Флюс ФСК	70033.200	309	0,00003	310,0	0,0093	2,87
Спирт-бенз. смесь	5977-72	309	0,00001	43,6	0,0031	0,14
Лак УР-231	6-10-1547	-	-	83,8	0,025	2,10
Стеклотекстолит СФ2	10316-78	-	-	11,1 $дм^2$	1,12 $дм^2$	12,43
Итого:						23,81

Припой ПОС-61 может быть заменен на аналогичный низкотемпературный припой с предельной температурой плавления 260°С, а флюс ФСК- на любой флюс на основе древесной канифоли, не содержащий кислотных компонентов. Указанные расходы материалов для пайки являются усредненными как для ручных способов, так и для групповых (окунание в расплавленный припой, пайка "волной" и др.).

Расчет затрат по статье "Покупные изделия и полуфабрикаты".

Цены на радиокомпоненты взяты из "Ведомости покупных изделий, согласованных к поставке на 2014 год для товаров народного потребления" по ЗАО "Утес". Расчетные данные сведены в таблицу 5.3.

Таблица 5.3

Расчетные данные по ст."Покупные изделия и п\фабрикаты"

Наименование	ГОСТ, ТУ	Кол-во, шт.	Цена, руб.	Стоимость, руб.
Резисторы				
С2-23	ОЖ0.467.104	22	0,30	6,60
СП5-2ВБ	ОЖ0.468.559	3	27,00	81,00
Конденсаторы				
К10-17б	ОЖ0.460.172	24	3,90	93,60
К50-35	ОЖ0.464.214	1	1,10	1,10
Микросхемы				
LM741	National Sem.	2	4,70	9,40
FX224J	CML	2	213,50	427,00
NE555	National Sem.	2	5,92	11,84
FX306	CML	1	121,90	121,90
CD4015BC	Fairchild Sem.	1	5,13	5,13
CD4011BC	Fairchild Sem.	1	4,18	4,18
FX416J	CML	1	116,70	116,70
74HC4066	Philips	1	9,45	9,45
КнопкаВ170G		1	6,70	6,70
Переключа-тельВДМ-1-02	DIP	1	29,50	29,50
ДиодыКД522Б	ДР3.362.029	4	1,00	2,00
Разъем DRB-7MA	D-SUB	1	8,10	8,10
Резонаторы РК170БА		2	12,00	24,00
Плата печатная (пр-во)	ТГАС.ФТС.БР.004	1	75,0	75,0
Итого:				1033,20

Затраты по статье "Зарплата основная". Процесс изготовления разработанного УЗРТС разбит на технологические операции, порядок и содержание которых определены в "Типовых технологических процессах изготовления радиоэлектронной аппаратуры". Расход материалов определяется из "Типовых норм расхода материалов на электромонтажные работы".

Общемашиностроительные нормы времени ("Сборник типовых норм") определяют разряд рабочего, выполняющего ту или иную технологическую операцию, и время на её выполнение.

Порядок технологических операций при изготовлении разработанного УЗРТС:

а) формовка выводов резисторов и конденсаторов:

разряд рабочего- 3, количество элементов - 49. Время операции на 1 элемент 0,00416 ч, общее время операции-0,2038 ч.

б) формовка выводов аналоговых интегральных микросхем:

разряд рабочего- 3, количество элементов- 2. Время операции на 1 элемент- 0,00615 ч, общее время операции- 0,0123 ч.

в) обрезка выводов:

разряд рабочего - 3, количество элементов - 51. Время операции на 1 элемент - 0,00345 ч, общее время операции - 0,1760 ч.

г) покрытие печатной платы флюсом:

Разряд рабочего - 2, время операции на 1дм^2 платы- 0,0161 ч.

Площадь печатной платы S = 1,12 дм^2. Полное время операции - 0,0180 часа.

д) пайка печатной платы:

Разряд рабочего - 3. Время операции на одну пайку- 0,00367 ч.

Общее время операции- 1,1340 часа.

е) установка подстроечных резисторов, разъема, переключателя и кнопки:

Разряд рабочего - 3, количество элементов - 6. Время операции на 1 элемент - 0,033 ч,общее время операции- 0,1980 ч.

ж) формовка и пайка проводов:

разряд рабочего- 3, количество элементов - 7.

Время операции на 1 элемент - 0,01 ч, общее время операции - 0,070 ч.

з) настройка устройства:

Разряд рабочего - 5. В соответствии с классификацией сложности радиотехнических устройств, разработанное УЗРТС относится к 5Д группе сложности.

