А.М. Голиков

ОСНОВЫ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Учебное пособие

для специалитетета: 10.05.02 Информационная безопасность телекоммуникационных систем

Курс лекций, компьютерный практикум, задание
на самостоятельную работу
Второе издание дополненное и переработанное

Томск 2017

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
Томский государственный университет систем управления и радиоэлектроники

А.М. ГОЛИКОВ

ОСНОВЫ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Учебное пособие

для специалитетета: 10.05.02 Информационная безопасность телекоммуникационных систем

Курс лекций, компьютерный практикум, задание на самостоятельную работу

Второе издание дополненное и переработанное

Томск 2017

УДК 621.39(075.8)
ББК 32.973(я73)
Г 60
Голиков А.М.
Основы проектирования защищенных телекоммуникационных систем.
Учебное пособие для специалитета: 10.05.02 Информационная безопасность телекоммуникационных систем. Курс лекций, компьютерный практикум, задание на самостоятельную работу. Второе издание дополненное и переработанное / А.М.Голиков. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2017. – 402 с.: ил. — (Учебная литература для вузов)

Учебное пособие предназначено для направления подготовки специалистов по направлению 10.05.02 Информационная безопасность телекоммуникационныхсистем. Современные учебные курсы редко рассматривают комплексно вопросы проектирования защищенных телекоммуникационных сетей. Мало учебников и для комьютерной реализации реализации современных телекоммуникационных систем. Актуальность пособия велика, так как в современных системах связи и телевидения, а также кабельных сетях применяются все более сложные виды модуляции и кодирования, обеспечивающие высокую помехоустойчивость.

Методология изучения курса состоит в закреплении теоретических знаний на примерах компьютерной реализации современных телекоммуникационных систем и индивидуальных заданий на самостоятельную работу.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В учебном пособии рассмотрены основы проектирования защищенных телекоммуникационных, проектирование защищеннах инфокоммуникационных систем и копьютерный практикум: 1. проектирование защищенной IP-АТС на базе программного обеспечения ASTERISK; 2. проектирование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения VIPNET OFFICE; 3. проектирование защищенной многоточечной видеоконференц связи на базе WEB-технологии. Проектирование защищенных систем мобильной радиосвязи и компь.терный практикум: 1. системы мобильной связи стандартов GSM; 2. системы мобильной связи стандарта CDMA; 3. системы мобильной связи стандарта IEEE 802.11 (WiFi); 4. системы мобильной связи стандарта IEEE 802.15.4 ZigBee; 5. системы мобильной связи стандарта IEEE 802.15.1 (Bluetooth); 6. системы мобильной связи стандарта IEEE 802.16 (WiMAX); 6. системы мобильной связи стандарта IEEE 802.20 LTE. Проектирование защищенных ситем цифрового телевизионного вещания и компьютерный практикум: 1. системы цифрового наземного телевизионного вещания DVB-T; 2. системы цифрового спутникового телевизионного вещания DVB-S и системы высокоскоростного цифрового спутникового ТВ-вещания DVB-S2; 3. системы цифрового кабельного телевизионного вещания DVB-C и системы высокоскоростного цифрового кабельного ТВ-вещания DVB-C2; 4. системы цифрового мобильного телевизионного вещания DVB-H и системы высокоскоростного цифрового мобильного ТВ-вещания DVB-H2.

Задания на самостоятельную работу: 1. Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем; 2. Криптоанализ классических шифров; 3. Криптоанализ шифротекстов, полученных методом гаммирования; 4. Криптоанализ алгоритма RSA.

1. ОСНОВЫ ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ [1]

По функциональному принципу сети ЕСЭ разделяются на транспортные сети и сети доступа.

Транспортной является та часть сети связи, которая выполняет функции переноса (транспортирования) потоков сообщений от их источников из одной сети доступа получателям сообщений другой сети доступа.

Сетью доступа сети связи является та ее часть, которая связывает источник (приемник) сообщений с узлом доступа, являющимся граничным между сетью доступа и транспортной сетью.

Основные принципы системного подхода в области оптимального проектирования могут быть сформулированы следующим образом.

Система, состоящая из оптимальных частей, в общем случае не является оптимальной. Подмена оптимизации системы в целом оптимизацией по частям во многих случаях может привести к ошибочным выводам. Оптимизация по частям приведет к тем же результатам, что и оптимизация в целом, только в том случае, если параметры одной части системы не влияют на выбор параметров другой части, что на практике встречается относительно редко.

Оптимизация системы должна проводиться по количественно определенному и единственному критерию, который в математической форме отражает цель оптимизации. Критерий оптимальности, представленный в виде функции оптимизируемых параметров системы, называется целевой функцией Наличие нескольких критериев оптимальности, которые, как правило, тем или иным способом связаны между собой, не позволяет довести процесс до логического завершения, а отсутствие количественно определенного критерия свидетельствует о недостаточном понимании разработчиком поставленной перед ним задачи.

Система должна оптимизироваться в условиях количественно определенных ограничений на оптимизируемые параметры. Последнее обстоятельство свидетельствует о том, что оптимальность системы всегда относительна, условна, так как зависит от условий оптимизации. Поэтому условия оптимизации должны достаточно точно соответствовать реальная масса и т.д. **Внутренние параметры** описывают систему с точки зрения разработчика. Такими параметрами для систем передачи являются: вид модуляции, тип кода, число ступеней преобразования, тип применяемых элементов и т.д. Уравнения связи между внешними и внутренними

параметрами системы в аналитической форме, широко используемые в последующих главах, могут быть получены в результате:

1. Теоретических исследований (например, уравнения связи для помехозащищенности, пропускной способности, надежности и т.д.);

2. Технико-экономических расчетов (например, уравнения связи для стоимости, приведенных затрат и т.д.);

3. Аппроксимация экспериментальных зависимостей или эмпирических данных (например, уравнения связи для вероятности ошибки, разборчивости речевых сигналов и т.д.);

имитационного моделирования системы или ее подсистемы на ЭВМ (например, уравнения связи для параметров системы синхронизации в зависимости от характера ошибок или помехозащищенности в зависимости от гипа используемого кода).

Задание на проектирование составляется заказчиком совместно с генеральным проектировщиком, а по необходимости и с субподрядным и специализированными организациями на основе решений, принятых на этапе разработки технико-экономического обоснования (ТЭО).

В задании на проектирование указываются:

- наименование проектируемой линии и основания для ее проектирования и строительства новых или использования существующих сетевых узлов связи (СУС);
- направление линии передачи с указанием оконечных узловых и промежуточных пунктов, в которых должны выделяться каналы связи;
- виды и объем информации, подлежащей передаче (телефонная, телеграфная и факсимильная связь, передача данных, Интернет, электронная почта, передача газетных полос, телевидение и вещание, роуминг мобильной радиосвязи и т.п.), приведенных к общему числу каналов тональной частоты (КТЧ), основных цифровых каналов (01ДК) или цифровых потоков различной иерархии;
- предварительные рекомендации по выбору цифровых систем передачи, типа кабеля и источников их поставки;
- рекомендации по топологии сети, элементом которой будет проектируемая линия пер е дач и;
- требования по организации соединительных линий первичной сети и временных обходных связей на период освоения проектной мощности или завершения реконструкции;

- обоснование необходимости строительства технических и вспомогательных зданий, проектирования источников и сетей электро-, теплоснабжения и инженерных коммуникаций для них;

- требования к показателям надежности линии передачи и мероприятиям по их защите как от различного вида влияний, так и от несанкционированного доступа;

- взаимосвязь линии передачи с другими сооружениями ЕСЭ и ее составляющими;

- мероприятия на случай чрезвычайных ситуаций;

- требования по организации эксплуатации линии передачи, экологии

и охране окружающей среды;

предварительные сведения о сейсмичности, вечной мерзлоте, группе.

Основные этапы проектирования

При проектировании линии передачи решаются следующие задачи: Выбор трассы линии передачи.

Социально-экономическая характеристика оконечных и промежуточных пунктов.

Обоснование и расчет потребного количества каналов. Выбор системы передачи и типа кабеля. Размещение регенерационных пунктов и др.

Инженерный расчет показателей надежности ВОЛП

Исходные данные для расчета и основные расчетные соотношения

Требуемые показатели надежности (без резервирования) для местных (МПС), зоновых (ЗПС) и магистральных (СМП) участков первичной сети ЕСЭ РФ с максимальной протяженностью L_M приведены в табл. 1.1, 1.2 и 1.3 соответственно.

Таблица 1.1

Показатели надежности с протяженностью сети L_M = 200 км

Показатель надежности	Канал ТЧ или ОЦК независимо от применяемой системы передачи	Канал ОЦК на перспективной цифровой сети	АЛТ
Коэффициент готовности $K_г$	> 0,997	> 0,9994	0,9987
Среднее время между отказами $T_о$, ч	> 400	> 7000	> 2500
Время восстановления $T_в$, ч	< 1,1	< 4,24	См. примечание

0,985, а аппаратуры - 0,995. Тогда на подземной кабельной линии должны обеспечиваться следующие показатели:

- коэффициент готовности - не менее 0,985;
- среднее время между отказами - не менее 340,5 ч;
- среднее время восстановления - не более 5,2 ч;
- плотность повреждений - не более 0,1823.

Нормирование параметров цифровых каналов и трактов при проектировании СП и ЛП

Общие принципы нормирования. Основные определения

Каналы и тракты проектируемых линий передачи должны отвечать определенным требованиям, предъявляемым к их параметрам, основными из которых являются: мощность шумов и вероятность ошибки. Для нормирования параметров цифровых каналов и трактов используются номинальные цепи, представляющие собой цифровые тракты определенной длины с установленным количеством оконечного и промежуточного оборудования.

Основные нормируемые показатели качества функционирования цифровых каналов и трактов

К основные нормируемым показателям качества функционирования каналов и трактов относятся:

- верность передачи;
- задержка;
- фазовые флуктуации;
- проскальзывания,

Главный нормативный показатель - верность передачи.

Таблица 2. Максимальная продолжительность измерения коэффициента ошибок $K_{ош}$ в зависимости от скорости передачи f

f, кбит/с	$K_{ош}$				
	10^{-6}	10^{-8}	10^{-10}	10^{-12}	10^{-14}
64 (ОЦК)	16,0 с	26 мин	43,4 ч	180,8 сут	49,5 лет
2048 (ПЦТ)	0,5 с	48,8 с	1,4 ч	5,6 сут	1,5 года
34368 (ТЦТ)	30 мс	2,9 с	4,8 мин	8,1 ч	33,7 сут
155520 (СТМ-1)	6 мс	0,6 с	64,3 с	1,8 ч	7,4 сут
2488320 (СТМ-16)	0,4 мс	40 мс	4 с	6,7 мин	11,2 ч
39813120 (СТМ-256)	25 мкс	2,5 мс	0,25 с	25,1 с	41,9 мин

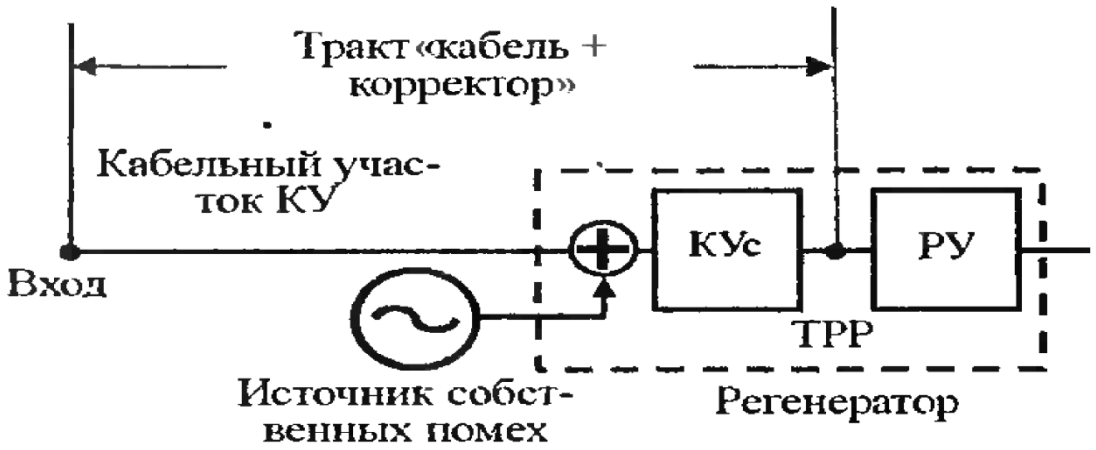


Рис. 1.1. Структурная схема участка регенирации

Расчет участков волоконно-оптической линии передачи

Длины участков на волоконно-оптической линии передачи (ВОЛП) следует выбирать возможно большими с тем, чтобы уменьшить количество необслуживаемых регенерационных пунктов (НРП). Максимальная длина участка рассчитывается цваждь.: исходя из потерь в физической среде передачи и в зависимости от дисперсионных свойств этой среды.

Основные параметры оптических воло*кон (ОВ) волоконно- оптических кабелей, используемых при проектировании ЛП, приведены в табл. 5.4, где приняты следующие обозначения: а - коэффициент затухания оптического волокна, дБ/км; AF - относительная полоса пропускания оптического волокна - его широкополосность, Мгц/км (^ля многомодовых волокон); Я -длина волны оптического излучения, мкм; а - коэффициент хроматической дисперсии оптического волокна, пс/нм-км (для одномодовых волокон).

ОВ, отвечающее рекомендации МСЭ-Т	λ_1, мкм	α, дБ / км	ΔF, МГц / км	σ, пс/нм·км
G.651	0,85 1,31	2,5…3,0 0,5…0,7	500 800	– –
G.652	1,31 1,55	0,35…0,5 0,22…0,25	- -	2,5…3,5 17…19
G.653	1,31 1,55	0,35…0,5 0,22…0,25	–	17…19 2,5…3,5
G.654	1,55	0,17…0,19	–	17…19
G.655	1,55	0,22…0,25	–	6…8

В техническом паспорте (сертификате) аппаратуры обычно указываются следующие параметры.

- Скорость п^едачи оптического сигнала B, Мбит/с.
- Длина волны источника излучения λ, мкм.
- Тип источника излучения.
- Ширина спектра источника излучения $\Delta\lambda$, мкм.
- Уровень излучаемой мощности $P_{ПЕР}$, дБм.
- Минимальный уровень приема $P_{ПР}$ б дБм.

Разность уровня передачи и минимального уровня приема называют энергетическим потенциалом системы

$$Э = P_{ПЕР} - P_{ПР\,МИН}$$

Для определения длины регенерационного участка составляется его расчетная схема, представленная на рис. 1.2.

На рисунке приняты следующие обозначения: ОС-Р — оптический соединитель разъемный; НРП — необслуживаемый регенерационный пункт; ППМ — приемопередающий оптический модуль, преобразующий оптический сигнал в электрический, восстанавливающий параметры последнего и преобразующий его в оптический (аппаратура окончания оптического тракта; ОС-Н — оптический соединитель неразъемный, ОВ — оптическое волокно. Как следует из рис. 5.4, затухание регенерационного участка равно

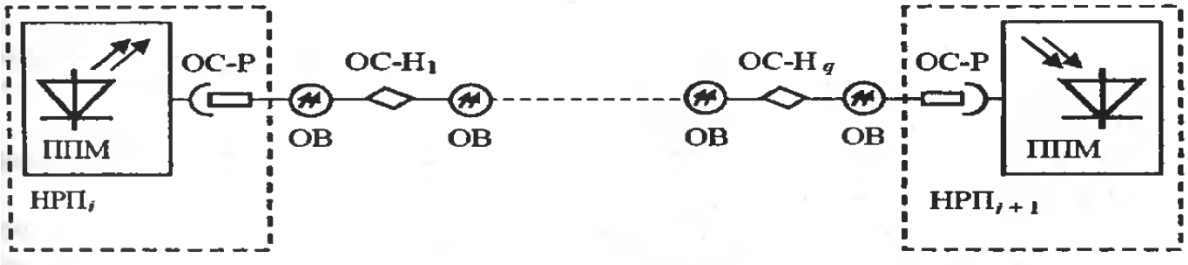


Рис. 1.2. Расчетная схема регенерационного участка ЦВОСП

№ п/п	Параметры	Обозначения	Единицы измерения	Значения параметра
1	Уровень мощности передачи оптического сигнала	$p_{пер}$	дБм	– 4
2	Минимальный уровень мощности приема оптического излучения	$p_{пр}$	дБм	– 35
3	Энергетический потенциал ЦВОСП	Э	дБ	31
4	Длина регенерационного участка	$l_{ру}$	км	24
5	Строительная длина оптического кабеля	$l_{стр}$	км	4
6	Количество разъемных соединений	$q_{рс}$	–	2
7	Затухание оптического сигнала на разъемном соединителе	$A_{р}$	дБ	0,5
8	Количество неразъемных соединений	q	–	7
9	Затухание оптического сигнала на неразъемном соединителе	$A_{нс}$	дБ	0,1
10	Коэффициент затухания оптического кабеля	α	дБ/км	0,7

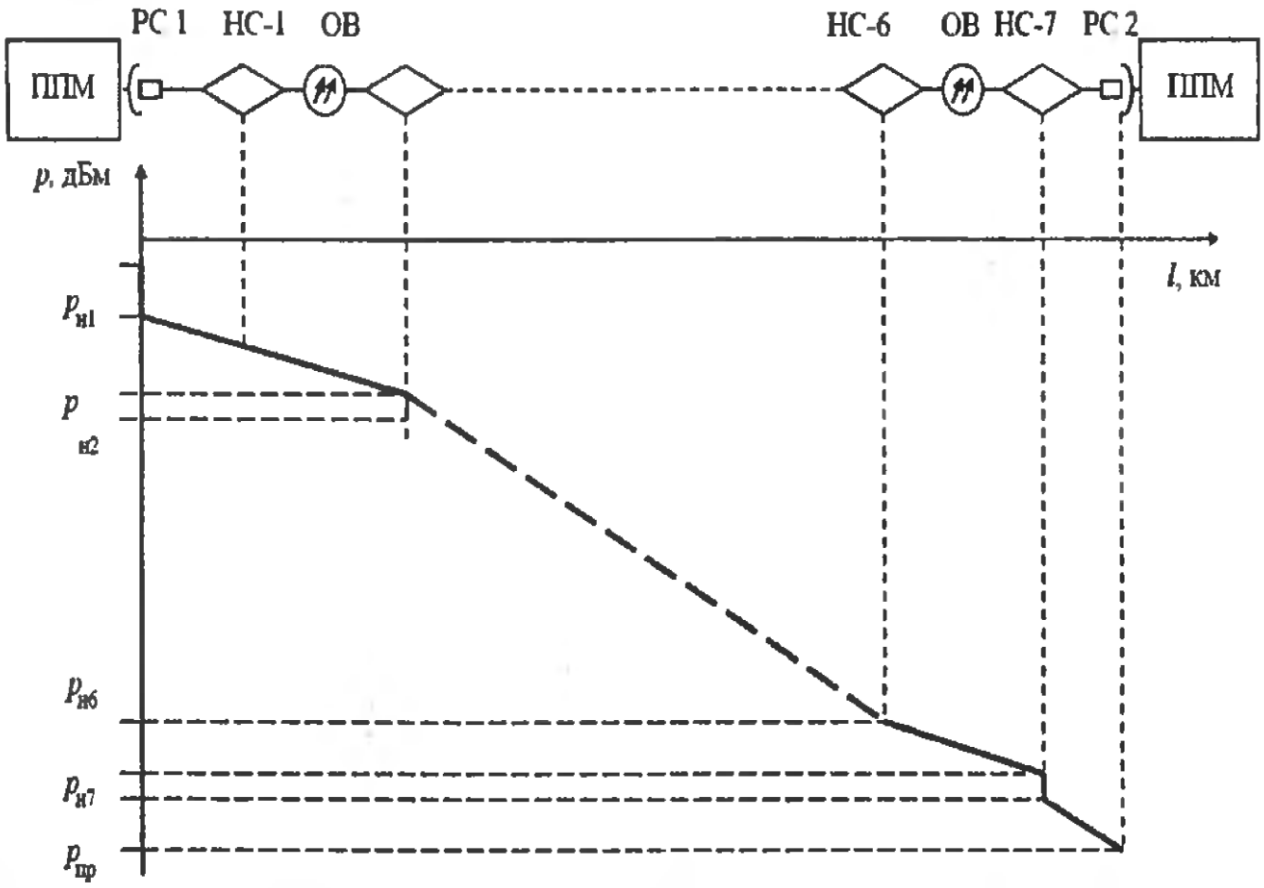


Рис.1.3. Диаграмма распределения энергетического потенциала

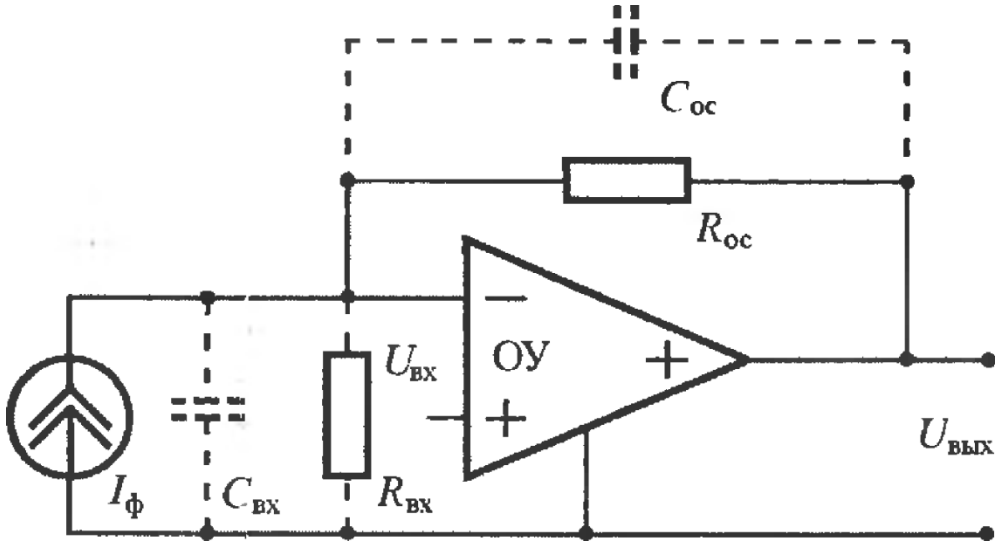


Рис. 1.4. Типовая схема усилителя фотодетектора

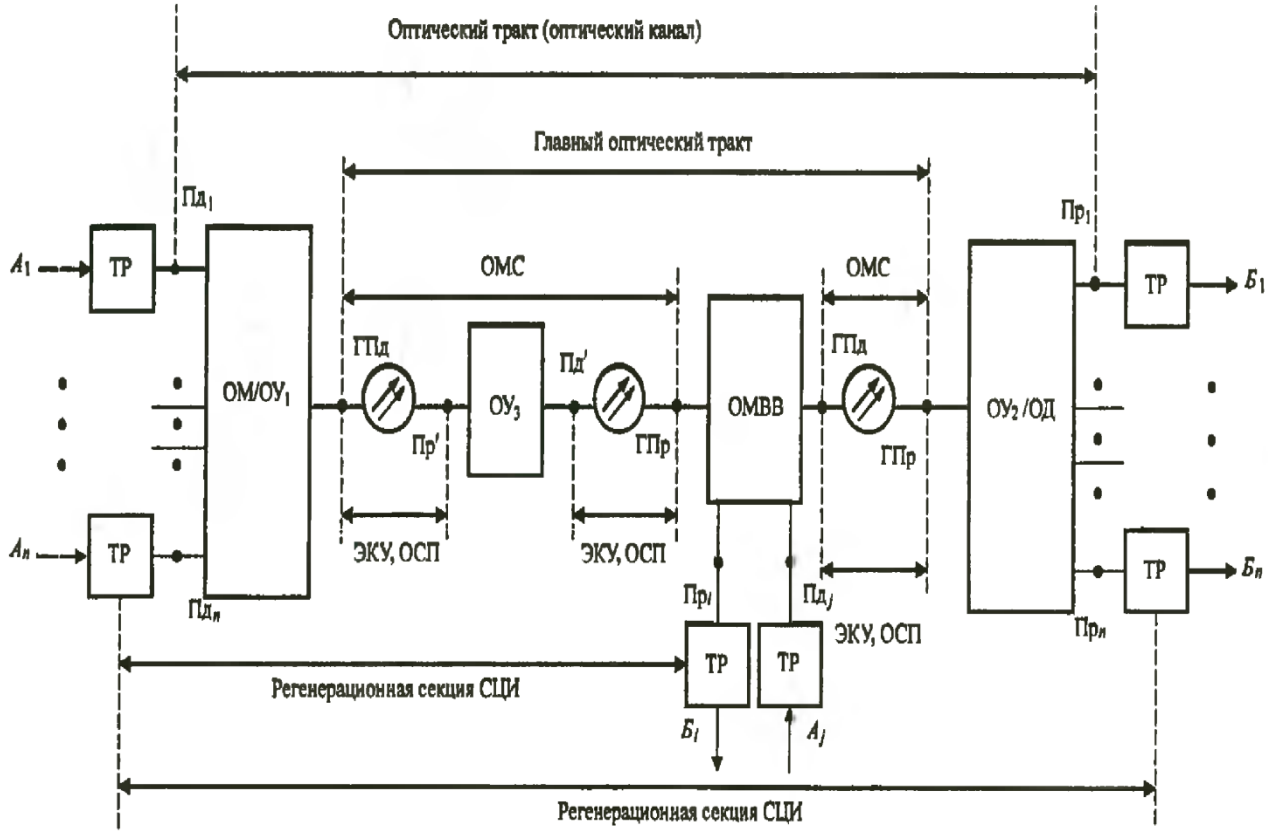


Рис. 1.5. Линейная сетевая структура ВОСП-СР (ВОЛС)

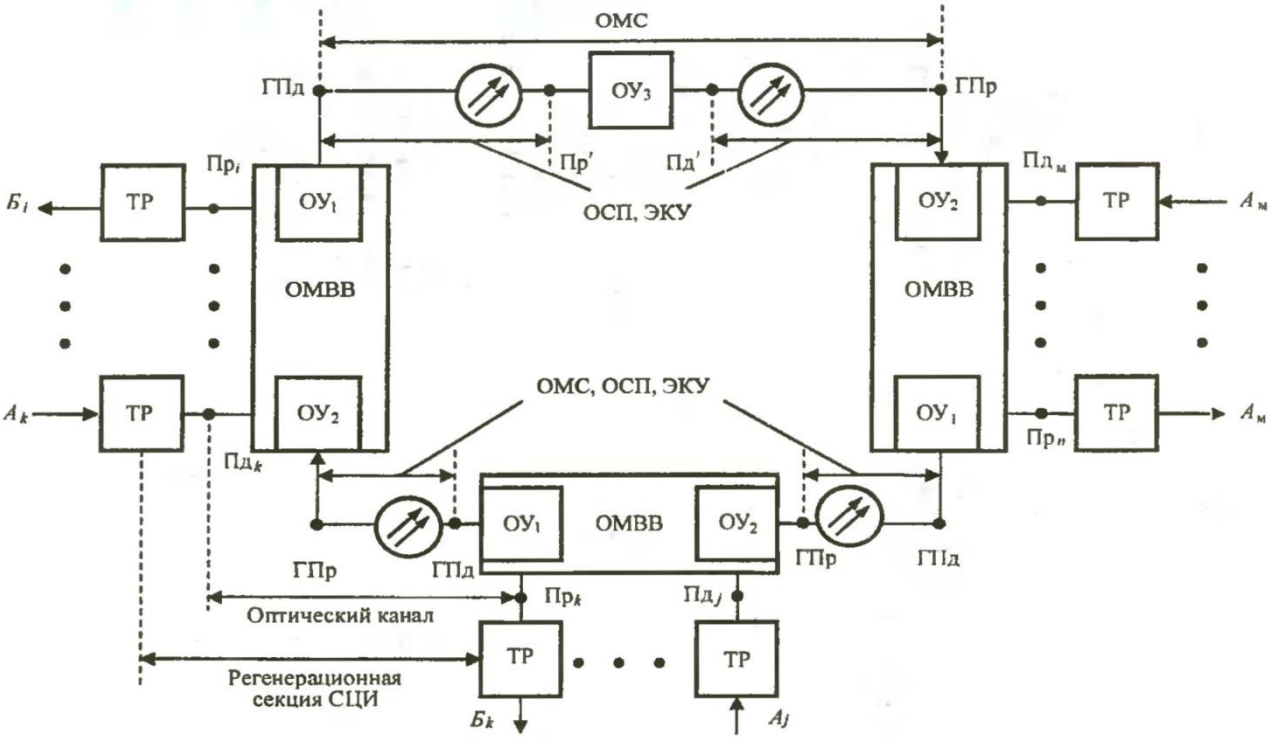


Рис. 1.6. Кольцевая структура ВОСП-СР (ВОЛС)

Система ВОСП-СР в основном нормируется по параметрам отиче- ского стыка на входах и выходах в соответствии с ОСТ 45.104 и перво г частью ОСТ 45.178 для одноканальных ВОСП. К нормируемым параметрам для каждого оптического канала дополни 1ельно относятся:

- центральная частота (длина волны) оптического канала;
- расстояние между оптическими каналами;
- отклонение центральной частоты оптического канала;
- ширина линии излучения лазера.

Кроме того, к нормируемым параметрам оптического стыка на границах ЭКУ (они являются общими для всех оптических каналов) добавляются также:

- отношение оптических сигнал-шум в каждом оптическом канале;
- суммарная мощность оптического излучения, вводимая в ОВ;
- перекрываемое затухание;
- суммарная дисперсия;
- оптическая переходная помеха между оптическими каналами,

максимум различия мощности в оптических каналах.

Центральная частота (длина волны) оптического канала определяется как центральная частота (длина волны) спектра оптического сигнала соответствующего оптического канала.

Расстояние между оптическими каналами определяется как разность между центральными частотами оптических каналов.

Отклонение нейтральной частоты оптического канала определяется как разность между номинальной и действительной центральными частотами оптического канала. При этом во внимание принимаются все процессы, ведущие к изменению частоты источника излучения при соответствующей скорости передачи сигнала в оптическом канале. К таким процессам относятся:

- импульсное смещение частоты источника излучения (чирп-эффект);
- влияние скорости передачи информационного сигнала;
- эффект расширения спектра сигнала за счет самомодуляции фазы;
- влияние температуры и старения.

Импульсным смешением частоты источника излучения называется изменение центральной частоты спектра источника излучения во время действия импульса, модулирующего ток накачки лазера.

Самомодуляция фазы — модуляция фазы оптического сигнала вызванная нелинейными эффектами в оптическом волокне при больших значениях мощности оптического сигнала.

Ширина линии излучения лазер— ширина спектра оптического излучения [1].

2. ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННАХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

2.1. Проектирование защищенной IP-АТС на базе программного обеспечения ASTERISK

Целью данной курсовой работы является проектирование АТС на основе протокола IP, на базе операционной системы Windows и программного обеспечения Asterisk. Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видеообщение по сети Интернет или любым другим IP-сетям. Организация сети телефонной связи сводится к таким вопросам как обеспечение качества услуг, предоставляемых абонентам, а так же защищенности конфиденциальной информации, которая может передаваться по речевым каналам. Для того чтобы начать проектирование такой системы, необходимо разработать ее структуру, зафиксировать основные функции, определить актуальные угрозы.

Аналитический обзор

VoIP: наведение мостов между традиционной и сетевой телефонией.

Хотя передача голоса по IP-протоколу (Voice over IP, VoIP) часто рассматривается как своего рода бесплатная междугородняя телефонная связь, настоящая ценность VoIP в том, что с его помощью голос становится всего лишь обычным приложением в сети передачи данных. Кажется, мы забыли о том, что назначение телефона – позволить людям общаться. Это простая цель на самом деле, и мы должны иметь возможность реализовывать ее намного более гибко и творчески, чем это предлагается сейчас. Поскольку отрасль продемонстрировала нежелание стремиться к данной цели, решением задачи занялись энтузиасты. Сложность состоит в том, что отрасль, которая практически не изменилась за последние сто лет, не проявляет особого интереса к этому и сейчас.

Проект телефонной связи Zapata (Zapata Telephony Project) был основан Джимом Диксоном, инженером-консультантом по связи. Его вдохновило невероятное увеличение частот ЦП (центрального процессора), которое в компьютерной отрасли сейчас уже воспринимается как должное. Диксон считал, что при наличии плат, включающих только базовые электронные компоненты, необходимые для взаимодействия с телефонной сетью, можно было бы создать намного более экономичные системы телефонной связи. Дорогие компоненты не нужны, потому что вся цифровая обработка сигнала (Digital Signal Processing, DSP – ЦОС) происходила бы в ЦП под управлением программного обеспечения. При этом нагрузка на ЦП сильно возросла бы, но Диксон был уверен, что низкая стоимость ЦП по

сравнению с их производительностью делает их применение намного более привлекательным, чем использование ЦОС, и, что еще более важно, соотношение цена/производительность продолжало бы улучшаться с повышением мощности ЦП. Как все мечтатели, Диксон верил, что эта идея откроется многим и ему просто надо подождать, пока кто-нибудь другой не реализует то, что он видел как очевидное усовершенствование. Но через несколько лет такие платы не только не были созданы, но, казалось, никто и не собирался ими заниматься. Тогда ему стало ясно, что если он хочет совершить революцию, то должен начинать ее самостоятельно. И родился проект телефонной связи Zapata.

Общие принципы IP-телефонии

Принципы пакетной передачи речи

«Классические» телефонные сети основаны на технологии коммутации каналов (рисунок 3.1), которая для каждого телефонного разговора требует выделенного физического соединения. Следовательно, один телефонный разговор представляет собой одно физическое соединение телефонных каналов. Основным недостатком телефонных сетей с коммутацией каналов является неэффективное использование полосы канала – во время пауз в речи канал не несет никакой полезной нагрузки.

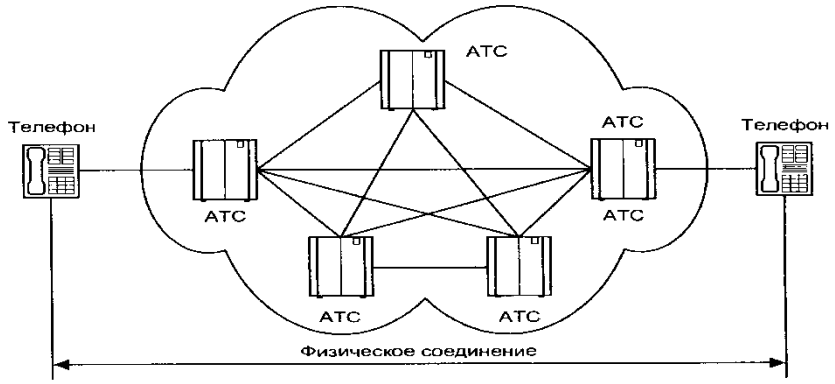


Рис. 2.1. Соединение в «классической» телефонной сети

Переход от аналоговых к цифровым технологиям стал важным шагом для возникновения современных цифровых телекоммуникационных сетей. Одним из таких шагов в развитии цифровой телефонии стал переход к пакетной коммутации. В сетях пакетной коммутации по каналам связи передаются единицы информации, которые не зависят от физического носителя. Такими единицами могут быть пакеты, кадры или ячейки (в зависимости от протокола), но в любом случае они передаются по разделяемой сети (рисунок 3.2), более того - по отдельным виртуальным каналам, не зависящим от физической среды. Каждый

пакет идентифицируется заголовком, который может содержать информацию об используемом им канале, его происхождении (то есть об источнике или отправителе) и пункте назначения (о получателе или приемнике).

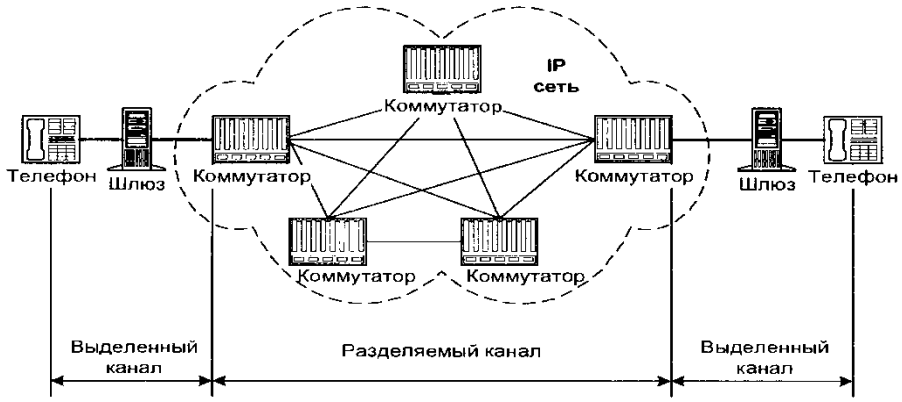


Рис. 2.2. Соединение в сети с коммутацией пакетов

В сетях на основе протокола IP все данные - голос, текст, видео, компьютерные программы или информация в любой другой форме - передаются в виде пакетов. Любой компьютер и терминал такой сети имеет свой уникальный IP-адрес, и передаваемые пакеты маршрутизируются к получателю в соответствии с этим адресом, указываемом в заголовке. Данные могут передаваться одновременно между многими пользователями и процессами по одной и той же линии. При возникновении проблем IP-сети могут изменять маршрут для обхода неисправных участков. При этом протокол IP не требует выделенного канала для сигнализации.

Процесс передачи голоса по IP-сети состоит из нескольких этапов [2-6].

На первом этапе осуществляется оцифровка голоса. Затем оцифрованные данные анализируются и обрабатываются с целью уменьшения физического объема данных, передаваемых получателю. Как правило, на этом этапе происходит подавление ненужных пауз и фонового шума, а также компрессирование.

На следующем этапе полученная последовательность данных разбивается на пакеты и к ней добавляется протокольная информация - адрес получателя, порядковый номер пакета на случай, если они будут доставлены не последовательно, и дополнительные данные для коррекции ошибок. При этом происходит временное накопление необходимого количества данных для образования пакета до его непосредственной отправки в сеть.

Извлечение переданной голосовой информации из полученных пакетов также происходит в несколько этапов. Когда голосовые пакеты приходят на терминал получателя, то сначала проверяется их порядковая последовательность. Поскольку IP-сети не гарантируют время доставки, то пакеты со старшими порядковыми номерами могут прийти

раньше, более того, интервал времени получения также может колебаться. Для восстановления исходной последовательности и синхронизации происходит временное накопление пакетов. Однако некоторые пакеты могут быть вообще потеряны при доставке, либо задержка их доставки превышает допустимый разброс. В обычных условиях приемный терминал запрашивает повторную передачу ошибочных или потерянных данных. Но передача голоса слишком критична ко времени доставки, поэтому в этом случае либо включается алгоритм аппроксимации, позволяющий на основе полученных пакетов приблизительно восстановить потерянные, либо эти потери просто игнорируются, а пропуски заполняются данными случайным образом.

Полученная таким образом (не восстановленная) последовательность данных декомпрессируется и преобразуется непосредственно в аудио-сигнал, несущий голосовую информацию получателю.

Таким образом, с большой степенью вероятности, полученная информация не соответствует исходной (искажена) и задержана (обработка на приёмной и передающей сторонах требует промежуточного накопления). Однако в некоторых пределах избыточность голосовой информации позволяет мириться с такими потерями.

Абонент, оплативший полосу 64 кбит/с, использует канал в среднем лишь на 25 %. Значит, оператор способен продать имеющийся у него ресурс в четыре раза большему числу пользователей, не перегружая свою сеть. Это выгодно обеим сторонам – и клиенту, и продавцу, - поскольку оператор увеличивает свои доходы и уменьшает абонентскую плату за счёт снижения издержек.

В настоящее время, в IP-телефонии существует два основных способа передачи голосовых пакетов по IP-сети:

- через глобальную сеть Интернет (Интернет-телефония);

- использую сети передачи данных на базе выделенных каналов (IP-телефония);

В первом случае, полоса пропускания напрямую зависит от загруженности сети Интернет пакетами, содержащими данные, голос, графику, а значит, задержки при прохождении пакетов могут быть самыми разными. При использовании же выделенных каналов исключительно для голосовых пакетов можно гарантировать фиксированную (или почти фиксированную) скорость передачи. Ввиду широкого распространения сети Интернет особый интерес вызывает реализация системы Интернет-телефонии, хотя в этом случае качество телефонной связи оператором не гарантируется.

Для того чтобы осуществить междугородную (международную) связь с помощью телефонных серверов, оператор услуги должны иметь по серверу в тех местах, куда и откуда

планируются звонки. Стоимость такой связи на порядок меньше стоимости телефонного звонка по обычным телефонным линиям.

Общий принцип действия телефонных серверов Интернет-телефонии таков: с одной стороны, сервер связан с телефонными линиями и может соединиться с любым телефоном мира. С другой стороны, сервер связан с Интернетом и может связаться с любым компьютером в мире. Сервер принимает стандартный телефонный сигнал, оцифровывает его (если он исходно не цифровой), значительно сжимает, разбивает на пакеты и отправляет через Интернет по назначению с использованием протокола IP. Для пакетов, приходящих из сети на телефонный сервер и уходящих в телефонную линию, операция происходит в обратном порядке. Обе составляющие операции (вход сигнала в телефонную сеть и его выход из телефонной сети) происходят практически одновременно, что позволяет обеспечить полнодуплексный разговор. На основе этих базовых операций можно построить много различных конфигураций. Например, звонок «телефон-компьютер» или «компьютер-телефон» может обеспечивать один телефонный сервер. Для организации связи телефон (факс)-телефон (факс) нужно два сервера.

С точки зрения масштабируемости (если отвлечься от проблем с неконтролируемым ухудшением качества при росте нагрузки на сеть) IP-телефония представляется вполне законченным решением. Во-первых, поскольку соединение на базе протокола IP может начинаться (и заканчиваться) в любой точке сети от абонента до магистрали. Соответственно, IP-телефонию в сети можно вводить участок за участком, что, кстати, на руку и с точки зрения миграции, так как ее можно проводить «сверху вниз», «снизу вверх» или по любой другой схеме. Для решений IP-телефонии характерна определенная модульность: количество и мощность различных узлов - шлюзов, gatekeeper («привратников» - так в терминологии VoIP именуются серверы обработки номерных планов) - можно наращивать практически независимо, в соответствии с текущими потребностями.

Межсетевой протокол IP

В настоящее время наиболее эффективная передача потока любых дискретных (цифровых) сигналов, в том числе и несущих речь (голос), обеспечивается цифровыми сетями электросвязи, в которых реализована пакетная технология IP.

Протокол IP – основной протокол сетевого уровня, позволяющий реализовывать межсетевые соединения.

Следует подчеркнуть, что протокол IP реализуется не только в глобальной сети Интернет, для которой он был первоначально разработан, он может быть применен и в других цифровых телекоммуникационных сетях.

Основным сдерживающим фактором на пути масштабного внедрения IP-телефонии является отсутствие в протоколе IP механизмов обеспечения гарантированного качества услуг, что делает его пока не самым надежным транспортом для передачи голосового трафика. Протокол IP обрабатывает каждый IP-пакет как независимую единицу, не имеющую связи ни с какими другими IP-пакетами. Сам протокол IP не гарантирует доставку пакетов, а также время их доставки, что вызывает такие проблемы, как «рваный голос» и просто провалы в разговоре. В протоколе IP нет механизмов, обычно применяемых для увеличения достоверности конечных данных: отсутствует квитирование – обмен подтверждениями между отправителем и получателем, нет процедуры упорядочения, повторных передач или других подобных функций. Если во время продвижения пакета произошла какая-либо ошибка, то протокол IP по своей инициативе ничего не предпринимает для исправления этой ошибки. Например, если на промежуточном маршрутизаторе пакет был отброшен по причине истечения времени жизни или из-за ошибки в контрольной сумме, то модуль IP не пытается заново послать испорченный или потерянный пакет. Все вопросы обеспечения надежности доставки данных по составной сети в стеке TCP/IP решает протокол TCP, работающий непосредственно над протоколом IP.

IP-адрес

Администратор сети присваивает оконечным устройствам IP-адреса в соответствии с тем, к каким IP-сетям они подключены. Для IP-адреса первоначально выбрали размер в 32 бита для удобства его обработки в 32 – разрядном регистре компьютера. Для обеспечения свойства иерархичности адрес содержит две части: номер сети и номер узла (рисунок 2.3). Число бит, отводимых для этих номеров, может быть переменным.

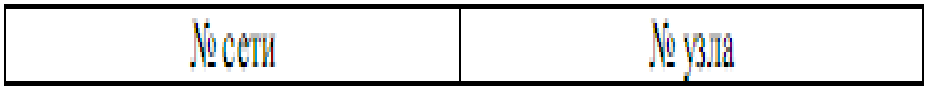


Рис. 2.3. Структура IP-адреса

Для того, чтобы можно было присваивать адреса и малым и большим сетям, ввели несколько классов адресов: A, B, C (рисунок. 2.4).

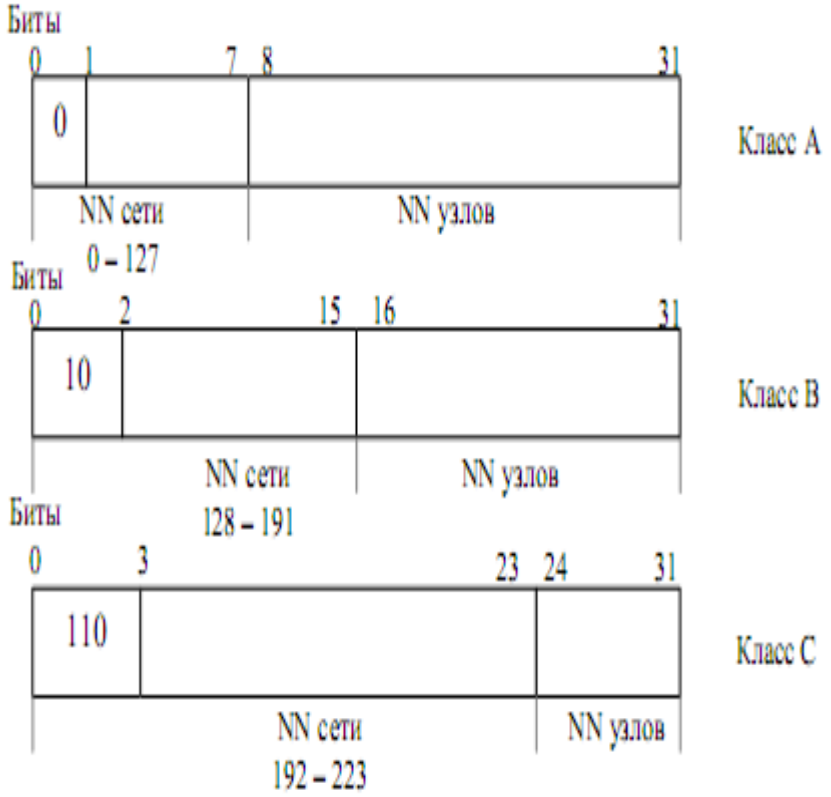


Рис. 2.4. Адреса класса A, B, C

1. Адреса класса A предназначены для организации очень больших сетей. Они обязательно начинаются с 0. Всего таких сетей 128. В каждой из них может быть 16777216 (2^{24}) адресов станций (узлов) и их объем составляет 50 % от общего количества всех IP-адресов.

2. Адреса класса B тоже дают возможность организовать достаточно большие сети в диапазоне номеров 128 – 191. Здесь под номер сети отводится уже два байта. Число сетей здесь – 2^{14} = 16384, а максимальное число узлов в сети – 2^{16} = 65536. Объем адресов класса B составляет 25 %.

3. Адреса класса C содержат три байта для номера сети и один байт для номера узла. Следовательно в одной сети класса C может быть не более 2^{8} = 256 адресов, а таких сетей довольно много – 2^{21} = 2097152. Сети класса C – это небольшие сети.

Кроме классов A, B, C существуют специальные классы D и E. Адреса класса D (224 – 239) используются для многоадресных рассылок в IP-сетях, когда одно сообщение распространяется среди группы разбросанных по сети станций. Адреса класса E(240 – 255) составляют резерв, который может использоваться в экспериментальных целях.

Описание основных протоколов систем IP-телефонии

Стандарт H.323

Набор рекомендаций МСЭ-Т H.323 определяет сетевые компоненты, протоколы и процедуры, позволяющие организовать мультимедиа-связь в пакетных сетях, в том числе в ЛВС Ethernet. Они определяют порядок функционирования абонентских терминалов в сетях с разделяемым ресурсом, не гарантирующих качества обслуживания QoS. H.323-совместимые устройства могут применяться для телефонной связи (IP-телефония), передачи звука и видео (видеотелефония), а также звука, видео и данных (мультимедийные конференции).

В связи с появлением множества аппаратно-программных средств организации телефонной связи по протоколу IP потребовалось внести изменения в спецификации H.323, так как эти средства зачастую оказывались несовместимыми друг с другом. В частности, понадобилось обеспечить взаимодействие телефонных устройств на базе ПК и обычных телефонов для сетей, функционирующих по принципу коммутации каналов. Стандарт H.323 входит в семейство рекомендаций H.32x, описывающих порядок организации мультимедиа-связи в сетях различных типов:

- H.320 - узкополосные цифровые коммутируемые сети, включая -ISDN;
- H.321 - широкополосные сети ISDN и ATM;
- H.322 - пакетные сети с гарантированной полосой пропускания;
- H.324 - телефонные сети общего пользования (ТфОП).

Одна из основных целей разработки стандарта H.323 - обеспечение взаимодействия с другими типами сетей мультимедиа-связи (рисунок 3.1). Данная задача реализуется с помощью шлюзов, осуществляющих трансляцию сигнализации и форматов данных. Стандарт H.323 позволяет создать надежные решения для организации коммуникаций по ненадежным сетям с переменной задержкой. При условии соответствия стандарту устройства с различными возможностями могут и взаимодействовать друг с другом. Например, терминалы с видео средствами могут участвовать в аудиоконференции. В совокупности с другими стандартами МСЭ-Т на мультимедийную связь и телеконференции рекомендации H.323 применимы для любых видов соединений - от многоточечных до соединений «точка-точка». Основные компоненты этого стандарта приведены в таблице 2.1.

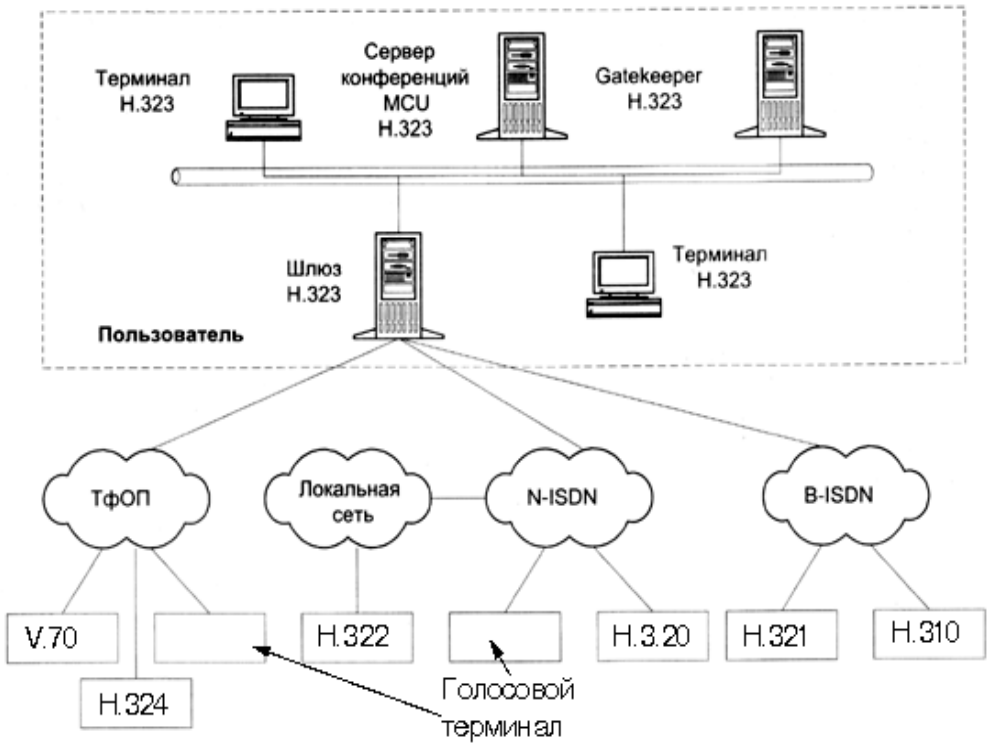


Рис. 2.5. Конфигурация сети на базе стандарта H.323

Стандарт H. 323 определяет также порядок взаимодействия с оконечными устройствами других стандартов. Наиболее часто такая задача возникает при сопряжении телефонных сетей с коммутацией пакетов и коммутацией каналов. Сети стандарта H.323 совместимы и с другими типами H.32x-сетей. Межсетевое взаимодействие различных H.32x-сетей определяет рекомендация H.246. На следующем этапе развития IP-телефонии к спецификациям H.323, соответствующим нижним уровням эталонной модели взаимодействия открытых систем (ЭМВОС), будут добавлены новые. Они зафиксируют возможности обеспечения классов (class-of-service, CoS) и качества обслуживания (quality-of-service, QoS), т. е. услуг, относящихся, соответственно, ко второму (канальному) и третьему (сетевому) уровням.

Таблица 2.1 – Основные компоненты стандарта H.323

Рекомендация	Описание
H.225	Определяет сообщения по управлению вызовом, включая сигнализацию и регистрацию, а также пакетизацию и синхронизацию потоков мультимедийных данных

H.245	Определяет сообщения для открытия и закрытия каналов для передачи потоков мультимедийных данных, а также другие команды и запросы
H.261	Видеокодек для аудиовизуальных сервисов на каналах P x 64 кбит/с
H.263	Описывает новый видеокодек для передачи видео по обычным телефонным сетям
G.711	Аудио кодек, 3,1 кГц на 48, 56, и 64 кбит/с
G.722	Аудио кодек, 7 кГц на 48, 56, и 64 кбит/с
G.728	Аудио кодек, 3,1 кГц на 16 кбит/с
G.723	Аудио кодек, для режимов 5,3 и 6,3 кбит/с
G.729	Аудио кодек

Протокол инициирования сеансов связи – SIP

Принципы протокола SIP

За годы работы с протоколом H.323 накоплен большой опыт использования, который позволил выявить как его положительные черты, так и недостатки, которые были учтены при разработке протокола SIP.

Протокол инициирования сеансов – Session Initiation Protocol (SIP) является протоколом прикладного уровня и предназначается для организации, модификации и завершения сеансов связи: мультимедийных конференций, телефонных соединений и передачи данных. Пользователи могут принимать участие в существующих сеансах связи, приглашать других пользователей и быть приглашенными ими к новому сеансу связи.

Приглашения могут быть адресованы определенному пользователю, группе пользователей или всем пользователям.

Протокол SIP разработан группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF (Internet Engineering Task Force), а спецификации протокола представлены в документе RFC 2543.

В основу протокола рабочая группа MMUSIC заложила следующие принципы:

- *Персональная мобильность пользователей.*

Пользователи могут перемещаться без ограничений в пределах сети, поэтому услуги связи должны предоставляться им в любом месте этой сети. Пользователю присваивается уникальный идентификатор, а сеть предоставляет ему услуги связи вне зависимости от того,

где он находится. Для этого пользователь с помощью специального сообщения – REGISTER – информирует о своих перемещениях сервер определения местоположения.

- *Масштабируемость сети.*

Она характеризуется, в первую очередь, возможностью увеличения количества элементов сети при ее расширении. Серверная структура сети, построенной на базе протокола SIP, в полной мере отвечает этому требованию.

- *Расширяемость протокола.*

Она характеризуется возможностью дополнения протокола новыми функциями при введении новых услуг и его адаптации к работе с различными приложениями.

Расширение функций протокола SIP может быть произведено за счет введения новых заголовков сообщений. При этом, если SIP-сервер принимает сообщения с неизвестными ему полями, то он просто игнорирует их и обрабатывает лишь те поля, которые он знает.

Для расширения возможностей протокола SIP могут быть также добавлены и новые типы сообщений.

- *Интеграция в стек существующих протоколов Internet, разработанных IETF.*

Протокол SIP является частью глобальной архитектуры мультимедиа, разработанной комитетом IETF. Эта архитектура включает в себя также протокол резервирования ресурсов (Resource Reservation Protocol - RSVP), транспортный протокол реального времени (Real-Time Transport Protocol - RTP), протокол передачи потоковой информации в реальном времени (Real-Time Streaming Protocol - RTSP). Однако функции протокола SIP не зависят ни от одного из этих протоколов.

- *Взаимодействие с другими протоколами сигнализации.*

Протокол SIP может быть использован совместно с протоколом H.323. Возможно даже взаимодействие протокола SIP с системами сигнализации ТфОП – DSS1 и ОКС7. Для упрощения такого взаимодействия сигнальные сообщения протокола SIP могут переносить не только специфический SIP-адрес, но и телефонный номер формата E.164 или любого другого формата.

Интеграция протокола SIP с IP-сетями

Одной из важнейших особенностей протокола SIP является его независимость от транспортных технологий. Но, в то же время, предпочтение отдается технологии маршрутизации пакетов IP и протоколу UDP. При этом, правда, необходимо создать дополнительные механизмы для надежной доставки сигнальной информации. К таким механизмам относятся повторная передача информации при ее потере, подтверждение приема и др.

Здесь же следует отметить то, что сигнальные сообщения могут переноситься не только протоколом транспортного уровня UDP, но и протоколом TCP. Протокол UDP позволяет быстрее, чем TCP, доставлять сигнальную информацию (даже с учетом повторной передачи неподтвержденных сообщений), а также вести параллельный поиск местоположения пользователей и передавать приглашения к участию в сеансе связи в режиме многоадресной рассылки.

Таблица 2.2. Место протокола SIP в стеке протоколов TCP/IP

Протокол инициирования сеансов связи (SIP)	Прикладной уровень
Протоколы TCP и UDP	Транспортный уровень
Протоколы IPv4 и IPv6	Сетевой уровень
PPP, ATM, Ethernet	Уровень звена данных
UTP5, SDH, PDH, V.34 и др	Физический уровень

По сети с маршрутизацией пакетов IP может передаваться пользовательская информация практически любого вида: речь, видео и данные, а также любая их комбинация, называемая мультимедийной информацией. При организации связи между терминалами пользователей необходим механизм обмена информацией о том, какие сервисы может использовать вызываемая\вызывающая стороны. Для этой цели используется протокол SDP (Session Description Protocol) - протокол описания сессии. Данный протокол позволяет определить, какие звуковые (видео и другие) кодеки и иные возможности может использовать удаленная сторона.

Для передачи речевой информации комитет IETF предлагает использовать протокол RTP (Real-time Transport Protocol, протокол транспортировки в реальном времени). Таким образом, сам протокол SIP непосредственного участия в передаче голосовых, видео и других данных не принимает, он отвечает только за установление связи (по протоколам SDP, RTP и др.), поэтому под SIP-телефонией понимается не передача голоса по протоколу SIP, а передача голоса с использованием протокола SIP. Использование протокола SIP предоставляет новые возможности установления соединений (а также возможность беспроблемного расширения данных возможностей), а не непосредственной передачи голосового и других видов трафика.

В глобальной информационной сети Интернет уже довольно давно функционирует экспериментальный участок Mbone, который образован из сетевых узлов, поддерживающих

режим многоадресной рассылки мультимедийной информации. Важнейшей функцией Mbone является поддержка мультимедийных конференций, а основным способом приглашения участников к конференции стал протокол SIP. Протокол SIP дает возможность присоединения новых участников к уже существующему сеансу связи, т.е. двусторонний сеанс может перейти в конференцию.

Предназначенный для инициации сеансов протокол SIP обеспечивает определение адреса пользователя и установления соединения с ним. Кроме этого, он служит основой для применения других протоколов, реализующих функции защиты, аутентификации, описания канала мультимедийной связи и т.д.

Адресация

Для организации взаимодействия с существующими приложениями IP-сетей и для обеспечения мобильности пользователей протокол SIP использует адрес, подобный адресу электронной почты. В качестве адресов рабочих станций используются специальные универсальные указатели ресурсов - URL (Universal Resource Locators), так называемые SIP URL.

SIP-адреса бывают четырех типов:

• имя@домен;

• имя@хост;

• имя@IP-адрес;

• №телефона@шлюз.

Таким образом, адрес состоит из двух частей. Первая часть - это имя пользователя, зарегистрированного в домене или на рабочей станции. Если вторая часть адреса идентифицирует какой-либо шлюз, то в первой указывается телефонный номер абонента.

Во второй части адреса указывается имя домена, рабочей станции или шлюза. Для определения IP-адреса устройства необходимо обратиться к службе доменных имен - Domain Name Service (DNS). Если же во второй части SIP-адреса размещается IP-адрес, то с рабочей станцией можно связаться напрямую.

В начале SIP-адреса ставится слово «sip:», указывающее, что это именно SIP-адрес, т.к. бывают и другие (например, «mailto:»). Ниже приводятся примеры SIP-адресов:

sip: als@rts.loniis.ru

sip: user1@192.168.100.152

sip: 294-75-47@gateway.ru

Архитектура сети SIP

SIP использует обычные текстовые сообщения и очень напоминает HTTP протокол (практически базируется на нем). Архитектура сети SIP базируется на клиент-серверном взаимодействии (рисунок 2.6).

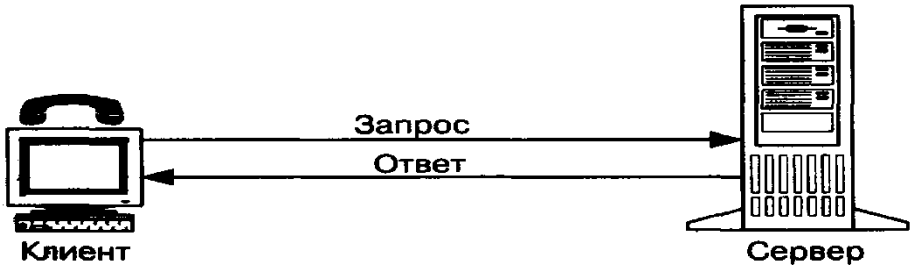


Рис. 2.6. Архитектура "клиент-сервер"

Стандартными элементами в SIP-сети являются:

1. User Agent: по протоколу SIP устанавливаются соединения "клиент-сервер". Клиент устанавливает соединения, а сервер принимает вызовы, но так обычно телефонный аппарат (или программный телефон) может, как устанавливать, так и принимать звонки, то получается, что он одновременно играет роль и клиента и сервера (хотя в реализации протокола это не является обязательным критерием) - в этом случае его называют User Agent (UA) или терминал.

В составе UA выделяются две логические составляющие:

- агент-клиент (UAC - user agent client) - посылает запросы и получает ответы;
- агент-сервер (UAS - user agent server) - принимает запросы и посылает ответы.

Ввиду того, что большинству устройств необходимо как передавать, так и принимать данные, в реальных устройствах присутствует как UAC, так и UAS.

2. Прокси-сервер: прокси-сервер принимает запросы и производит с ним некоторые действия (например, определяет местоположение клиента, производит переадресацию или перенаправление вызова и др.). Он также может устанавливать собственные соединения. Зачастую прокси-сервер совмещают с сервером определения местоположения (Register-сервер), в таком случае его называют Registrar-сервером.

3. Сервер определения местоположения или сервер регистрации (Register): данный вид сервера служит для регистрации пользователей. Регистрация пользователя производится для определения его текущего IP-адреса, для того чтобы можно было произвести вызов user@IP-

адрес. В случае если пользователь переместится в другое место и/или не имеет определенного IP-адреса, его текущий адрес можно будет определить после того, как он зарегистрируется на сервере регистрации. Таким образом, клиент останется доступен по одному и тому же SIP-адресу вне зависимости от того, где на самом деле находится.

4. Сервер переадресации (Redirect): обращается к серверу регистрации для определения текущего IP-адреса пользователя, но в отличие от прокси-сервера только «переадресует» клиента, а не устанавливает собственные соединения.

В результате SIP архитектура выглядит следующим образом (рисунок 2.7):

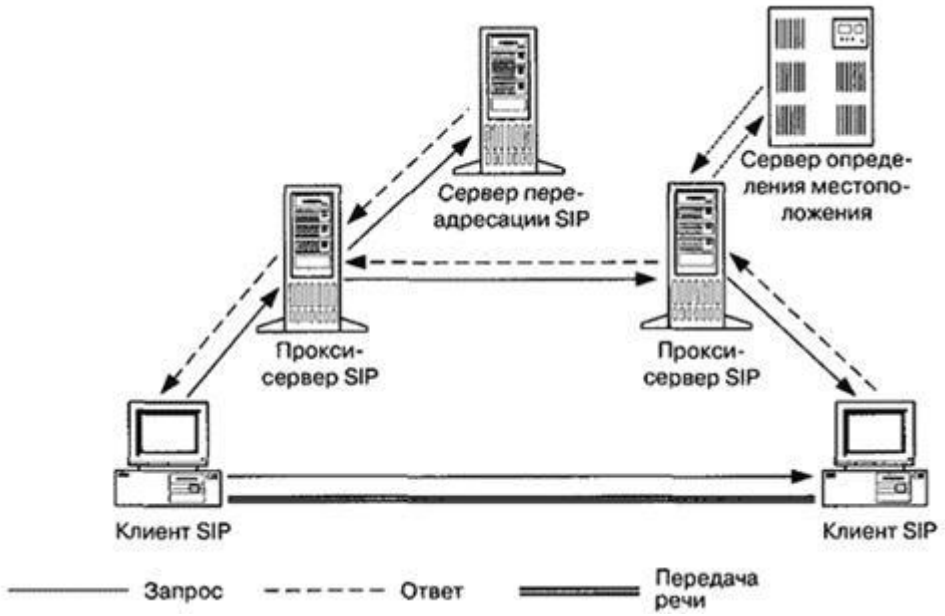


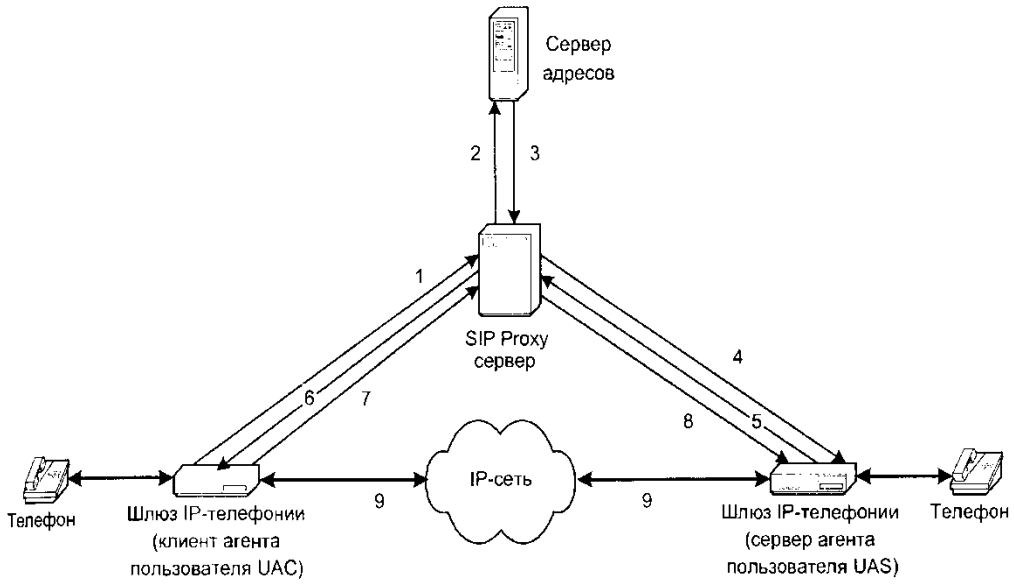
Рис. 2.7. Архитектура сети на базе протокола SIP

Сигнализация на основе протокола SIP

При организации мультимедийного сеанса используется два основных метода для нахождения и информирования заинтересованных участников:

- Уведомление о сеансе с использованием разных средств – электронной почты, новостных групп, WEB-страниц или специального протокола SAP (Session Announcement Protocol);
- Приглашение к участию в сеансе с помощью протокола SIP.

Ниже приведена на рисунке 3.4 схема сигнализации по протоколу SIP.



1 SIP INVITE; 2 Поиск сервера адресов; 3 Ответ сервера адресов; 4 Пересылка INVITE; 5 Ответ; 6 Пересылка ответа; 7 АСК; 8 Пересылка АСК; 9 Мультимедийный поток

Рис. 2.8. Схема сигнализации по протоколу SIP

Обработка вызовов осуществляется сервером SIP, который может работать в режиме непосредственного установления связи или в режиме переадресации. В обоих режимах сервер принимает запросы на определение местоположения нужного пользователя, но если в первом режиме он сам доводит вызов до адресата, то во втором – возвращает адрес конечного пункта запрашиваемому клиенту.

В протоколе SIP определены два вида сигнальных сообщений – запрос и ответ.

Они имеют текстовый формат (кодировка символов согласно RFC 2279) и базируются на протоколе HTTP. В запросе указываются процедуры, вызываемые для выполнения требуемых операций, а в ответе – результаты их выполнения. Определены шесть процедур:

- INVITE - вызывает адресата для установления связи. С помощью этого сообщения адресату передаются виды поддерживаемых сервисов (которые могут быть использованы инициатором сеанса), а также виды сервисов, которые желает передавать инициатор связи;
- ACK - сообщение, подтверждающее согласие адресата установить соединения. В этом сообщении могут быть переданы окончательные параметры сеанса связи (окончательно выбираются виды сервисов и их параметры которые будут использованы);
- Cancel – прекращает поиск пользователя;
- BYE - запрос завершения соединения;
- Register - данным запросом пользователь идентифицирует свое текущее местоположение;

- OPTIONS - запрос информации о функциональных возможностях терминала (применяется в случае, если эти данные нужно получить до установления соединения, то есть до фактического обмена данной информацией с помощью запросов INVITE и ACK).

Предназначенный для инициации сеансов протокол SIP обеспечивает определение адреса пользователя и установление соединения с ним. Кроме этого, он служит основой для применения других протоколов, реализующих функции защиты, аутентификации, описания канала мультимедийной связи и т.д.

Обеспечение качества IP-телефонии

Показатели качества IP-телефонии

Традиционные телефонные сети коммутируют электрические сигналы с гарантированной полосой пропускания, достаточной для передачи сигналов голосового спектра. При фиксированной пропускной способности передаваемого сигнала цена единицы времени связи зависит от удаленности и расположения точек вызова и места ответа.

Сети с коммутацией пакетов не обеспечивают гарантированной пропускной способности, поскольку не обеспечивают гарантированного пути между точками связи.

IP-телефония является одной из областей передачи данных, где важна динамика передачи сигнала, которая обеспечивается современными методами кодирования и передачи информации, а также увеличением пропускной способности каналов, что приводит к возможности успешной конкуренции IP-телефонии с традиционными телефонными сетями.

Основными составляющими качества IP-телефонии являются:

- Качество речи, которое включает:

- *диалог* – возможность пользователя связываться и разговаривать с другим пользователем в реальном времени и полнодуплексном режиме;

- *разборчивость* – чистота и тональность речи;

- *эхо* – слышимость собственной речи;

- *уровень* – громкость речи.

- Качество сигнализации, включающее:

- *установление вызова* – скорость успешного доступа и время установления соединения;

- *завершение вызова* – время отбоя и скорость разъединения;

- *DTMF* – определение и фиксация сигналов многочастотного набора номера.

Факторы, которые влияют на качество IP-телефонии, могут быть разделены на две категории:

- Факторы качества IP- сети:

- *максимальная пропускная способность* – максимальное количество полезных и избыточных данных, которая она передает;

- *задержка* – промежуток времени, требуемый для передачи пакета через сеть;

- *джиттер* - задержка между двумя последовательными пакетами;

- *потеря пакета* – пакеты или данные, потерянные при передачи через сеть.

- Факторы качества шлюза:

- *требуемая полоса пропускания* - различные кодеки требуют различную полосу. Например, кодек G.723 требует полосы 16,3 кбит/с для каждого речевого канала;

- *задержка* - время, необходимое цифровому сигнальному процессору DSP или другим устройствам обработки для кодирования и декодирования речевого сигнала;

- *буфер джиттера* - сохранение пакетов данных до тех пор, пока все пакеты не будут получены, и можно будет передать в требуемой последовательности для минимизации джиттера;

- *потеря пакетов* - потеря пакетов при сжатии и/или передаче в оборудовании IP-телефонии;

- *подавление эхо* — механизм для подавления эхо, возникающего при передаче по сети;

- *управление уровнем* - возможность регулировать громкость речи.

Влияние сети на показатели качества IP-телефонии

Задержка

Задержка создает неудобство при ведении диалога, приводит к перекрытию разговоров и возникновению эхо. Эхо возникает в случае, когда отраженный речевой сигнал вместе с сигналом от удаленного конца возвращается опять в ухо говорящего. Эхо становится трудной проблемой, когда задержка в петле передачи больше, чем 50 мс. Так как эхо является проблемой качества, системы с пакетной коммутацией речи должны иметь возможность управлять эхо и использовать эффективные методы эхоподавления.

Затруднение диалога и перекрытие разговоров становятся серьезным вопросом качества, когда задержка в одном направлении передачи превышает 250 мс. Можно выделить следующие источники задержки при пакетной передаче речи из конца в конец [1].

- Задержка накопления (иногда называется алгоритмической задержкой): эта задержка обусловлена необходимостью сбора кадра речевых отсчетов, выполняемая в речевом кодере. Величина задержки определяется типом речевого кодера и изменяется от небольших величин (0,125 мкс) до нескольких миллисекунд. Например, стандартные речевые кодеры имеют следующие длительности кадров:

G.729 CS-ACELP (8 кбит/с) – 10 мс

G.723.1 – Multi Rate Coder (5,3; 6,3 кбит/с) – 30 мс.

- Задержка обработки: процесс кодирования и сбора закодированных отсчетов в пакеты для передачи через пакетную сеть создает определенные задержки. Задержка кодирования или обработки зависит от времени работы процессора и используемого типа алгоритма обработки.
- Сетевая задержка: задержка обусловлена физической средой и протоколами, используемыми для передачи речевых данных, а также буферами, используемыми для удаления джиттера пакетов на приемном конце. Сетевая задержка зависит от емкости сети и процессов передачи пакетов в сети.

Время задержки при передачи речевого сигнала можно отнести к одному из трех уровней:

- первый уровень до 200 мс – отличное качество связи. Для сравнения, в телефонной сети общего пользования допустимы задержки до 150-200 мс;
- второй уровень до 400 мс – считается хорошим качеством связи. Но если сравнивать с качеством связи по сетям ТФОП, то разница будет видна. Если задержка постоянно удерживается на верхней границе 2-го уровня (на 400 мс), то не рекомендуется использовать эту связь для деловых переговоров;
- третий уровень до 700 мс – считается приемлемым качеством связи для ведения неделовых переговоров. Такое качество связи возможно также при передаче пакетов по спутниковой связи.

Качество Интернет-телефонии попадает под 2-3 уровни, провайдеры IP-телефонии, работающие по выделенным каналам попадают под 1-2 уровни. Также необходимо учитывать задержки при кодировании/декодировании голосового сигнала. Средние суммарные задержки при использовании IP-телефонии обычно находятся в пределах 150-250 мс.

Джиттер

Когда речь или данные разбиваются на пакеты для передачи речи через IP-сеть, пакеты часто прибывают в пункт назначения в различное время и в разной последовательности. Это создает разброс времени доставки пакетов (джиттер). Джиттер приводит к специфическим нарушениям передачи речи, слышимым как трески и щелчки.

Для того, чтобы компенсировать влияние джиттера, в терминалах используется так называемый джиттер-буфер. Этот буфер хранит в памяти прибывшие пакеты в течение времени, определяемого ее емкостью (длиной). Пакеты, прибывшие слишком поздно, когда буфер заполнен, отбрасываются. Интервалы между пакетами восстанавливаются на основе

значений временных меток RTP-пакетов. В функции джиттер-буфера входит и восстановление исходной очередности следования пакетов, если при транспортировки по сети они оказались «перепутаны».

Слишком короткий буфер будет приводить к слишком частым потерям «опоздавших» пакетов, а слишком длинный – к неприемлемо большой дополнительной задержке. Обычно предусматривается динамическая подстройка длины буфера в течение всего времени существования соединения.

Для оптимизации джиттер-буфера в VoIP-устройстве следует повышать размер буфера, что позволяет снижать или вообще устранять джиттер, размер буфера, превышающий 150 мс, достаточно сильно влияет на качество разговора.

Потеря пакетов

Потерянные пакеты в IP-телефонии нарушают речь и создают искажения тембра. В существующих IP-сетях все голосовые данные. При пиковых нагрузках и перегрузках голосовые кадры будут отбрасываться, как и кадры данных. Однако кадры данных не связаны со временем, и отброшенные пакеты могут быть успешно переданы путем повторения. Потеря голосовых пакетов, в свою очередь, не может быть восполнена таким способом и в результате произойдет неполная передача информации. Предполагается, что потеря до 5% пакетов незаметна, а свыше 10-15% - недопустима. Причем данные величины существенно зависят от алгоритмов компрессии/декомпрессии.

Существенно, что потеря большой группы пакетов приводит к необратимым локальным искажениям речи, тогда как потери одного, двух, трех пакетов можно пытаться компенсировать.

Взаимосвязь методов обеспечения качества IP-телефонии, показателей качества сети и качества вызова представлена на рисунке 2.9.

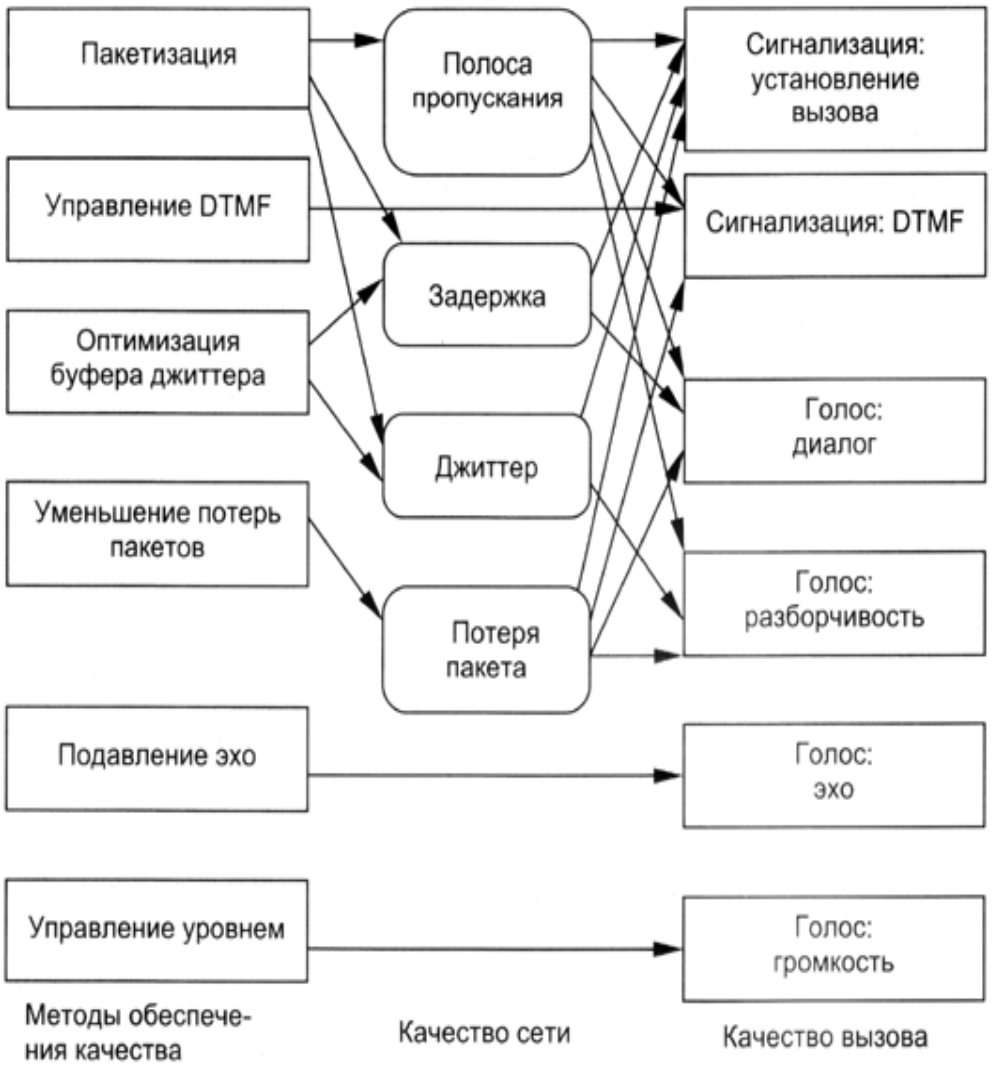


Рис. 2.9. Схема обеспечения качества IP-телефонии

Asterisk

Asterisk — свободное решение компьютерной телефонии (в том числе, VoIP) с открытым исходным кодом от компании Digium, первоначально разработанное Марком Спенсером. Приложение работает на операционных системах Linux, FreeBSD, OpenBSD и Solaris. Имя проекта произошло от названия символа «*» (англ. asterisk — «звездочка»).

Asterisk в комплексе с необходимым оборудованием обладает всеми возможностями классической АТС, поддерживает множество VoIP-протоколов и предоставляет богатые функции управления звонками, среди них:

- Голосовая почта.
- Конференции.
- Интерактивное голосовое меню (IVR).
- Центр обработки вызовов (постановка звонков в очередь и распределение их по

агентам используя различные алгоритмы).

- Запись (Call Detail Record).

Для создания дополнительной функциональности можно воспользоваться собственным языком Asterisk для написания плана нумерации, написав модуль на языке Си, либо воспользовавшись AGI — гибким и универсальным интерфейсом для интеграции с внешними системами обработки данных. Модули, выполняющиеся через AGI, могут быть написаны на любом языке программирования.

Asterisk распространяется на условиях двойной лицензии, благодаря которой одновременно с основным кодом, распространяемым по открытой лицензии GNU GPL, возможно создание закрытых модулей, содержащих лицензируемый код.

Asterisk может работать как с аналоговыми линиями (FXO/FXS модули), так и цифровыми (ISDN, BRI и PRI — потоки T1/E1). С помощью определённых компьютерных плат (наиболее известными производителями которых являются Digium, Sangoma, OpenVox, Rhino, AudioCodes) Asterisk можно подключить к высокопропускным линиям T1/E1, которые позволяют работать параллельно с десятками и сотнями телефонных соединений. Полный список поддерживаемого оборудования для соединения с телефонной сетью общего пользования определяется поддержкой оборудования в модулях ядра.

Для создания дополнительной функциональности можно воспользоваться собственным языком Asterisk для написания плана нумерации, написав модуль на языке C, либо воспользовавшись AGI - гибким и универсальным интерфейсом для интеграции с внешними системами обработки данных. Модули, выполняющееся через AGI, могут быть написаны на любом языке программирования.

Asterisk распространяется на условиях двойной лицензии, благодаря которой одновременно с основным кодом, распространяемым по открытой лицензии GNU GPL, возможно создание закрытых модулей, содержащих лицензируемый код: например, модуль для поддержки кодека G.729.

Благодаря свободной лицензии Asterisk активно развивается и поддерживается тысячами людей со всей планеты. В течение последних двух лет рынок Asterisk-приложений активно развиваются в США и уже заняли прочное место на рынке IT-технологий (более 1000 компаний, центры поддержки, online-консультации). В Россию данный продукт попал позже, но интерес российского потребителя растёт, и в первую очередь, благодаря открытости системы. Многие компании применяют Asterisk в своих серийных VoIP-устройствах, например компании Linksys, Nateks.

Поддерживаются следующие протоколы:

- SIP,

- H.323,
- IAX2,
- MGCP,
- Skinny/SCCP,
- XMPP (Google Talk),
- Unistim,
- Skype, через коммерческий канал.

Настройка и программирование производится с помощью нескольких механизмов:

- диалплан, который пишется на специальном языке. Доступна как старая версия, так и новая — AEL, а также на языке Lua.
- AGI.
- AMI.
- Конфигурация из баз данных.

IP-АТС на основе Asterisk обладает возможностями:

- Запись телефонных разговоров
- Конференц-комнаты с использованием виртуальных номеров
- Голосовая почта и пересылка на e-mail
- Поддержка протоколов SIP, IAX2, H.323, MGCP, Skinny
- Инструменты разработчика для создания расширений, предоставляющие новые услуги
- Поддержка кодеков: ADPCM, G.711 (A-Law и μ-Law), G.722, G.723.1, G.726, G.728, G.729, GSM, ILBC, Speex.
- Виртуальный секретарь - IVR
- Поддержка аналоговых интерфейсов FXS / FXO
- Голосовой синтез речи
- Поддержка цифровых интерфейсов (E1/T1/J1) и протоколов PRI/BRI/R2/SS7
- Автоконфигурация IP-телефонов
- АОН определитель номера
- Программное эхоподавление
- Работа с несколькими операторами связи
- Маршрутизация входящих и исходящих вызовов по различным правилам
- Поддержка Видеотелефонов
- Интерфейс обнаружения телефонного оборудования
- Поддержка групповой переадресации вызовов

- DHCP сервер для распределения динамических IP адресов
- Панель оператора. Оператор может видеть всю телефонную деятельность в виде графиков и выполнять простые операции по управлению телефонными звонками
- Поддержка протокола пейджинга (intercom) и домофонов
- Веб-панель управления
- Поддержка временных условиях
- Парковка и перехват звонка
- Запрет вызова по PIN коду
- Call Detail Record (CDR) отчеты
- Прямой доступ в систему (DISA)
- Биллинг, отчеты, статистика, анализ по использованию
- Поддержка обратного звонка
- Поддержка динамических очередей

Структурная схема IP АТС на базе Asterisk

Asterisk, благодаря гибкой системе настроек, позволяет строить различные решения голосовой связи, в зависимости от требований.

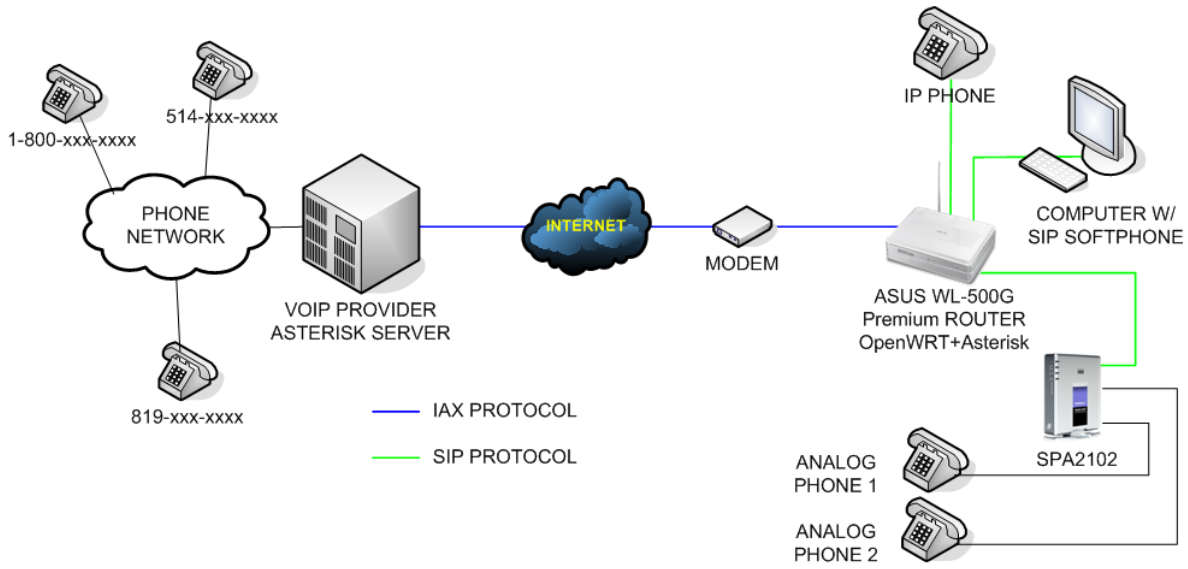


Рис. 2.10. структурная схема сетевого решения на базе Asterisk

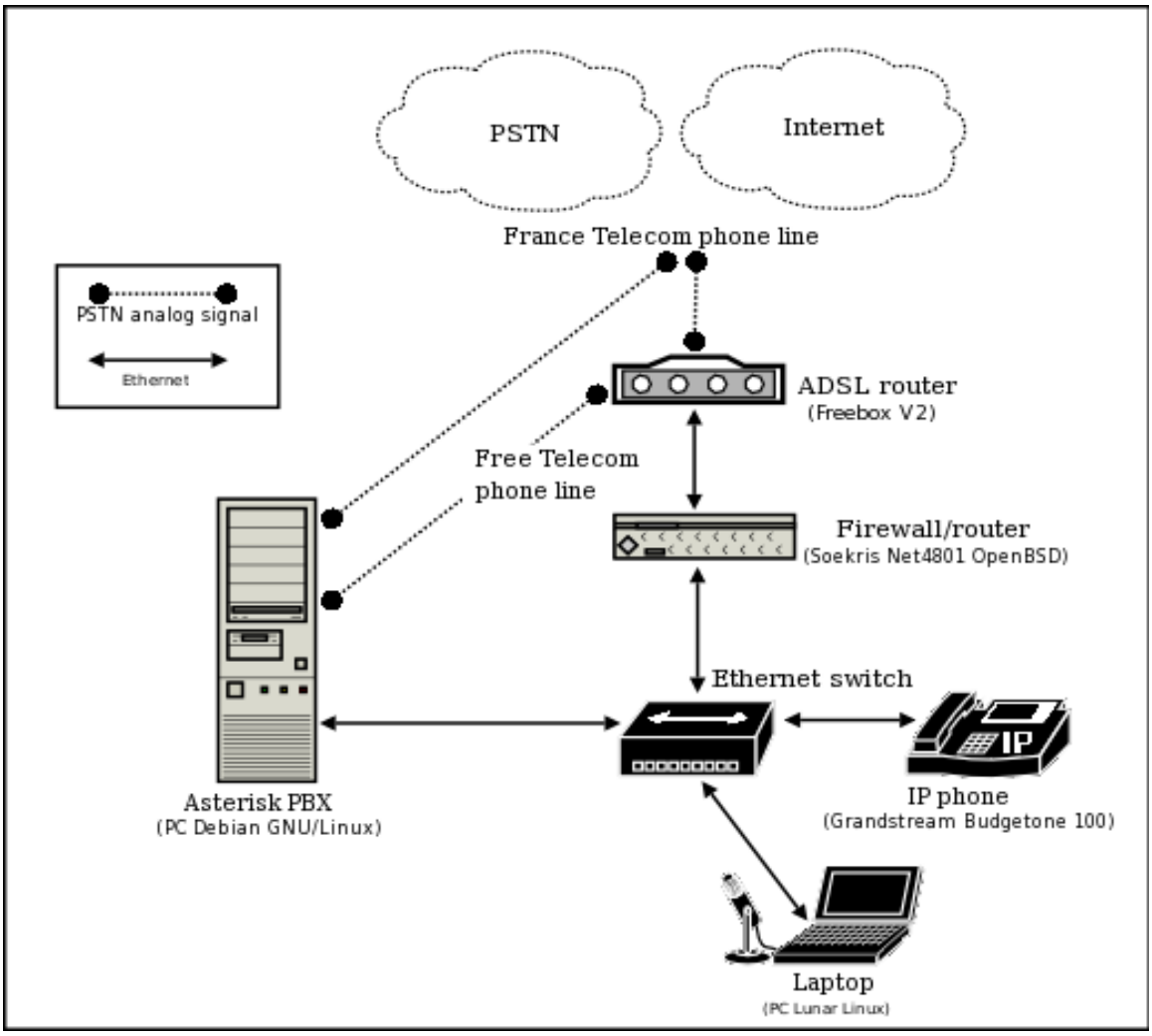


Рис. 2.11. Структурная схема сетевого решения на базе Asterisk

Блок-схема IP-АТС на базе Asterisk

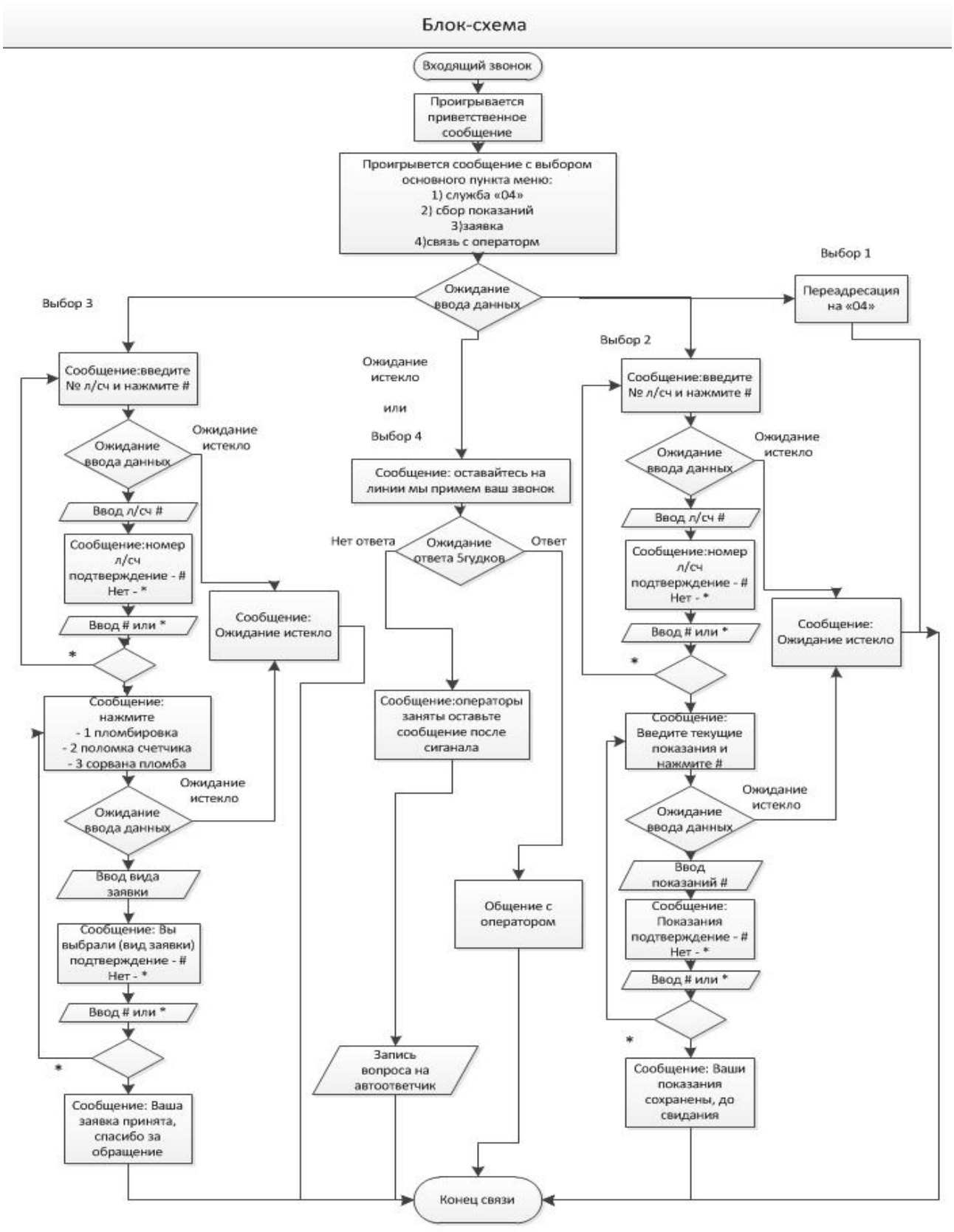


Рис. 2.12. Блок схема агроритма IP АТС

В результате проделанной работы была спроектирована защищенная сеть связи на основе технологии IP-телефонии на базе ОС Windows.