Отсюда, согласно "Типовым технологическим процессам", с учетом того, что

в разработанном устройстве имеется 3 подстроечных резистора, требующих регулировочных операций, время регулировки составит 0,42 часа.

и) установка печатной платы УЗРТС в корпус телефонного аппарата (радио гарнитуры):

Разряд рабочего- 3. Количество винтов - 4. Время операции на 1 элемент- 0,0113 ч, общее время операции - 0,0452 ч.

Полученные расчетные данные по статье "Зарплата основная" сведены в таблицу 5.4.

Таблица 5.4

Расчетные данные по статье "Зарплата основная".

Наименование технологической операции	Разряд рабочего	Трудоемкость операции, час	Тарифная ставка, руб./час	Прем-е доплаты, %	Общая стоимость работ, руб.
Формовка выводов резисторов, конденсаторов и резон.	3	0,2038	18,60	22	4,625
Формовка выводов аналоговых ИС	3	0,0123	18,60	22	0,279
Обрезка выводов	3	0,1760	18,60	22	3,994
Покрытие печатной платы флюсом	2	0,0180	16,20	20	0,350
Пайка печат. платы	3	1,1340	18,60	22	25,733
Установка подстроечных резисторов	3	0,1980	18,60	22	4,493
Формовка и пайка проводов	3	0,0700	18,60	23	1,588
Настройка печатной платы	5	0,4200	24,40	28	13,117
Покрытие платы лаком УР-231	2	0,0860	16,20	20	1,672
Установка платы УЗРС в корпус	3	0,0452	18,60	22	1,026
Итого:		2,3633			56,877

При составлении таблицы использованы данные по заработной плате ЗАО

"Утес" в 1 квартале 2014 г. с учетом поправочных коэффициентов к зарплате и действующих тарифов.

Зарплата дополнительная. Это сумма доплат к основной зарплате за не проработанное, но оплачиваемое согласно КЗоТу время: за отпуска, за выполнение гособязанностей, за сокращенный рабочий день и т.д.

$З_{доп}$= 56,88· 0,1 = 5,69 руб.

Отчисления на социальное страхование (единый социальный налог)

$О_{сс} = (З_{осн.}+З_{доп})\cdot У_{сс}/100$ = 62,57 · 0,356= 22,27 руб.

Накладные расходы на содержание и эксплуатацию оборудования

$Н_{со} = З_{осн}\cdot У_{со}$ = 56,88· 0,222= 12,63 руб.

Накладные общецеховые расходы

$Н_{оц} = З_{осн}\cdot У_{оц}$ = 56,88· 0,78 = 44,37 руб.

Цеховая себестоимость

$С_{ц}$ = М+ П+ $З_{осн.}$+ $З_{доп.}$+ $О_{сс}$ + $Н_{со}$ + $Н_{оц}$ = 23,81+ 1033,20+ 56,88+ 5,69+ 22,27+ 12,63+ 44,37 = 1198,85 руб.

Общезаводские расходы

$Н_{оз} = З_{осн}\cdot У_{оз}$ = 56,88 · 1,187 = 67,52 руб.

Производственная себестоимость

$С_{пр} = С_{ц} + Н_{оз}$ = 1198,85 + 67,52 = 1265,77 руб.

Внепроизводственные расходы

$В_{пр} = С_{пр}\cdot У_{впр}$ = 1265,77 · 0,06 = 75,95 руб.

Полная себестоимость изделия. Включает производственную себестоимость $С_{пр}$ и внепроизводственные расходы $В_{пр}$:

$С_{п} = С_{2} = С_{пр} + В_{пр}$ = 1265,77+ 75,95= 1341,72 ≈ 1342 руб.

Для комплексной технико-экономической оценки нового изделия рассчитаем его проектную оптовую цену $Ц_{опт}$.

Она больше полной себестоимости на величину прибыли Пр, которая определяется в зависимости от установленного уровня рентабельности Р в процентах от $С_{п}$.

$Ц_{опт} = С_п + Пр = С_п(1+Р) = 1341,72 \cdot 1,30 = 1744,24 \approx 1744$ руб.

Используя полученные данные, определим эффективность разработанного блока управления в сфере производства. Экономия условно - годовая в расчете на единицу составит

$Э_{г.у.пр.} = С_1 - С_2 = 2345 - 1342 = 1003$ руб.,

здесь $С_1$- себестоимость базового скремблера Q-MAC HF-90.