В процессе проектирования были рассмотрены основные принципы построения сетей IP-телефонии, выполнена оценка уровня качества разрабатываемой системы. Был произведен выбор, и сравнительный анализ основных протоколов, на базе которых реализована сеть IP-телефонии, произведен выбор необходимого оборудования, построена структурная схема сети, функциональная схема, а так же блок схема алгоритма защиты сети IP-телефонии.

Компьютерный практикум

Методические указания по настройке системы

Поскольку требования, предъявляемые Asterisk к производительности, главным образом, обусловлены большим объемом производимых математических вычислений, естественным будет выбор процессора с мощным FPU. Выведем рекомендуемые технические характеристики сервера в таблицу 2.3.

Таблица 2.3. Рекомендации по выбору технических характеристик системы

Назначение	Количество каналов	Рекомендуемые параметры
Любительская система	Не более 5	400 МГц x86, 256 М6 оперативной памяти
SOHO-система (малый офис)	От 5 до 10	1 ГГц x86, 512 М6 оперативной памяти
Малая бизнес-система	До 25	3 ГГц x86, 1 Гб операт-й памяти

Все ниже написанное было протестировано на операционных системах Windows 7 и Windows 2008.

Шаг 1

Скачайте и установите *asteriskwin32 version 0.66b.* Линк: http://www.asteriskwin32.com/.

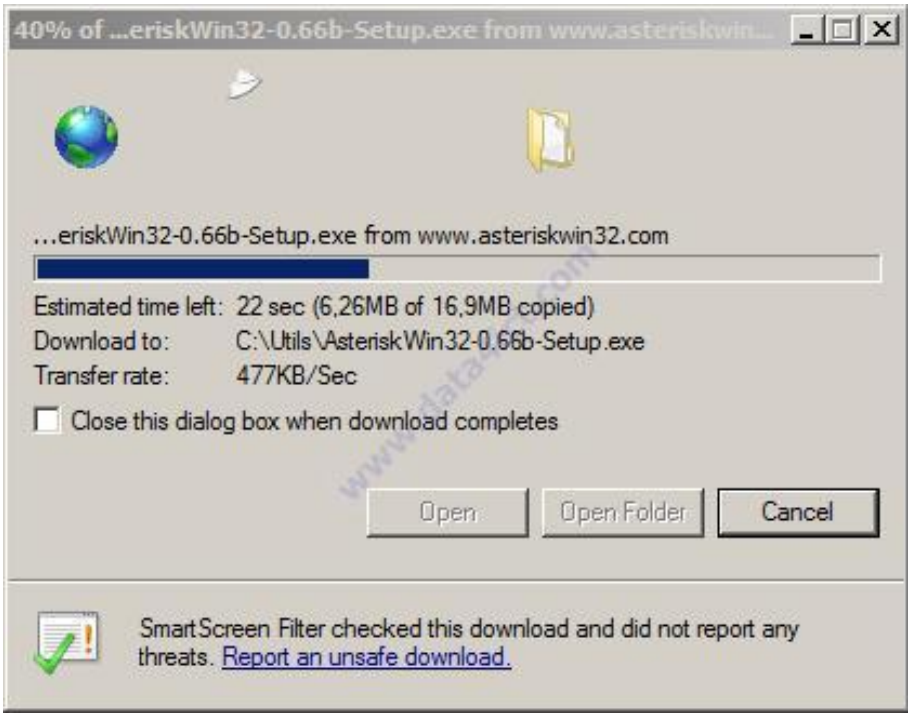


Рис. 2.13. Скачка ПО AsteriskWin32

Шаг 2

Установка скачанного файла начнется после двойного клика по файлу «AsteriskWin32-0.66b-Setup»

Рисунок 2.14. Установка AsteriskWin32

Выберите *I accept the agreement*

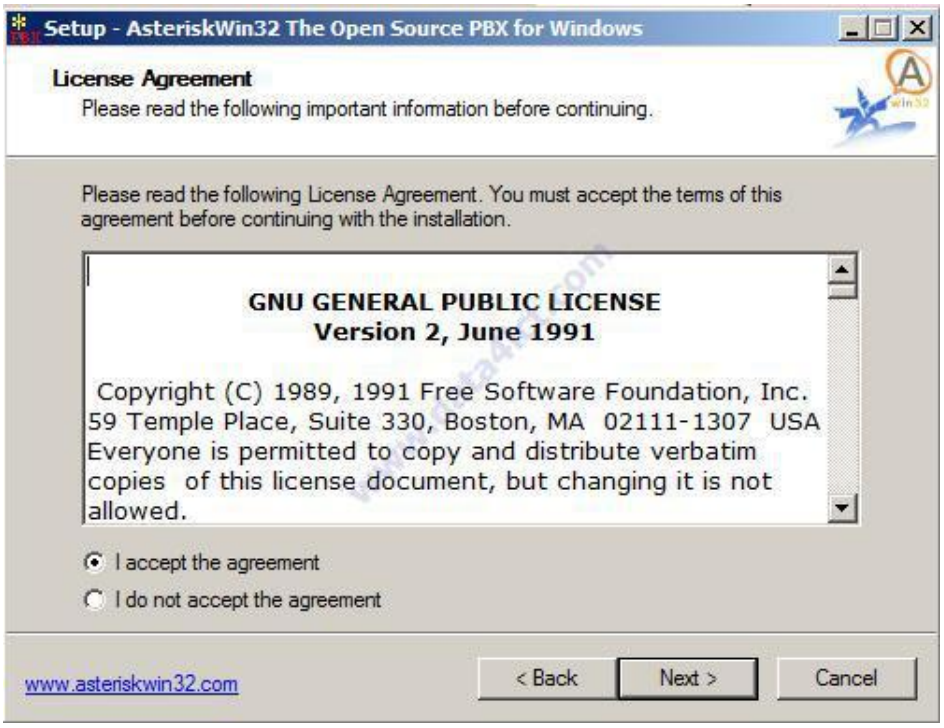


Рис. 2.15. Установка AsteriskWin32

Нажмите *next*

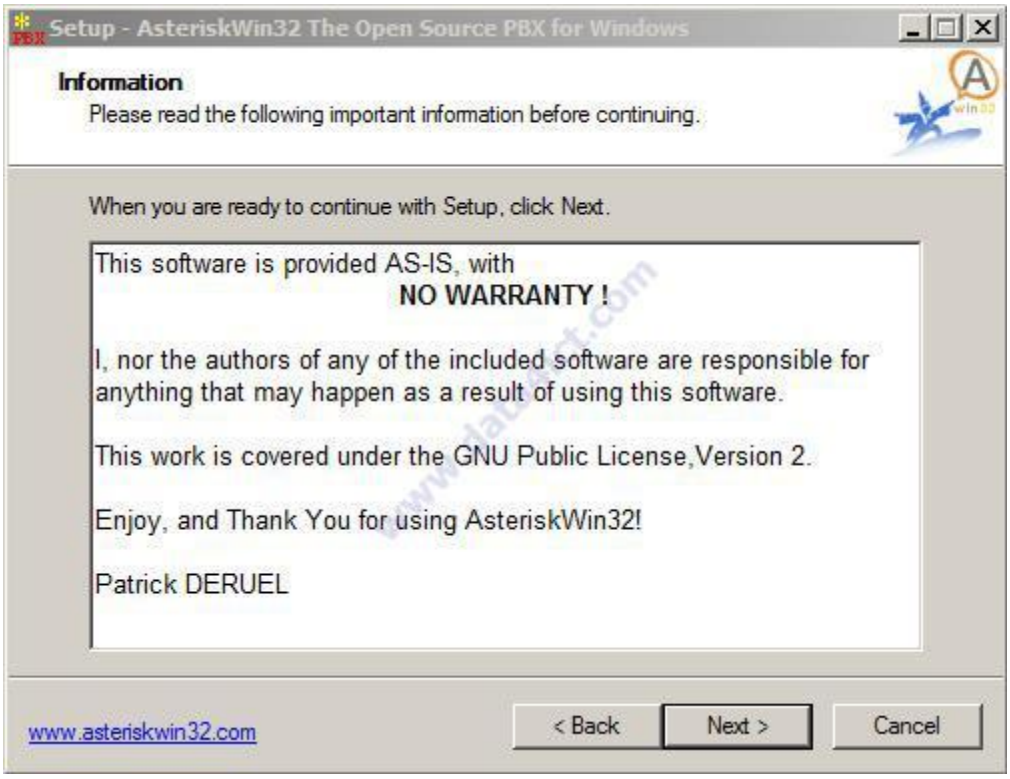


Рис. 2.16. Установка AsteriskWin32

Выберите директорию установки программы, рекомендуется устанавливать в папку cygroot

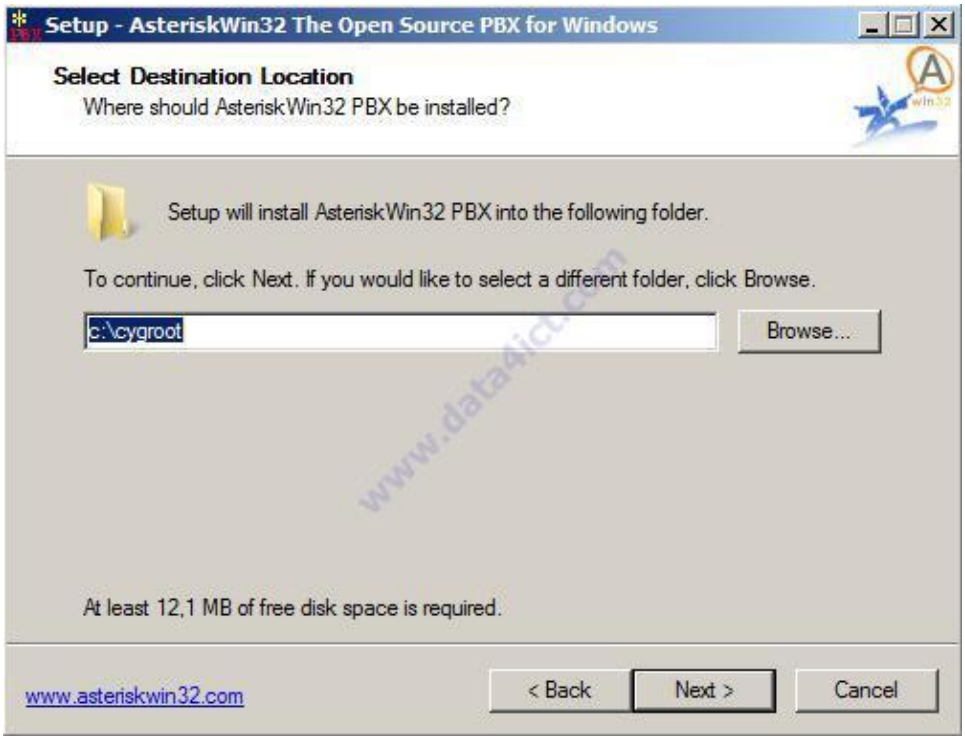


Рис. 2.17. Установка AsteriskWin32

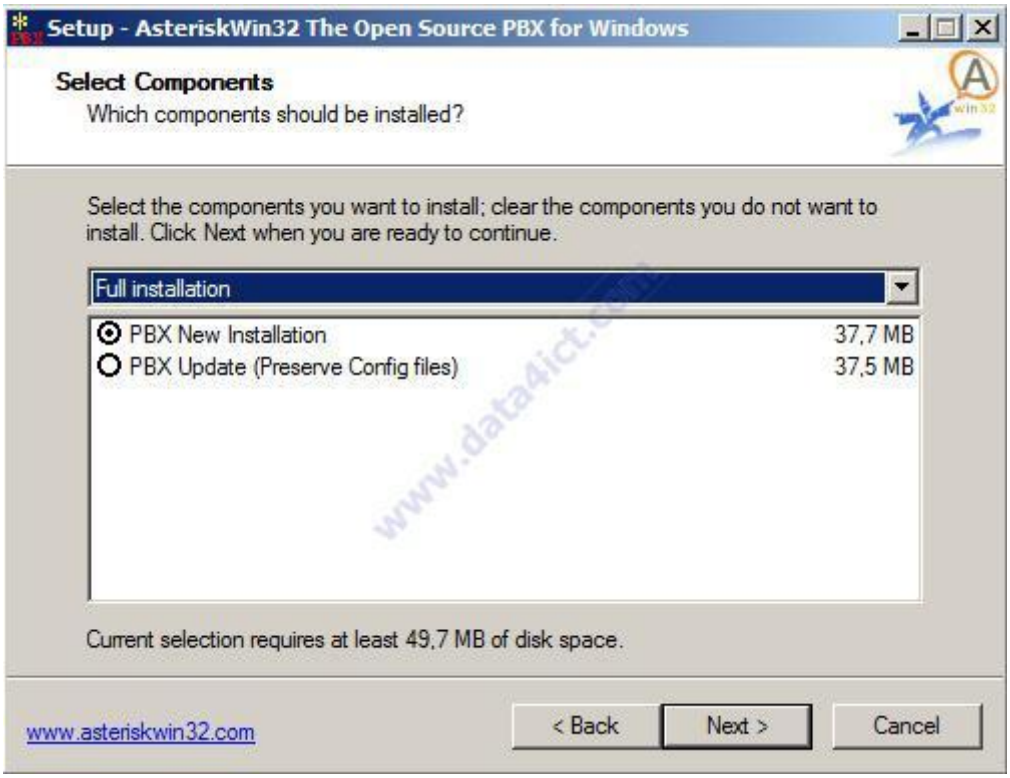


Рис. 2.18. Установка AsteriskWin32

Клик *Install*

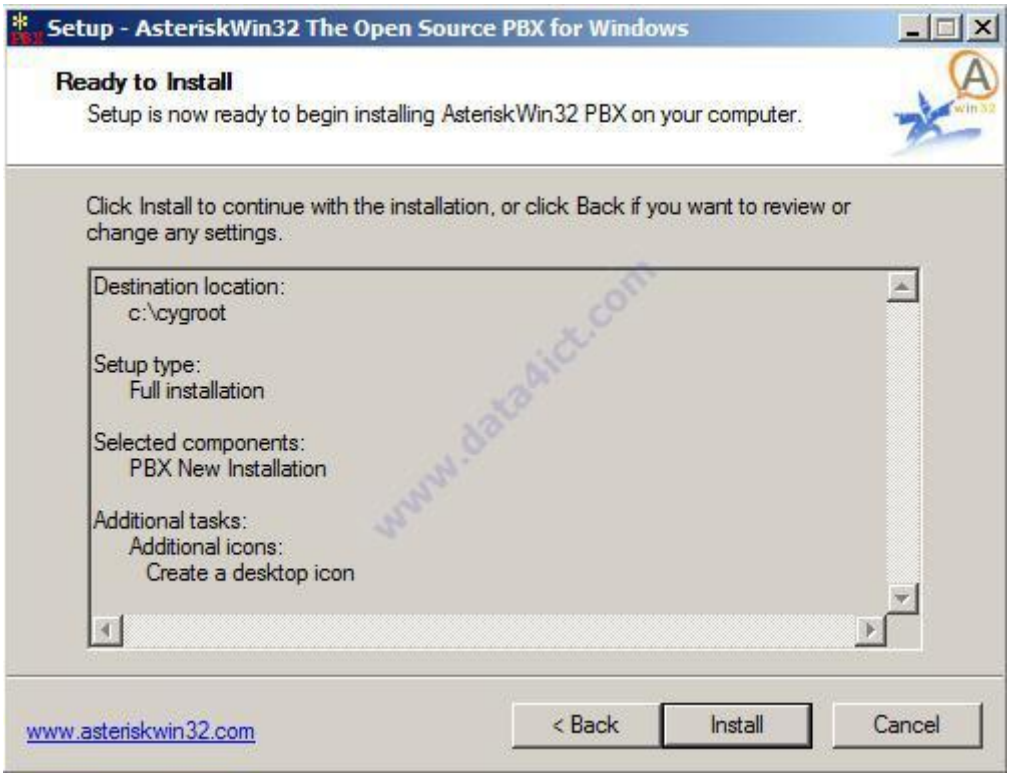


Рис. 2.19. Установка AsteriskWin32

Ждите пока полностью не установится

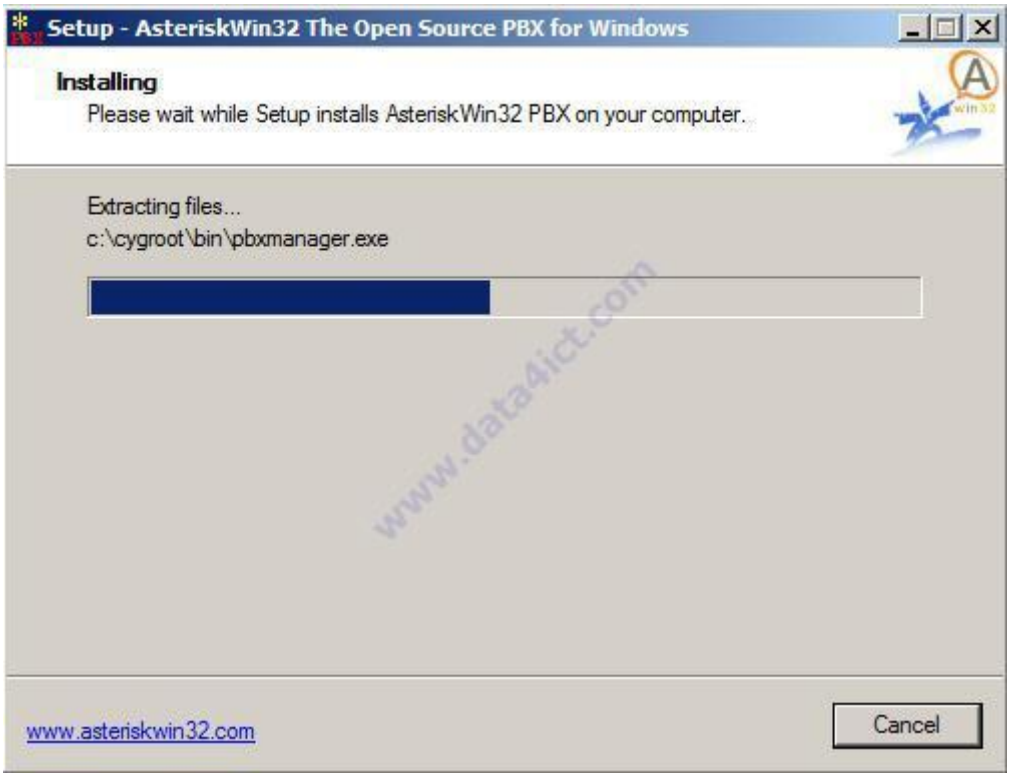


Рис. 2.20. Установка AsteriskWin32

Рис. 2.21. Установка AsteriskWin32

Поздравляю, установка AsteriskWin32 завершена.

Запуск AsteriskWin32

Начните работу Asterisk, дважды кликнув по иконке AsteriskW32 GUI

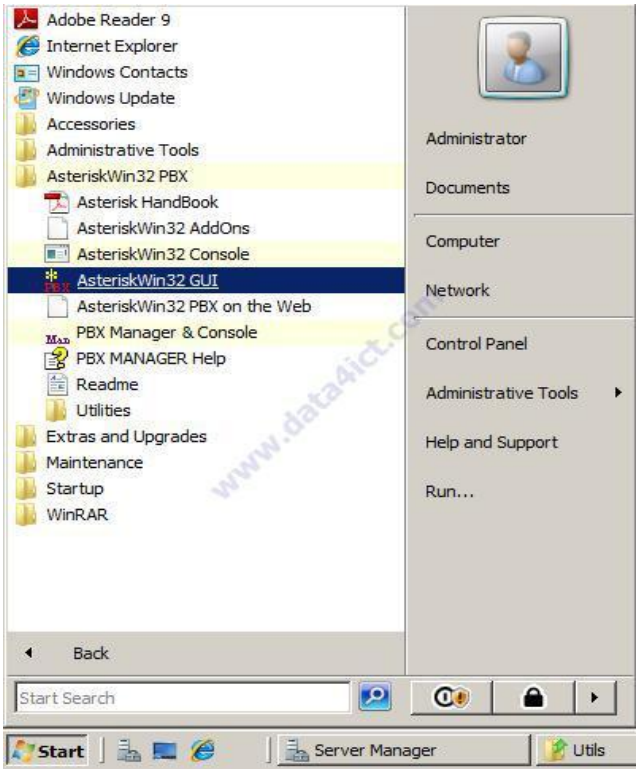


Рис. 2.22. Запуск AsteriskWin32

После запуска программы в командном окне появится несколько ошибок, которые не дадут к корректной работе системы.

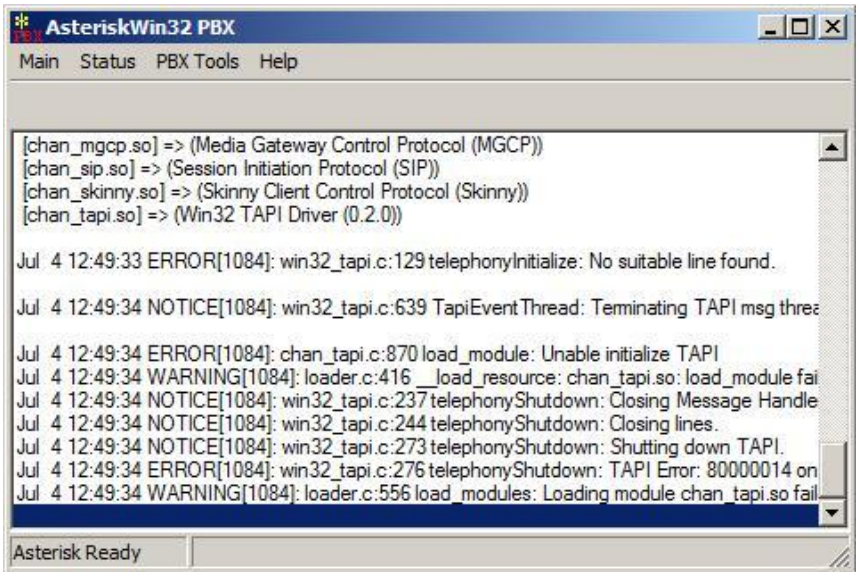


Рис. 2.23. Запуск AsteriskWin32

Для решения данной проблемы, мы скачиваем эмулятор **Linux Emulator (cygwin)** по линку http://www.cygwin.com/. В пособие рассматривается установка ***cygwin version 1.7.5.***

Устанавливаем скачанный файл

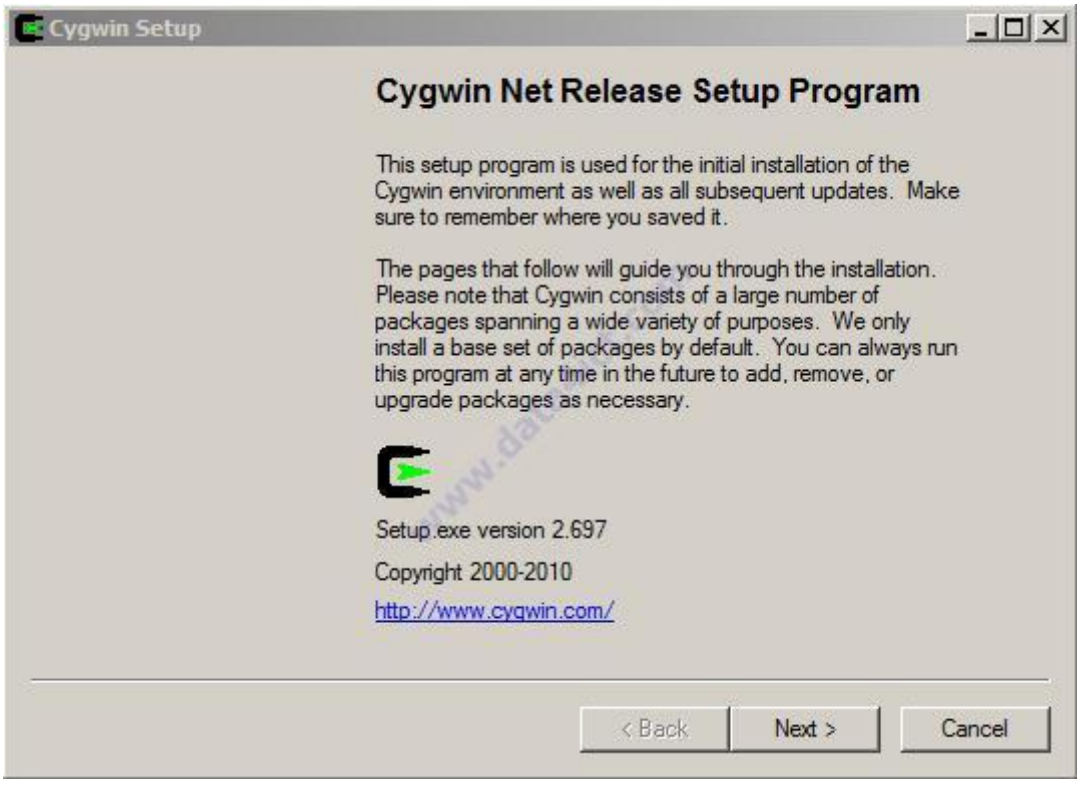


Рис. 2.24. Установка cygwin

Выберем *Install from Internet*

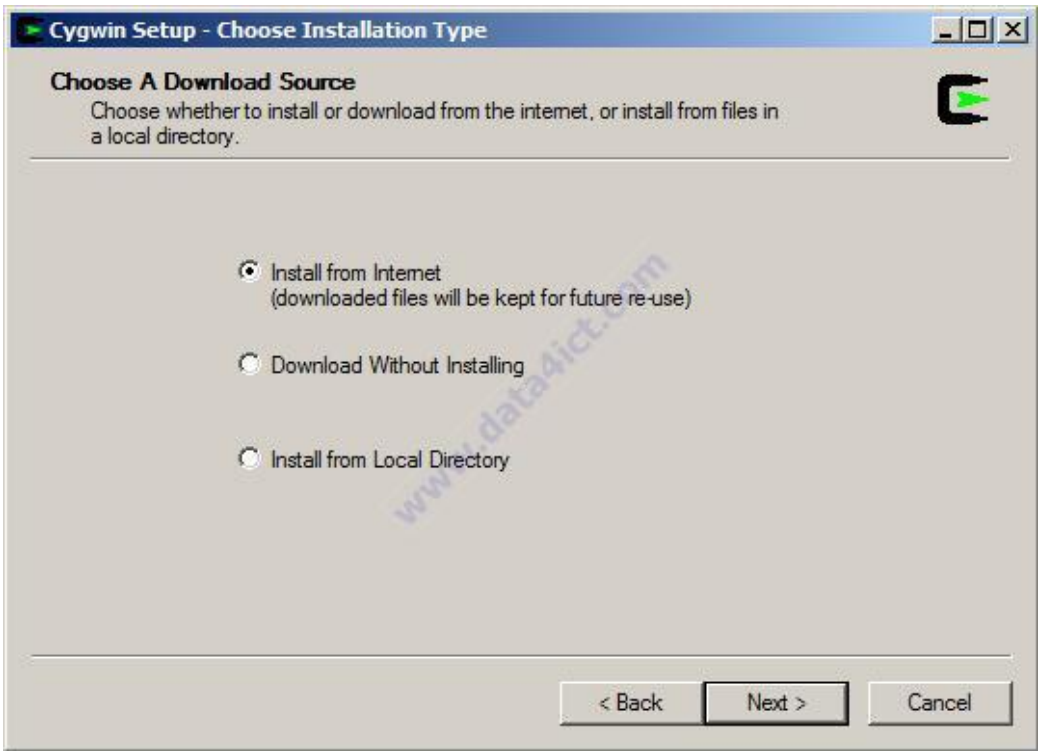


Рис. 2.25. Установка cygwin

Изменяем директорию установки на C:\cygroot и нажинаем Next.

Рис. 2.26. Установка cygwin

Изменяем на C:\Utils

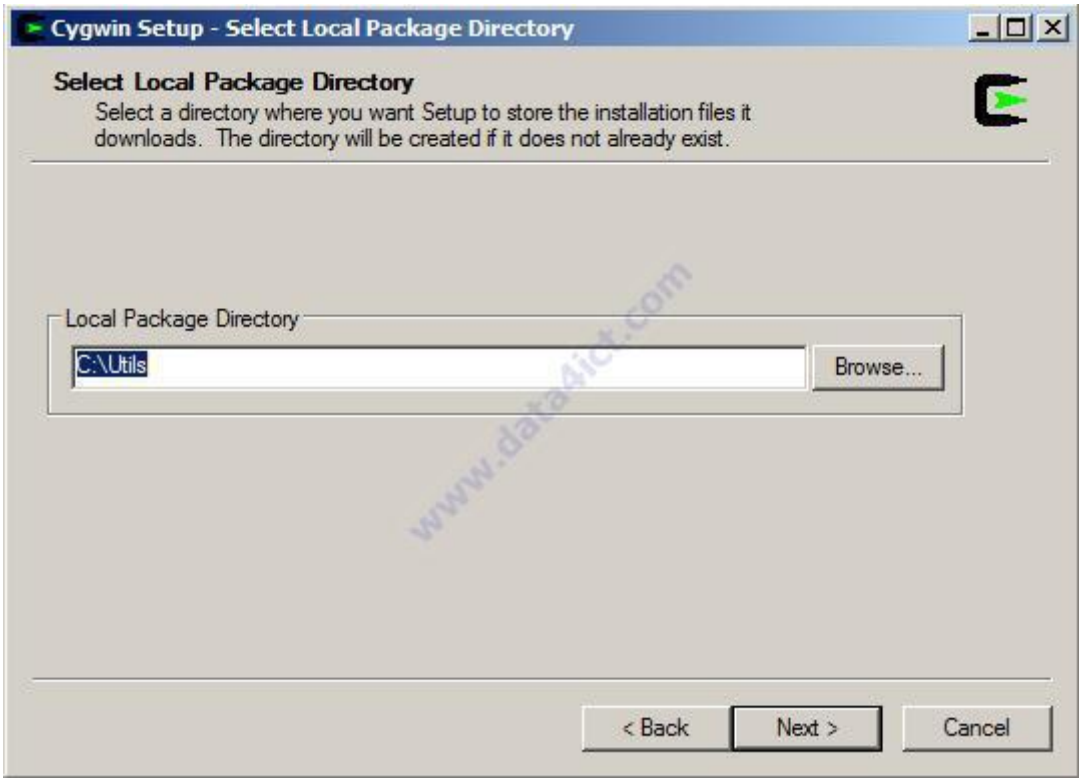


Рис. 2.27. Установка cygwin

Выбираем Direct connection

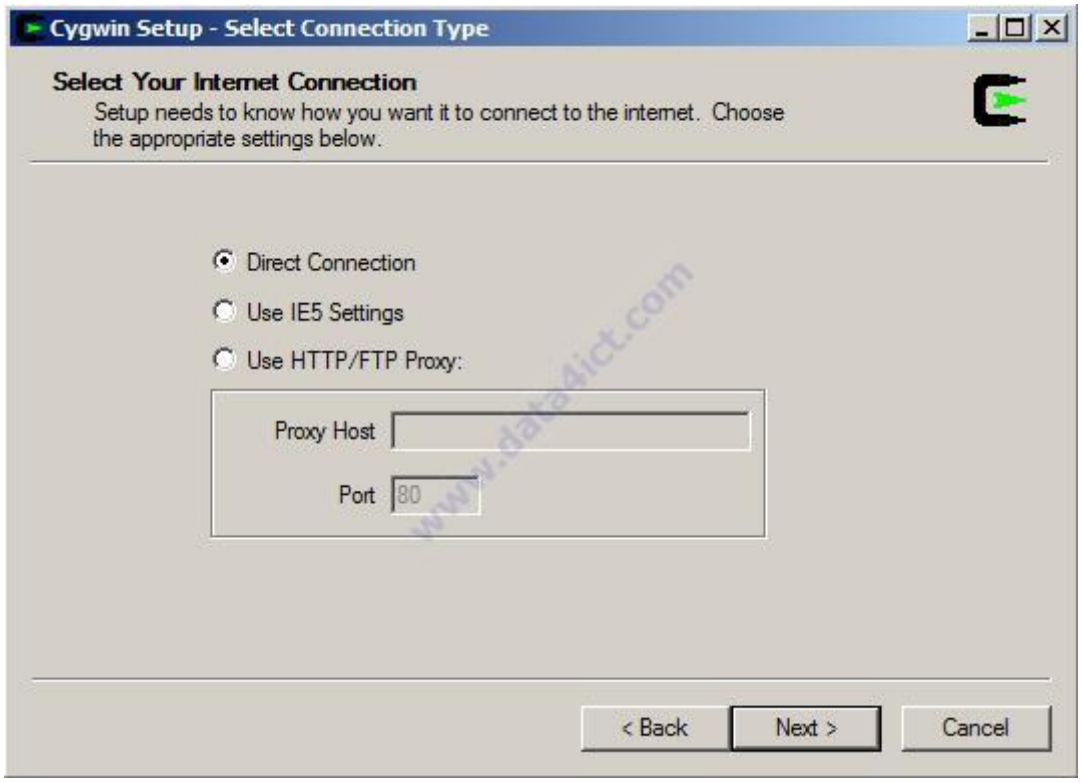


Рис. 2.28. Установка cygwin

Выбираем сайт, с которого будет идти скачивание

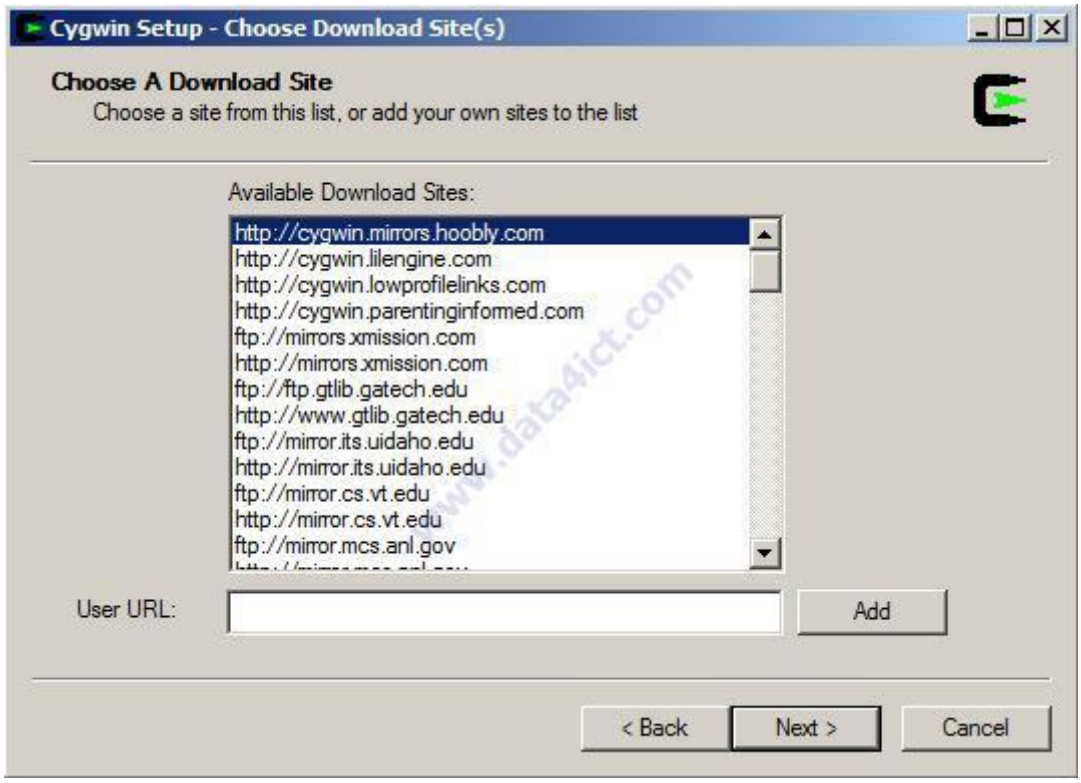


Рис. 2.29. Установка cygwin

Дождитесь до полной скачки файлов

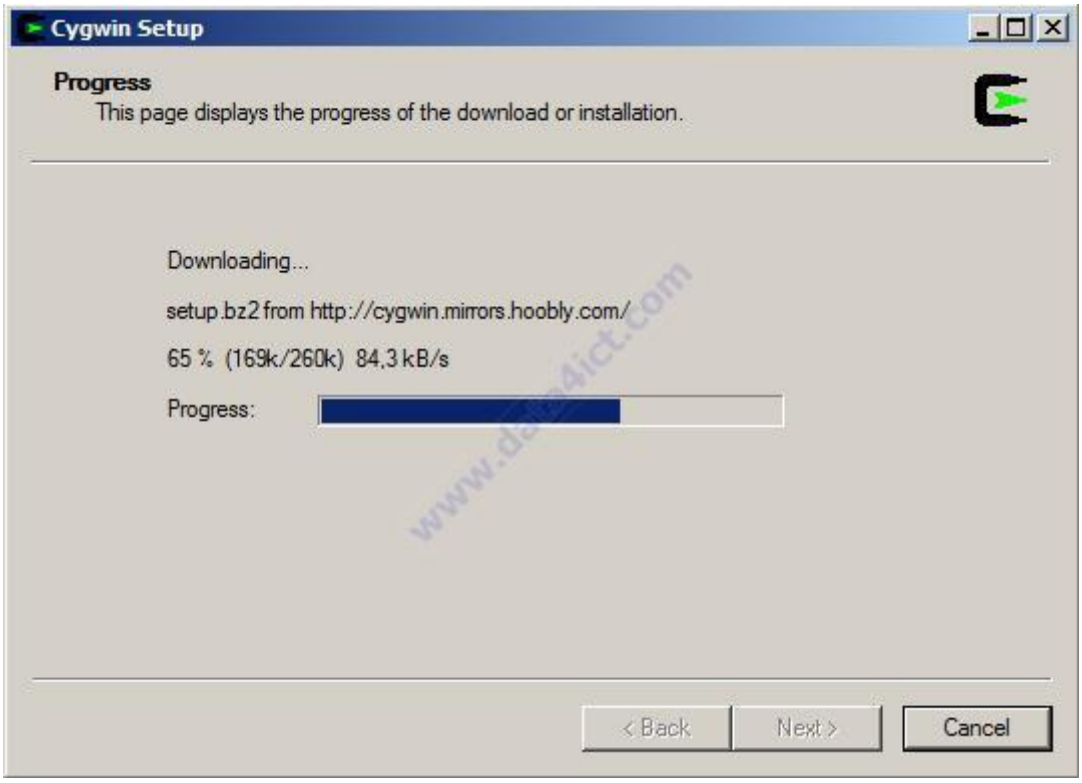


Рисунок 2.30. Установка cygwin

При выскакивании ошибки нажмите Ок

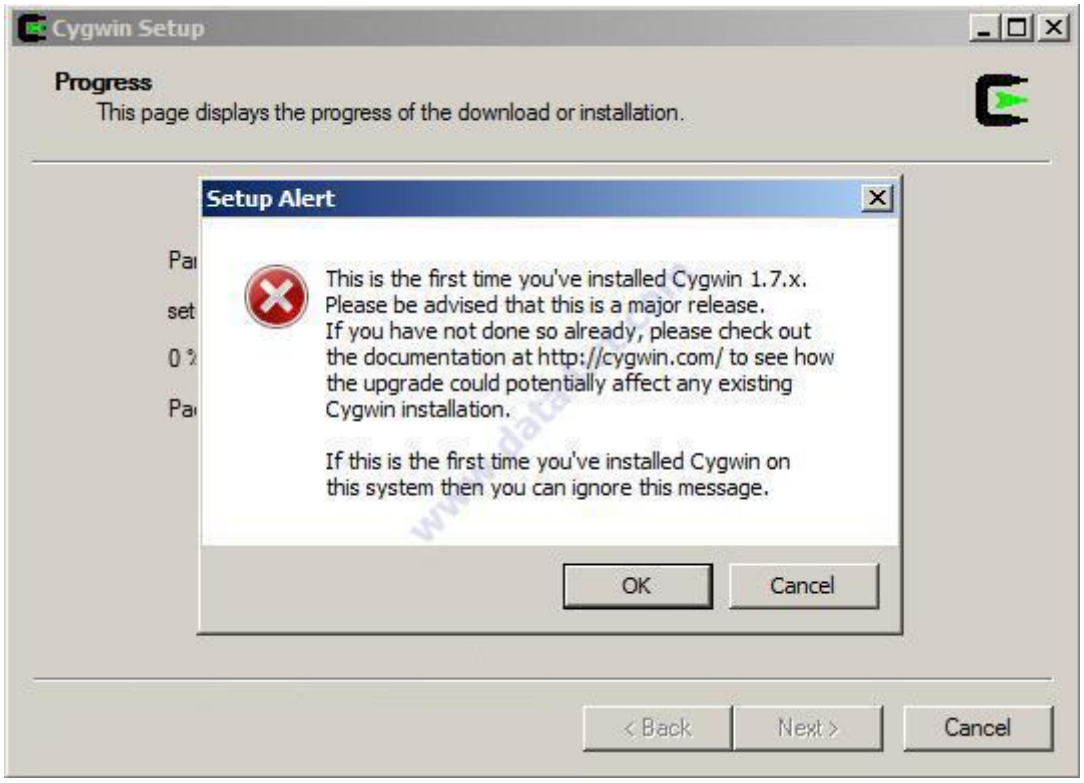


Рис. 2.31. Установка cygwin

Нажмите next

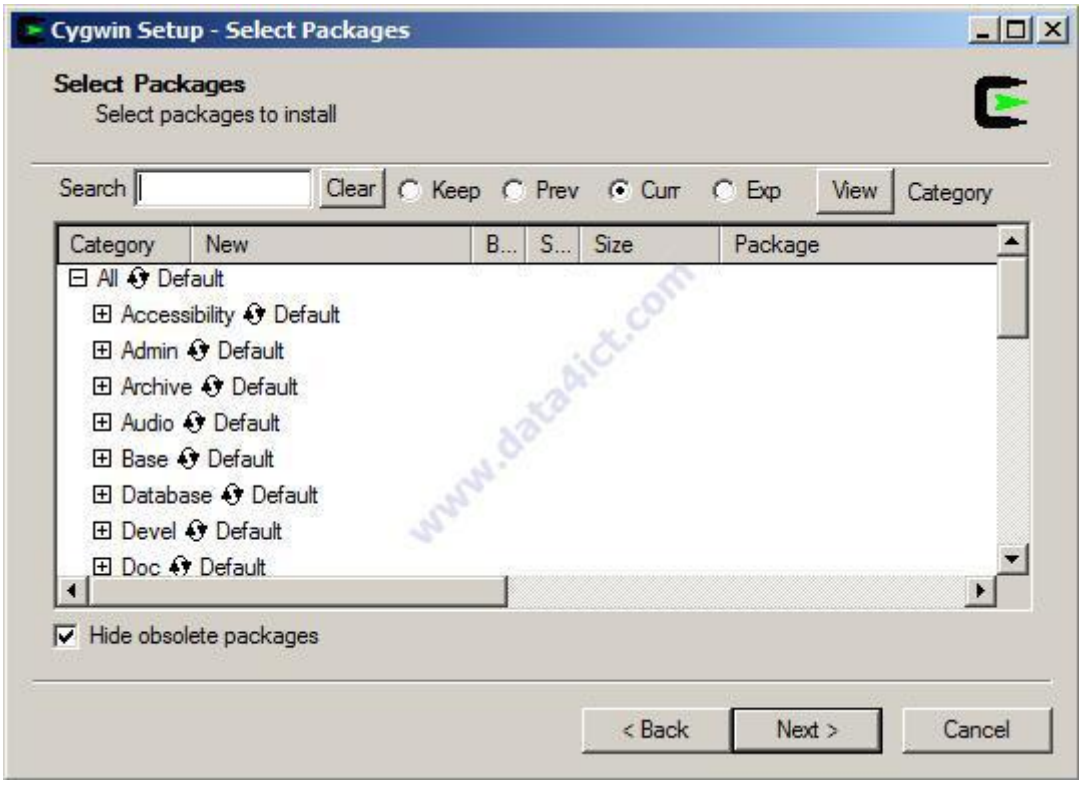


Рис. 2.32. Установка cygwin

Дождитесь полного скачивания

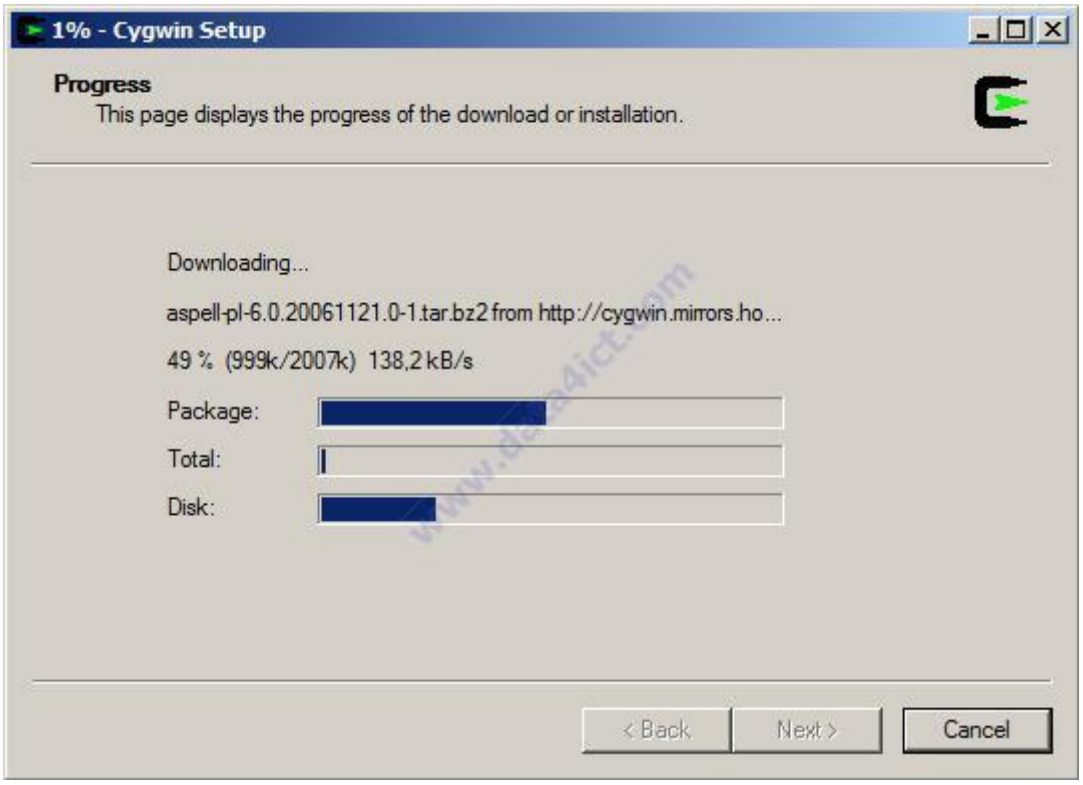


Рис. 2.33. Установка cygwin

Клик finish

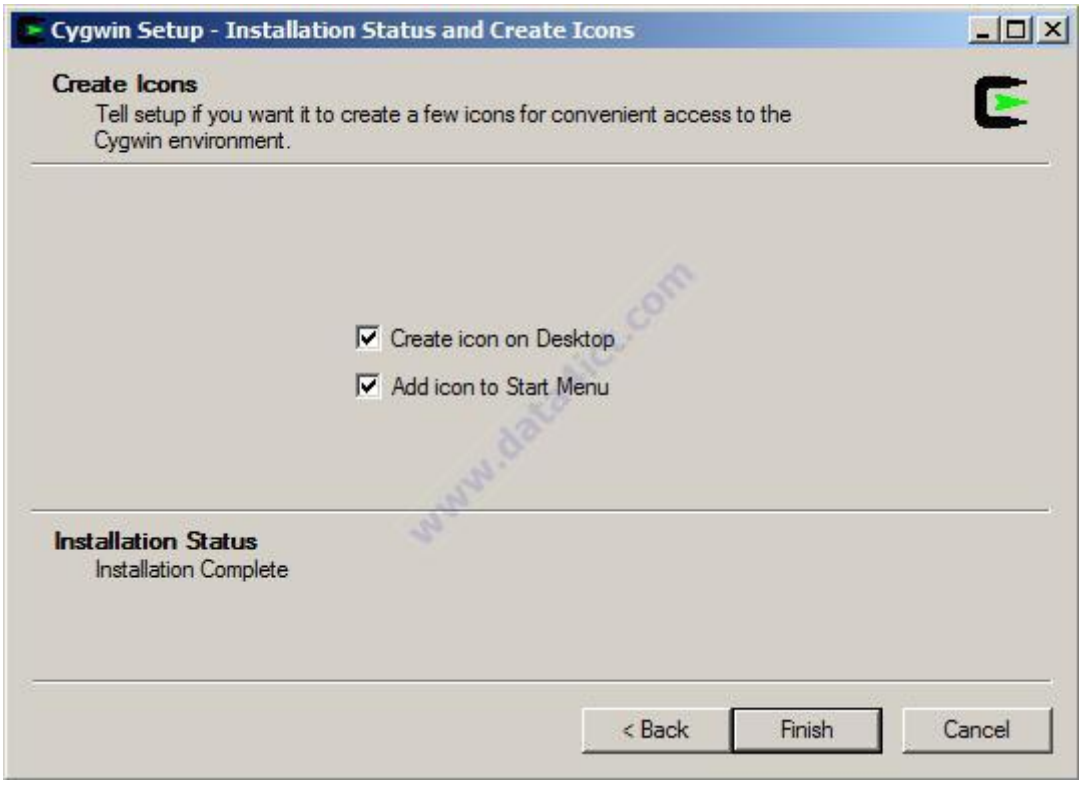


Рис. 2.34. Установка cygwin

Настройка модулей

Чтобы избежать ошибок при запуске программы, нужно настроить файл "modules.conf". Откройте "C:\cygroot\asterisk\etc\modules.conf" файл с помощью блокнота и добавьте следующие строки в конце файла:

noload = pbx_dundi.so

noload = chan_capi.so

noload = chan_fx.so

noload = chan_tapi.so

И удалите:

noload = app_queue.so

В итоге файл должен выглядеть так

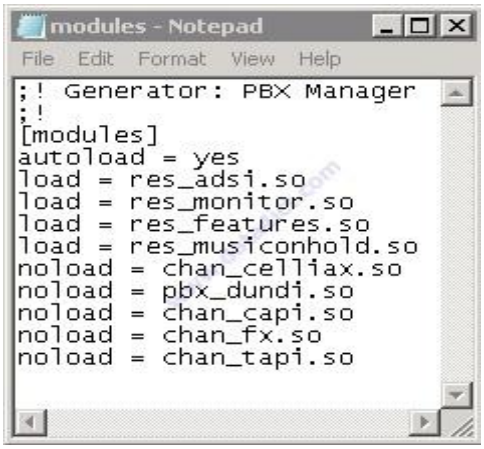


Рис. 2.35. Настройка файла "modules.conf

Теперь снова попробуйте запустить AsteriskW32 GUI , ошибок возникнуть не должно.