Выбранный в качестве изготовителя цех №8 ЗАО "Утес" (Ульяновский приборостроительный завод) предназначен для мелкосерийного производства. Цех имеет универсальное контрольно - измерительное и технологическое оборудование.

Аналогичность элементной базы, технологии производства и настройки, используемого технологического и испытательного оборудования, отсутствие специальных требований к квалификации персонала обеспечивают отсутствие капитальных затрат при замене выпускаемого скремблера Q-MAC HF-90 на разработанный (как более эффективный).

На 2014г. программа выпуска скремблера Q-MAC HF-90 составляет N = 650 штук. При указанной замене годовой экономический эффект ($\Delta К = 0$) составит

$Э_{э.пр} = N \cdot (С_1 - С_2) = 650 \cdot (2345 - 1342) = 651950$ руб.

Опираясь на результаты расчетов можно сделать вывод о целесообразности производства разработанного УЗРТС и рекомендовать его для замены менее эффективного скремблера Q-MAC HF-90. Дополнительные капиталовложения для этого не потребуются.

Годовой экономический эффект составит более 650 тыс. рублей при программе выпуска изделия 650 штук в год.

6.Безапасность жизнедеятельности.

6.1. Воздействие акустических колебаний на психоэмоциональное состояние работников.

Для интенсификации технологических процессов применяют различные физические факторы воздействия, в частности акустические колебания.

Акустические колебания частотой более 20 кГц называют ультразвуковыми колебаниями, а в диапазоне (15 – 20000) Гц - звуковыми, в то время как частоты значениями менее 15 Гц - инфразвуковыми.

Ультразвуковые колебания (УК) не отличается от слышимого человеком звука однако, при этом частотные колебания сопутствуют значительному затуханию колебаний из – за преобразования их энергии в тепловую.

По частоте колебаний ультразвук делится на:

- низкочастотный - $1{,}12*10^{4}$-$1{,}0*10^{5}$ Гц;
- высокочастотный - 1,0*10 -1,0*10 Гц,

а по характеру распределения - на воздушный и контактный ультразвук.

Действия УК на живые организмы определяется интенсивностью и длительности действия, а также от размеров тела.

Продолжительное и регулярное влияние ультразвука, приводит к функциональным нарушениям в нервной, сердечно - сосудистой и эндокринной системах, слухового и вестибулярного аппаратов человека.

Гигиенические нормативы ультразвука установлены ГОСТом 12.1.001 - 89 «Ультразвук».

Гигиенической характеристикой воздушных УК на рабочих позициях служат уровни звукового давления (дБ) в треть октавных полосах со среднегеометрическими частотными значениями в диапазоне(12,5÷100) кГц, что и проиллюстрировано в таблице 6.1.

Таблица 6.1

Допустимые уровни звукового давления на рабочих местах

Среднегеометрические частоты третьоктавных полос, кГЦ	Уровень звукового давления,дБ
12,5	80
16	80(90)
20	100
25	105
31,5-100	ПО

Инфразвук представляет собой акустические колебания с частотой ниже (16÷20) Гц. Причем на производстве инфразвук, обычно, комбинируется с низкочастотным (НЧ) шумом, а иногда и с НЧ вибрациями.

Длина инфразвуковой волны имеет большое значение, так на частоте 3,5 Гц она соответствует 100 метрам и обладает способностью проникновения в ткани организма человека. То есть человек как бы «слышит» инфразвук всем телом. Негативные последствия проникновения в тело человека инфразвука следующие.

Инфразвук с частотами ниже 16 Гц, обычно не воспринимаемый на слух. Опасным же является промежуток частот от 6 до 9 Гц. Психотропное же влияние сильнее всего сказывается на частоте 7 Гц, так как она соответствует ритму колебаний головного мозга. При этом умственная работа становится невозможной, из – за ощущения, что голова сиюминутно разлетится на части. Инфразвук не большой интенсивности приводит к тошноте и звону в ушах. Вместе с тем ухудшает зрительные восприятия и вызывает безотчетный страх. Инфразвук средней интенсивности приводит к расстройству пищеварительного тракта и порождает паралич, общую слабость, а в редких случаях слепоту. Мощный инфразвук обладает свойством полной остановки деятельности сердца. Установлено, что негативные ощущения чувствуются начиная со 120 дБ интенсивности, травмирующие воздействия - со 130 дБ, а инфразвук частотой около 12 Гц и интенсивности

(85÷110) дБ, формируют приступы морской болезни, головокружения. Колебания частотой (15÷18) Гц при той же интенсивности проявляются в виде чувства беспокойства, неуверенности, панического страха.