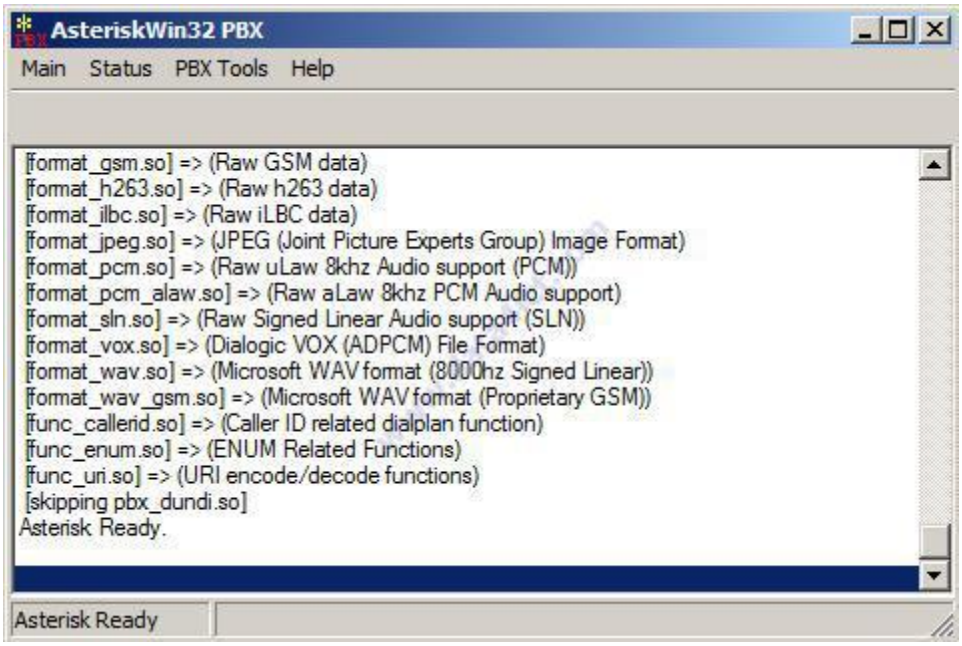


Рис. 2.36. Запуск AsteriskWin32

Настройка Windows Firewall

Откройте Windows Firefall

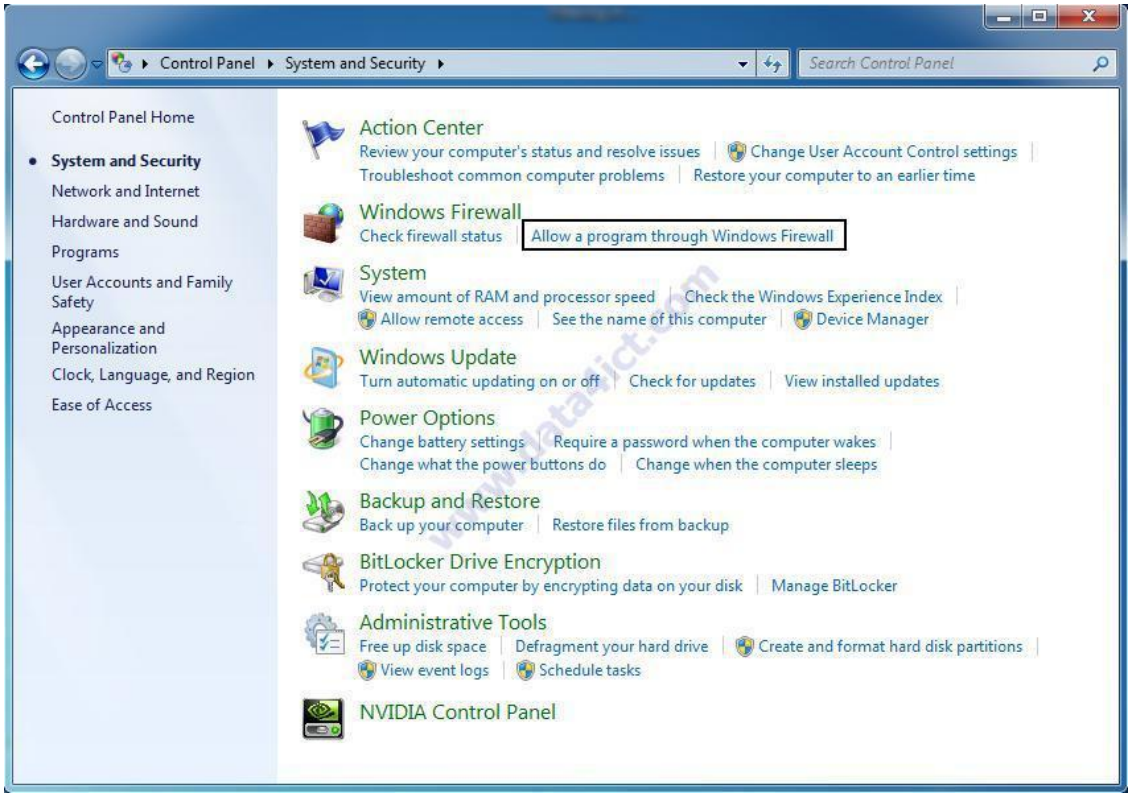


Рис. 2.37. Запуск Windows Firewall

Затем кликните настройки

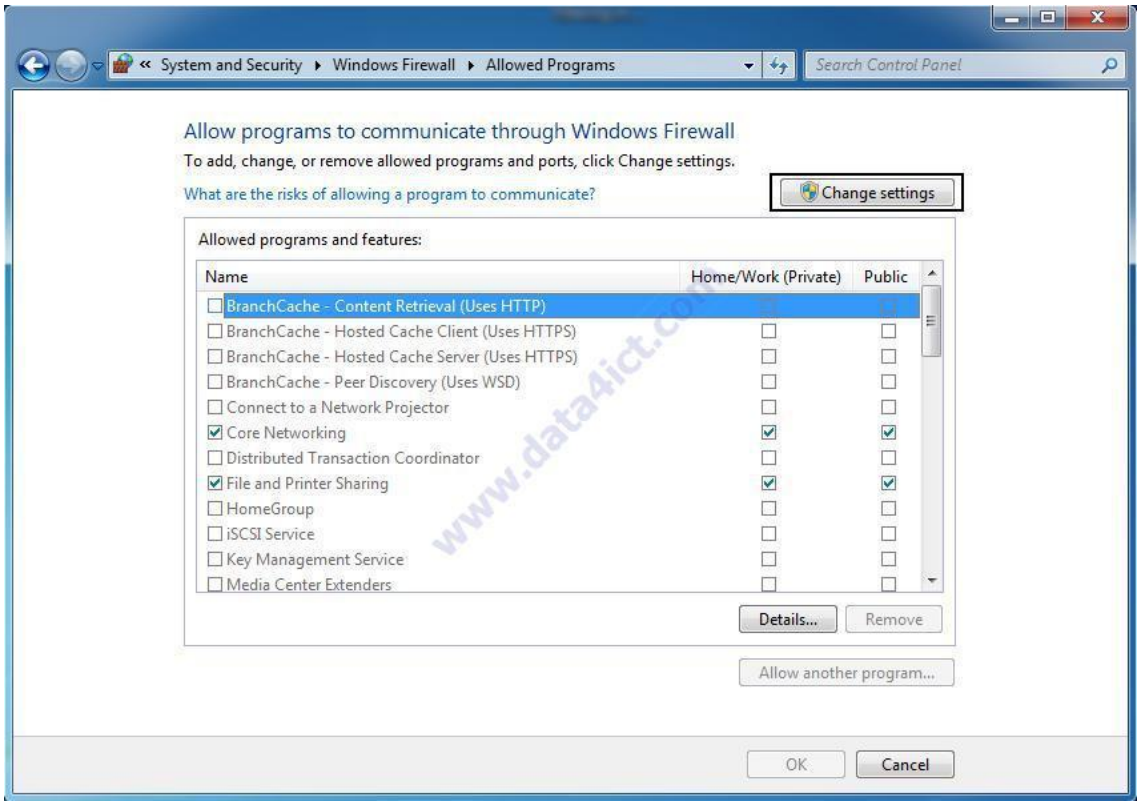


Рис. 2.38. Запуск Windows Firewall

Выберите добавить другую программу

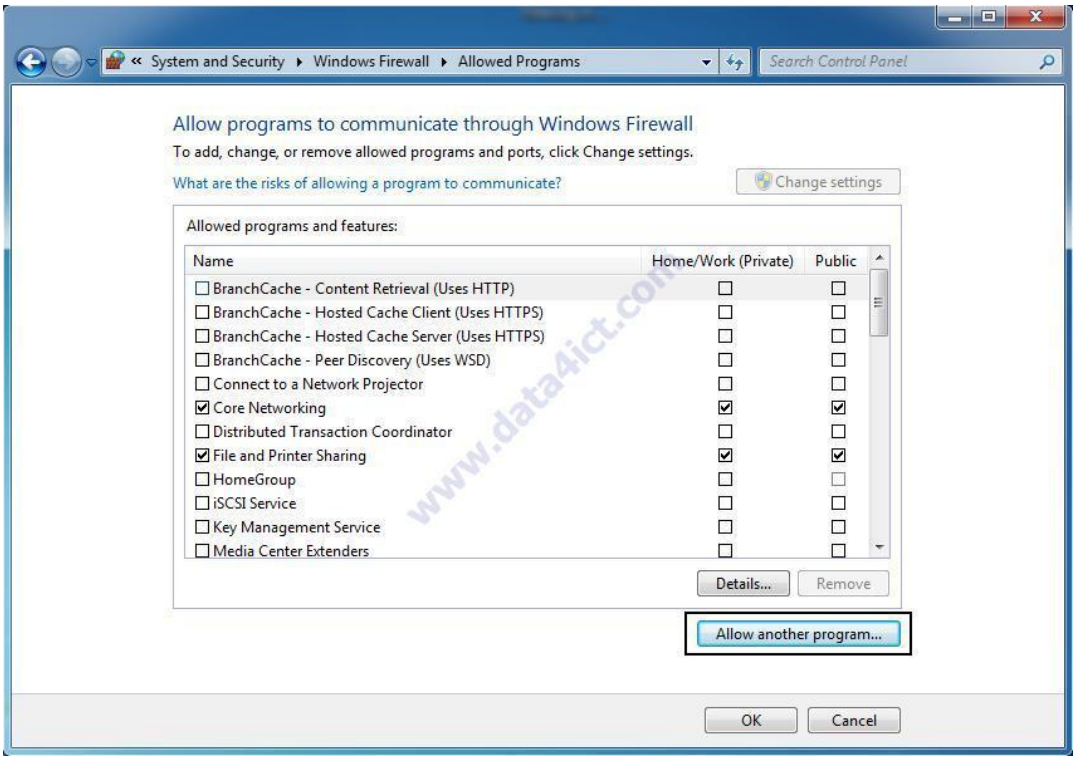


Рис. 2.39. Запуск Windows Firewall

Найдите в списке AsteriskWin32 GUI и нажмите добавить, затем закройте все окна с Windows Firefall

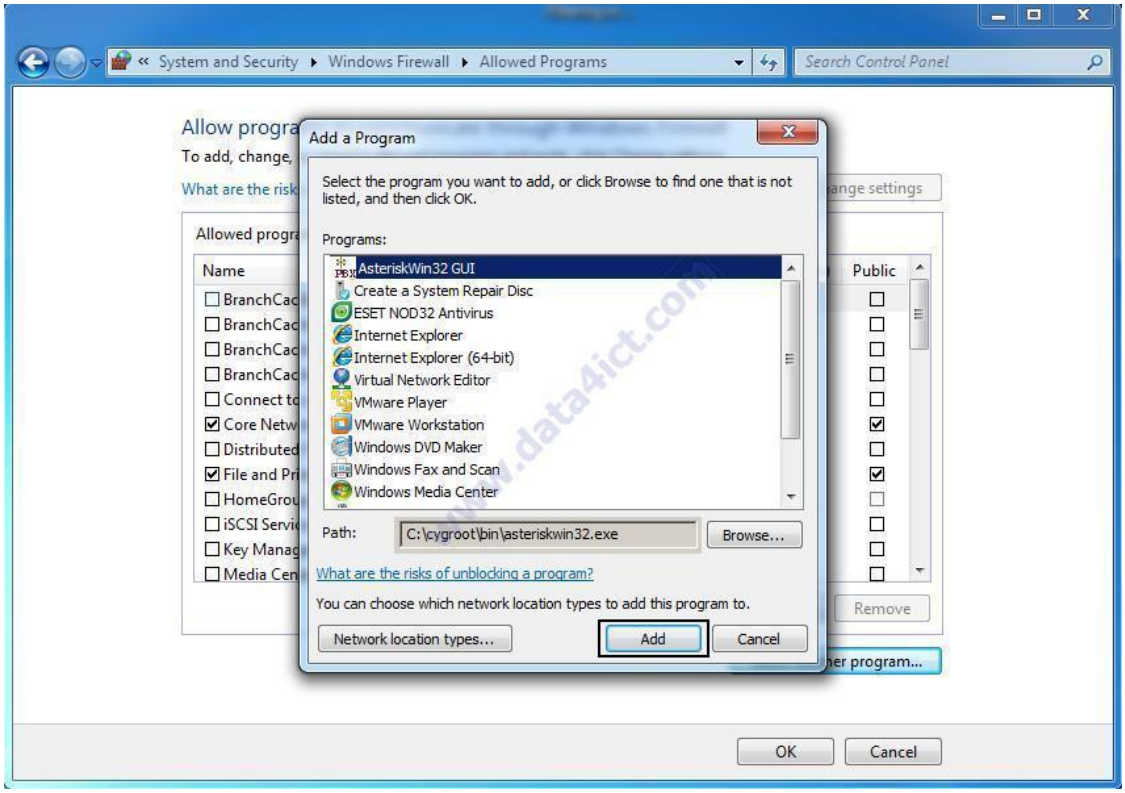


Рис. 2.40. Запуск Windows Firewall

Регистрация в AsteriskWin32

Asterisk имеет различные типы сообщений, которые могут быть зарегистрированы. К ним относятся:

- debug
- notice
- warning
- error
- verbose
- dtmf

logger.conf

Asterisk предоставляет ряд способов для регистрации . Файл logger.conf (Местонахождение: C:\cygroot\asterisk\etc\logger.conf) содержит элементы конфигурации для регистрирования.

;
; Logging Configuration
;
[general]
;
[logfiles]
debug => debug
messages => warning,error
console => notice,warning,error,debug,verbose,dtmf,fax

Первая строка говорит Asterisk, что войти log debug (правая сторона =>) в файл с именем отладки (на левом фланге из =>), расположенный в C:\cygroot\asterisk\log\.

Вторая строка сообщает Asterisk, что возможно зарегистрировать предупреждения и сообщения об ошибках в файл с именем сообщения, расположенные в C:\cygroot\asterisk\log\.

Третья строка говорит Asterisk отправлять все сообщения в CLI консоли.

asterisk.conf

Каталог журнала может быть изменен путем изменения линия astlogdir => asterisk/log to point, чтобы указать на нужный каталог в файле asterisk.conf (C:\cygroot\asterisk\etc\asterisk.conf).

Существуют различные уровни verbosity и debugging. Используйте установить многословным или установить отладки с последующим числовым значением их изменения.

Полезные значения от 0 (disabled) до 10 (maximum) за verbosity и отладки уровнях.

Выставите в окне PBX Manager **set verbose 10**

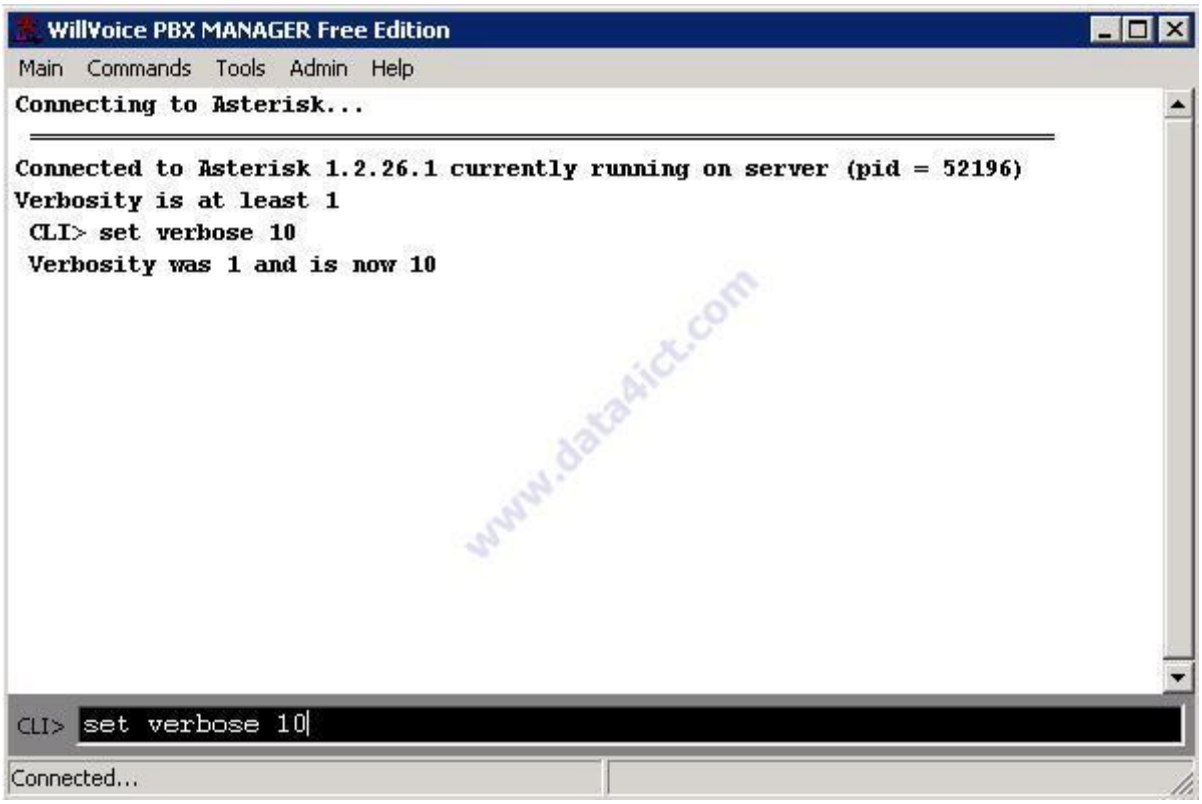


Рис. 5.41. Настройка PBX Manager

Затем выставите **set debug 10**

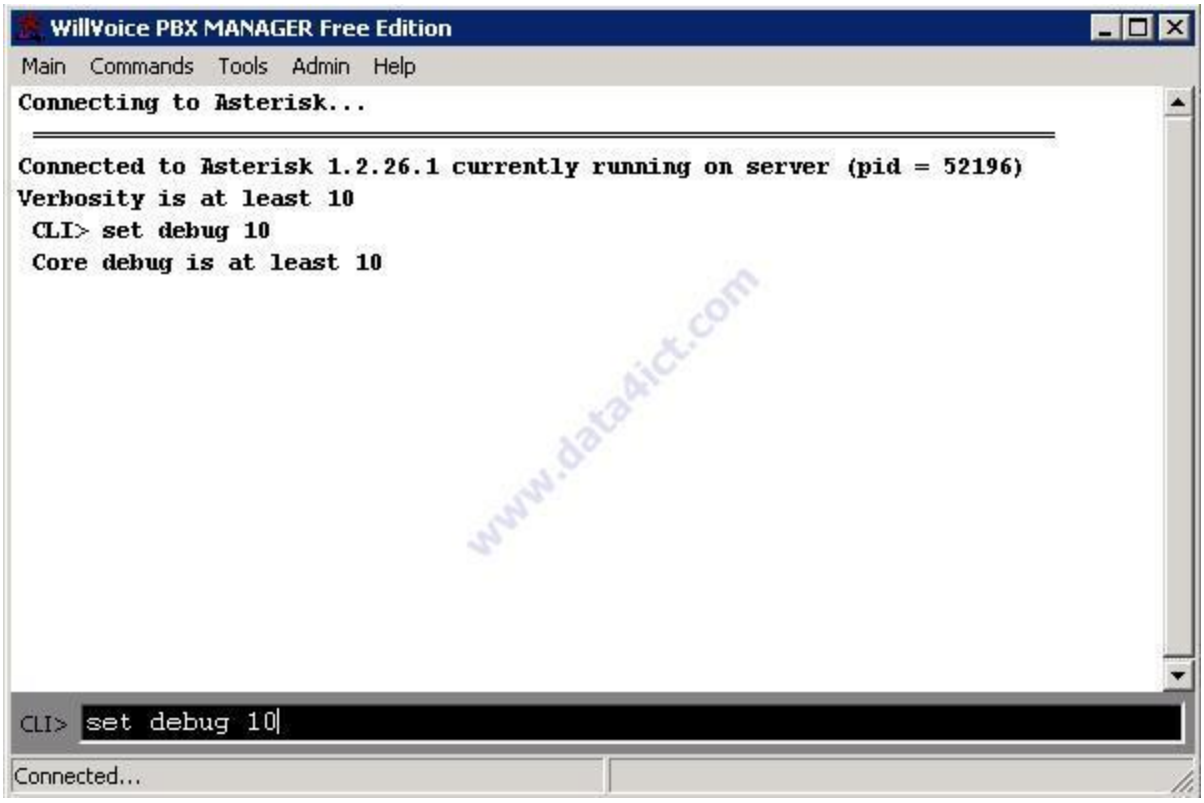


Рис. 5.42. Настройка PBX Manager

Так же возможно активировать другие типы отладки системы: (see asterisk CLI command)

- debug channel / no debug channel

- agi debug / agi no debug
- iax2 debug / iax2 no debug
- sip debug / sip no debug

Воспроизведение основных звонков

sip.conf

Измените название файла sip.conf file (Location: C:\cygroot\asterisk\etc\sip.conf) на sip_old.conf. Затем создайте новый файл sip.conf и вставьте следующее:

```
[general]
context = asterisk        ; Default context for incoming calls
allowguest = no        ; Allow or reject guest calls (default is yes, this can also be set to 'osp'
realm=data4ict.com        ; Realm for digest authentication
bindport = 5060         ; UDP Port to bind to (SIP standard port is 5060)
bindaddr = 0.0.0.0        ; IP address to bind to (0.0.0.0 binds to all)
srvlookup = yes         ; Enable DNS SRV lookups on outbound calls
disallow = all        ; First disallow all codecs
allow = ulaw        ; Allow codecs in order of preference
allow = alaw
allow = gsm
dtmfmode = rfc2833        ; Set default dtmfmode for sending DTMF.
canreinvite=no
nat=yes
[authentication]
[1001]
type=friend
context=asterisk
username=1001
secret=1001
host=dynamic
callerid="Phone1"
[1002]
type=friend
context=asterisk
username=1002
secret=1002
```

host=dynamic

callerid="Phone2"

extensions.conf

The second file to configure is the extensions.conf file (Location: C:\cygroot\asterisk\etc\extensions.conf). Rename it to extensions_old.conf and create a new extensions.conf empty file. Insert the following lines into the file:

Сконфигурируйте файл extensions.conf file (Location: C:\cygroot\asterisk\etc\extensions.conf). Переименуйте его в extensions_old.conf и создайте новый файл extensions.conf, включающий себя :

[general]

;

; If static is set to no, or omitted, then the pbx_config will rewrite

; this file when extensions are modified. Remember that all comments

; made in the file will be lost when that happens.

static=yes

;

; if static=yes and writeprotect=no, you can save dialplan by

; CLI command 'save dialplan' too

;

writeprotect=yes

;

; If autofallthrough is set, then if an extension runs out of

; things to do, it will terminate the call with BUSY, CONGESTION

; or HANGUP depending on Asterisk's best guess (strongly recommended).

;

autofallthrough=yes

;

; If clearglobalvars is set, global variables will be cleared

; and reparsed on an extensions reload, or Asterisk reload.

;

clearglobalvars=no

;

; If priorityjumping is set to 'yes', then applications that support

; 'jumping' to a different priority based on the result of their operations

; will do so (this is backwards compatible behavior with pre-1.2 releases

```
; of Asterisk). Individual applications can also be requested to do this
; by passing a 'j' option in their arguments.
;
priorityjumping=yes
;
;[globals]
;
[internal]
exten => 1001,1,Dial(SIP/1001,20,Tr)
exten => 1001,2,Hangup()
exten => 1002,1,Dial(SIP/1002,20,Tr)
exten => 1002,2,Hangup()
[asterisk]
include => internal
;
; Create an extension, 600, for evaluating echo latency.
;
exten => 600,1,Playback(demo-echotest)    ; Let them know what's going on
exten => 600,2,Echo            ; Do the echo test
exten => 600,3,Playback(demo-echodone)    ; Let them know it's over
```

Настройка ответных звонков

sip.conf

Чтобы включить эту функцию, аккаунт нуждается в номере sip оператора.

С этим аккаунтом вы получите имя пользователя, пароль и sip- адрес или IP- адрес поставщика шлюза sip.

Конфигурация для основных и обратных звонков почти тоже самое, за исключением параметра "type=friend" становится "type=peer". Добавьте следующие строки в sip.conf file (Location: C:\cygroot\asterisk\etc\sip.conf).

```
[DATA4ICT]      - Your provider name
type=peer
username=1008100945      - Your account username
fromuser=1008100945      - Your account username
secret=aZ4kbY3i      - Your account password
host=178.63.114.87      - Your provider gateway
```

В sip.conf file до [general] добавить регистрационное определение:

register => 1008100945:aZ4kbY3i@178.63.114.87

В итоге файл sip.conf должен содержать:

```
[general]
context = asterisk              ; Default context for incoming calls
allowguest = no                 ; Allow or reject guest calls (default is yes, this can
also be set to 'osp'
realm=data4ict.com              ; Realm for digest authentication
bindport = 5060                 ; UDP Port to bind to (SIP standard port is 5060)
bindaddr = 0.0.0.0              ; IP address to bind to (0.0.0.0 binds to all)
srvlookup = yes                 ; Enable DNS SRV lookups on outbound calls
videosupport = yes              ; Enable video
disallow = all                  ; First disallow all codecs
allow = ulaw                    ; Allow codecs in order of preference
allow = alaw
allow = gsm
allow = h263                    ; H.263 is our video codec
allow = h263p                   ; H.263p is the enhanced video codec
dtmfmode = rfc2833              ; Set default dtmfmode for sending DTMF.
canreinvite=no
nat=yes
register => 1008100945:aZ4kbY3i@178.63.114.87
 [authentication]
[1001]
type=friend
context=asterisk
username=1001
secret=1001
host=dynamic
callerid="Phone1"
[1002]
type=friend
context=asterisk
username=1002
```

secret=1002

host=dynamic

callerid="Phone2"

[DATA4ICT]

type=peer

username=1008100945

fromuser=1008100945

secret=aZ4kbY3i

host=178.63.114.87

extensions.conf

Во втором файле настройте extensions.conf (Местонахождение: C:\cygroot\asterisk\etc\extensions.conf). Вставьте следующую строку:

exten => _0.,1,Dial(SIP/DATA4ICT/${EXTEN})

В итоге файл должен содержать:

[general]

;

; If static is set to no, or omitted, then the pbx_config will rewrite

; this file when extensions are modified. Remember that all comments

; made in the file will be lost when that happens.

static=yes

;

; if static=yes and writeprotect=no, you can save dialplan by

; CLI command 'save dialplan' too

;

writeprotect=yes

;

; If autofallthrough is set, then if an extension runs out of

; things to do, it will terminate the call with BUSY, CONGESTION

; or HANGUP depending on Asterisk's best guess (strongly recommended).

;

autofallthrough=yes

;

; If clearglobalvars is set, global variables will be cleared

; and reparsed on an extensions reload, or Asterisk reload.

;

```
clearglobalvars=no
;
; If priorityjumping is set to 'yes', then applications that support
; 'jumping' to a different priority based on the result of their operations
; will do so (this is backwards compatible behavior with pre-1.2 releases
; of Asterisk). Individual applications can also be requested to do this
; by passing a 'j' option in their arguments.
;
priorityjumping=yes
;
;[globals]
;
[internal]
exten => 1001,1,Dial(SIP/1001,20,Tr)
exten => 1001,2,Hangup()
exten => 1002,1,Dial(SIP/1002,20,Tr)
exten => 1002,2,Hangup()
[asterisk]
include => internal
;
; Create an extension, 600, for evaluating echo latency.
;
exten => 600,1,Playback(demo-echotest)    ; Let them know what's going on
exten => 600,2,Echo                       ; Do the echo test
exten => 600,3,Playback(demo-echodone)  ; Let them know it's over


exten => _0.,1,Dial(SIP/DATA4ICT/${EXTEN})
```

Установка ПО

ПО на первом компьютере (серверный)

Сейчас основная установка системы завершена. Скачайте софтфон X-Lite (бесплатный sip телефон) и установите его. Линк: http://www.counterpath.com/x-lite-download.html/.

Двойной клик по скачанному файлу"X-Lite_Win32_4.0_58832" и начнется установка. После запустите программу, кликните "Softphone", затем по "Account Settings"

Рис. 2.43. Настройка X-Lite

В поле User ID введите : 1001

- Domain: IP address of the asterisk server
- Password: 1001
- Display name: 1001
- Click "OK"

Как показано на рисунке 2.44

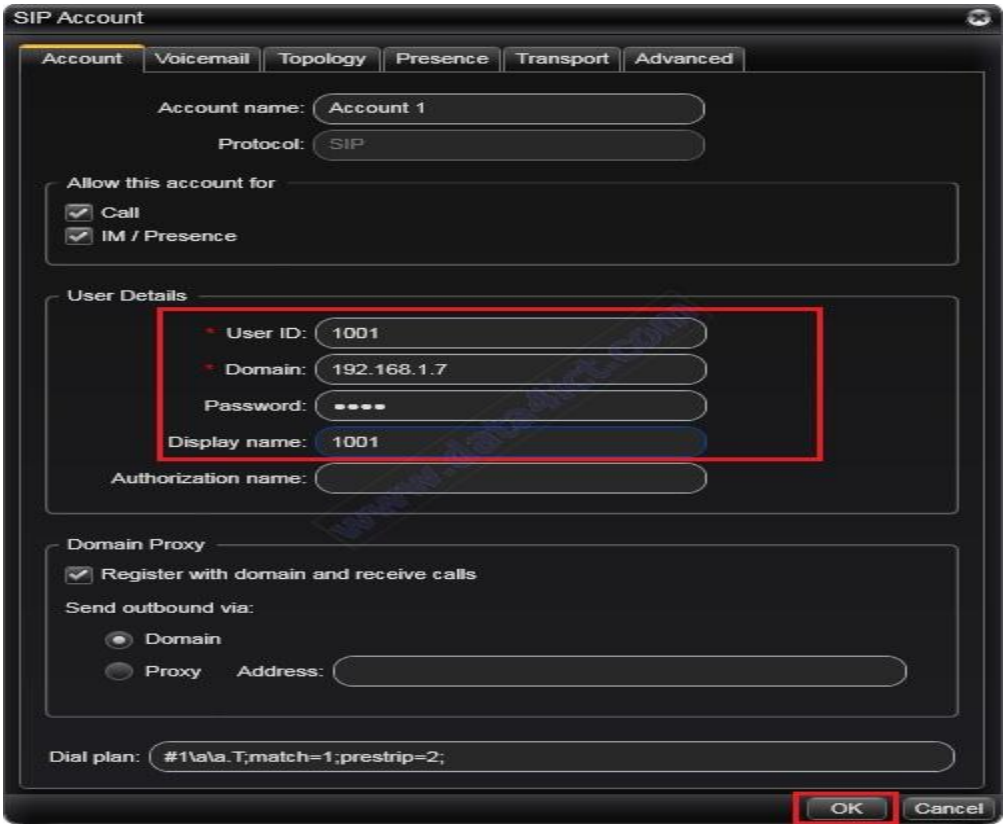


Рис. 2.44. Регистрация абонента

После регистрации , телефон готов производить звонки.

X-Lite (Второй компьютер)

Установите Xlite на втором компьютере по следующим конфигурациям:

- User ID: 1002
- Domain: IP address of the asterisk server
- Password: 1002
- Display name: 1002

Проверка

Откройте AsteriskWin32 PBX, откройте вкладку Status, затем CLI Console.

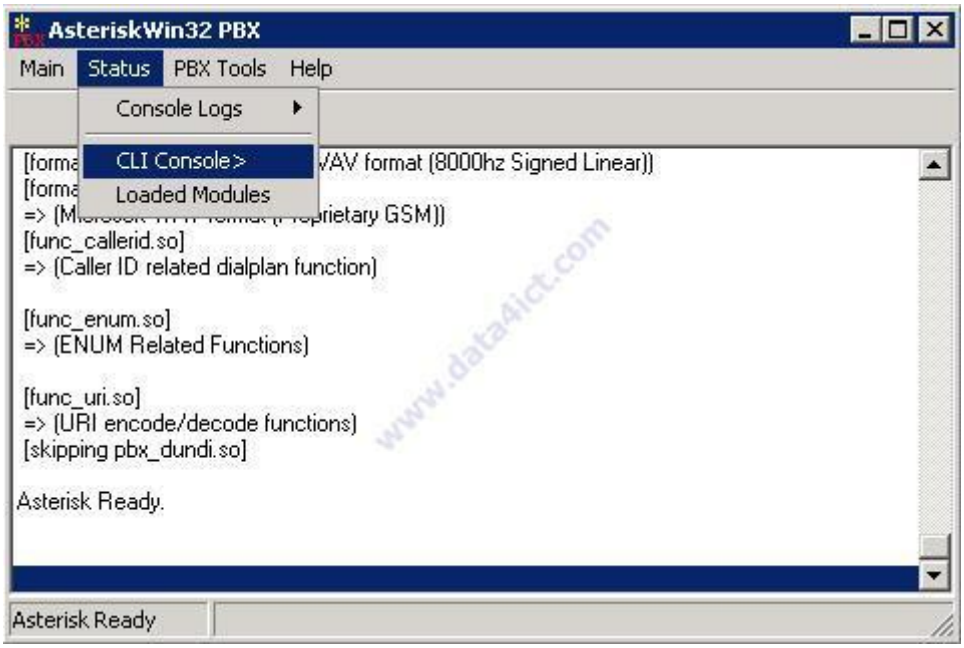


Рис. 2.45. Проверка правильности регистрации абонентов

В открытом окне CLI Console введите команду sip show peers, эта команда позволит просмотреть сведения о зарегистрированных абонентах в сети.

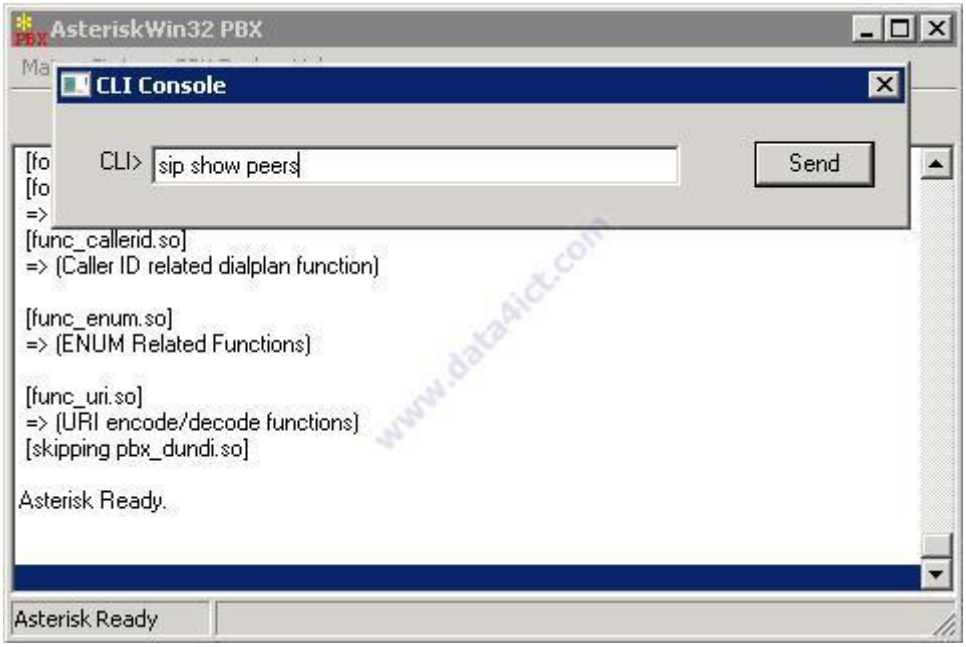


Рис. 2.46. CLI Console

Если все сделали по инструкции, то должно вывести информацию об абонентах: Имя,IP-адрес, Порт, Статус.

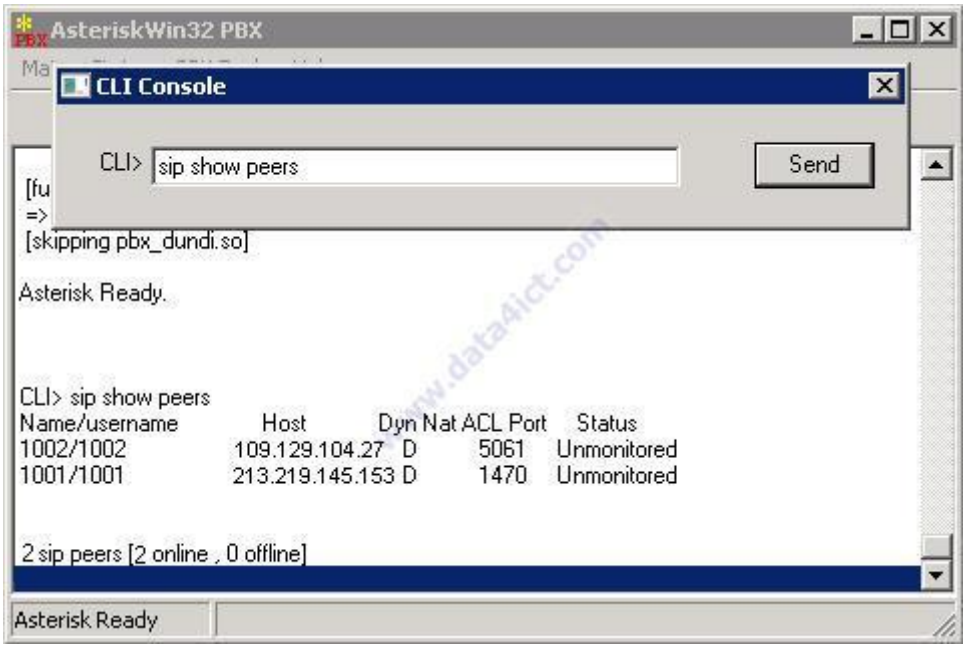


Рис. 2.47. Информация об абонентах

2.2. Проектирование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения VIPNET OFFICE [7, 8]

В связи с широким распространением персональных компьютеров не только как средств обработки информации, но и как оперативных средств коммуникации (электронная почта), возникают проблемы, связанные с обеспечением защиты информации от ее перехвата, преднамеренных или случайных искажений. Развитие информационных технологий сопровождается, к сожалению, ростом компьютерных преступлений, связанных с хищением конфиденциальной и другой информации, а также обусловленных этим обстоятельством материальных потерь. Первое компьютерное преступление, совершенное в городе Миннеаполисе в 1958 г., состояло в подделке банковских документов с помощью компьютера. По некоторым данным, утечка 20 % коммерческой информации в 60 % случаев приводит к банкротству фирмы. И это немудрено, поскольку по существующей статистике

при ограблении банка потери (в среднем) составляют 19 тысяч долларов, а при компьютерном преступлении – 560 тысяч долларов.

Актуальность проблемы защиты информации подчеркивается тем обстоятельством, что персональный компьютер или автоматизированное рабочее место является частью систем обработки информации, систем коллективного пользования, вычислительных сетей. Причины активизации компьютерных преступлений заключаются именно в том, что информационные технологии позволили реализовать идею академика В. М. Глушкова о безбумажных технологиях [1], создающих «…прочную основу для перестройки управления социально-экономическими процессами на основе безбумажной технологии в масштабах целой отрасли, крупного региона и даже целой страны». Однако обоснованное им еще в XX в. объединение вычислительных машин в крупные сети, впоследствии реализованное в виде всемирной сети Интернет, вызвало необходимость в предъявлении достаточно жестких требований к надежности и достоверности передаваемой информации, к предотвращению несанкционированного доступа к документам, передаваемым по сетям связи.

ViPNet OFFICE

ViPNet OFFICE — программное обеспечение для организации виртуальных частных защищенных сетей (VPN) типовых конфигураций (защищенных сетей ViPNet™). ViPNet OFFICE предназначен для использования в небольших локальных и распределенных IP-сетях и обеспечивает защищенную работу удаленных пользователей с любым типом подключения к сети Интернет.

ViPNet OFFICE — это программный комплекс, в состав которого входит три основных компонента:

1. ViPNet Manager (Менеджер) — рабочее место Администратора защищенной сети, предназначенное для развертывания и управления VPN-сетью. ViPNet Менеджер обладает интерфейсом, удобным и доступным даже для неподготовленных пользователей, что позволяет более простым и понятным образом задавать и изменять структуру защищенной VPN-сети.
2. ViPNet Coordinator (Координатор) — серверное программное обеспечение, которое выполняет функции межсетевого экрана, сервера IP-адресов, сервера защищенной почты.
3. ViPNet Client (Клиент) — программное обеспечение, которое устанавливается на рабочее место пользователя и выполняет функцию персонального сетевого экрана. В состав ViPNet Client входят такие программы как «Деловая почта», «Файловый обмен», «Обмен защищенными сообщениями» (чат), «Контроль приложений», а также поддерживаются

механизмы ЭЦП — всё это делает рабочее место пользователя не только защищенным, но и многофункциональным.

При первоначальном развертывании ViPNet OFFICE обладает фиксированной конфигурацией. Существуют 4 фиксированные конфигурации:

ViPNet OFFICE 1–5 (1 — ViPNet Менеджер, 1 — ViPNet Координатор, 5 — ViPNet Клиент, 5 — туннельных лицензий);

ViPNet OFFICE 2–10 (1 — ViPNet Менеджер, 2 — ViPNet Координатор, 10 — ViPNet Клиент, 10 — туннельных лицензий);

ViPNet OFFICE 2–0 (1 — ViPNet Менеджер, 2 — ViPNet Координатор, 20 — туннельных лицензий);

ViPNet Office 3–0 (1 — ViPNet Менеджер, 3 — ViPNet Координатор, 30 — туннельных лицензий).

Основные отличия между ViPNet CUSTOM и ViPNet OFFICE:

- Основное отличие программного комплекса ViPNet OFFICE от ViPNet CUSTOM состоит в том, что для развертывания, модификации и управления защищенной VPN-сетью в ViPNet OFFICE используется ViPNet Manager, а не ViPNet Administrator.
- ViPNet Manager обладает интерфейсом, удобным и доступным даже для неподготовленных пользователей, что позволяет более простым и понятным образом задавать и изменять структуру защищенной VPN-сети.
- При необходимости, ViPNet OFFICE позволяет расширять фиксированную конфигурацию (путем добавления лицензий на программные компоненты ViPNet Coordinator и ViPNet Client), изменять количество туннельных лицензий, в зависимости от необходимого количества данных компонент в защищенной сети.
- ViPNet OFFICE позволяет осуществлять межсетевое взаимодействие между двумя VPN-сетями, построенными как на базе ViPNet OFFICE, так и на базе ViPNet CUSTOM. Благодаря этому возможно организовать VPN-сети любых произвольных конфигураций.