Гигиенические нормативы инфразвука производятся по санитарным нормам СН 2.2.4/2.1.8.583-96 «Инфразвук на рабочих местах, в жилых и общественных помещениях и на территории жилой застройки». Данные нормативы определяют предельно допустимые уровни звукового давления на различных рабочих местах, в жилых и общественных помещениях, а также на территориях жилой застройки (таблице 6.2)

Таблица 6.2

Предельно допустимые уровни инфразвука в октавных полосах частот со среднегеометрическими частотами (Гц) на рабочих местах и на территории жилой застройки.

Название помещений	**Уровни звукового давления, дБ**				**Общий уровень звукового давления,** $L_{лин}$, дБ
	2	**4**	**8**	**16**	
Производственное:					
работа различной степени тяжести	100	95	90	85	100
работа различной степени интеллектуально-эмоциональной напряженности	95	90	85	80	95
территория жилой застройки	90	85	80	75	90
помещения жилых и общественных зданий	75	70	65	60	75

Шум трактуют совокупностью различных апериодических звуковых колебаний различной интенсивности.

Сопутствующие человеку - индивидуму шумы, имеют различную интенсивность. Например речь – (50÷60) дБ, автомобильная сирена - 100 дБ, шум работающего двигателя легкового автомобиля - 80 дБ, громкая музыка - 70 дБ, шум движения трамвая – (70÷80) дБ, а наличие шума в жилой квартире –(30÷40) дБ.

По частотному значению определяются низко - (ниже 400 Гц), средне-(400÷1000)Гц и высокочастотные шумы (свыше 1000 Гц).

Нормируемые параметры шума на рабочих местах установлены ГОСТом 12.1.003 - 83* и Санитарными нормами СН 2.2.4/2.1.8.562 - 62 «Шум на рабочих местах, в помещениях жилых, общественных зданий и на территории жилой застройки».

Данные материалы классифицируют шумы по частотному спектру на широкополосные и тональные, в то время как по временным характеристикам - на постоянные и непостоянные.

Для определения постоянных шумов используют допустимые уровни звукового давления в девяти октавных полосах частот, которые устанавливаются по видам производственной деятельности работников.

Для приблизительной оценки в качестве характеристики постоянного широкополосного шума на рабочих местах принимают уровень звука, определенный по шкале А шумомера.

Непостоянные виды шумов классифицируются по времени на прерывистые и импульсные. Нормируемой характеристикой непостоянного шума служит эквивалентный по мощности уровень звуковых колебаний в дБ. Допустимые значения эквивалентных уровней непостоянных широкополосных шумов сведены в таблицу 6.3, причем для тонального и импульсного шума допустимый уровень звука на 5 дБ меньше значений, указанных в таблица 6 3.

При количественной оценке уровня шума разрешается применять дозу шума, так как теоретически определена линейная зависимость доза - эффект по временному смещению порога слуха. Такой дозовый подход обеспечивает оценку шумового воздействия на рабочих за трудовую смену.

Оценивать и предсказывать потери слуха, связанные с производственным шумом, позволяет стандарт ИСО 1999: (1975) «Акустика - определение профессиональной экспозиции шума и оценка нарушений слуха, вызванных шумом».

Таблица 6.3

Допустимые уровни звукового давления, уровни звука и эквивалентного уровня звука на рабочих местах в производственных помещениях и на территории предприятий (извлечение)

Рабочие места	Уровни звукового давления, дБ, в октавных полосах со среднегеометрическими частотами, Гц									Уровни звука и эквивалентные уровни звука, дБ
	31,5	63	125	**250**	500	1000	2000	4000	**8000**	
Помещения конструкторских бюро, расчётчиков, программистов вычислительных машин, лабораторий для теоретических работ	86	71	61	54	49	45	42	40	**38**	50
Помещения управления, рабочие комнаты	93	79	70	68	58	55	52	50	49	60
Кабины наблюдений и дистанционного управления:										
Без речевой связи по телефону	**103**	94	87	82	78	75	73	**71**	**70**	**80**
С речевой связью по телефону	96	83	74	68	63	60	57	55	54	65
Помещения и участки точной сборки, машинописные бюро	96	83	74	68	63	60	57	55	**54**	65

Помещения лабораторий для проведения экспериментальных работ, для размещения шумных агрегатов, вычислительных машин	107	94	87	82	78	75	73	71	70	80
Постоянные рабочие места и рабочие зоны в производственных помещениях и на территории предприятий	ПО	99	92	86	83	80	78	76	74	85

Возникающие в городской жилой застройки шумы по характеру проявления делятся на две большие группы. Первая - расположенные в свободном пространстве, вне жилых зданий и сооружений и вторая - находящиеся внутри зданий и сооружений (внутренние источники шума).