Основные преимущества:

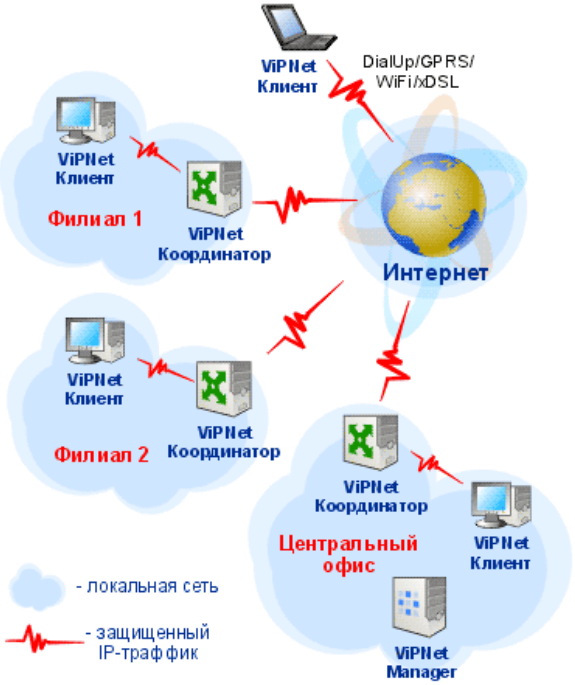
- Простое и понятное программное обеспечение для создания защищенной сети, для использования которого не требуется специальных познаний в области защиты информации, а также приобретения дополнительного оборудования и изменения структуры уже существующей сети.
- Минимальные затраты на создание и обслуживание собственной VPN-сети.
- Надежная защита сетевого трафика, не мешающая работе дополнительных приложений и прикладных задач.

- Гибкий подход к построению VPN-сетей на базе уникальных технологий ViPNet позволяет создавать и связывать между собой разные сети ViPNet, обеспечивать более гибкий подход к созданию различных сетевых конфигураций, создавать территориально распределенные подсети, управляемые из центрального офиса.
- Мастер развертывания сети позволяет пошагово создать структуру сети без дополнительных настроек на сетевых узлах.
- Возможность ограничивать интерфейс пользователя на сетевом узле позволяет централизованно управлять политиками безопасности в защищенной сети.
- Автоматизированная обработка и прием запросов на сертификаты ЭЦП.
- Совместимость с решениями Linux, включая возможность централизованного обновления ПО на Linux-координаторах и ПАК.

С помощью ViPNet OFFICE Вы сможете:

- Обеспечить защищенный обмен данными, в том числе и защищенный документооборот между несколькими офисами или филиалами компании. При этом в каждом из филиалов может быть собственная VPN-сеть либо подсеть, управляемая из центрального офиса.
- Организовать удаленный защищенный доступ сотрудников компании или руководства через Интернет к конфиденциальным ресурсам локальной сети компании и одновременно обеспечить защиту их мобильных компьютеров от возможных сетевых атак.
- Обеспечить разграничение доступа внутри локальной сети, например, обеспечить доступ к серверу с конфиденциальной информацией определенной группе лиц, при этом остальные пользователи той же сети не будут даже подозревать о его существовании.
- Обеспечить простое и удобное использование электронно-цифровой подписи как внутри VPN-сети, так и с помощью стандартных почтовых офисных приложений (Microsoft Outlook, Outlook Express).

Типовая схема защищенной сети на базе решения ViPNet OFFICE:



Комментарии к схеме:

- ПО ViPNet Manager устанавливается в Центральном офисе компании.
- ПО ViPNet Coordinator устанавливается в Центральном офисе и Филиалах компании, на входе в локальную сеть, на серверы-маршрутизаторы, и выполняет роль межсетевого экрана и криптошлюза для организации защищенных туннелей между удаленными локальными сетями.
- ПО ViPNet Client может быть установлено как внутри локальных сетей (на рабочих станциях сотрудников), так и на мобильные компьютеры для организации защищенного удаленного доступа к ресурсам локальных сетей. ViPNet Client в этом случае выполняет роль персонального сетевого экрана и шифратора IP-трафика.
- Одновременно с работой в защищенной сети ViPNet Coordinator и ViPNet Client могут выполнять фильтрацию обычного, незашифрованного IP-трафика, что позволяет обеспечить необходимую работу серверов и рабочих станций с открытыми ресурсами Интернета (веб-страницами) или локальных сетей (сетевыми принтерами, незащищенными рабочие станции и серверами).

Испытание системы защищенного межсетевого взаимодействия

В качестве объекта испытания будет выступать виртуальная сеть, состоящая из четырех виртуальных машин (далее ВМ), развернутая в среде VMwareWorkstation. На трех ВМ выполняется установка ПО ViPNetOFFICE, обеспечивая, таким образом, защищенное

межсетевое взаимодействие в данном сегменте сети. Четвертая ВМ служит интересам предполагаемого злоумышленника и предназначена для захвата циркулирующего в сети трафика с помощью программы-сниффера Wireshark .

Данный макет моделирует межсетевое взаимодействие между компьютерами головного отделения и филиала учреждения посредствам открытых ССОП. Так как ССОП находятся вне контролируемой зоны, возможен перехват ПДн злоумышленником и нарушение их конфиденциальности, целостности и доступности.

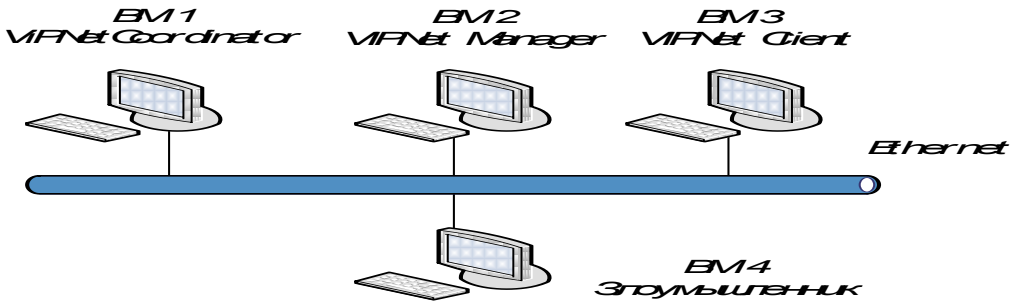


Рис. 2.47. Схема макета VIPNet

План испытания

Испытание состоит из нескольких этапов, характерной особенностью которых является исследование открытого и защищенного сетевого взаимодействия:

1) развораччивание виртуальной сети;
2) исследование открытого сетевого взаимодействия:
– перехват и анализ текстового файла;
– перехват и анализ ping-пакетов;
3) установка ПО ViPNetOFFICE;
4) исследование защищенного сетевого взаимодействия:
– перехват и анализ текстового файла;
– перехват и анализ ping-пакетов.

Ход испытания

Разворачивание виртуальной сети

После выполнения установки VMwareWorkstationв ней создаются четыре ВМ со следующими основными параметрами:

– объем ОЗУ 512 Мбайт;
– объем жесткого диска 10 Гбайт;
– ОСWindowsXP.

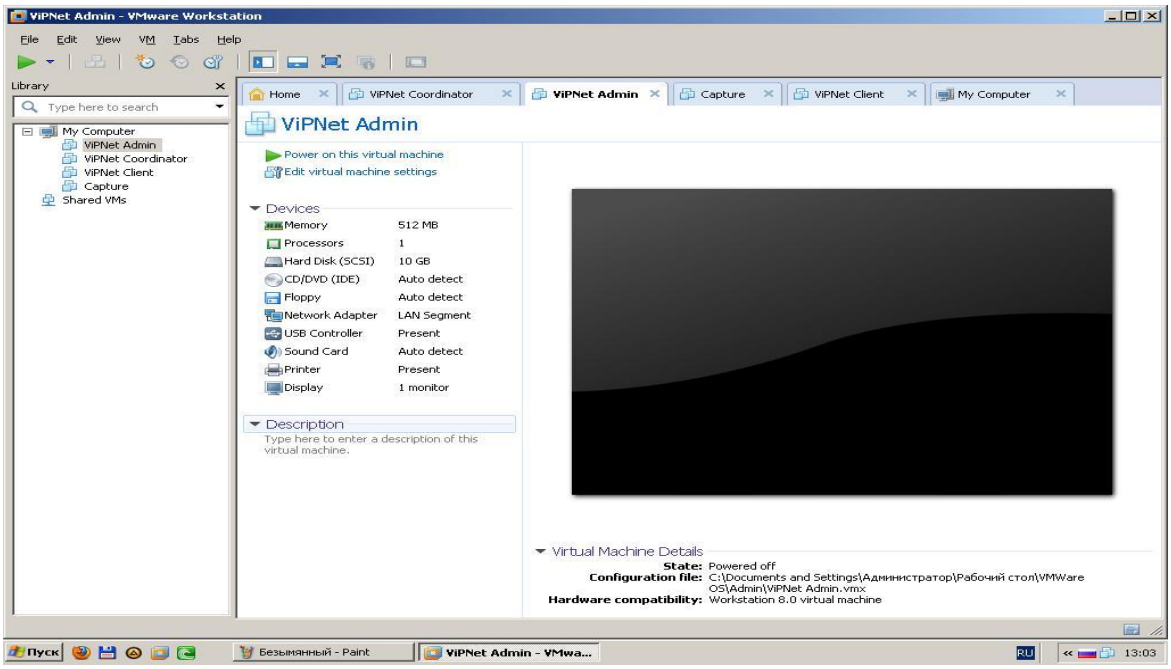


Рис. 2.48. ОбщийвидVMwareWorkstation

Виртуальные машины объединяются в виртуальную сеть с адресацией, представленной в таблице 2.4.

Таблица 2.4. Сетевая адресация виртуальных машин

	ВМ 1	ВМ 2	ВМ 3	ВМ 4
IPадрес	192.186.1.1	192.186.1.2	192.186.1.3	192.186.1.4
Маска подсети	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

На ВМ 4 устанавливается программа-сниффер Wireshark, с помощью которой захватывается и анализируется сетевой трафик. Процесс установки отображен на следующих рисунках.

Рис. 2.49. Мастер установки Wireshark

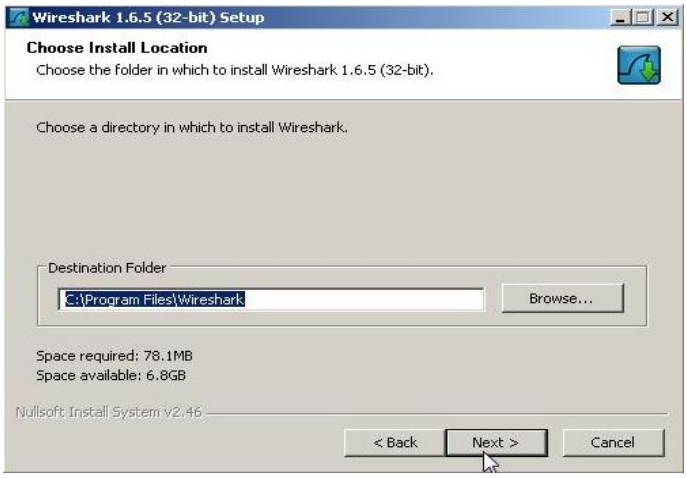


Рис. 2.50. Выбор директории установки

Рис. 2.51. Завершение установки

Исследование открытого сетевого взаимодействия

Для исследования открытого сетевого взаимодействия на ВМ 2 создается текстовый файл Test.txt, который передается на ВМ 3 по протоколу SMB (ServerMessageBlock).

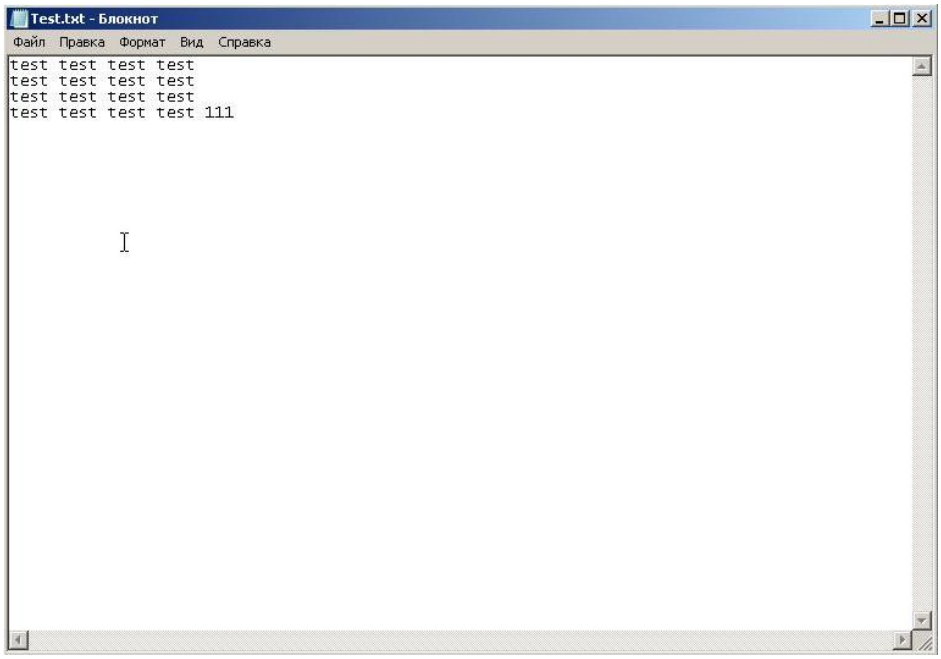


Рис. 2.52. Текстовый файл Test.txt

При передаче происходит захват пакетов на ВМ 4, что отображается в окне сниффера Wireshark. Протокол SMB принадлежит стеку TCP, поэтому при анализе отображается содержимое TCP-пакетов.

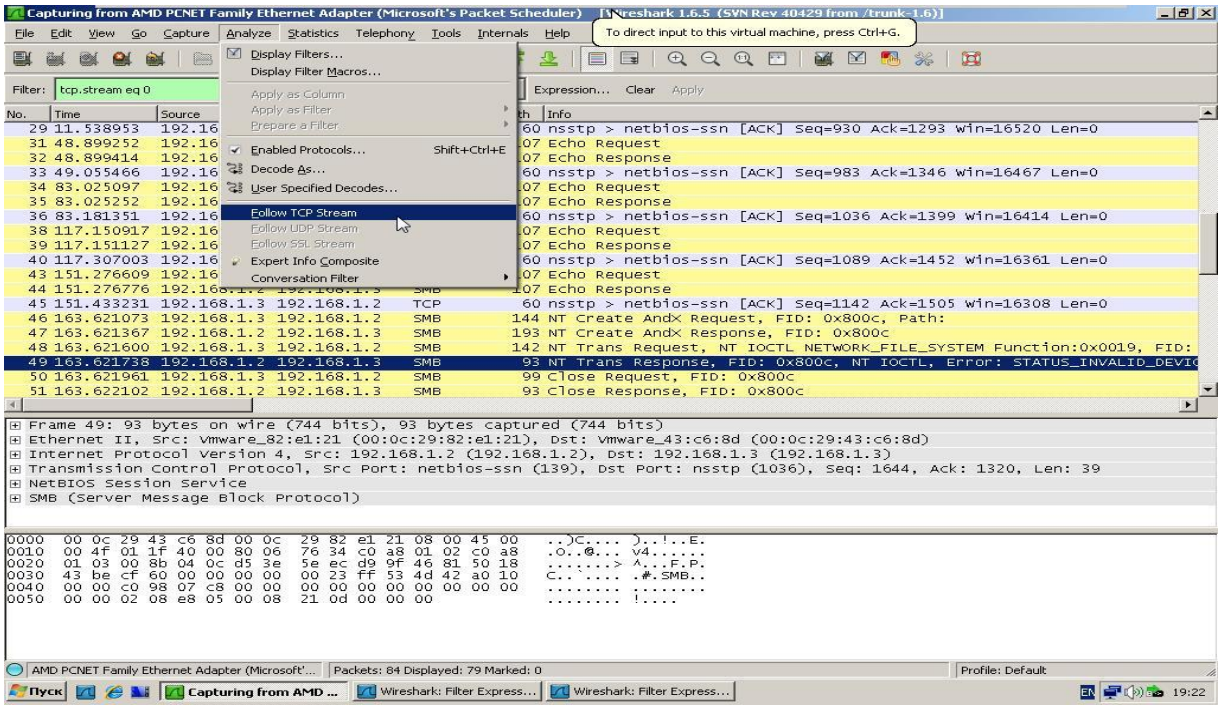


Рис. 2.53. Процесс отображения TCP-пакетов

На следующем рисунке видно, что среди содержимого пакетов отображается переданный текст файла Test.txt.

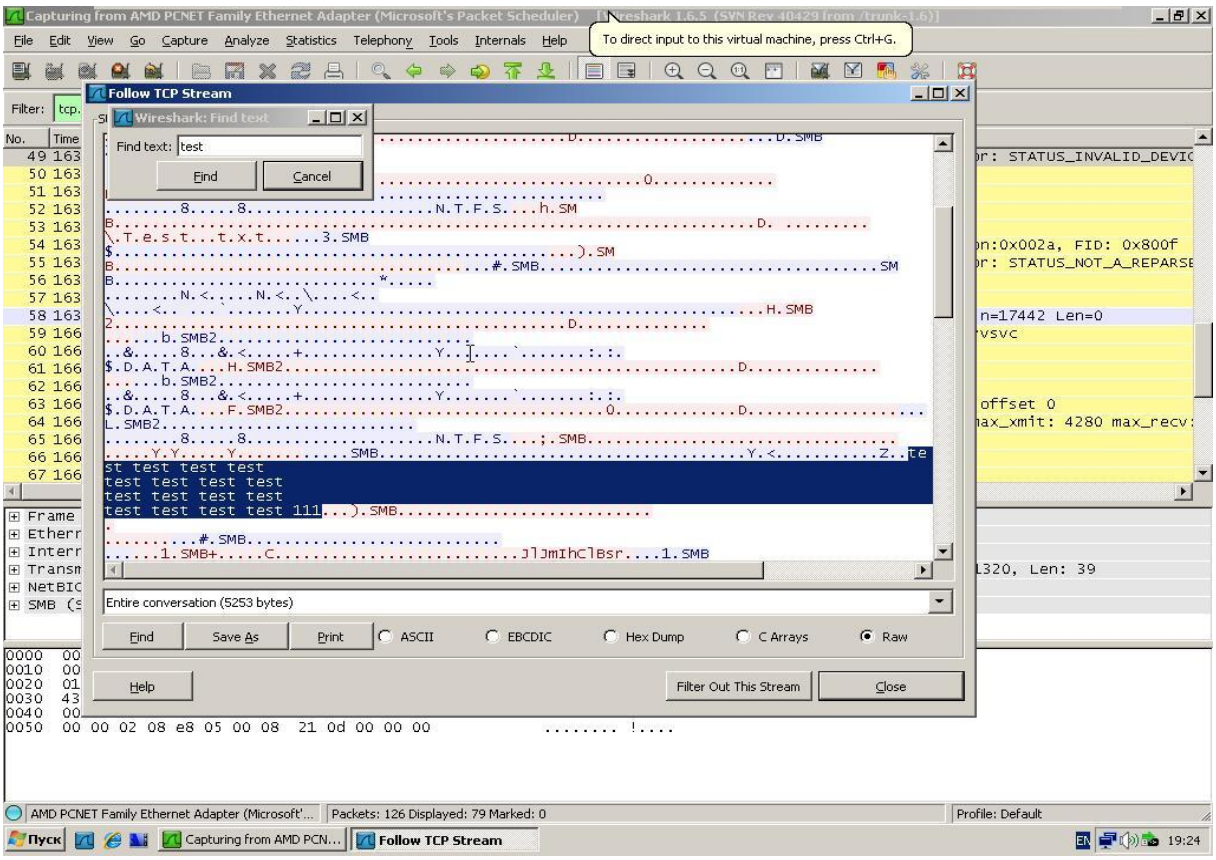


Рис. 2.54. Содержимое TCP-пакетов

Так же в программе Wireshark существует возможность работать с SMBтрафиком, то есть непосредственно перехватить передаваемый файл Test.txt. Этот процесс отображается на следующих рисунках.

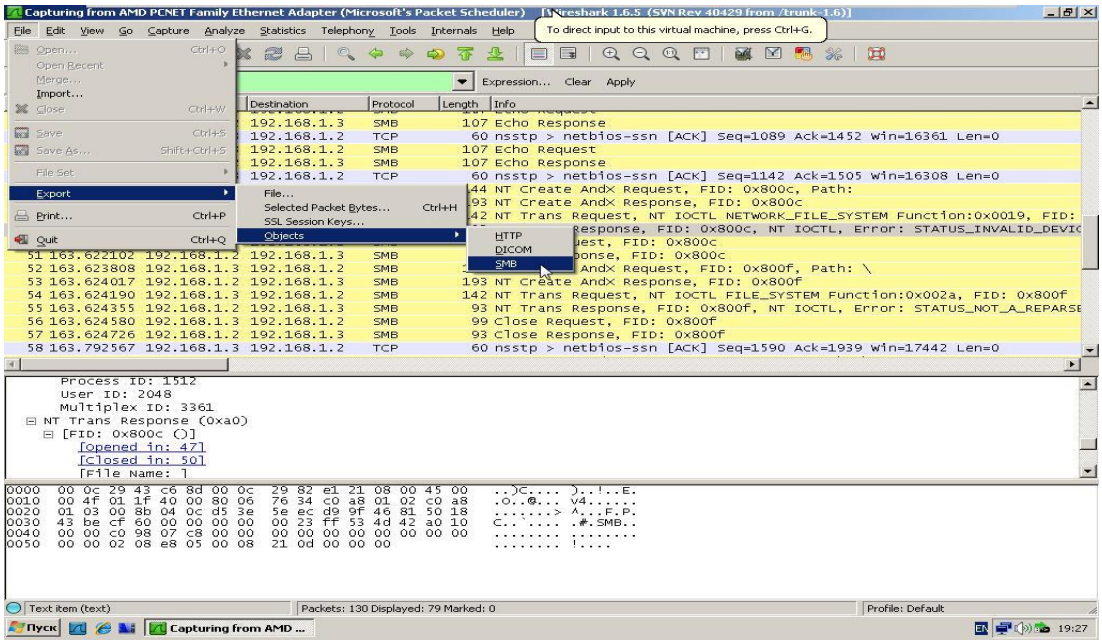


Рис. 2.55. Выбор SMB объекта для экспорта

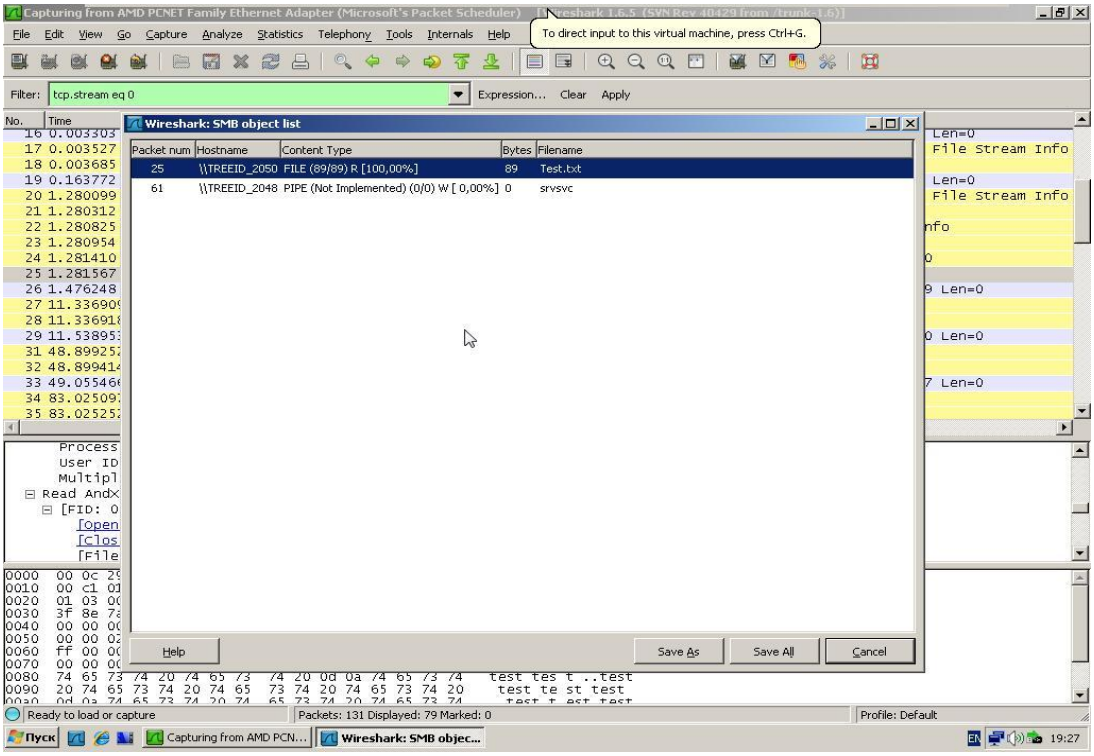


Рис. 2.56. Отображение захваченного SMB объекта

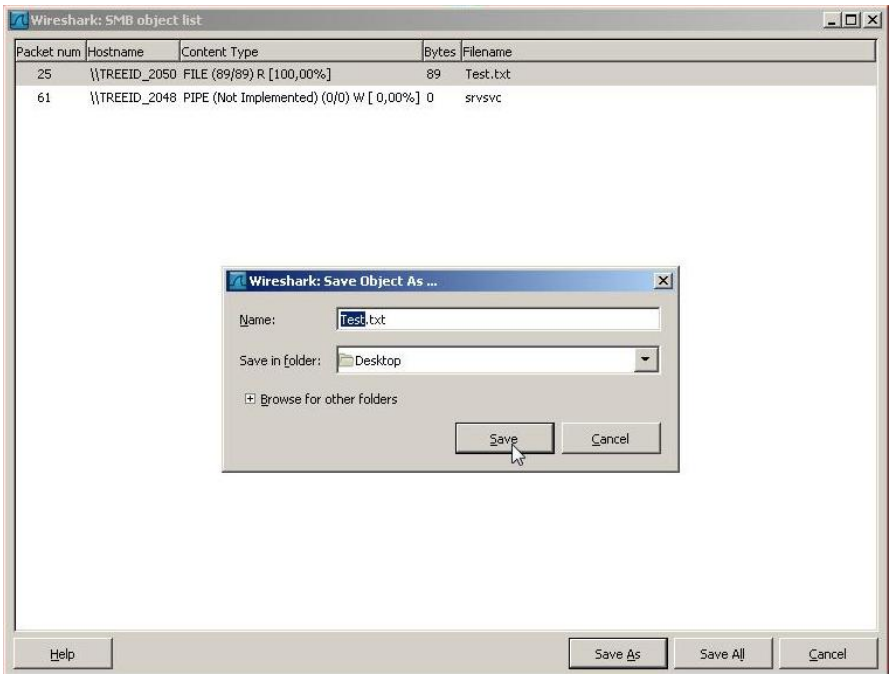


Рис. 2.57. Сохранение перехваченного объекта

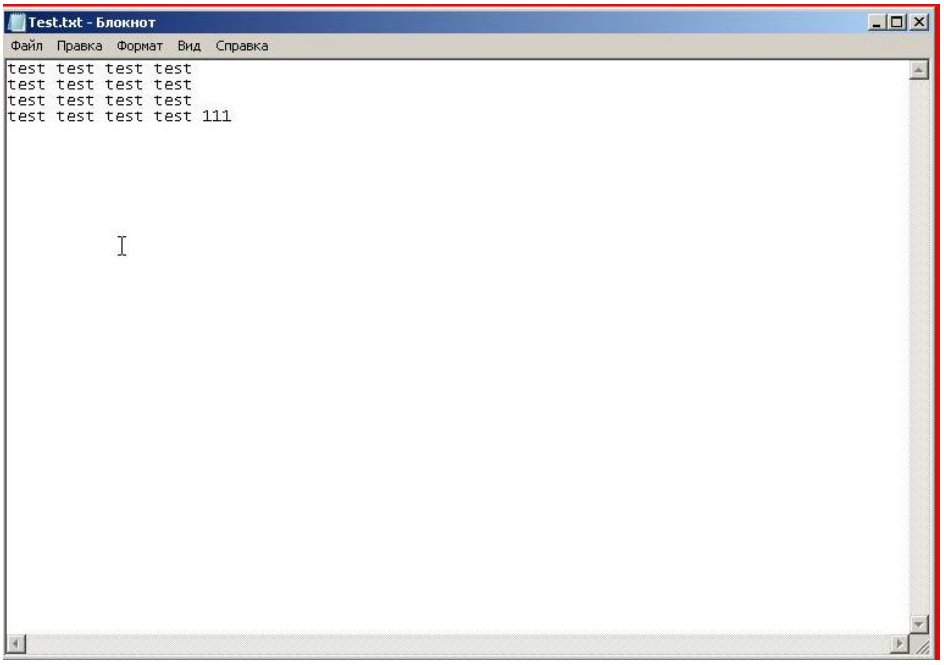


Рис. 2.58. Содержимое перехваченного объекта

Далее происходит запуск утилиты ping на ВМ 2 для проверки соединения с ВМ 3.

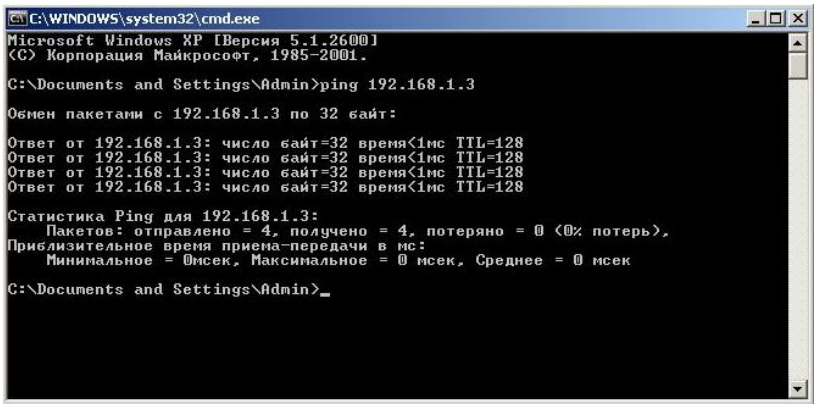


Рис. 2.59. Запуск утилиты ping

В результате в сети появляются ICMP-пакеты (Internet Control Message Protocol), которые захватываются снифферо.

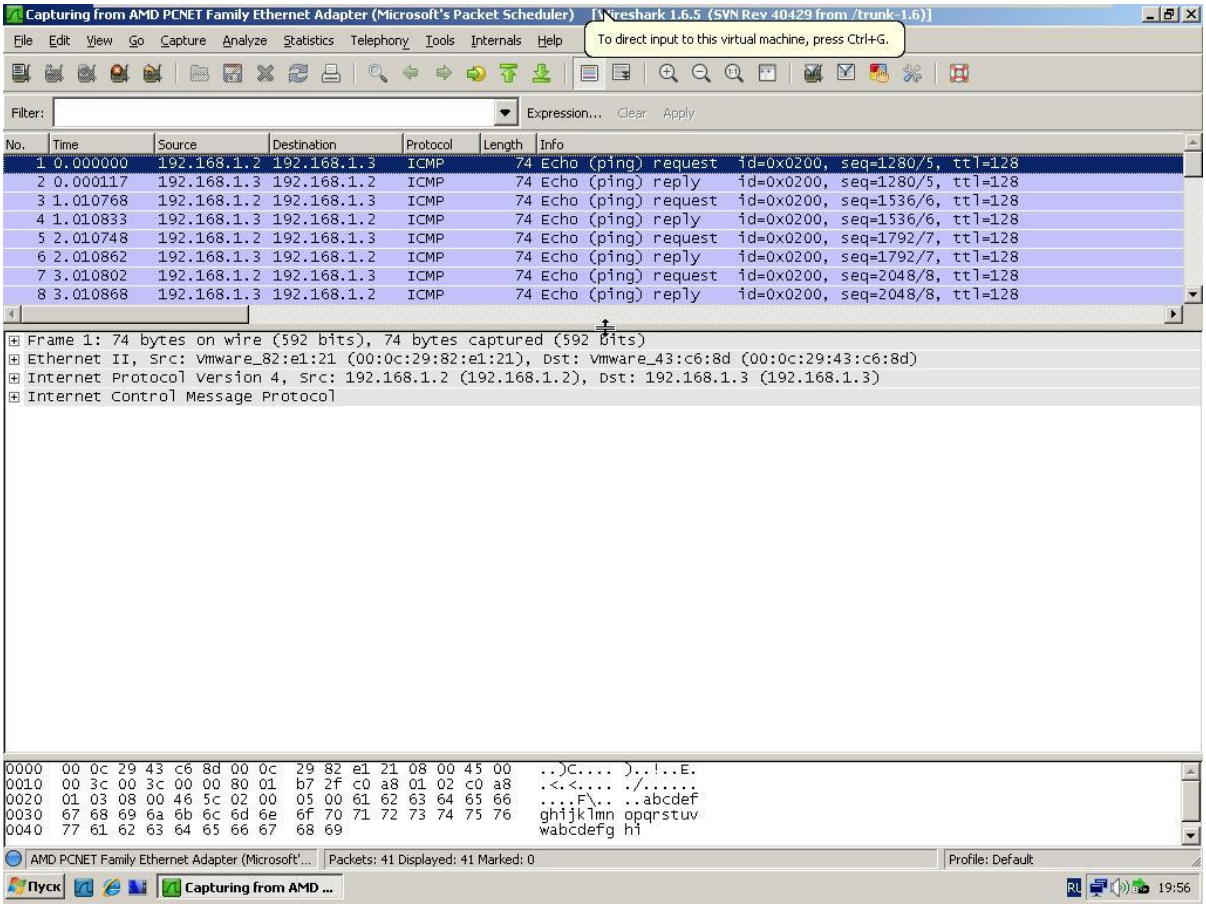


Рис. 2.60. Захваченные ICMP-пакеты

Таким образом, весь передаваемый трафик при передаче в открытом виде представляется неизменным, что подтверждается его анализом в снифферe.

Установка ПО ViPNet OFFICE

Для организации защищенного сетевого взаимодействия на ВМ устанавливается специализированное ПО ViPNet.

При этом в качестве менеджера (ViPNetManager) сети ViPNetвыступает ВМ 2, в качестве координатора (ViPNet Coordinator) сети – ВМ 1, и в качестве клиента (ViPNet Client) – ВМ 3. Процесс установки и конфигурирования ПО отображается на следующих рисунках.

Установка ПО начинается с установки ViPNet Manager и ViPNet Client на ВМ 2.

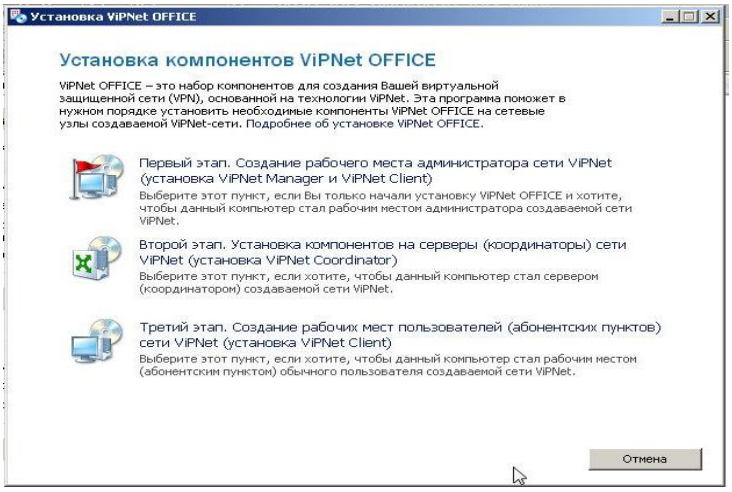


Рис. 2.61. Первый этап - создание рабочего места администратора сети ViPNet

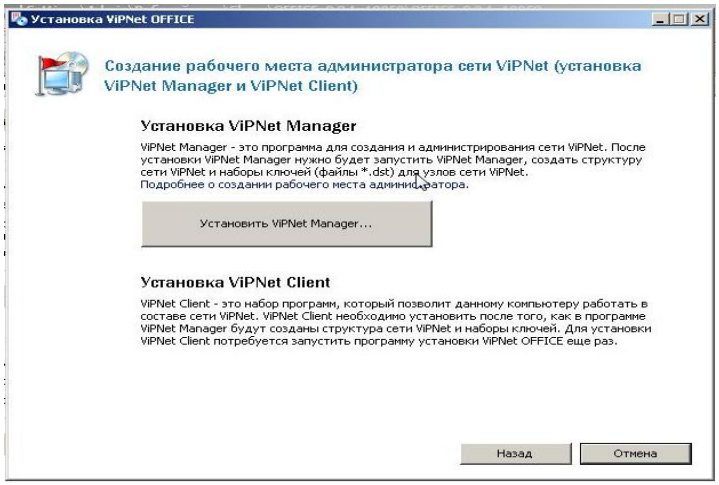


Рис. 2.62. Установка ViPNetManager

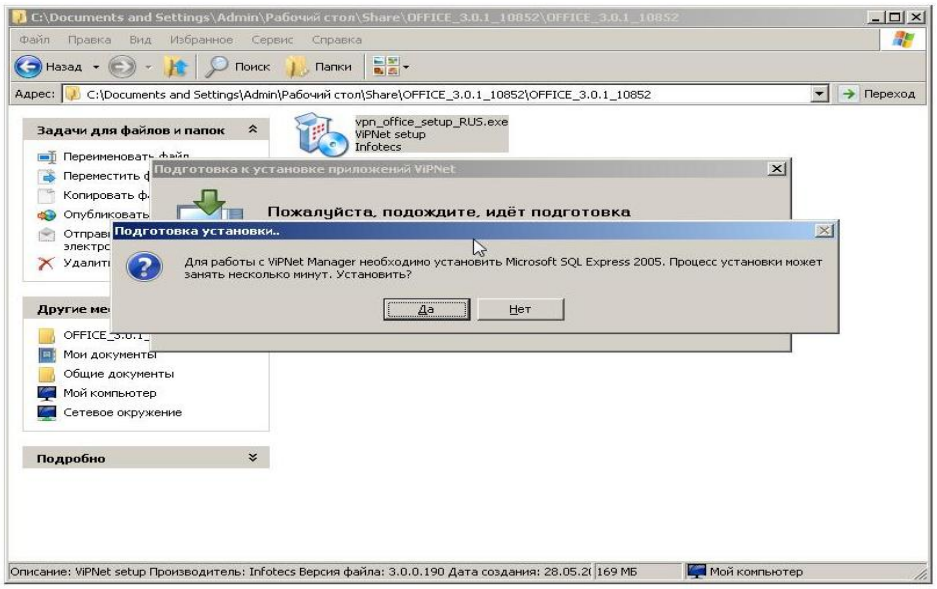


Рис. 2.63. Установка MicrosoftSQLExpress 2005

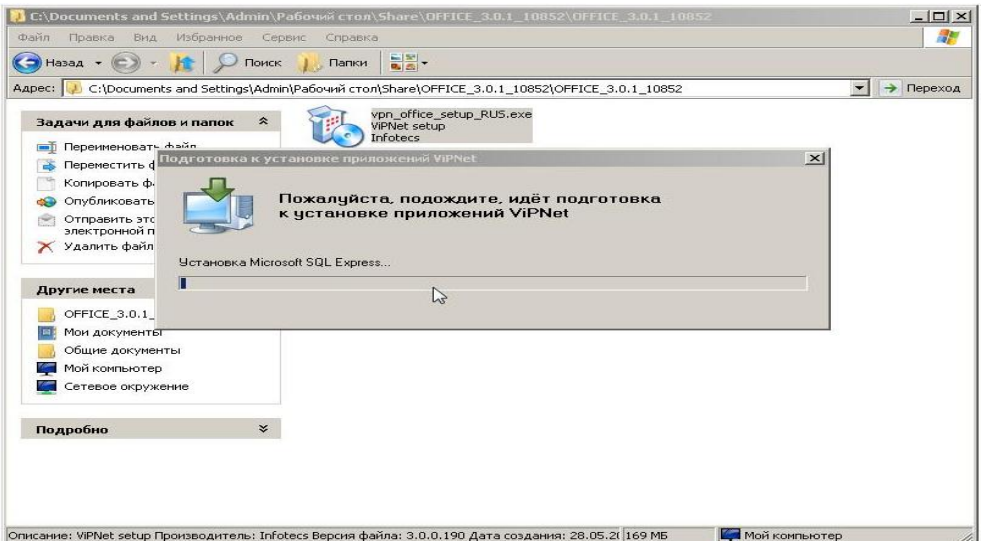


Рис. 2.64. Продолжение установки Microsoft SQL Express 2005

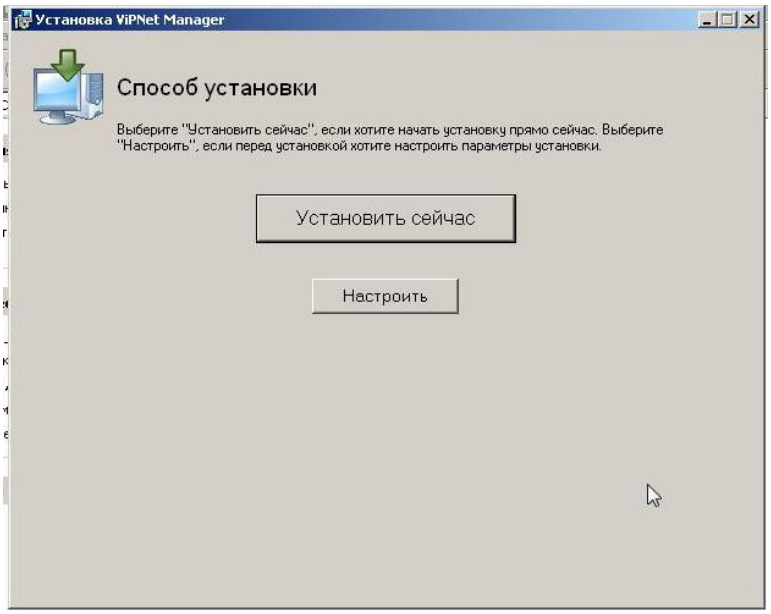


Рис. 2.65. Переход к установке ViPNet Manager

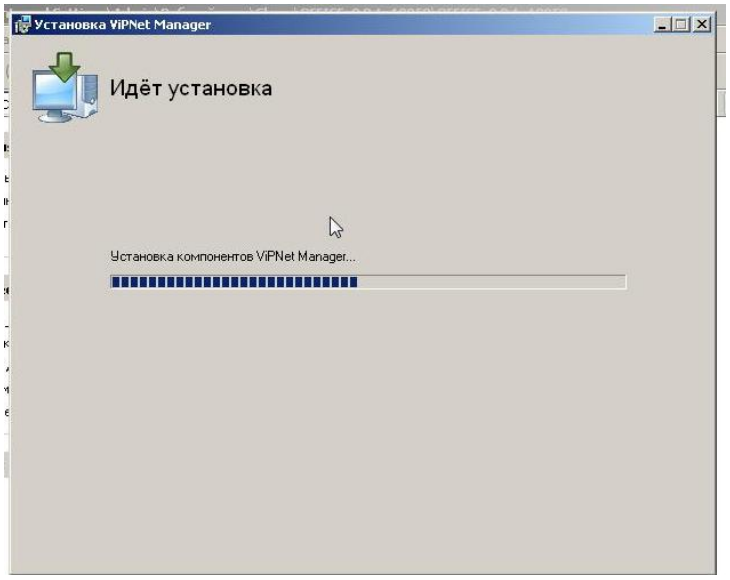


Рис. 2.66. Продолжение установки ViPNet Manager

Рис. 2.67. Завершение установки ViPNetManager

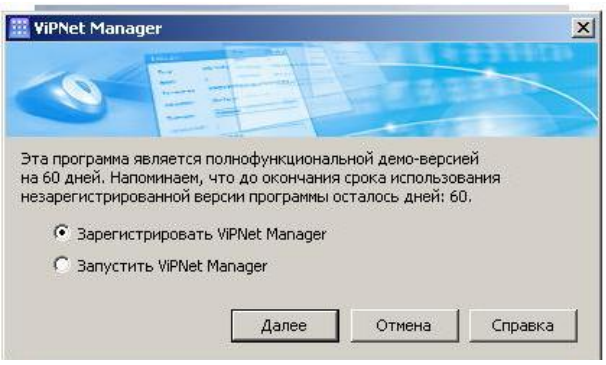


Рис. 2.68. Напоминание о том, что ПО является демо-версией

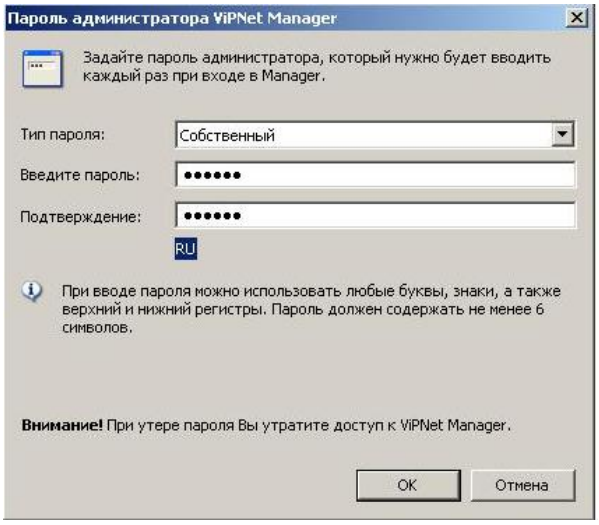


Рис. 2.69. Создание пароля администратора

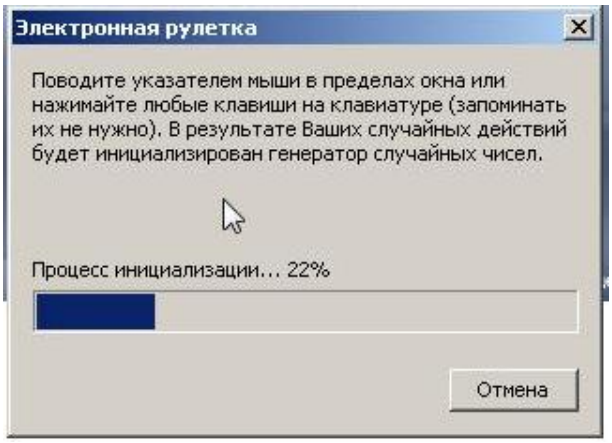


Рис. 2.70. Инициализация генератора случайных чисел

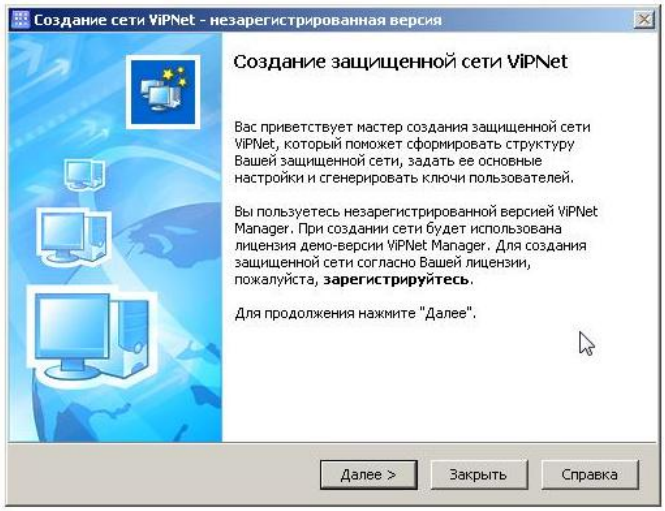


Рис. 2.71. Мастер защищенной сети Установка ViPNet

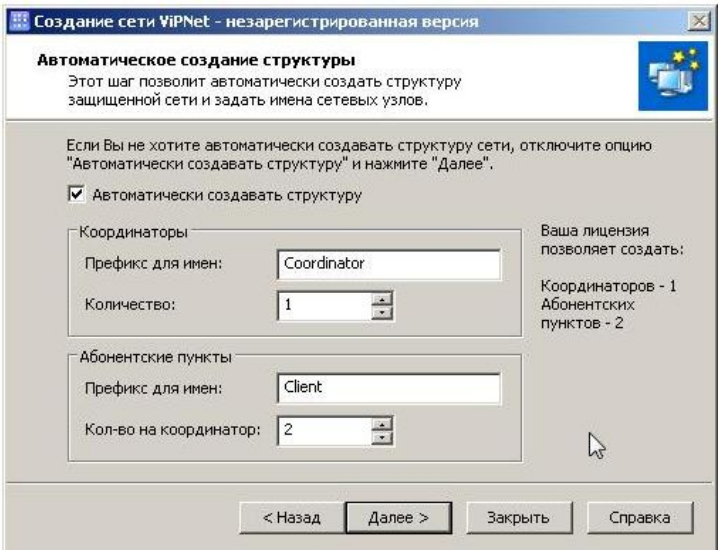


Рис. 2.72. Автоматическое создание структуры сети ViPNet

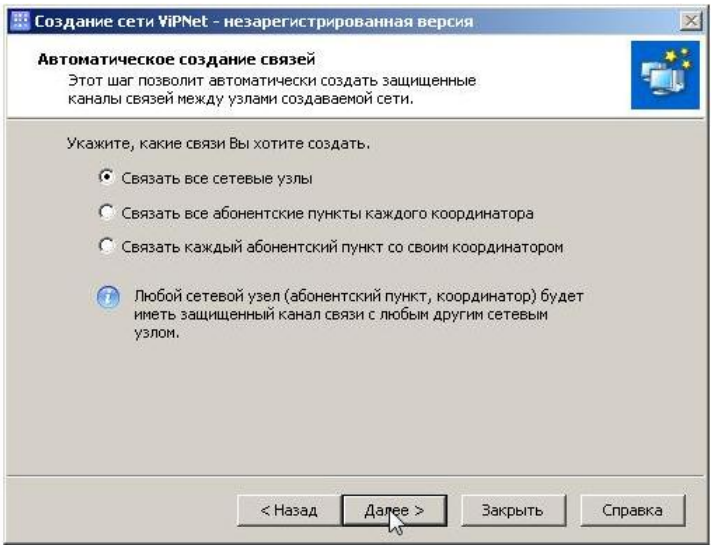


Рис. 2.73. Создание каналов связи между узлами сети ViPNet

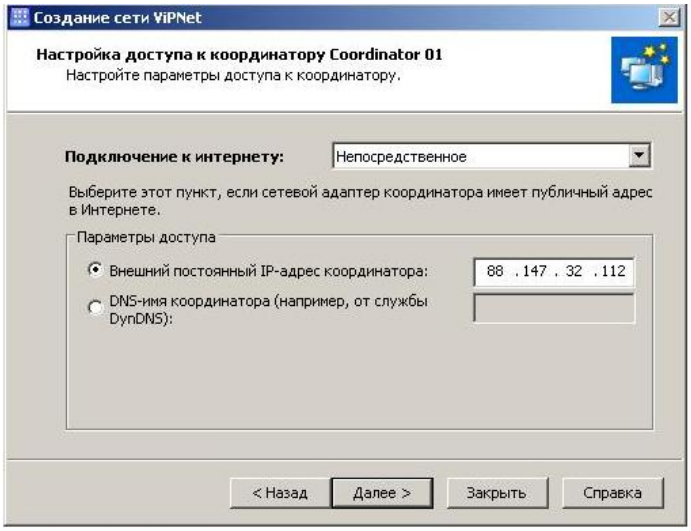


Рис. 2.74. Настройка доступа к координатору

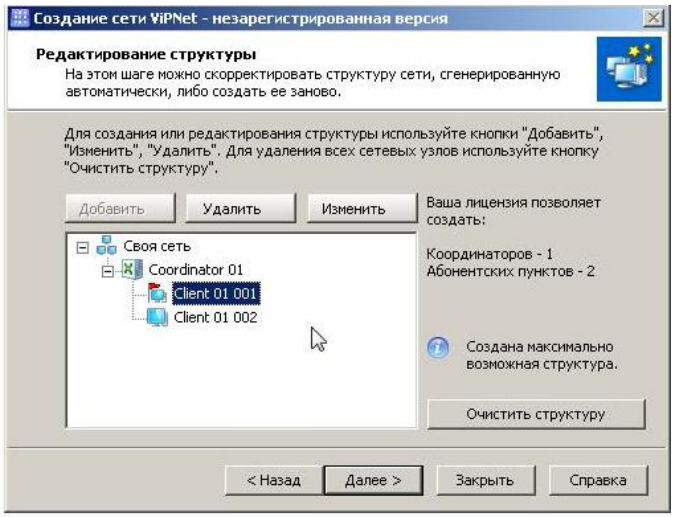


Рис. 2.75. Редактирование структуры сети ViPNet

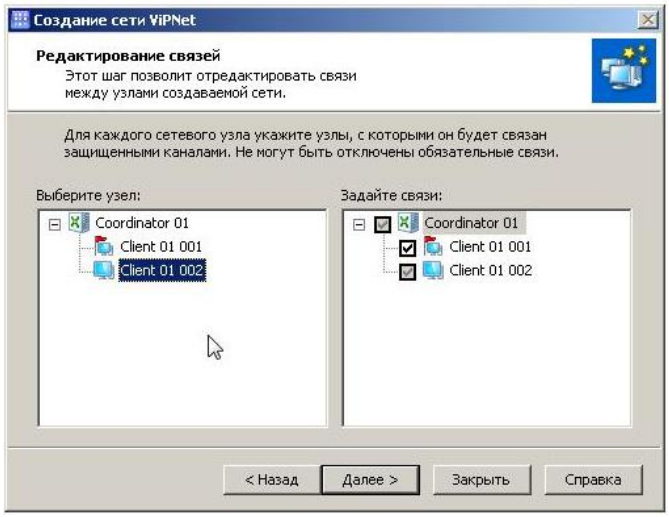


Рис. 2.76. Редактирование связей между узлами сети ViPNet

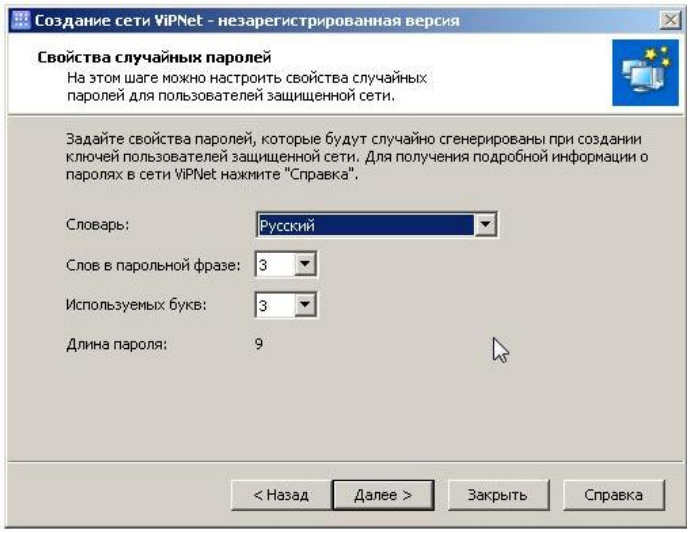


Рис. 2.77. Настройка паролей пользователей сети ViPNet

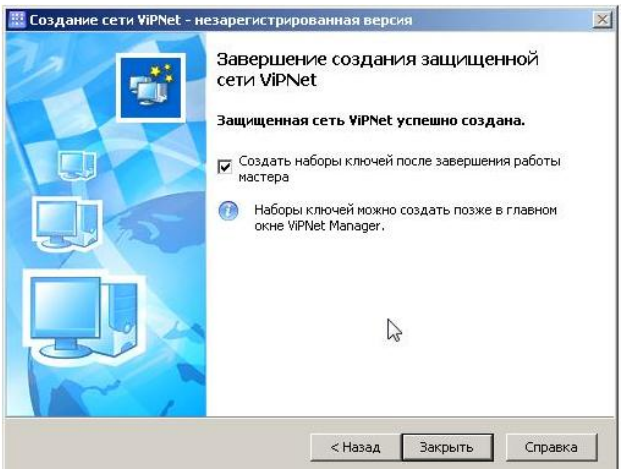


Рис. 2.78. Завершение работы мастера создания защищенной сети Установка ViPNet

Рис. 2.79. Запрос на сертификат сети ViPNet

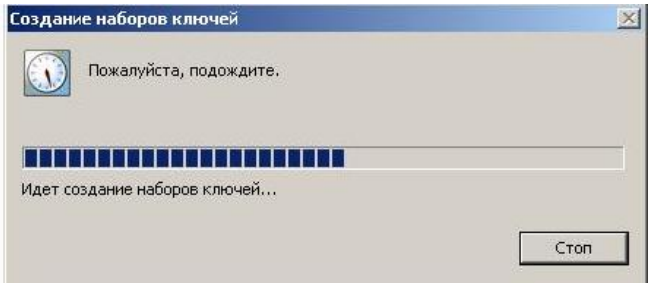


Рис. 2.80. Создание наборов ключей

Следующий шаг установка ПО ViPNet Client на рабочее место администратора (ВМ 2).

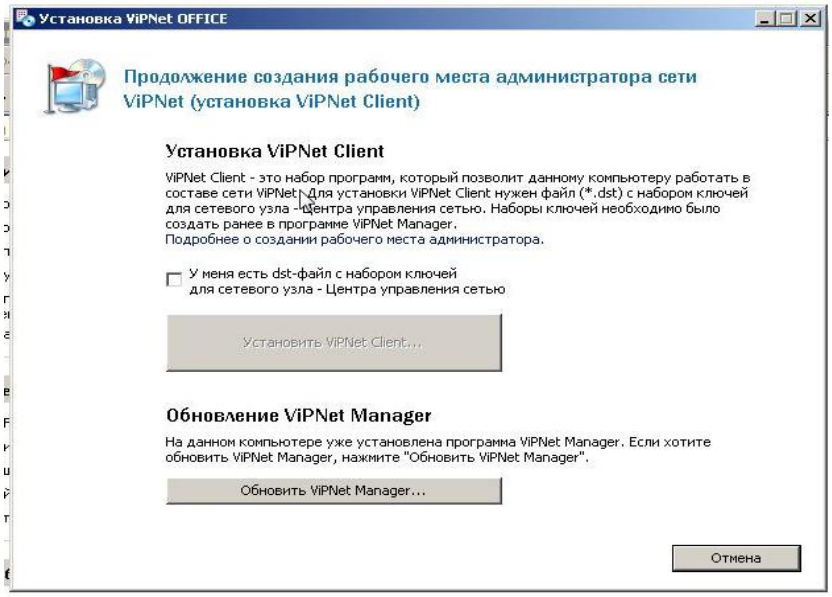


Рис. 2.81. Установка ViPNet Client

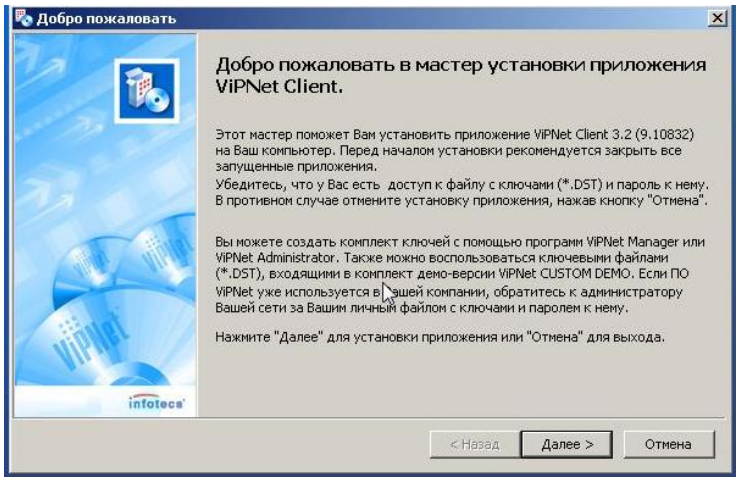


Рис. 2.82. Продолжение установки ViPNet Client

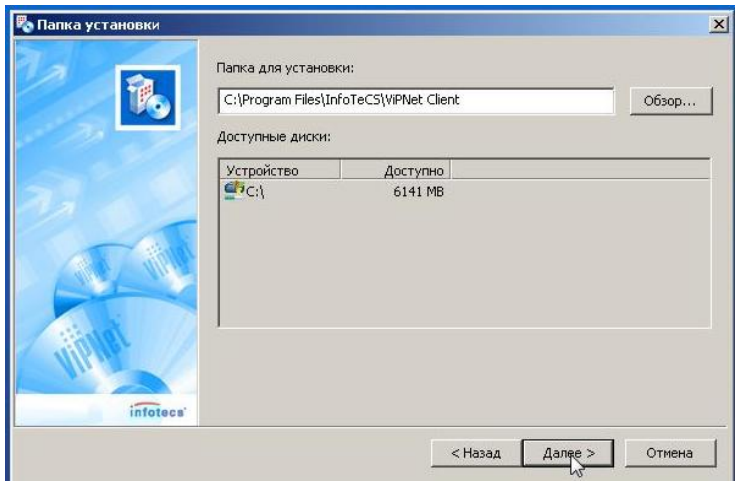


Рис. 2.83. Задание директории установки ViPNet Client

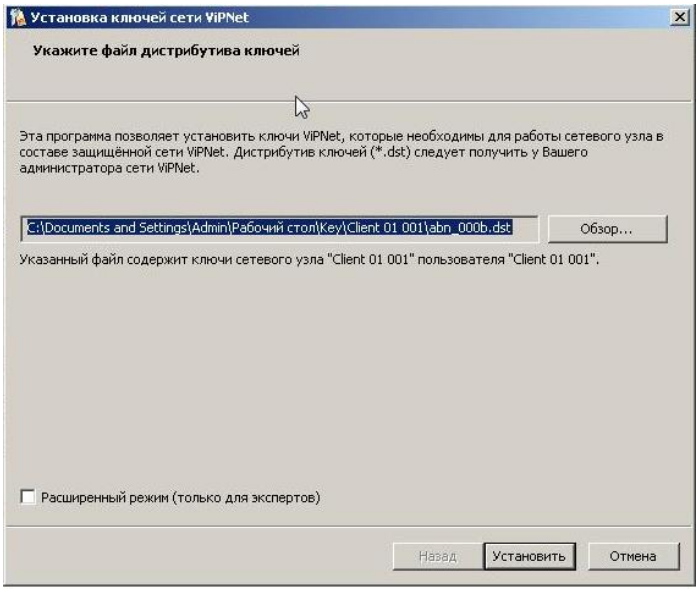


Рис. 2.84. Установка ключей сети ViPNet

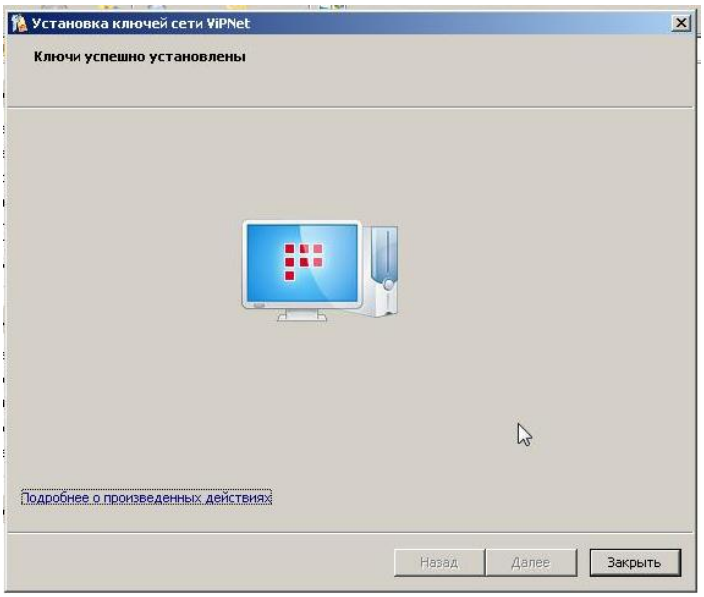


Рис. 2.85. Завершение установки ключей сети ViPNet

Установка ПО ViPNetCoordinatorна ВМ 2 описана ниже.

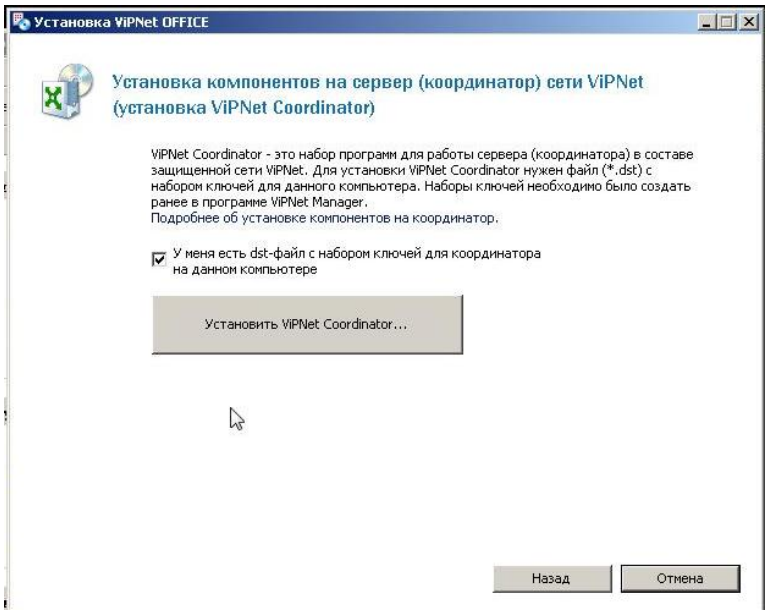


Рис. 2.86. Установка ViPNet Coordinator

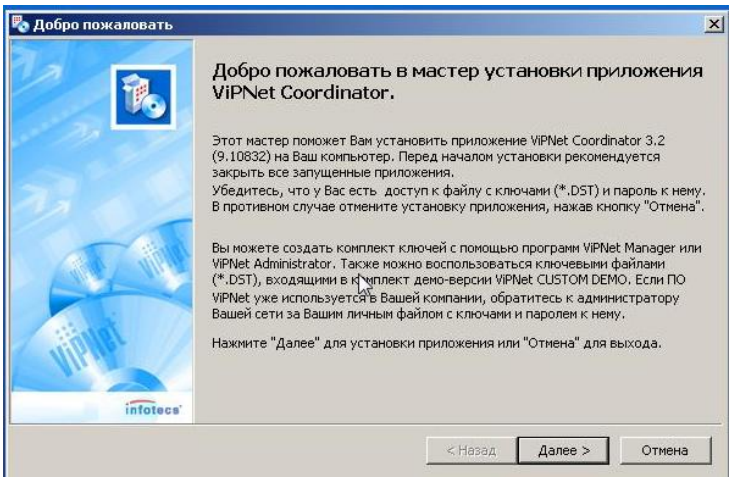


Рис. 2.87. Продолжение установки ViPNet Coordinator

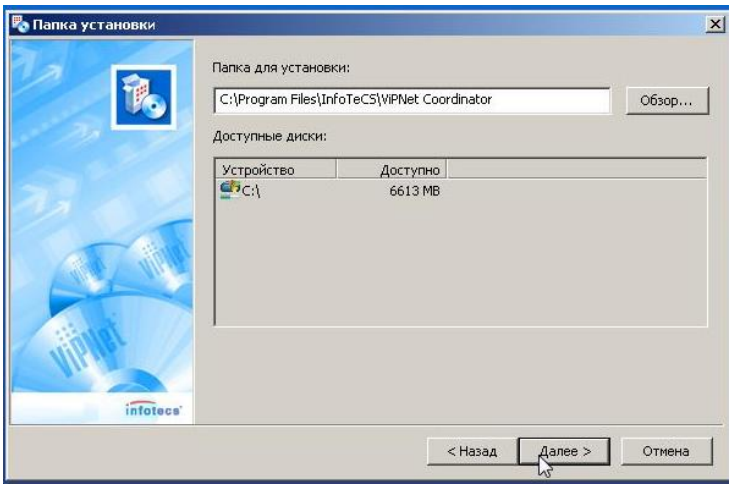


Рис. 2.88. Задание директории установки ViPNet Coordinator

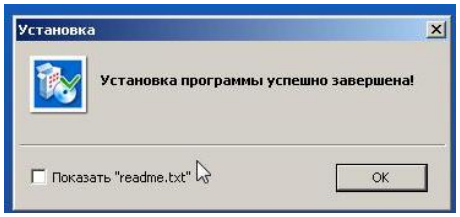


Рис. 2.89. Завершение установки ViPNet Coordinator

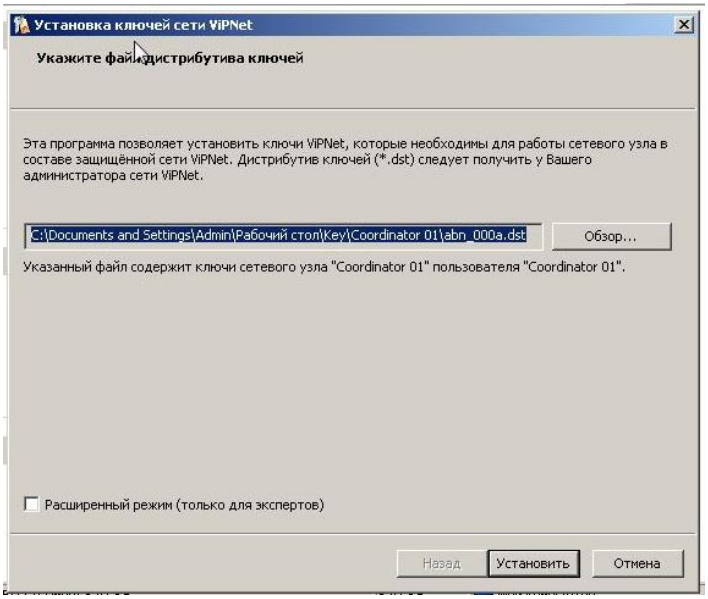


Рис. 2.90. Установка ключей для ViPNet Coordinator

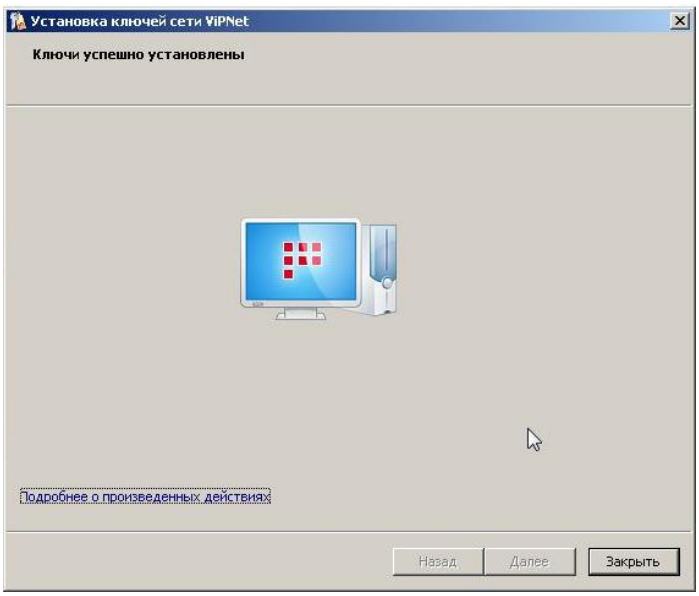


Рис. 2.91. Завершение установки ключей для ViPNet Coordinator

Очередным этапом установки ПО ViPNet является установка ViPNetClientна ВМ 3.

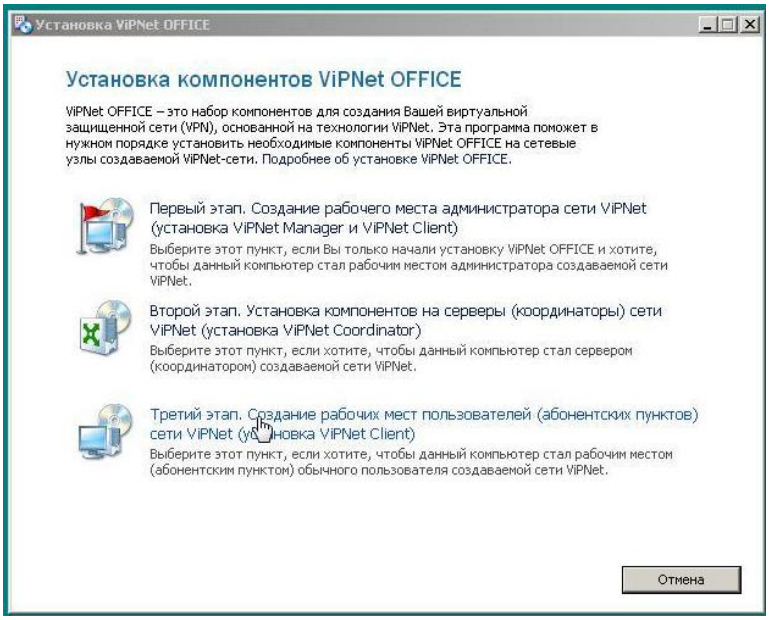


Рис. 2.92. Третий этап установки ПО ViPNet

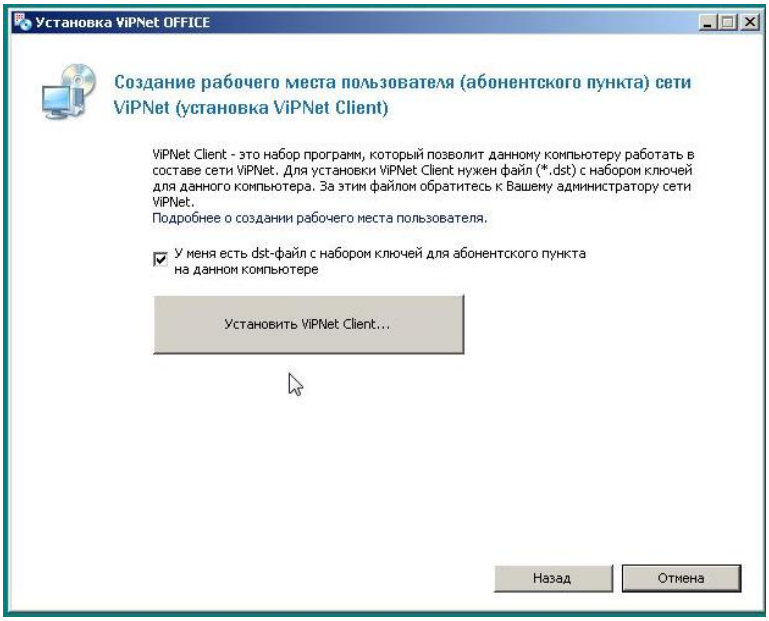


Рис. 2.93. Установка ViPNetClient

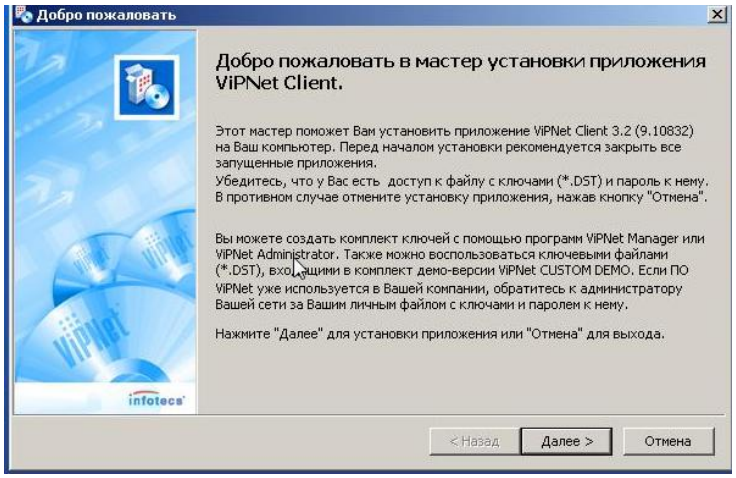


Рис. 2.94. Продолжение установки ViPNet Client

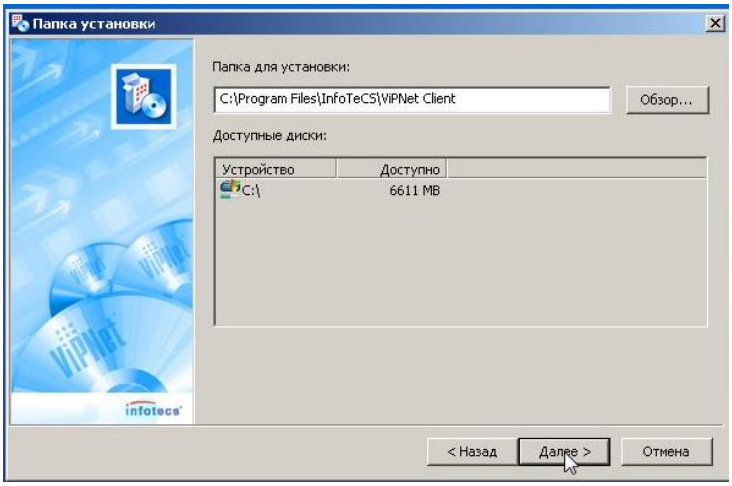


Рис. 2.95. Задание директории установки ViPNet Client

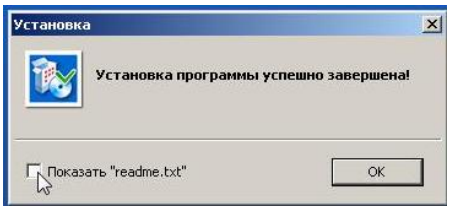


Рис. 2.96. Завершение установки ViPNet Client

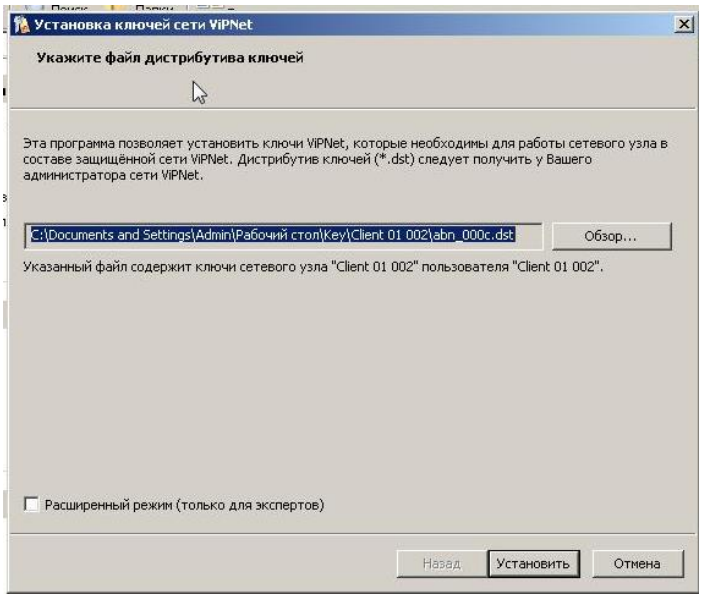


Рис. 2.97. Установка ключей для ViPNet Client

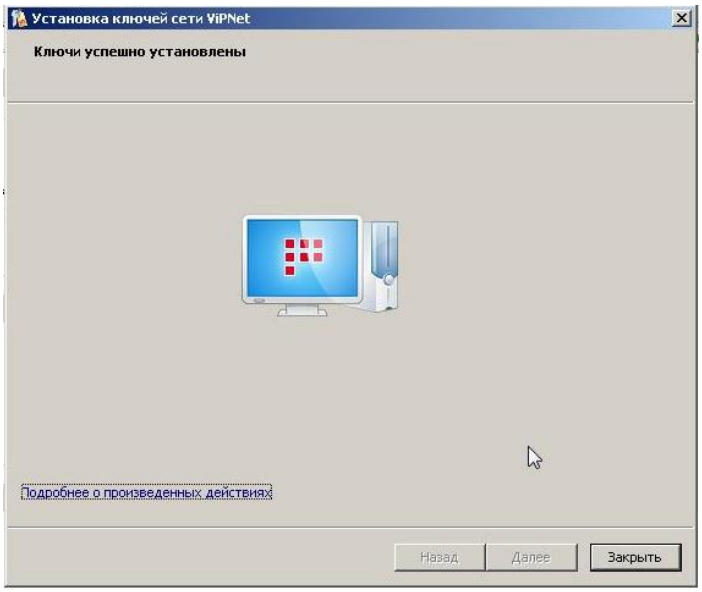


Рис. 2.98. Завершение установки ключей для ViPNet Client

Исследование защищенного сетевого взаимодействия

После установки ПО ViPNet на виртуальные машины сетевое взаимодействие становится защищенным. Для удостоверения в этом производится аналогичная процедура, что и во втором пункте испытания. По протоколу SMB передается текстовый файл Test.txt с ВМ 2 на ВМ 3. Производится захват передаваемого трафика. При этом становится видно, что захваченный трафик представлен уже не TCP-пакетами, а UDP или IPv4 (IP/241-проприетарный ViPNet протокол). При попытке выделить SMB- объект (текстовый файл test.txt)анализатор трафика таковой не обнаруживает.

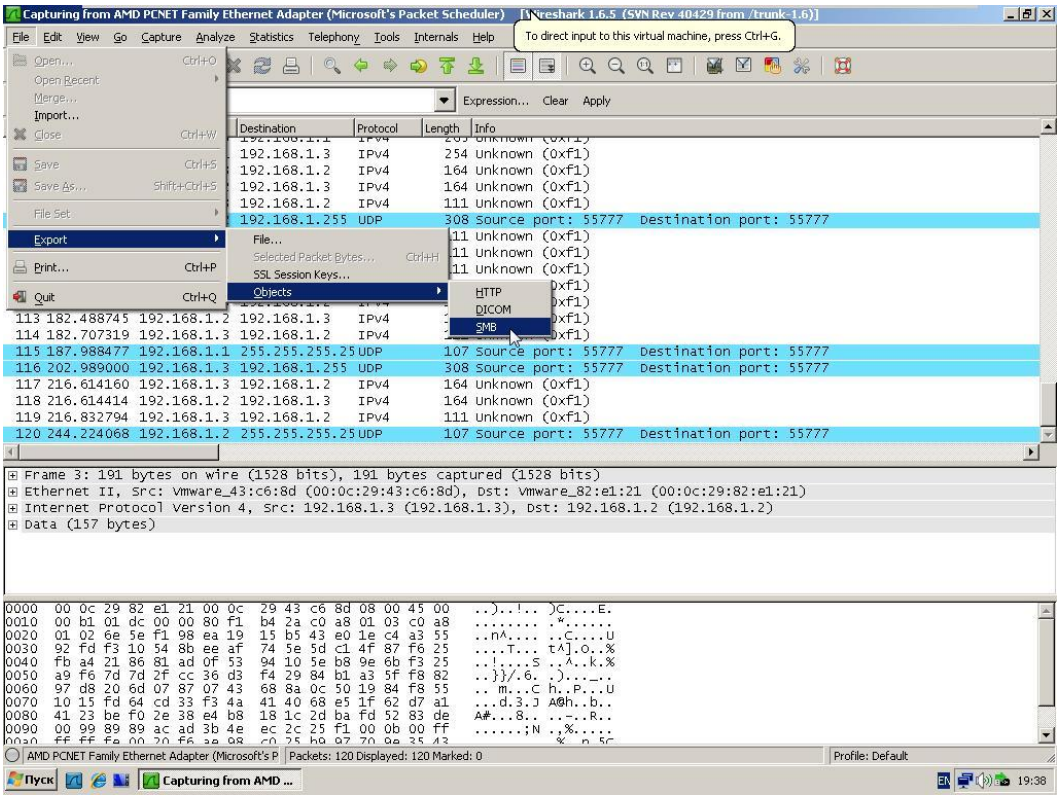


Рис. 2.99. Выделение SMB объекта

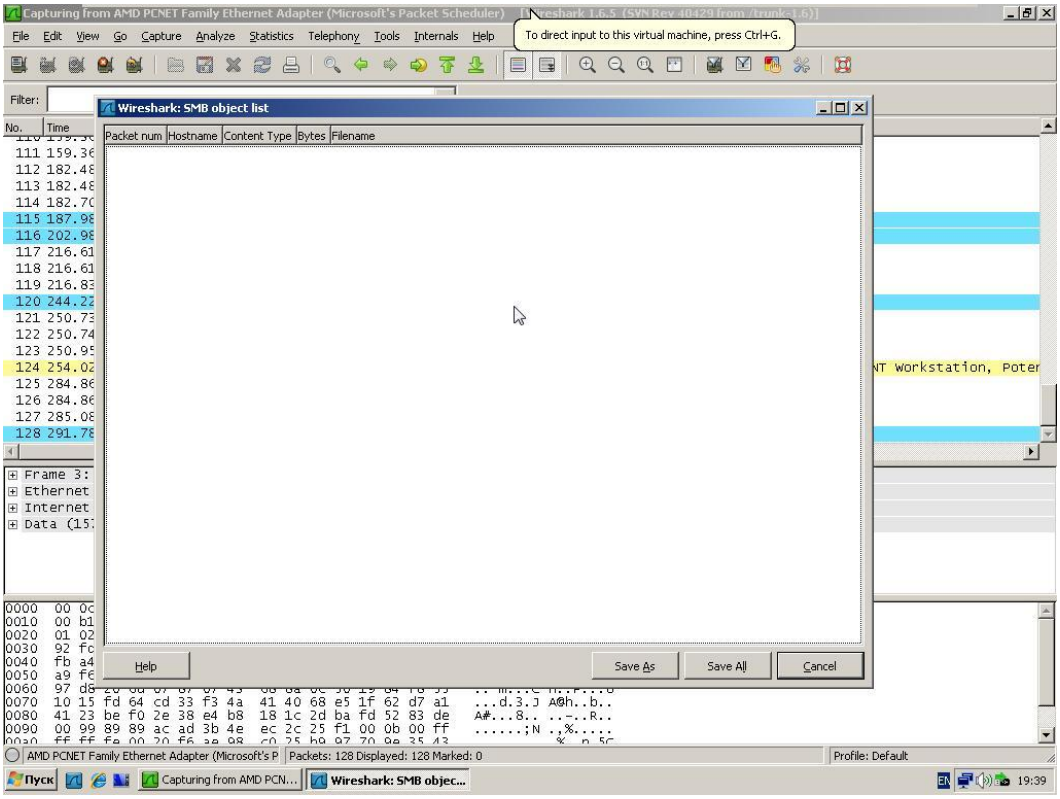


Рис. 2.100. Обнаружение SMB объекта

Аналогичным образом производится захват трафика при использовании утилиты ping на ВМ 2 для проверки связи с ВМ 3.

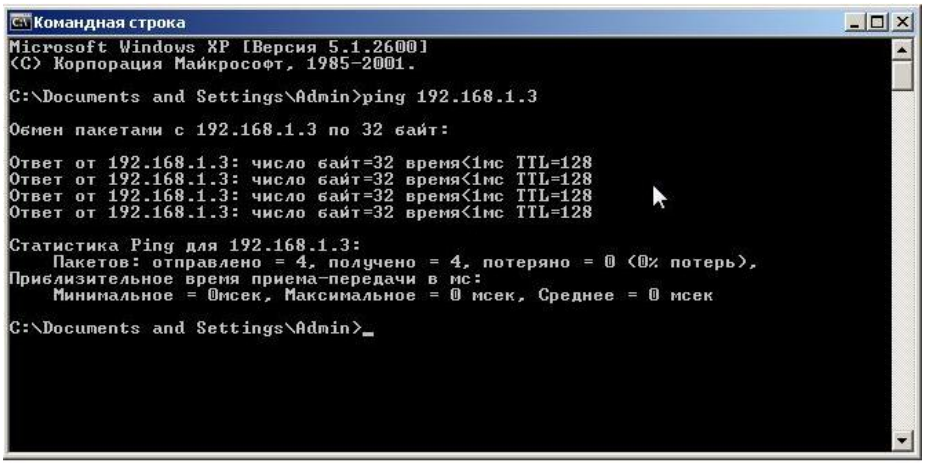


Рис. 2.101. Проверка связи с ВМ 2 с ВМ 3 с помощью утилиты ping

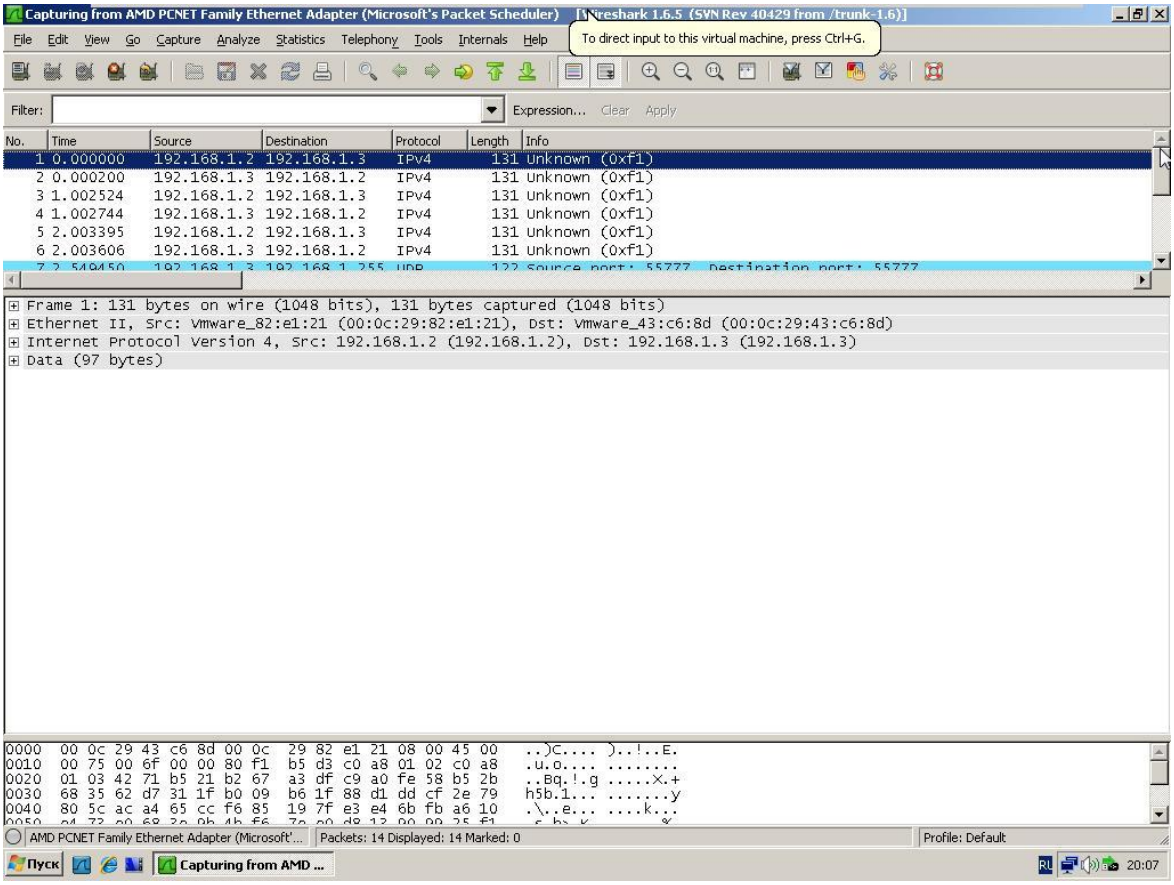


Рис. 2.102. Захваченный трафик при инициализации утилиты ping

В окне анализатора видно, что вместо ICMP-пакетов отображены IPv4-пакеты.

Было продемонстрировано испытание сетевого взаимодействия в открытом виде и в защищенном. При открытом взаимодействии не составляет труда перехватить и интерпретировать передаваемую по сети информацию. При защищенном взаимодействии, после установки ПО ViPNet, передаваемый трафик предварительно обрабатывается ViPNet-драйвером. Он преобразует, при необходимости реальный IP-адрес отправителя в виртуальный адрес, добавляет к пакету уникальные идентификаторы узла отправителя и получателя, зашифровывает исходный IP-пакет (алгоритм ГОСТ 28147-89) и часть служебной информации, инкапсулирует исходный IP-пакет в UDP- или IP/241-пакет. В таком виде пакет отправляется в сеть, что и было обнаружено при захвате. Таким образом интерпретировать захваченную информацию не представляется возможным, так как расшифрование по алгоритму ГОСТ 28147-89, не зная ключей, практически не реализуемо.

2.3. Проектирование защищенной многоточечной видеоконференц связи на базе WEB-технологии [9-13]

Цель работы: изучение и исследование принципов работы программного комплекса многоточечной видеоконференцсвязи на базе Web-технологии

Видеоконференция — это технология, которая позволяет людям видеть и слышать друг друга, обмениваться данными и совместно обрабатывать их в интерактивном режиме, используя возможности привычного всем компьютера, максимально приближая общение на расстоянии к реальному живому общению.

Видеоконференцсвязь — область информационной технологии, обеспечивающая одновременно двустороннюю передачу, обработку, преобразование и представление интерактивной информации на расстояние в режиме реального времени с помощью аппаратно-программных средств вычислительной техники двух и более пользователей.

Видеоконференция применяется как средство оперативного принятия решения в той или иной ситуации; при чрезвычайных ситуациях; для сокращения командировочных расходов в территориально распределенных организациях; повышения эффективности; проведения судебных процессов с дистанционным участием осужденных, а также как один из элементов технологий теле медицины и дистанционного обучения.

В многих государственных и коммерческих организациях видеоконференция приносит большие результаты и максимальную эффективность, а именно:

- снижает время на переезды и связанные с ними расходы;
- ускоряет процессы принятия решений в чрезвычайных ситуациях;
- сокращает время рассмотрения дел в судах общей юрисдикции;

- увеличивает производительность труда;
- решает кадровые вопросы и социально-экономические ситуации;
- дает возможность принимать более обоснованные решения за счёт привлечения при необходимости дополнительных экспертов;
- быстро и эффективно распределяет ресурсы, и так далее.

Для общения в режиме видеоконференции абонент должен иметь терминальное устройство (кодек) видеоконференцсвязи, видеотелефон или иное средство вычислительной техники. Как правило, в комплекс устройств для видеоконференцсвязи входит:

- Центральное устройство — кодек с видеокамерой и микрофоном, обеспечивающего кодирование/декодирование аудио- и видео- информации, захват и отображение контента;
- устройство отображения информации и воспроизведения звука.

В качестве кодека может использоваться персональный компьютер с программным обеспечением для видеоконференций.

Большую роль в видеоконференции играют каналы связи, то есть транспортная сеть передачи данных. Для подключения к каналам связи используются сетевые протоколы IP или ISDN.

Существует два режима работы ВКС, которые позволяют проводить двусторонние (режим «точка-точка») и многосторонние (режим «многоточка») видеоконференции.

Как правило, видеоконференцсвязь в режиме «точка-точка» удовлетворяет потребности только на начальном этапе внедрения технологии, и довольно скоро возникает необходимость одновременного взаимодействия между несколькими абонентами. Такой режим работы называется «многоточечный» или многоточечной видеоконференцсвязью. Для реализации данного режима требуется наличие активации многоточечной лицензии в кодеке при условии, если устройство поддерживает данную функцию, либо специального видеосервера MCU или программно-аппаратной системы управления.

Режимы видеоконференцсвязи

Существует два основных типа видеоконференций - персональная и групповая. Персональная видеоконференция подразумевает сеанс видеосвязи, в котором участвует всего два абонента. Под групповыми же видеоконференциями подразумеваются все остальные виды видеоконференций. Различные устоявшиеся правила отображения участников видеоконференции для каждой из сторон называются видами видеоконференций.