Источники шума, первой группы, по своему проявлению делятся на подвижные и стационарные.

Внутренние источники шума подразделяются в свою очередь на следующие под группы:

- техническая обеспеченность зданий, это лифты, вентиляционные системы, трансформаторные станции и так далее;
- технологическая оснащенность зданий и сооружений, в частности морозильные камеры магазинов, оборудование небольших мастерских и так далее;
- санитарная оснастка зданий и сооружений, например водопроводные и канализационные сети и т.д.;
- приборы бытового обихода, как то холодильники, пылесосы, стиральные машины и другие;

- электронная аппаратура для воспроизведения музыки, радио - и теле - приемники, музыкальные инструменты.

Шум транспорта по способу воздействия на окружающую среду относится к непостоянным внешним шумам, в виду того что его уровень изменяется во времени на пять и более децибел.

Уровни транспортных шумов определяются интенсивностью и составом транспортных потоков, профилем улиц, высотой и плотностью застройки, а также наличием элементов благоустройства, например типом дорожного покрытия проезжей части, зелеными насаждения и т.д. Имеется также зависимость уровней звука на дорогах от режимов движения транспорта времени суток.

Изменение колебаний между фоновыми и наибольшим уровнями звука, отображают шумовой режим около магистральной территории и в дневное время определяется значениями в (20÷30) дБ. В ночной период суток этот размах колебаний фона возрастает, что связано с интенсивностью движения, которая в это время уменьшается (2÷3) раза.

Интенсивный шум в условиях производства приводит к понижению внимания и возрастанию количества ошибок входе трудовой деятельности. Очень большое влияние шум оказывает на быстроту реакции, сбор информации и аналитические виды работ, из - за шума понижается производительность трудовой деятельности, а также понижается и качество проделанной работы. Воздействие шума препятствует своевременному восприятию работниками предупредительных сигналов внутрицехового транспорта, например автопогрузчиков, мостовых кранов, что приводит к несчастным случаям на производстве.

Шум оказывает влияние на весь организм человека. Он угнетает центральную – нервную систему, приводит к изменению дыхания и пульса, стимулирует нарушения обмена веществ, возникновению сердечно - сосудистых заболеваний, гипертонической болезни и ведет к профессиональным заболеваниям.

Обычно шум с уровнем звукового давления до (30÷35) дБ не тревожит человека, однако его повышение до (40÷70) дБ в условиях среды проживания формирует солидную нагрузку на нервную систему и вызывает понижение самочувствия, а

при длительном воздействии становится причиной неврозов. Воздействие шума уровнем свыше 75 дБ может привести к потере слуха - профессиональной тугоухости. Шум уровнем более 140 дБ приводит к поражению барабанных перепонок, контузии, а при более 160 дБ и к летальному исходу.

Научными исследованиями последних лет доказано, что под воздействием шума появляются изменения в органах зрения человека, которые приводят к понижению устойчивого и ясного видения и остроты зрения, изменению чувствительность к различным цветам и ряду других изменений. Также нарушается деятельность вестибулярного аппарата, функция желудочно - кишечного тракта, повышается внутричерепное давление, нарушаются обменные процессы в организме человека.

Прерывистый, импульсный шум понижает точность выполнения рабочих операций, прием и осмысление информации. В регламентирующих документах Всемирной организации здравоохранения особо уточняется, что наиболее негативно предрасположены к шуму следующие трудовые операции: слежение, сбор и обработка информации, творческое мышление.

В результате неблагоприятного воздействия шума на работающего человека происходит снижение производительности труда, увеличивается брак в работе, создаются предпосылки к происхождению несчастных случаев.

В области гигиенического нормирования наша страна первая и мире в 1956г. установила нормы по ограничению шума. Действующие в настоящее время нормативы шума на рабочих местах устанавливаются ГОСТом 12.1.003-83 «ССБТ. Шум Общие требования безопасности».