Видеоконференция 1-на-1:

Участвуют два абонента, оба видят и слышат друг друга одновременно. Сразу оговоримся, что во время любого сеанса видеоконференции могут использоваться различные инструменты для совместной работы, такие как обмен текстовыми сообщениями, файлами, презентациями и прочими медиаданными.

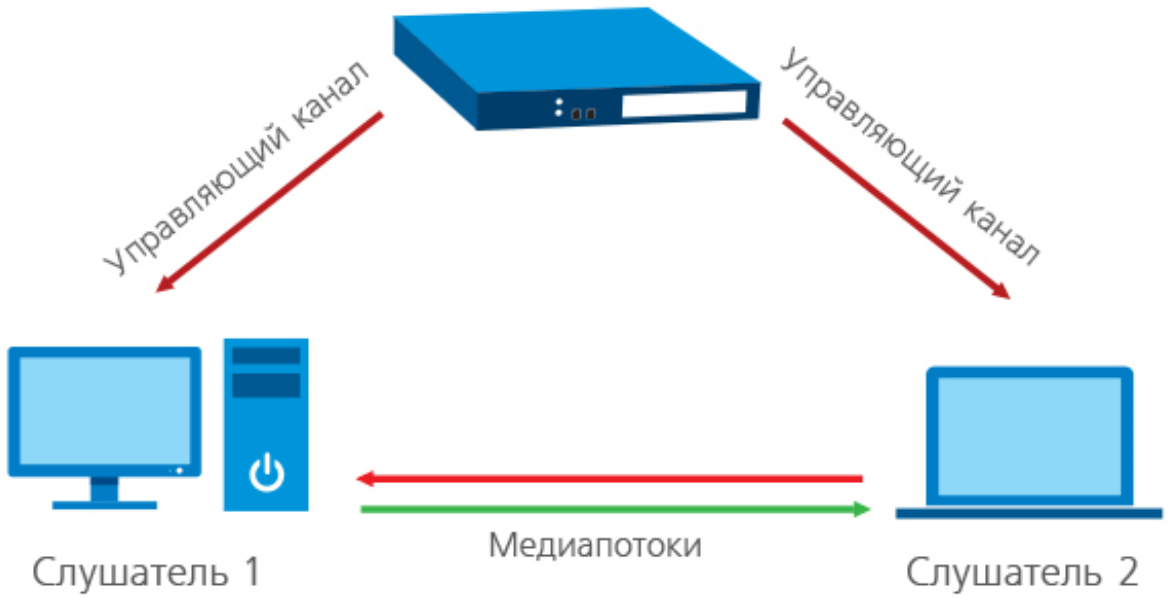


Рис. 2.103. Структура видеоконференции «1 на 1»

Симметричная видеоконференция

Она же видеоконференция с постоянным присутствием. Так называют сеанс видеоконференции, в котором участвуют более 2 человек и все участники видят и слышат друг друга одновременно. Естественно, видеоконференция подразумевает полнодуплексное общение. Другими словами, это аналог круглого стола, где у всех равные права. Групповая видеоконференция подходит для встреч, где требуется максимальная вовлеченность каждого участника.

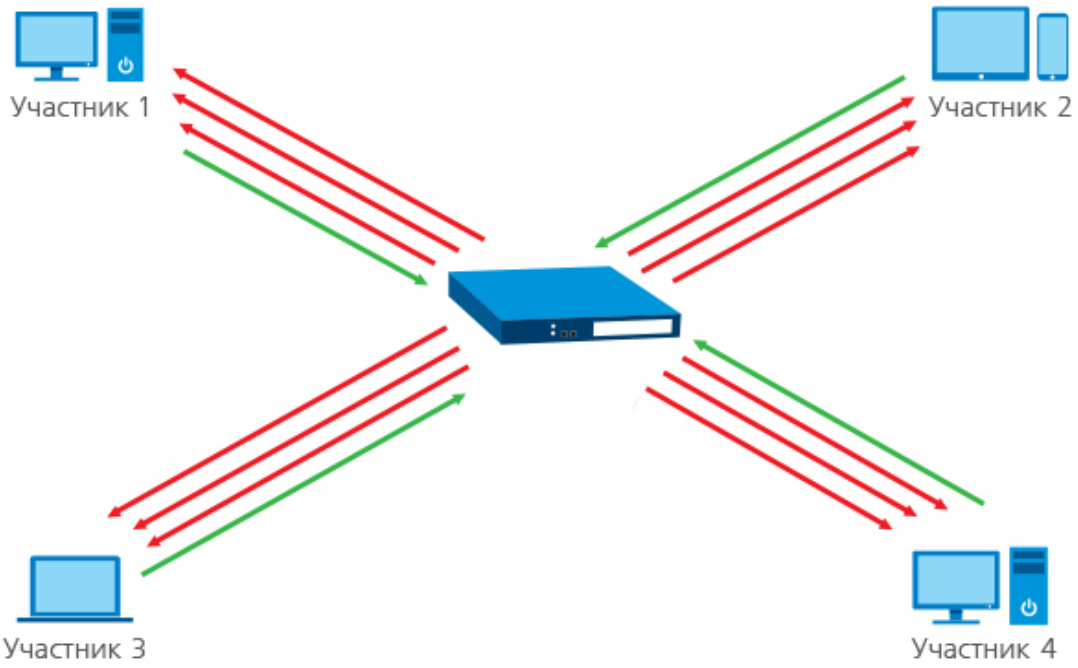


Рис. 2.104. Структура «симметричной» видеоконференции

Видеоконференция с активацией по голосу

Название такого режима пошло от английского обозначения Voice Activated Switching (VAS). Эта видеоконференция предполагает следующий формат общения: все участники сеанса слышат и видят на своих экранах только выступающего докладчика, в то время как он сам видит себя либо предыдущего оратора. Возможны небольшие вариации данного механизма, но суть остаётся следующей: сервер ВКС отслеживает голосовую активность абонентов и переключает транслируемое всем участников изображение на говорящего. У данного режима есть существенные недостатки, например, ложные срабатывания на шум, кашель или звонок мобильного телефона.

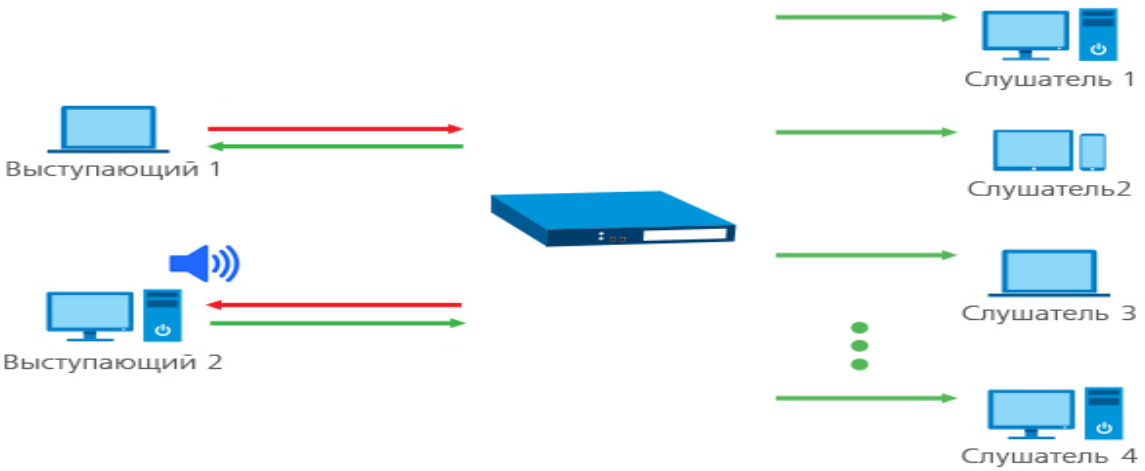


Рис. 2.105. Структура видеоконференции «с активацией по голосу»

Селекторная видеоконференция

Режим в котором участники делятся на два вида: докладчики и слушатели, где каждый из слушателей может стать докладчиком (с разрешения организатора конференции). Ведущий такой конференции сам назначает докладчиков и может удалить их с видео-трибуны в любой момент.

Этот режим может так же называться ролевой видеоконференцией. Селекторная видеоконференция используется чаще всего при проведении веб-конференций (вебинаров).

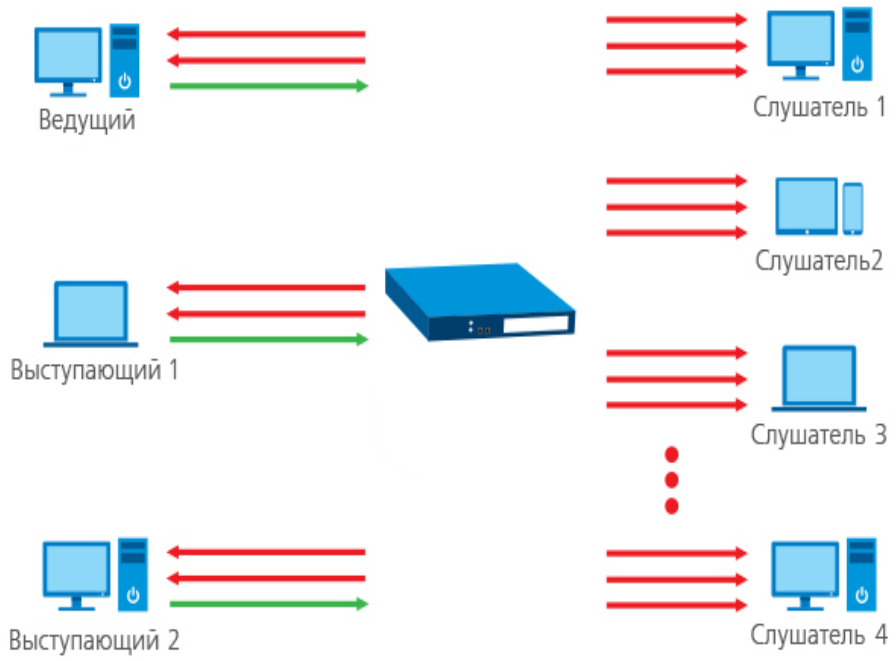


Рис. 2.106. Структура «селекторной» видеокнференции

Видеоконференция для дистанционного образования

Специальный режим "Видеоурок", в котором что все участники(ученики) будут видеть и слышать только одного вещающего(преподавателя), а он будет видеть и слышать всех участников видеоконференции. То есть, ученики не имеют обратной связи между собой.

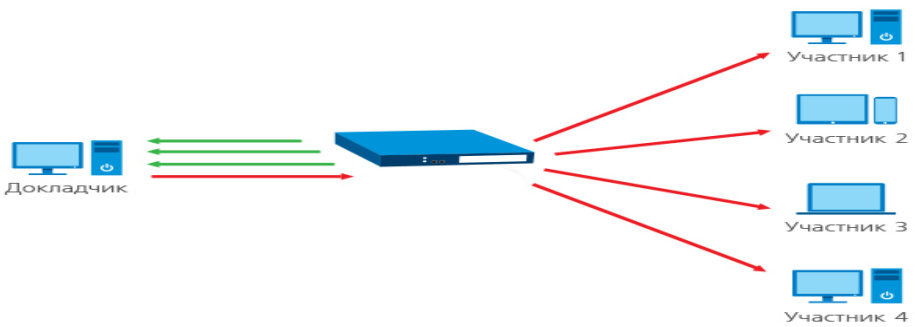


Рис. 2.107. Структура видеоконференции «для дистанционного образования»

Видеотрансляция

Вид видеоконференции, в котором докладчик вещает на широкую аудиторию слушателей, при этом он не видит и не слышит их. Остальные участники видят и слышат только докладчика. Обратная связь возможна только через текстовый чат.

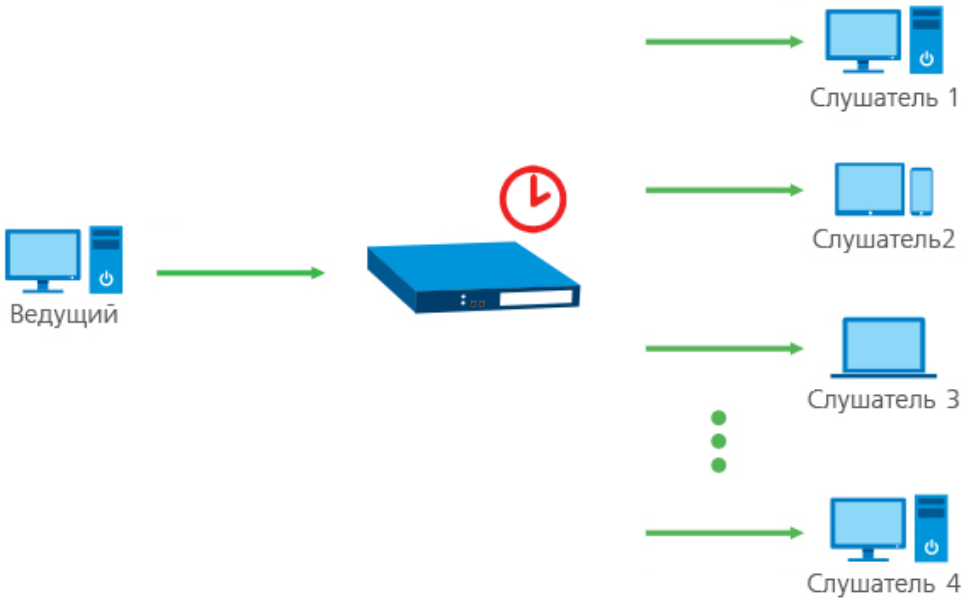


Рис. 2.108. Структура «видеотрансляции»

Организация видеосвязи для различных каналов связи

По локальной сети:

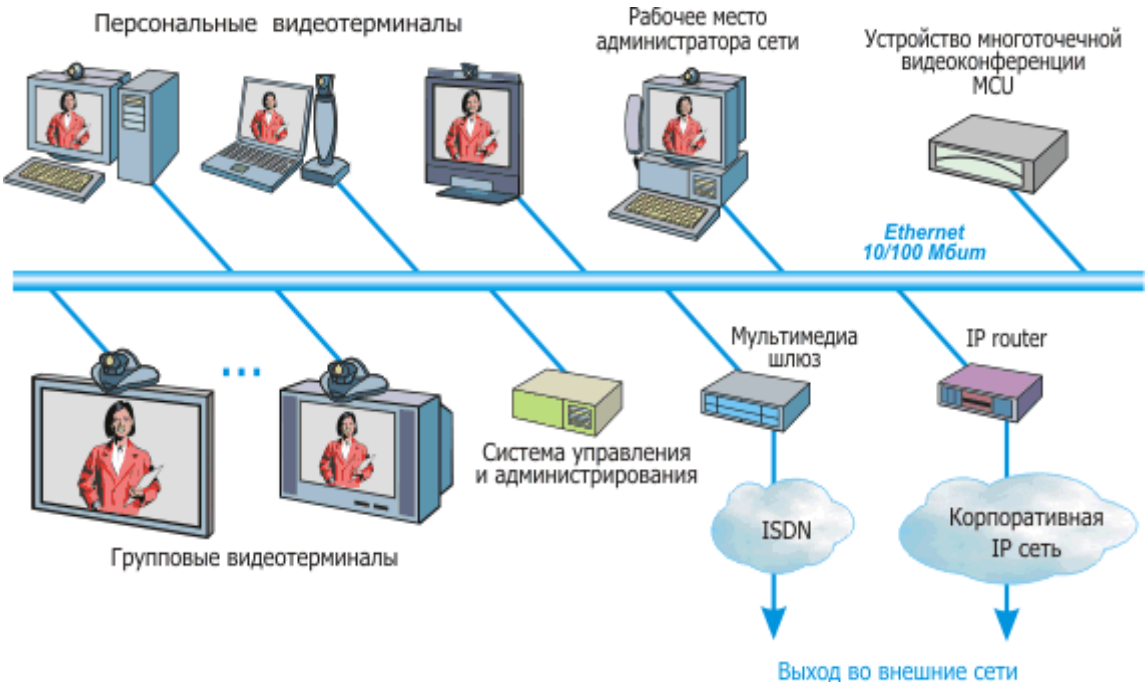


Рис. 2.109. Структурная схема многоточечной видеоконференции в локальной сети.

В сети Интернет:

Самый простой и дешевый метод организации видеоконференцсвязи через Интернет. Для организации видеоконференцсвязи через Интернет требуется иметь статические IP-адреса и каналы связи с пропускной способностью не менее 512 кБит/св обе стороны (для исходящего и входящего трафика).

Основным недостатком систем КВКС в Интернет можно считать существенную зависимость качества видео- и аудиопотоков от загрузки сети. В проведенных экспериментах качество аудиопотока изменялось от близкого к качеству звука при телефонном разговоре до плохого, при котором наблюдались прерывания звука. Передача видеопотоков в условиях недостаточной пропускной способности канала сопровождалась уменьшением числа передаваемых кадров в секунду с 8-10 до 1-2, мозаичностью передаваемого подвижного изображения. Тем не менее в условиях неудовлетворительного качества звука интерактивность может эффективно поддерживаться путем обмена текстовыми сообщениями в режиме on-line, а надежный режим обмена данными (в первую очередь, приложения Whiteboard и Filetransfer) позволяет считать такие системы достаточно эффективным средством поддержки процесса обучения в среде Интернет.

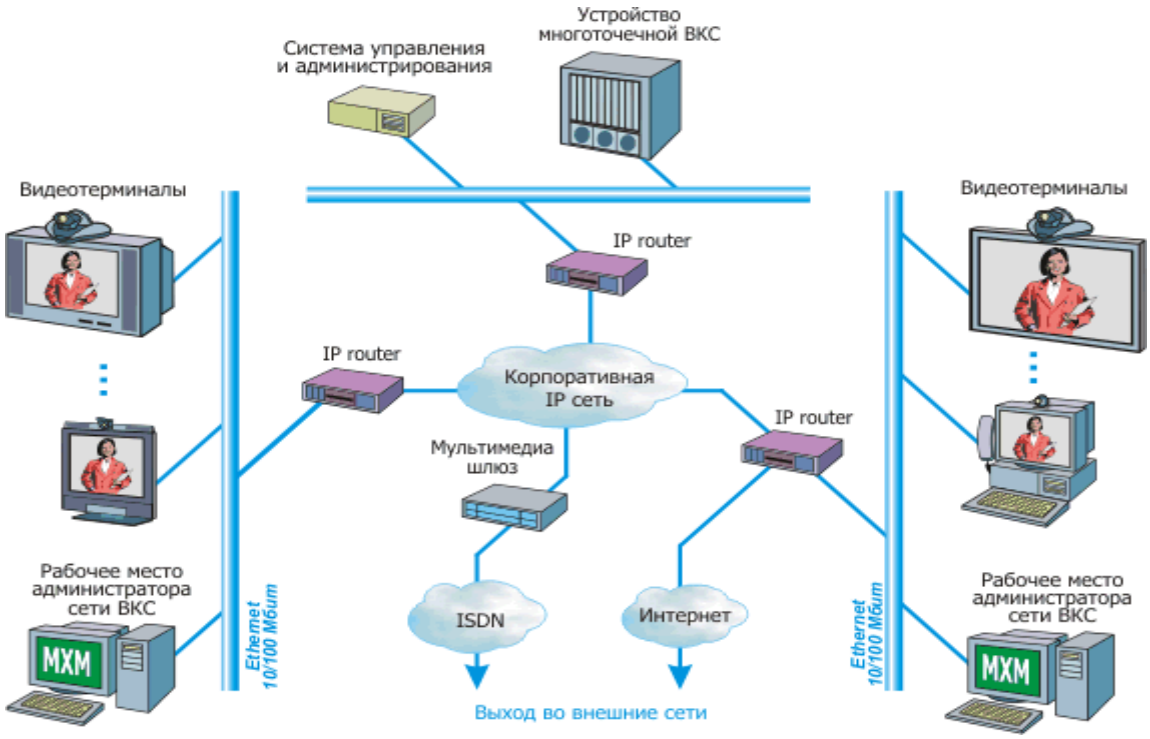


Рис. 3.110. Структурная схема многоточечной видеоконференциивтерриториально распределенной IP-сети.

По протоколу ISDN:

Аббревиатура ISDN расшифровывается как цифровая сеть с интеграцией услуг. Цифровые сети с интегральными услугами относятся к сетям, в которых основным режимом связи является режим коммутации каналов, а данные обрабатываются в цифровой форме.

Необходимо отметить, что ISDN имеет ряд преимуществ по сравнению с традиционными аналоговыми сетями, но вот по сравнению с новыми телекоммуникационными технологиями передачи данных имеет ряд критичных недостатков:

- тяжело отследить, на каком участке произошел сбой связи;
- низкая оперативность восстановления каналов связи;
- небольшая распространенность на территории РФ;
- всего несколько операторов связи поддерживают данную технологию;
- сравнительно высокая стоимость применения услуги связи при межрегиональном соединении.

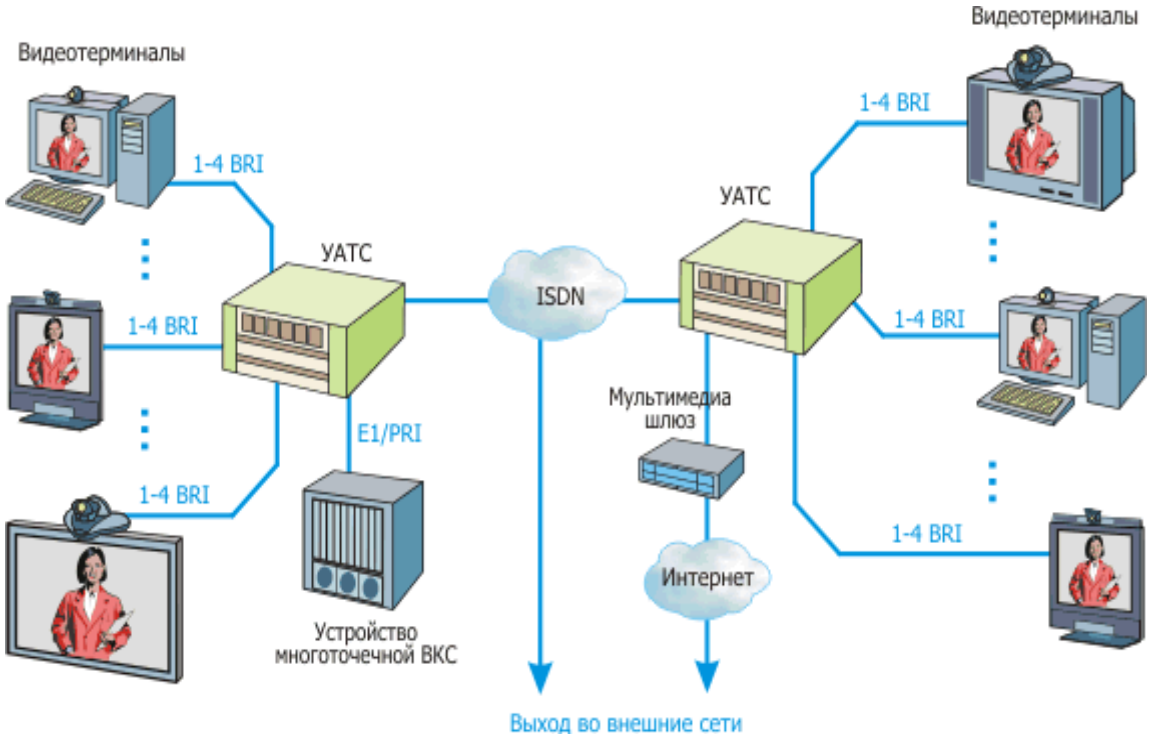


Рис. 2.111. Структурная схема многоточечной видеоконференции ISDN.

Современные методы и средства управления в сетях видеоконференцсвязи

Для любой информационной сети — телефонной, вычислительной и т.д. можно сформулировать общий принцип: чем она больше, тем сложнее в управлении. Не являются исключением из этого правила и сети видеоконференцсвязи (ВКС), более того, если в общие задачи управления сетями обычно не включается требование управления оборудованием, установленным на рабочих местах пользователей, то для сетей ВКС это становится одной из

основных функций. Ситуация осложняется тем, что современная архитектура сетей ВКС требует высокой работоспособности от гетерогенных решений, построенных с использованием разнородных технологий на основе оборудования разных производителей.

Для обеспечения безопасности и повышения надежности вычислительных сетей используются технологии, получившие название управления сетями — наблюдение за функционированием, тестирование, предотвращение, выявление и устранение сбоев, обеспечение функционирования сетевых сервисов с задаваемым качеством обслуживания.

Принятые рекомендации МСЭ-Т X.700 и близкий к ним стандарт ISO/IEC 7498-4 ввели концептуальную модель управления сетями. Задачи систем управления сетями в них разбиваются на пять функциональных групп: обработка ошибок (fault management), управление конфигурацией (configuration management), учет (accounting management), управление производительностью (performance management), управление безопасностью (security management). Все они объединяются под общим названием FCAPS.

Применительно к сетям видеоконференцсвязи задачи, предусмотренные моделью управления, должны включать в себя следующие функции:

- Обработка ошибок — обеспечение администратора сети необходимыми инструментами для обнаружения сбоев и отказов сетевых и терминальных устройств ВКС, определения их причин и принятия действий по восстановлению. Для этого предоставляются механизмы: уведомления о сбоях; регистрации ошибок и ведения журнала; анализа сообщений об ошибках и выявление их источника; проведения диагностического тестирования; коррекции и восстановления от сбоев (по возможности в автоматическом режиме); резервирования и оперативного подключения ресурсов сети.
- Управление конфигурацией — отслеживание и настройка конфигурации сетевого программного и аппаратного обеспечения (настройки и состояние отдельных сетевых устройств и сети в целом). Может предоставляться функциональность по инициализации, реконфигурации, модернизации программного обеспечения, запуску и отключению управляемых устройств. Сюда же включаются механизмы обеспечения единого плана нумерации.
- Учет — измерение использования и доступности сетевых ресурсов для: учета имеющихся сетевых ресурсов; экономического учета (выставление счетов и т. п.); управления пользователями (учет использования сети в разрезе отдельных пользователей и групп).

- Управление производительностью — измерение производительности сети, сбор и анализ статистической информации о поведении сети для ее поддержания на приемлемом уровне как для оперативного управления, так и для планирования ее развития. Управление производительностью предоставляет возможность: получить уровень загрузки и ошибок сетевых устройств; обеспечивать соответствующий уровень производительности за счет необходимых сетевых ресурсов.
- Управление безопасностью — контроль доступа к оборудованию и сетевым ресурсам (с ведением журналов доступа), предотвращение, обнаружение и пресечение несанкционированного доступа.

Открытый сервер видеоконференций OpenMeetings

OpenMeetings - это серверное программное обеспечение с открытым исходным кодом (Open Sorce), предназначенное для проведения вебконференций.

OpenMeetings позволяет мгновенно создать конференцию в Интернете, для участия в которой нужен лишь браузер. В OpenMeetings можно использовать микрофон и веб-камеру, делиться документами и экраном, рисовать на белой доске, приглашать участников по e-mail, записывать встречи. Можно также создавать опросы и голосовать по ходу встречи. Для модератора OpenMeetings предоставляет полный контроль над возможностями пользователей. Так что OpenMeetings вполне подойдет для в школ, университетов и других учебных заведений.

OpenMeetings доступен как готовый веб-сервис на сайте разработчика, но за определенную плату. Здесь же можно бесплатно зарегистрироваться и испытать его.

Чтобы использовать OpenMeetings бесплатно, и при этом безо всяких ограничений и контрибуций, нужно загрузить инсталляционный пакет, и установить его на веб-сервере своего учебного заведения (установка OpenMeetings).

Пользователь OpenMeetings должен зарегистрироваться на сервере. Общение происходит в различных комнатах для встреч, в которых различные группы могут настроить свои отдельные режимы работы видео, списки участников, возможности обмена информацией и политики безопасности.

Презентации с экрана OpenMeetings можно загрузить на свой ПК, в том числе в формате PDF, причем с очень хорошим качеством. В этом смысле OpenMeetings очень подходит для конвертирования презентаций из PPT в PDF. Видеозапись конференции можно сохранить в формате AVI / FLV. Есть чат и личные сообщения. Имеется календарь с системой уведомлений (электронная почта или Ical). Возможна интеграция с Moodle, Joomla, Wordpress, Drupal и другими популярными LMS и CMS.

Порядок установки OpenMeetings

Устанавливаем вспомогательные пакеты необходимые для работы Openmeeting:
1. Запустить flashplayer10_1_p3_plugin_022310.exe, нажать установка
2. Запустить ImageMagick-6.6.0-0-Q16-windows-dll.exe, нажать «Next», «Next», «Next»
3. Запустить установку пакета OOo_3.2.0_Win32Intel_install_wJRE_ru.exe (OpenOffice), выбирайте полную установку. В том числе установится Java JDK 1.6 необходимая для работы openview.
4. Создать папку ffmpeg в например и скопировать туда файл ffmpeg.exe
5. Распаковать sox-14.3.0-win32.zip в например .

6. Установить Postgres и создать базу Openmeetings

7. Распаковываем openmeetings_1_1_r2905.zip и запускаем red5.bat

8. Копируем \webapps\openmeetings\conf\postgres_hibernate.cfg.xml в \webapps\openmeetings\conf\hibernate.cfg.xml

9. Редактируем файл \webapps\openmeetings\conf\hibernate.cfg.xml, указываем параметры авторизации СУБД.

10. Создаем переменную окружение JAVA_PATH с путем до java, в нашем случае «C:\Program Files(x86)\Java\jre6

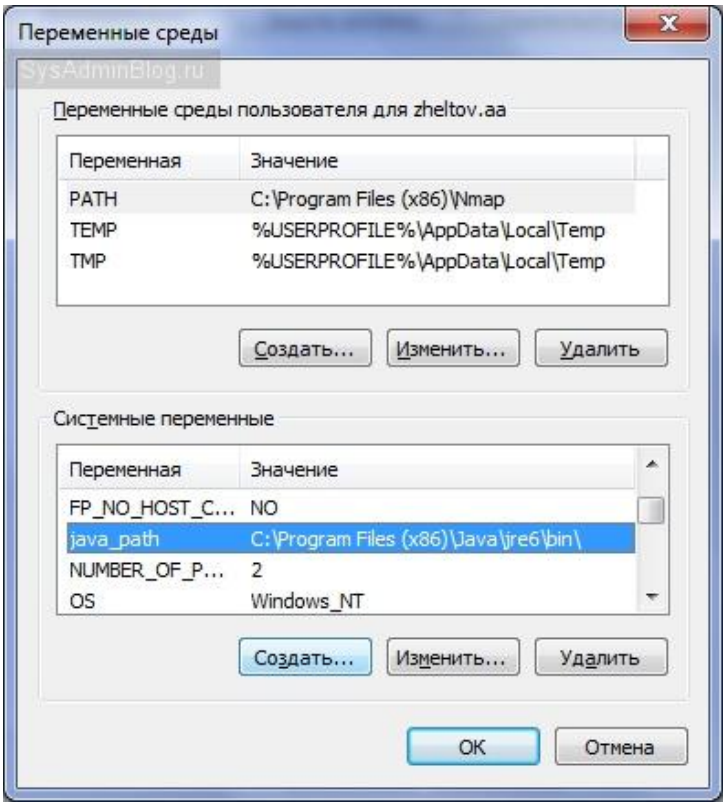


Рис. 2.112. Окно переменных сред

11. Перегружаем сервер

12. Открываем адрес http://servername:5080/openmeetings/install

13. Указываем свои настройки и пути до установленных пакетов swftools, ffmpeg, ImageMagick, sox и жмем Install.

Если предустановка выполнена правильно, при открытии адреса выведется следующее:

Рисунок 2.113. Установка OpenMeetings (шаг 1)

Ввод данных представлен на рисунке 2.114

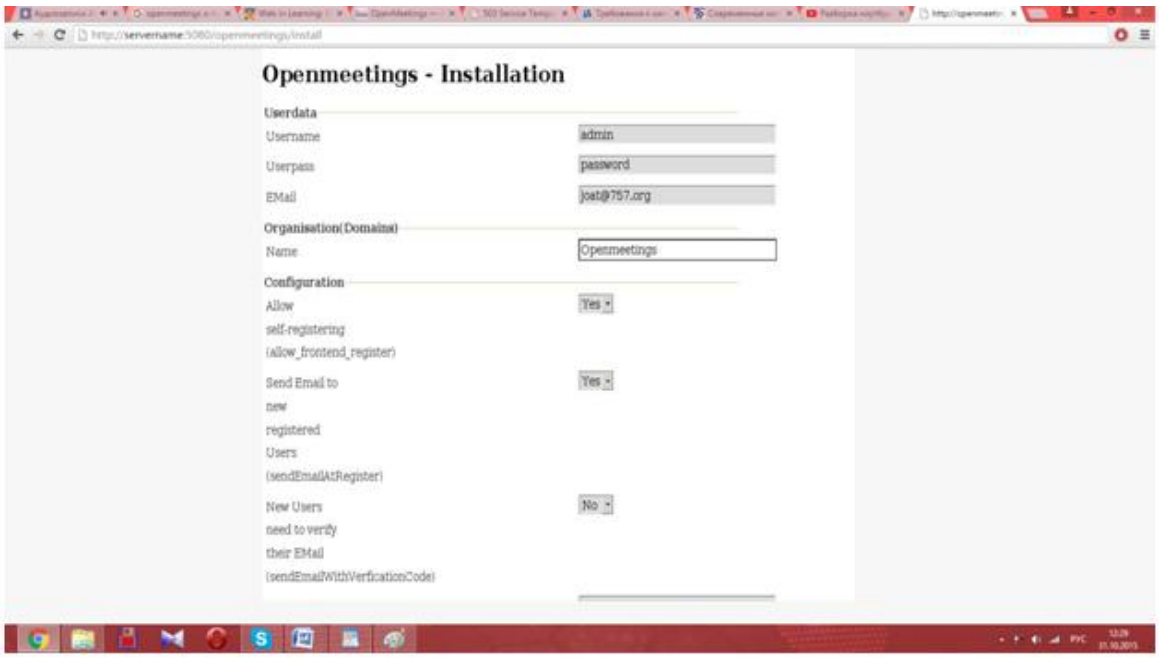


Рис. 2.114. Установка OpenMeetings (шаг 2)

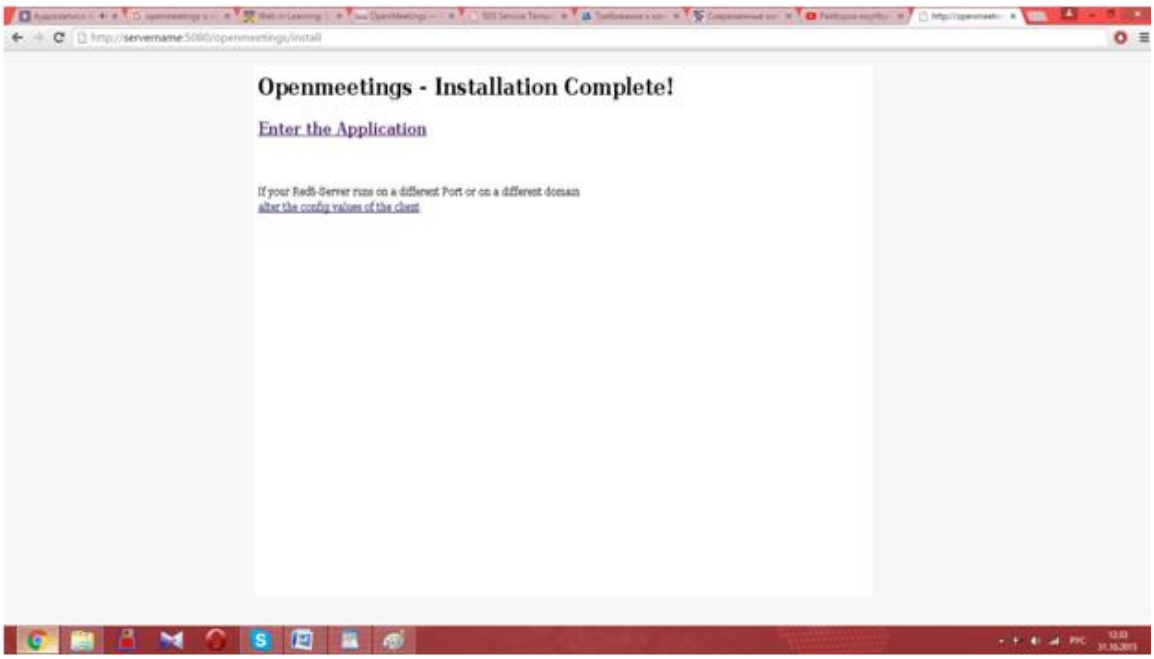


Рис. 2.115. Установка OpenMeetings выполнена

Авторизация представлена на рисунке

2.116

Рис. 5.116. Авторизация OpenMeetings

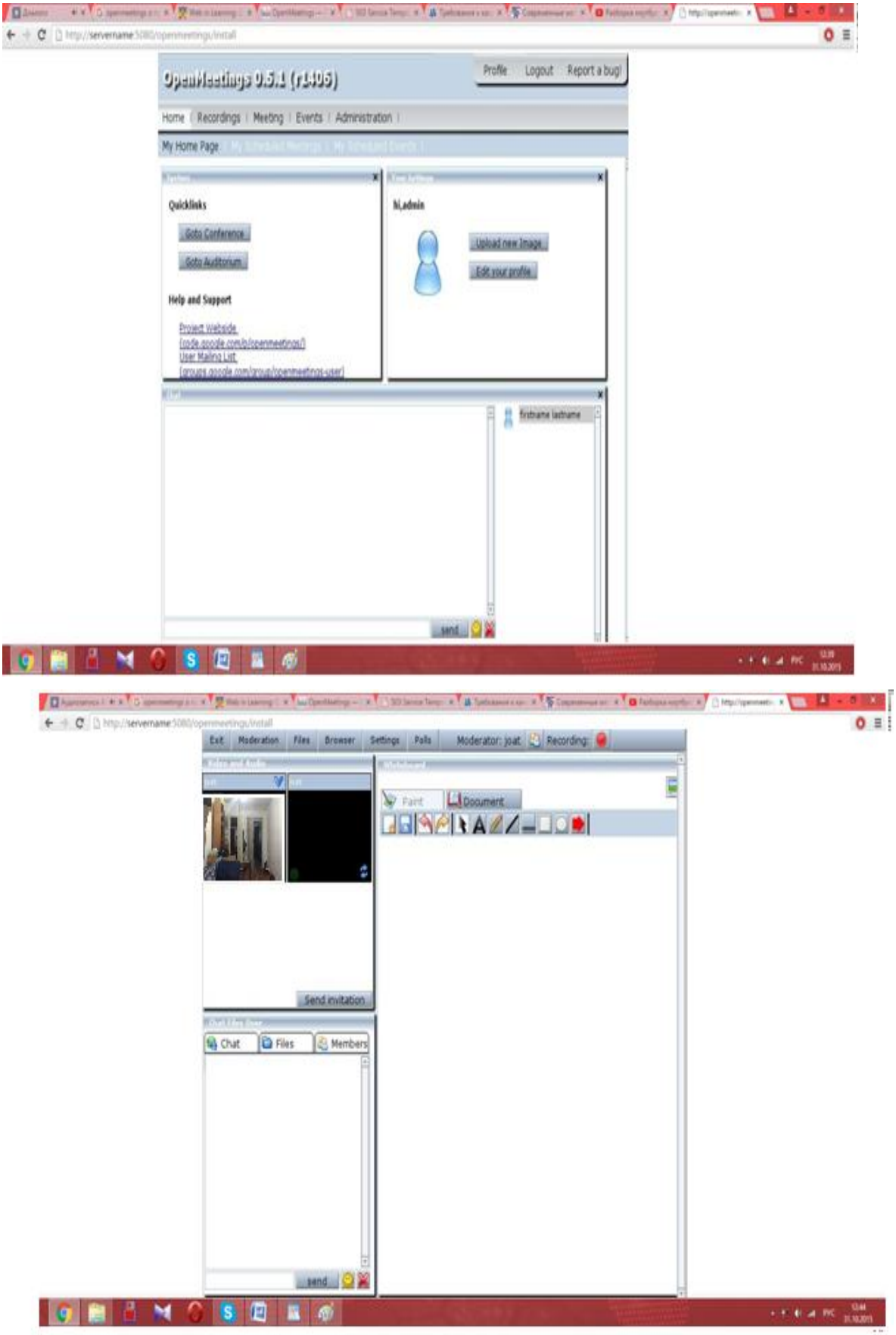


Рис. 2.117. Рабочий интерфейс программы

Использование OpenMeetings

Требования к использованию системы видеоконференций:

Для полноценной возможности использовать видеоконференции необходимо:

- Веб-Камера, подключённая и настроенная
- Микрофон
- Наличие динамиков.

При входе в систему будет предложено авторезироваться, либо зарегистрироваться, если вы этого еще не сделали. Окно входа в систему представлено на рисунке 2.118

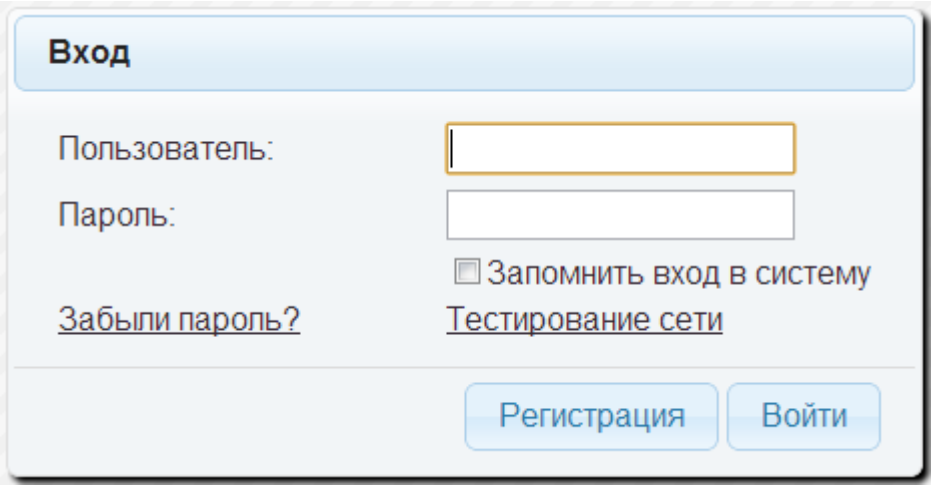


Рис. 2.118. Окно авторизации.

Если нажать кнопку «Регистрация» появится форма представленная на рисунке 2.119, где необходимо ввести требуемые учетные данные.

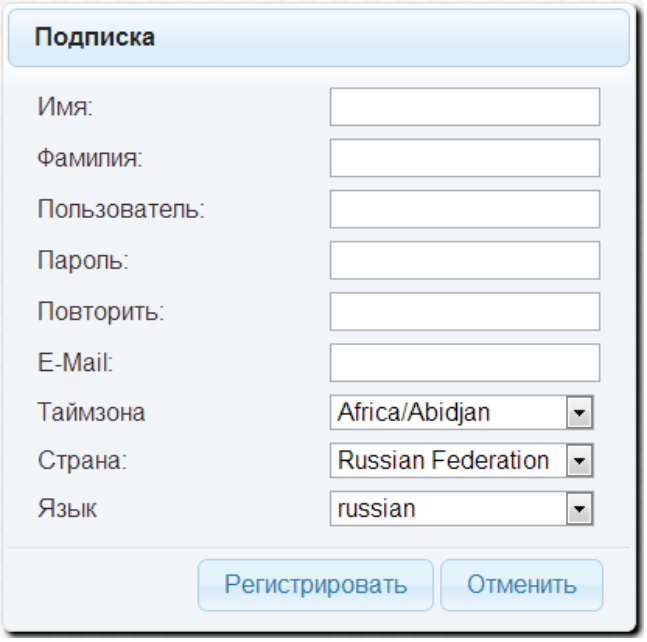


Рис. 2.119. Форма регистрации

После авторизации появляется основное командное окно, представленное на рисунке 2.121

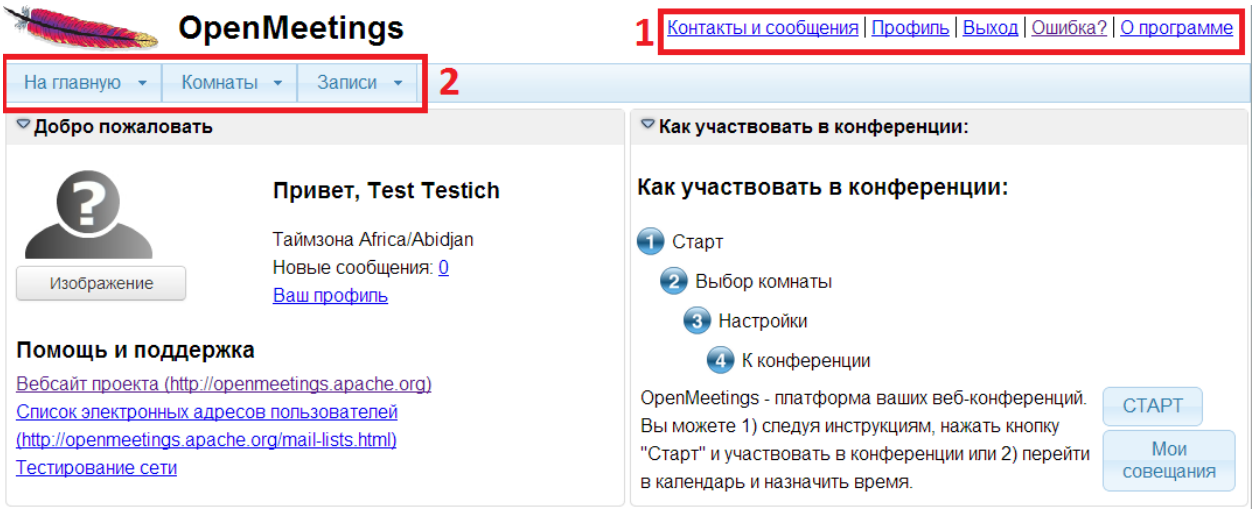


Рис. 2.120. Основное командное окно

Содержит две основные панели.

Первая панель:

Контакты и сообщения – будут отображаться ваши личные сообщения

Профиль – редактирование ваших личных данных

Выход – выйти из текущего пользователя

Ошибка? – сообщить об ошибке

О программе – о программе

Вторая панель:

На главную

* Моя домашняя страница – возращение на главную страницу
* Мои совещания – календарь с предстоящими совещаниями

Комнаты

* Публичные комнаты – публичные комнаты, которые доступны для всех
* Приватные комнаты – комнаты, которыми могут пользоваться пользователи из той же группы
* Мои комнаты – комнаты предназначенные для персонального использования.

Записи

* Записи – просмотр записей прошедших конференций

Так же можно изменить свой профиль и использовать поиск пользователей, скриншоты представлены на рисунках 2.121, 2.122.