ЗАКЛЮЧЕНИЕ

В настоящее время обладание информацией имеет огромное значение для процессов экономического развития, хода конкурентной борьбы на национальном и международном рынках. Анализ различных способов получения информации о конкурентах указывает на то, что подслушивание телефонных переговоров служит эффективным методом несанкционированного получения конфиденциальной информации. В связи с этим защита (сокрытие) информации является актуальной задачей. Действенным методом защиты телефонных сообщений от несанкционированного доступа является их криптографическое преобразование. При этом в обыденной жизни весьма существенным фактором является соотношение затрат на защиту информации и стоимости секретов, которые таким образом защищены.

Использование в разработанном скремблере специализированных ИС FX224 фирмы CML обеспечивает частотную инверсию аудиосигнала с помощью меняющегося кода (rollingcode), формируемого генератором псевдослучайной последовательности (PRCG- Pseudo-RandomCodeGenerator). Кроме этого, возможность изменения частоты смены 3 - х частотной комбинации речевого спектра (6 вариантов) дополнительно увеличивает секретность передаваемой информации. Введение синхроимульсов в передаваемые сигналы обеспечивает синхронность операций шифрования\дешифрования на передающей и приемной стороне, за счет чего повышается разборчивость речи. Применение специализированных ИС активных фильтров 6-го и даже 12-го порядков обеспечивает выполнение весьма жестких требований аналоговой сотовой связи стандартов NMT, TASK и AMPS.

В экономическом разделе бакалаврской работы подтверждена эффективность производства разработанного устройства.

Разработанное устройство полностью соответствуют требованиям технического задания, а с учетом достигнутых характеристик, относительно малых аппаратурных затрат и высокой технологичности, можно полагать, что разработанное устройство будет конкурентоспособно на рынке систем защиты коммерческой и личной информации.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. С.В. Дворянкин, Д.В. Девочкин. Методы закрытия речевых сигналов в телефонных каналах// "Конфидент".- №5.- 1995.
2. В. Мочкин. Микроэлектронные устройства защиты речевой информации для радиостанций и телефонных аппаратов.// CHIP NEWS.- №5.- 1997.
3. В.В.Фомин, В.Н.Дудник, В.Е. Лепин и др. Способ кодирования речевых сигналов для устройств радио - и телефонной связи.// Сб. "Техника радиосвязи".- Вып.3.- 1997г.
4. Дж. Л. Месси. Введение в современную криптологию.//ТИИЭР, т.76, №5. – М.: Мир, 1988.- С.24-42.
5. У. Диффи. Первые десять лет криптографии с открытым ключом.//ТИИЭР, т.76, №5.– М.: Мир, 1988.- С.54-74.
6. А.В. Спесивцев и др. Защита информации в персональных компьютерах. – М., Радио и связь. 1992, с.140-149.
7. В. Жельников. Криптография от папируса до компьютера. – М.: ABF, 1996.
8. Hal Tipton and Micki Krause. Handbook ofInformation Security Management – CRC Press LLC, 1998.
9. Уитсон Дж. 500 практических схем на ИС. Пер. с англ.- М. : Мир, 1992.
10. Хоровиц П., Хилл У. Искусство схемотехники: В 2-х т. Пер. с англ.- М.: - Мир, 2006.
11. 750 практических электронных схем: Справочное руководство. Пер. с англ./Сост. и ред. Р.Фелпс.- М.: Мир, 1986.
12. Ленк Дж. Электронные схемы: Практическое руководство. Пер.с англ.- М.: Мир, 1985.
13. Основы эксплуатации радиоэлектронной аппаратуры/ А.К.Быкадоров, Л.И. Кульбак, В.Ю. Лавриненко и др.; Под ред. В.Ю.Лавриненко.- М.: Высшая школа, 1978.- 320с.
14. Андрианов В.И., Соколов А.В. Средства мобильной связи. – СПб.: BHV-Санкт-Петербург, 1998.- 256с.

15. Основы физики. Том 2. Колебания и волны квантовой физики. Учебное пособие под.ред. Б.М. Яворовского, А.А. Пинского - М: "Наука", 2001г.

16.Безопасность жизнедеятельности. Учебник для вузов под ред. В.В. Белова, А.В. Ильинской, А.Ф. Козьякова - М: Высшая школа, 1999г.

17.Материалы четвертой научно-практической конференции по экологии, состоявшейся 18-19 ноября 2004г. в г. Тольятти.

18.ГОСТ 12.1.029.- 80 (СТ СЭВ 1928 - 79) ССБТ. Средства и методы защиты от шума. Классификация.