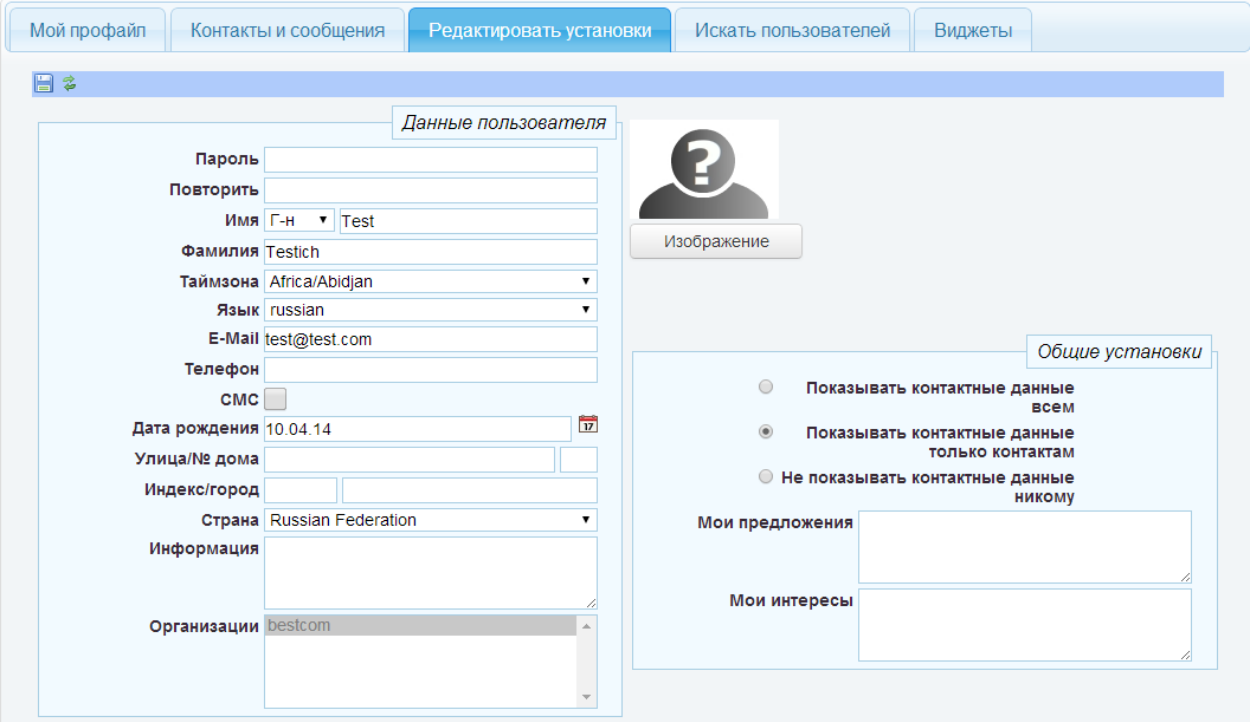


Рис. 2.121. Окно изменение учетной записи

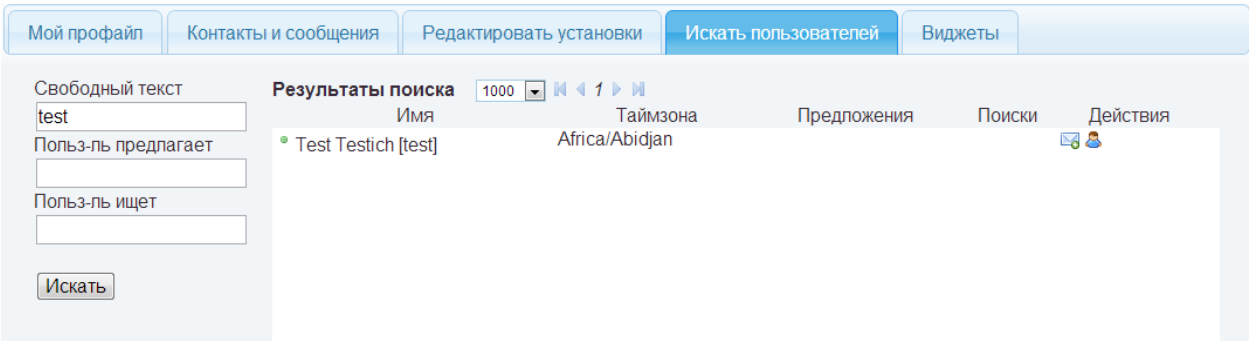


Рис. 2.122. Окно поиска пользователей

Вход в комнату конференции производиться следующим образом: нажимается кнопка «комнаты» и после выхода контекстного меню выбирается тип комнаты (приватные, публичные, мои), как представлено на рисунке 2.123

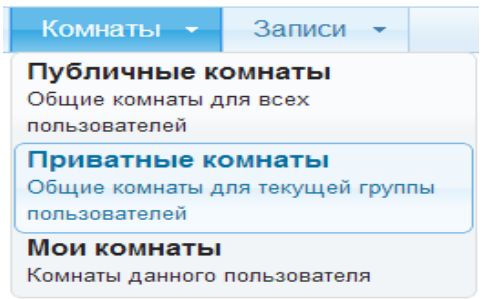


Рис. 2.123. Окно выбора типа комнат

После выбора высветится список всех доступных комнат с их описанием и количеством участников в конференции.

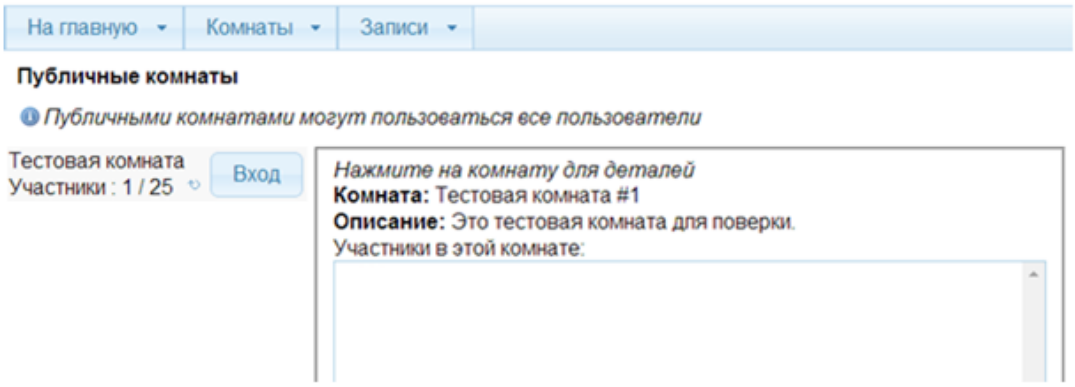


Рис. 2.124. Комната конференции

На рисунке 2.125 представлен скриншот окна конференции.

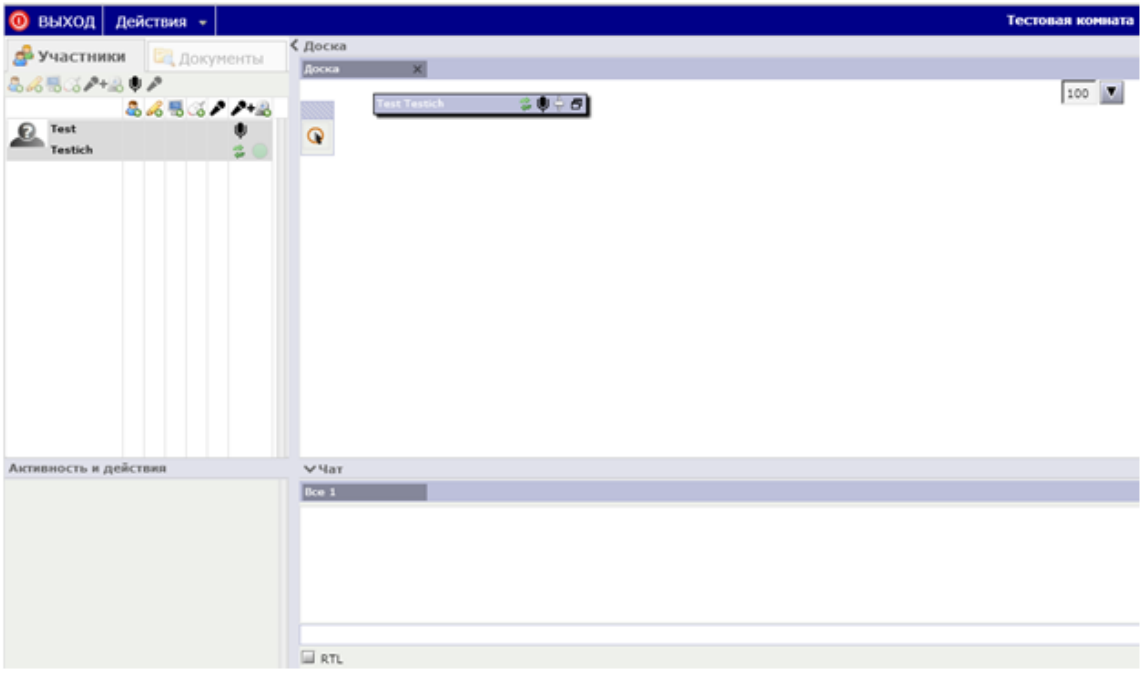


Рис. 2.125. Окно конференции

Слева представлен список участников конференции, а так же их права в данной конференции.

Наличие либо отсутствие определённых типов прав можно определить по зелёным галочкам в соответствующем столбце напротив участника конференции.

Также в нижней части окна представлена панель для Чата, что позволяет быстро обмениваться сообщениями со всеми участниками конференции

В результате проделанной работы было изучена теория построения видеоконференцсвязи, а так же установлен и исследован открытый сервер видеоконференций OpenMeetings.

С ростом технологий и развитием малого и крупного бизнеса, все актуальней становится использование многоточечной видеоконференцсвязи.

3. ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ СИСТЕМ МОБИЛЬНОЙ РАДИОСВЯЗИ [17]

3.1. Проектирование защищенной системы мобильной связи стандарта GSM

GSM относится к сетям второго поколения (2 Generation) (1G — аналоговая сотовая связь, 2G — цифровая сотовая связь, 3G — широкополосная цифровая сотовая связь, коммутируемая многоцелевыми компьютерными сетями, в том числе Интернет).

Мобильные телефоны выпускаются с поддержкой 4 частот: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц.

В зависимости от количества диапазонов, телефоны подразделяются на классы и вариацию частот в зависимости от региона использования.

- Однодиапазонные — телефон может работать в одной полосе частот. В настоящее время не выпускаются, но существует возможность ручного выбора определённого диапазона частот в некоторых моделях телефонов, например Motorola C115, или с помощью инженерного меню телефона.
- Двухдиапазонные (Dual Band) — для Европы, Азии, Африки, Австралии 900/1800 и 850/1900 для Америки и Канады.
- Трёхдиапазонные (Tri Band) — для Европы, Азии, Африки, Австралии 900/1800/1900 и 850/1800/1900 для Америки и Канады.
- Четырехдиапазонные (Quad Band) — поддерживают все диапазоны 850/900/1800/1900.

В стандарте GSM применяется GMSK-модуляция с величиной нормированной полосы BT — 0,3, где B — ширина полосы фильтра по уровню минус 3 дБ, T — длительность одного бита цифрового сообщения.

GSM на сегодняшний день является наиболее распространённым стандартом связи. По данным ассоциации GSM (GSMA) на данный стандарт приходится 82 % мирового рынка мобильной связи, 29 % населения земного шара использует глобальные технологии GSM. В GSMA в настоящее время входят операторы более чем 210 стран и территорий.

История развития

GSM сначала означало *Groupe Spécial Mobile*, по названию группы анализа, которая создавала стандарт. Теперь он известен как *Global System for Mobile Communications* (Глобальная Система для Мобильной Связи), хотя слово «Связь» не включается в сокращение. Разработка GSM началась в 1982 году группой из 26 Европейских национальных телефонных компаний. *Европейская конференция почтовых и телекоммуникационных администраций* (CEPT), стремилась построить единую для всех европейских стран сотовую систему диапазона 900 МГц. Достижения GSM стали «одними из

наиболее убедительных демонстраций какое сотрудничество в Европейской промышленности может быть достигнуто на глобальном рынке».

В 1989 году *Европейский Телекоммуникационный Институт Стандартов* (ETSI) взял ответственность за дальнейшее развитие GSM. В 1990 году были опубликованы первые рекомендации. Спецификация была опубликована в 1991 году.

Коммерческие сети GSM начали действовать в Европейских странах в середине 1991 г. GSM разработан позже, чем аналоговая сотовая связь и во многих отношениях была лучше спроектирована. Северо-Американский аналог — PCS, вырастил из своих корней стандарты включая цифровые технологии TDMA и CDMA, но для CDMA потенциальное улучшение качества обслуживания так и не было никогда подтверждено.

GSM Phase 1

1982 (Groupe Spécial Mobile) — 1990 г. Global System for Mobile Communications. Первая коммерческая сеть в январе 1992 г. Цифровой стандарт, поддерживает скорость передачи данных до 9,6 кбит/с. Полностью устарел, производство оборудования под него прекращено.

В 1991 году были введены услуги стандарта GSM «ФАЗА 1».

В них входят:

- Переадресация вызова (Call forwarding). Возможность перевода входящих звонков на другой телефонный номер в тех случаях, когда номер занят или абонент не отвечает; когда телефон выключен или находится вне зоны действия сети и т. п. Кроме того, возможна переадресация факсов и данных.
- Запрет вызова (Call barring). Запрет на все входящие/исходящие звонки; запрет на исходящие международные звонки; запрет на входящие звонки, за исключением внутрисетевых.
- Ожидание вызова (Call waiting). Эта услуга позволяет принять входящий вызов во время уже продолжающегося разговора. При этом первый абонент или по-прежнему будет находиться на связи, или разговор с ним может быть завершён.
- Удержание вызова (Call Holding). Эта услуга позволяет, не разрывая связь с одним абонентом, позвонить (или ответить на входящий звонок) другому абоненту.
- Глобальный роуминг (Global roaming). При посещении любой из стран, с которой ваш оператор подписал соответствующее соглашение, вы можете пользоваться своим сотовым телефоном GSM без изменения номера.

GSM Phase 2

Стандарт GSM Phase 2 принят в 1993 г.[3] Цифровой стандарт, поддерживает скорость передачи данных до 9,6 кбит/с. С 1995 г. включает диапазон 1900 МГц. Второй этап развития GSM — GSM «Фаза 2», который завершился в 1997 г., предусматривает такие услуги:

- Определение номера вызывающей линии (Calling Line Identification Presentation). При входящем звонке на экране высвечивается номер вызывающего абонента.
- Антиопределитель номера (Calling Line Identification Restriction). С помощью этой услуги можно запретить определение собственного номера при соединении с другим абонентом.
- Групповой вызов (Multi party). Режим телеконференции или конференц-связи позволяет объединить до пяти абонентов в группу и вести переговоры между всеми членами группы одновременно.
- Создание закрытой группы до десяти абонентов (Closed User Group). Позволяет создавать группу пользователей, члены которой могут связываться только между собой. Чаще всего к этой услуге прибегают компании, предоставляющие терминалы своим служащим для работы.
- Информация о стоимости разговора. Сюда входят таймер, который считает время на линии, и счётчик звонков. Также благодаря этой услуге можно проверять оставшийся на счёте кредит. Возможна и другая услуга: «Совет по оплате» (Advice of Charge). По требованию пользователя происходит проверка стоимости и длительности разговора в то время, когда аппарат находится на связи.
- Обслуживание дополнительной линии (Alternative Line Service). Пользователь может приобрести два номера, которые будут приписаны к одному модулю SIM. В этом случае связь выполняется по двум линиям, с предоставлением двух счетов, двух голосовых ящиков и т. п.
- Короткие текстовые сообщения (Short Message Service). Возможность приёма и передачи коротких текстовых сообщений (до 160 знаков).
- Система голосовых сообщений (Voice Mail). Услуга позволяет автоматически переводить входящие звонки на персональный автоответчик (голосовая почта). Пользоваться этим можно только в том случае, если у абонента активизирована услуга «переадресация вызовов».

Стандарт GSM Phase 2 считается устаревшим; но так как стандарт GSM подразумевает обратную совместимость, то старое оборудование базовых станций и телефоны могут работать (и работают) в современных сетях.

GSM Phase 2+

Следующий этап развития сетей стандарта GSM «ФАЗА 2+» не связан с конкретным годом внедрения. Новые услуги и функции стандартизируются и внедряются после подготовки и утверждения их технических описаний. Все работы по этапу «Фаза 2+» проводились *Европейским институтом стандартизации электросвязи* (ETSI). Количество

уже внедрённых и находящихся в стадии утверждения услуг превышает 50. Среди них можно выделить следующие:

- улучшенное программное обеспечение SIM-карты;
- улучшенное полноскоростное кодирование речи EFR (Enhanced Full Rate);
- возможность взаимодействия между системами GSM и DECT;
- повышение скорости передачи данных благодаря пакетной передаче данных GPRS (General Packet RadioService) или за счёт системы передачи данных по коммутируемым каналам HSCSD (High Speed Circuit Switched Data).

Стандарты и радиоинтерфейс

Стандарты GSM создаются и публикуются Европейским институтом телекоммуникационных стандартов. Документы обозначаются GSM nn.nn, например широко известен стандарт на GSM SIM-карточки GSM 11.11.

На сегодняшний день разработано множество различных стандартов сотовой связи. Существенная часть из них уже и морально, и физически устарела, часть не нашла распространения, а другие, напротив, распространились по всему миру и нашли сотни миллионов пользователей. Вот список самых распространенных стандартов:

* AMPS
* DAMPS
* NMT-450
* GSM 900,1800,1900
* CDMA
*DECT

Наибольшее распространение, благодаря отличным функциональным возможностям (передача SMS, MMS, EMS, факсов, возможность доступа в интернет по GPRS, система GPS и т.д.), нашли полностью цифровые стандарты GSM и CDMA.

GSM-900

Цифровой стандарт мобильной связи в диапазоне частот от 890 до 915 МГц (от телефона к базовой станции) и от 935 до 960 МГц (от базовой станции к телефону). Количество *реальных* каналов связи гораздо больше чем написано выше в таблице, т.к присутствует еще и временное разделение каналов TDMA, т.е на одной и той же частоте могут работать несколько абонентов с разделением во времени.

В некоторых странах диапазон частот GSM-900 был расширен до 880—915 МГц (MS -> BTS) и 925—960 МГц (MS <- BTS), благодаря чему максимальное количество каналов связи увеличилось на 50. Такая модификация была названа **E-GSM** (extended GSM).

GSM-1800

Модификация стандарта GSM-900, цифровой стандарт мобильной связи в диапазоне частот от 1710 до 1880 МГц.

Особенности:

- Максимальная излучаемая мощность мобильных телефонов стандарта GSM-1800 — 1 Вт, для сравнения у GSM-900 — 2 Вт. Большее время непрерывной работы без подзарядки аккумулятора и снижение уровня радиоизлучения.
- Высокая ёмкость сети, что важно для крупных городов.
- Возможность использования телефонных аппаратов, работающих в стандартах GSM-900 и GSM-1800, одновременно. Такой аппарат функционирует в сети GSM-900, но, попадая в зону GSM-1800, переключается — вручную или автоматически. Это позволяет оператору рациональнее использовать частотный ресурс, а клиентам — экономить деньги за счёт низких тарифов. В обеих сетях абонент пользуется одним номером. Но использование аппарата в двух сетях возможно только в тех случаях, когда эти сети принадлежат одной компании, или между компаниями, работающими в разных диапазонах, заключено соглашение о роуминге.

Сеть GSM 900-1800 — это единая сеть, с общей структурой, логикой и мониторингом в которой телефон никуда не переключается. Вручную можно только запретить использовать один из диапазонов в тестовых или очень старых аппаратах.

Проблема состоит в том, что зона охвата для каждой базовой станции значительно меньше, чем в стандартах GSM-900, AMPS/DAMPS-800, NMT-450. Необходимо большее число базовых станций. Чем выше частота излучения, тем хуже проникающая способность радиоволн в городской застройке.

Дальность связи в GSM лимитирована задержкой сигнала Timing advance и составляет до 35 км. При использовании режима extended cell возрастает до 75 км. Практически достижимо только в море, пустыне и горах.

CDMA

Тип стандарта: цифровой

Полоса частот: 1,23 МГц

Статус: Активно эксплуатируется

Краткое описание: Технология CDMA (система множественного доступа с кодовым разделением) изначально разработана для военных целей США, но, благодаря отличным показателям, нашла после модернизации широкое применение и в гражданской связи.

Особенности:

* Сигнал каждого абонента модулируется псевдослучайным, уникальным кодом (шумоподобным сигналом, отправляемым клиенту в начале разговора). Несущая частота

сигнала меняется, согласно этому случайному правилу, в результате чего узкополосный информационный сигнал каждого пользователям расширяется во всю ширину частотного спектра (1,23 МГц в случае CDMA). В приемнике сигнал демодулируется с помощью идентичного кода, в результате чего восстанавливается изначальный сигнал. Но в то же время сигналы остальных пользователей для данного приемника продолжают оставаться расширенными и воспринимаются им лишь как шум, незначительно мешающий нормальной работе приемника.

* Отличные показатели шумоустойчивости, как следствие - снижение стоимости развертывания CDMA-сетей.

* Высокое качество передачи речи при низких показателях излучаемой мощности.

* Большая, по сравнению с GSM, емкость сети.

* Высокое качество связи в зданиях.

NMT-450

Тип стандарта: аналоговый

Частотный диапазон: 453-468 МГц

Статус: устарел и морально, и физически

Краткое описание: NMT-450 (Nordic Mobile Telephone) разработан скандинавскими учеными. Первые сотовые сети в России строились именно на базе этого стандарта - федеральная сеть "СОТЕЛ" работала именно на NMT.

Особенности:

* Большая площадь покрытия одним ретранслятором, а значит, меньшие затраты на организацию сети.

* Малое затухание сигнала на открытом пространстве, что для России с ее плотностью заселения - огромный плюс.

* Сигнал ретранслятора может добивать на 100 километров!

* Благодаря тому, что стандарт - аналоговый, обеспечивается более высокое качество передачи речи - отсутствует грубая дискретизация голосовых отсчетов.

* Плохая помехоустойчивость из-за используемых частот. Уровень индустриальных помех в этом диапазоне значительно выше, чем, скажем, на 800, 900 и 1800 МГц.

* Отсутствие секретности разговоров - их можно слушать УКВ-приемником.

* Низкая емкость сетей, что не позволяет массово использовать стандарт в крупных городах.

* Список дополнительных услуг издевательски пуст.

* NMT-трубки весят в несколько раз больше своих цифровых собратьев и крайне расточительны в плане электроэнергии и здоровья владельца.

AMPS

Тип стандарта: аналоговый

Частотный диапазон: 825-890 МГц

Статус: устарел и морально, и физически

Краткое описание: В конце восьмидесятых американские специалисты разработали специально для своей страны стандарт AMPS (Advanced Mobile Phone Service - усовершенствованная мобильная телефонная система). Завоевав популярность в других странах, в 1993 стандарт пришел в Россию. Такие сети по сей день эксплуатируются в 55 регионах, часть из них работает в аналоговом стандарте AMPS, часть - в усовершенствованном цифровом D-AMPS.

Особенности:

* Более высокая, чем у NMT-450, емкость сетей.

* Низкий уровень индустриальных и атмосферных помех благодаря используемому частотному диапазону.

* Более надежная, чем у NMT-450, связь в помещениях.

* Меньшая зона устойчивой связи для одной базовой станции, что вынуждает операторов ставить их ближе друг к другу - большие затраты.

* Почти не распространен в Европе и Азии.

AMPS уже давным-давно морально устарел, и в 1990 г. в США был разработан D-AMPS.

D-AMPS

Тип стандарта: цифровой

Частотный диапазон: 825-890 МГц

Статус: устарел морально

Краткое описание: Когда AMPS морально устарел - а это произошло довольно быстро, в 1990 году - в Штатах был разработан D-AMPS.

Особенности:

* Емкость сетей на несколько порядков выше, чем у NMT-450 и AMPS.

* Возможность эксплуатации мобильных аппаратов как в цифровом, так и в аналоговом режимах.

* Расширенный спектр дополнительных услуг.

* Емкость DAMPS-сетей ниже, чем в полностью цифровых системах, но выше, чем в аналоговых.

GPRS

Главным недостатком стандарта GSM на сегодня является низкая скорость передачи данных - максимум 9,6 Кбит/с, да и сам процесс реализован довольно убого - под данные

выделяется один голосовой канал; оплата услуги, соответственно, осуществляется исходя из времени соединения, причем по тарифам, весьма схожим с речевыми. Для решения этой проблемы и был разработан стандарт передачи данных GPRS (General Packet Radio Service - услуга пакетной передачи данных по радиоканалу).

Новая система предложила пользователям мобильной связи уже совсем другие условия - максимальная скорость соединения составляет 171,2 Кбит/с, а оплата осуществляется исходя из количества реально переданной информации, трафика.

В GSM-сетях, оборудованных GPRS-модулями, более рационально распределяется радиочастотный ресурс. Не вдаваясь в сложные технические детали, можно сказать, что выигрыш в скорости достигается за счет одновременного использования для передачи данных нескольких свободных в настоящий момент каналов. Тут следует отметить, что скорость передачи информации определяется не столько теоретическими возможностями сетевого и абонентского оборудования, сколько загрузкой сети - так, из собственного опыта могу сказать, что скорость соединения в России в ближайшие несколько лет у тебя не превысит 5-6 Кбит/с.

Благодаря тому, что пакеты данных имеют значительно меньший приоритет, по сравнению с голосовой информацией, внедрение систем GPRS не приводит к ухудшению качества услуг передачи речи.

Система GPRS состоит из двух основных модулей: SGSN (Serving GPRS Support Node - узел поддержки GPRS) и GGSN (Gateway GPRS Support Node - шлюзовой узел GPRS). В некотором смысле SGSN можно назвать аналогом коммутатора сети GSM. SGSN обеспечивает доставку пакетов информации пользователям, взаимодействует с реестром абонентов, проверяет, разрешены ли запрашиваемые услуги, ведет мониторинг пользователей, организует регистрацию вновь прибывших абонентов и т.п.

Назначение GGSN легко понять из расшифровки названия - это шлюз между сотовой сетью (вернее, SGSN) и внешними информационными сетями (интернетом, провайдерскими Intranet-сетями и т.д.).

Основной задачей GGSN, таким образом, является маршрутизация (обычно совмещенная с NAT'ом) пакетов, генерируемых абонентом через SGSN. Вторичными функциями GGSN являются: динамическая выдача IP-адресов (а-ля DHCP-сервер :)), отслеживание информации о внешних сетях, подсчет трафика, тарификация и т.д.

Благодаря хорошей масштабируемости системы GPRS, оператор может увеличивать число SGSN и GGSN по мере роста числа пользователей и их суммарного трафика.

Как известно, для работы с GPRS необходимо иметь специальный телефон, поддерживающий эту технологию.

Основная характеристика такого телефона - так называемый класс GPRS. Это максимальное количество каналов, которое может задействовать аппарат для передачи данных - напомню, что один канал обеспечивает передачу данных со скоростью до 13,4 Кбит/с.

Самым первым производителем телефонов с GPRS стала французская фирма Sagem - на проходящей в Женеве выставке Telecom'99 она представила телефон Sagem MC-850, имеющий 3 канала на прием и 1 на передачу данных.

Современные телефоны способны использовать десять и более каналов для передачи данных, что, теоретически, обеспечивает отличную скорость соединения - до 20 килобайт в секунду.

В стандарте GSM определены 4 диапазона работы (ещё есть пятый):

900/1800 МГц (используется в Европе, Азии)

Характеристики	**GSM-900**	**GSM-1800**
Частоты передачи MS и приёма BTS (uplink), МГц	890 — 915	1710 — 1785
Частоты приёма MS и передачи BTS (downlink), МГц	935 — 960	1805 — 1880
Дуплексный разнос частот приёма и передачи, МГц	45	95
Количество **частотных** каналов связи с шириной 1 канала связи в 200 кГц	124	374
Ширина полосы канала связи, кГц	200	200

850/1900 МГц (используется в США, Канаде, отдельных странах Латинской Америки и Африки)

Характеристики	**GSM-850**	**GSM-1900**
Частоты передачи MS и приёма BTS, МГц	824 — 849	1850 — 1910
Частоты приёма MS и передачи BTS, МГц	869 — 894	1930 — 1990
Дуплексный разнос частот приёма и передачи, МГц	45	80

Структура GSM

Система GSM состоит из трёх основных подсистем:

- подсистема базовых станций (BSS — Base Station Subsystem),
- подсистема коммутации (NSS — Network Switching Subsystem),
- центр технического обслуживания (OMC — Operation and Maintenance Centre).

В отдельный класс оборудования GSM выделены терминальные устройства — подвижные станции (MS — Mobile Station), также известные как мобильные (сотовые) телефоны.

Подсистема базовых станций

Рис.3.1. Антенны трех базовых станций на мачте

BSS состоит из собственно базовых станций (BTS — Base Transceiver Station) и контроллеров базовых станций (BSC — Base Station Controller). Область, накрываемая сетью GSM, разбита на условные шестиугольники, называемые *сотами* или *ячейками*. Диаметр каждой шестиугольной ячейки может быть разным — от 400 м до 50 км. Максимальный теоретический радиус ячейки составляет 120 км, что обусловлено ограниченной возможностью системы синхронизации к компенсации времени задержки сигнала. Каждая ячейка покрывается находящейся в её центре одной базовой станцией, при этом ячейки частично перекрывают друг друга, тем самым сохраняется возможность передачи обслуживания без разрыва соединения при перемещении абонента из одной соты в другую. Естественно, что на самом деле сигнал от каждой станции распространяется, покрывая площадь в виде круга, а не шестиугольника, последний же является лишь упрощением представления зоны покрытия. Каждая базовая станция имеет шесть соседних в связи с тем, что в задачи планирования размещения станций входила минимизация стоимости системы. Меньшее количество соседних базовых станций приводило бы к большему перехлёсту зон

покрытия с целью избегания "мёртвых зон", что в свою очередь потребовало бы более плотного расположения базовых станций. Большее количество соседних базовых станций приводило бы к излишним расходам на дополнительные станции, в то время как выигрыш от уменьшения зон перехлёста был бы уже весьма незначительным.

Базовая станция (BTS) обеспечивает приём/передачу сигнала между MS и контроллером базовых станций. BTS является автономной и строится по модульному принципу. Направленные антенны базовых станций могут располагаться на вышках, крышах зданий и т. д.

Контроллер базовых станций (BSC) контролирует соединения между BTS и подсистемой коммутации. В его полномочия также входит управление очерёдностью соединений, скоростью передачи данных, распределение радиоканалов, сбор статистики, контроль различных радиоизмерений, назначение и управление процедурой Handover.

Подсистема коммутации

NSS состоит из нижеследующих компонентов.

Центр коммутации (MSC — Mobile Switching Center)

MSC контролирует определённую географическую зону с расположенными на ней BTS и BSC. Осуществляет установку соединения к абоненту и от него внутри сети GSM, обеспечивает интерфейс между GSM и ТфОП, другими сетями радиосвязи, сетями передачи данных. Также выполняет функции маршрутизации вызовов, управление вызовами, эстафетной передачи обслуживания при перемещении MS из одной ячейки в другую. После завершения вызова MSC обрабатывает данные по нему и передаёт их в центр расчётов для формирования счета за предоставленные услуги, собирает статистические данные. MSC также постоянно следит за положением MS, используя данные из HLR и VLR, что необходимо для быстрого нахождения и установления соединения с MS в случае её вызова.

Домашний регистр местоположения (HLR — Home Location Registry)

Содержит базу данных абонентов, приписанных к нему. Здесь содержится информация о предоставляемых данному абоненту услугах, информация о состоянии каждого абонента, необходимая в случае его вызова, а также Международный Идентификатор Мобильного Абонента (IMSI — International Mobile Subscriber Identity), который используется для аутентификации абонента (при помощи AUC). Каждый абонент приписан к одному HLR. К данным HLR имеют доступ все MSC и VLR в данной GSM-сети, а в случае межсетевого роуминга — и MSC других сетей.

Гостевой регистр местоположения (VLR — Visitor Location Registry)

VLR обеспечивает мониторинг передвижения MS из одной зоны в другую и содержит базу данных о перемещающихся абонентах, находящихся в данный момент в этой зоне, в том

числе абонентах других систем GSM — так называемых роумерах. Данные об абоненте удаляются из VLR в том случае, если абонент переместился в другую зону. Такая схема позволяет сократить количество запросов на HLR данного абонента и, следовательно, время обслуживания вызова.

Регистр идентификации оборудования (EIR — Equipment Identification Registry)

Содержит базу данных, необходимую для установления подлинности MS по IMEI (International Mobile Equipment Identity). Формирует три списка: белый (допущен к использованию), серый (некоторые проблемы с идентификацией MS) и чёрный (MS, запрещённые к применению). У российских операторов (и большей части операторов стран СНГ) используются только белые списки, что не позволяет раз и навсегда решить проблему кражи мобильных телефонов.

Центр аутентификации (AUC — Authentification Center)

Здесь производится аутентификация абонента, а точнее — SIM (Subscriber Identity Module). Доступ к сети разрешается только после прохождения SIM процедуры проверки подлинности, в процессе которой с AUC на MS приходит случайное число RAND, после чего на AUC и MS параллельно происходит шифрование числа RAND ключом Ki для данной SIM при помощи специального алгоритма. Затем с MS и AUC на MSC возвращаются «подписанные отклики» — SRES (Signed Response), являющиеся результатом данного шифрования. На MSC отклики сравниваются, и в случае их совпадения аутентификация считается успешной.

Подсистема OMC (Operations and Maintenance Center)

Соединена с остальными компонентами сети и обеспечивает контроль качества работы и управление всей сетью. Обрабатывает аварийные сигналы, при которых требуется вмешательство персонала. Обеспечивает проверку состояния сети, возможность прохождения вызова. Производит обновление программного обеспечения на всех элементах сети и ряд других функций.

Преимущества и недостатки

Преимущества стандарта GSM:

- Меньшие по сравнению с аналоговыми стандартами (NMT-450, AMPS-800) размеры и вес телефонных аппаратов при большем времени работы без подзарядки аккумулятора. Это достигается в основном за счёт аппаратуры базовой станции, которая постоянно анализирует уровень сигнала, принимаемого от аппарата абонента. В тех случаях, когда он выше требуемого, на сотовый телефон автоматически подаётся команда снизить излучаемую мощность.
- Хорошее качество связи при достаточной плотности размещения базовых станций.

- Большая ёмкость сети, возможность большого числа одновременных соединений.
- Низкий уровень индустриальных помех в данных частотных диапазонах.
- Улучшенная (по сравнению с аналоговыми системами) защита от подслушивания и нелегального использования, что достигается путём применения алгоритмов шифрования с разделяемым ключом.
- Эффективное кодирование (сжатие) речи. EFR-технология была разработана фирмой Nokia и впоследствии стала промышленным стандартом кодирования/декодирования для технологии GSM (см. GSM-FR, GSM-HR и GSM-EFR)
- Широкое распространение, особенно в Европе, большой выбор оборудования.
- Возможность роуминга. Это означает, что абонент одной из сетей GSM может пользоваться сотовым телефонным номером не только у себя «дома», но и перемещаться по всему миру переходя из одной сети в другую не расставаясь со своим абонентским номером. Процесс перехода из сети в сеть происходит автоматически, и пользователю телефона GSM нет необходимости заранее уведомлять оператора (в сетях некоторых операторов, могут действовать ограничения на предоставление роуминга своим абонентам, более детальную информацию можно получить обратившись непосредственно к своему GSM оператору)

Недостатки стандарта GSM

- Искажение речи при цифровой обработке и передаче.
- Связь возможна на расстоянии не более 120 км от ближайшей базовой станции даже при использовании усилителей и направленных антенн. Поэтому для покрытия определённой площади необходимо большее количество передатчиков, чем в NMT-450 и AMPS.

Моделирование канала стандарта GSM в MATLAB Simulink [17]

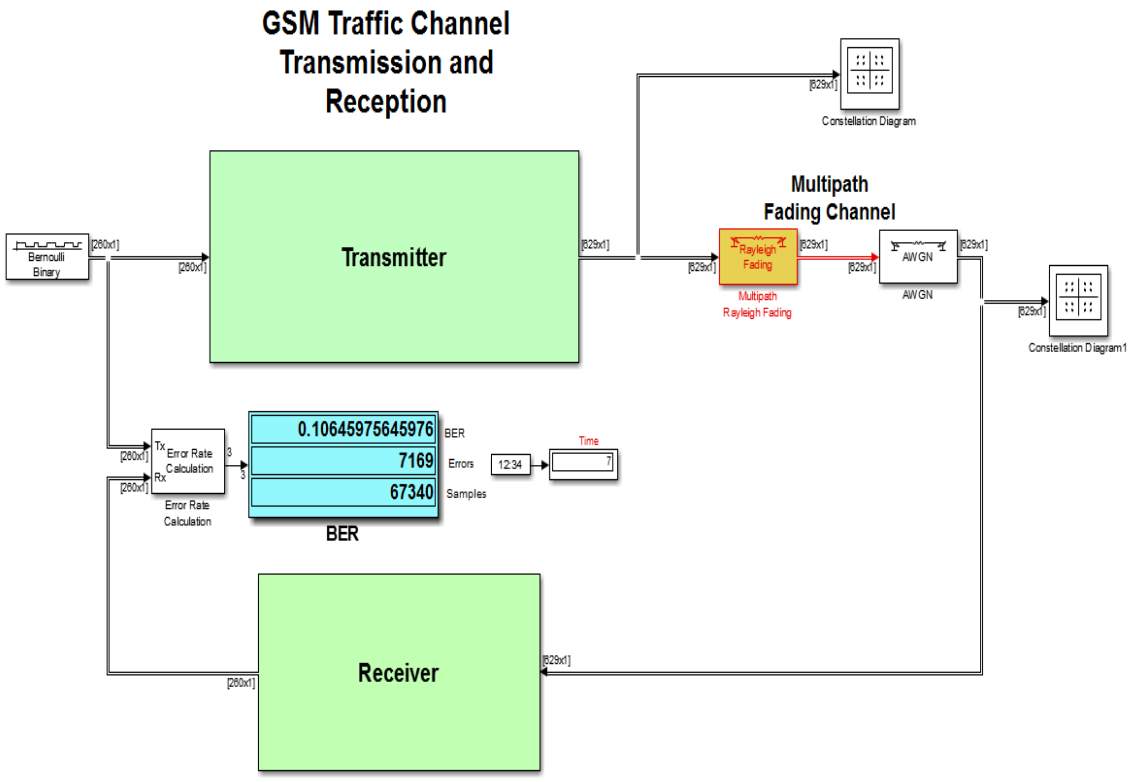


Рис. 3.2. Модель GSM в Simulink MATLAB 2015

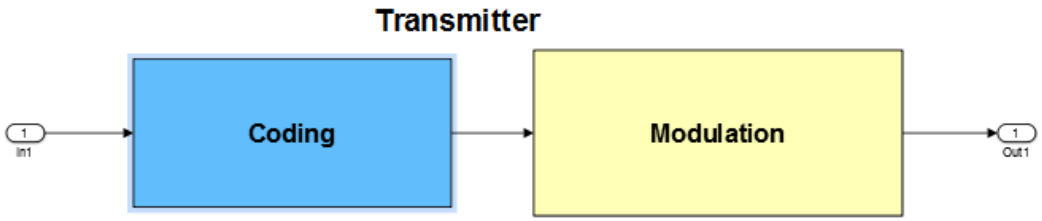


Рис. 3.3. Схема передатчика

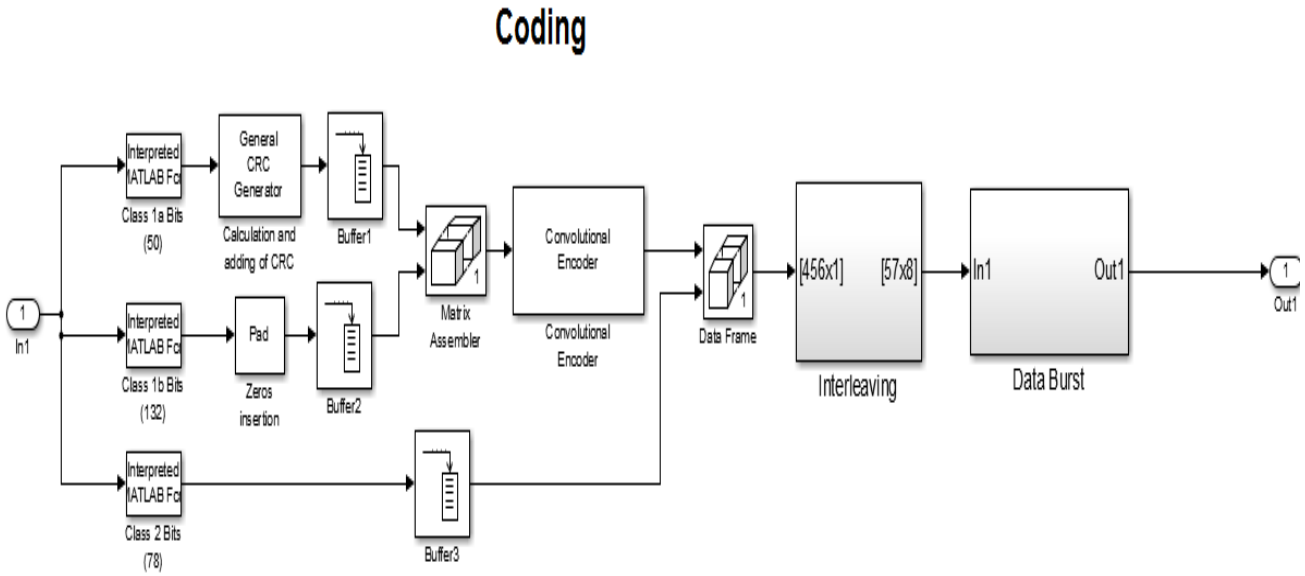


Рис. 3.4. Схема кодера

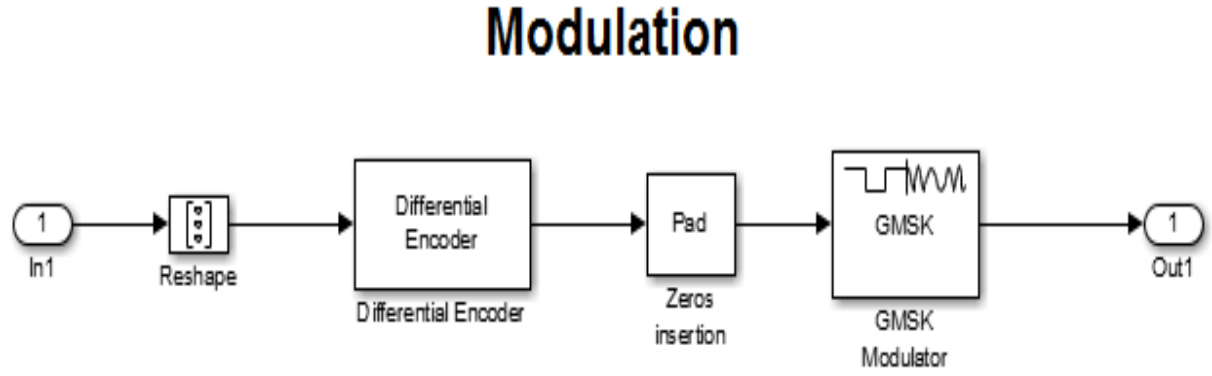


Рис. 3.5. Схема модулятора

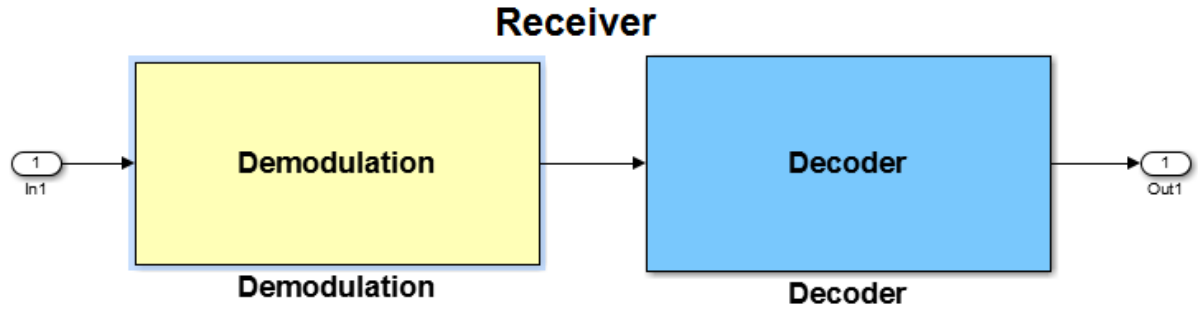


Рис. 3.6. Схема приемника

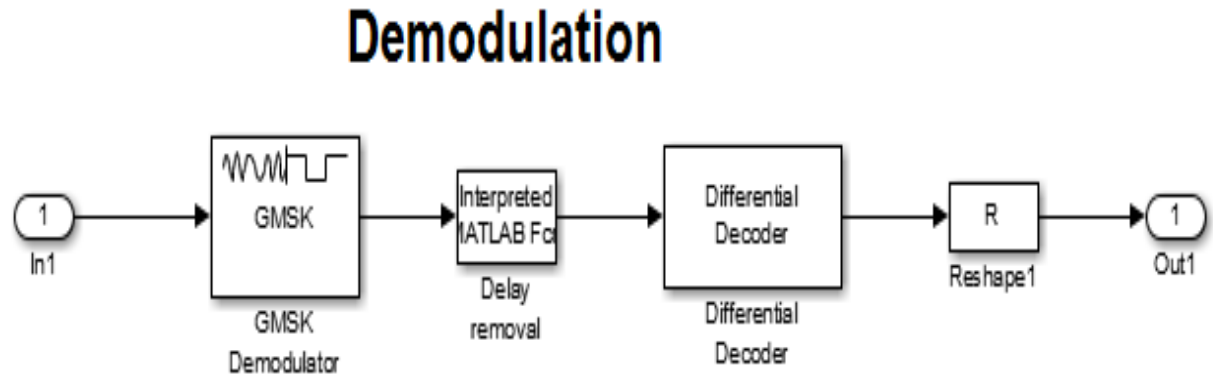


Рис. 3.7. Схема демодулятора

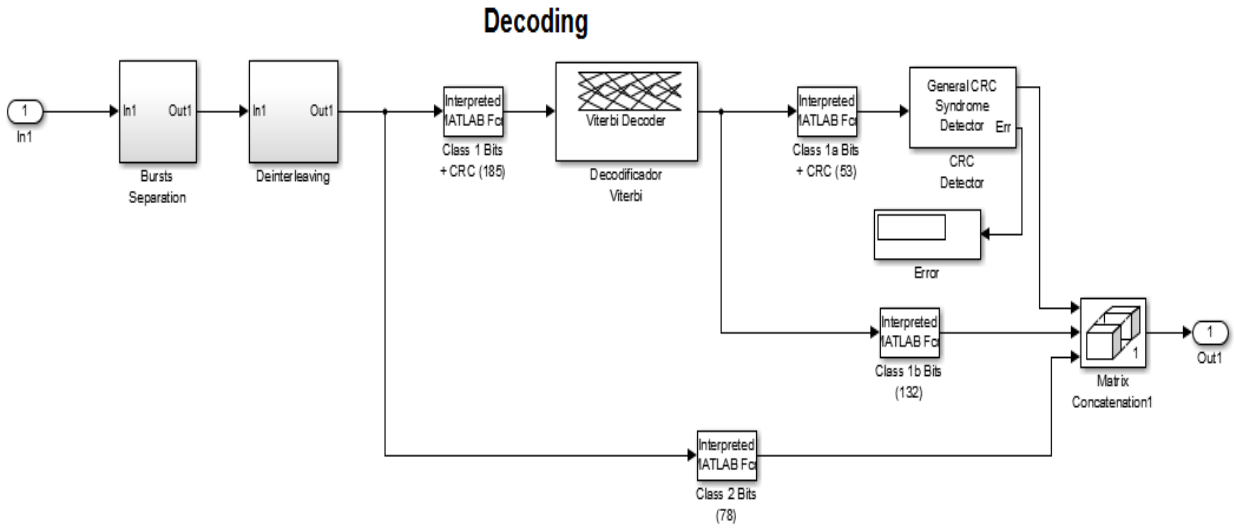


Рис. 3.8. Схема декодера

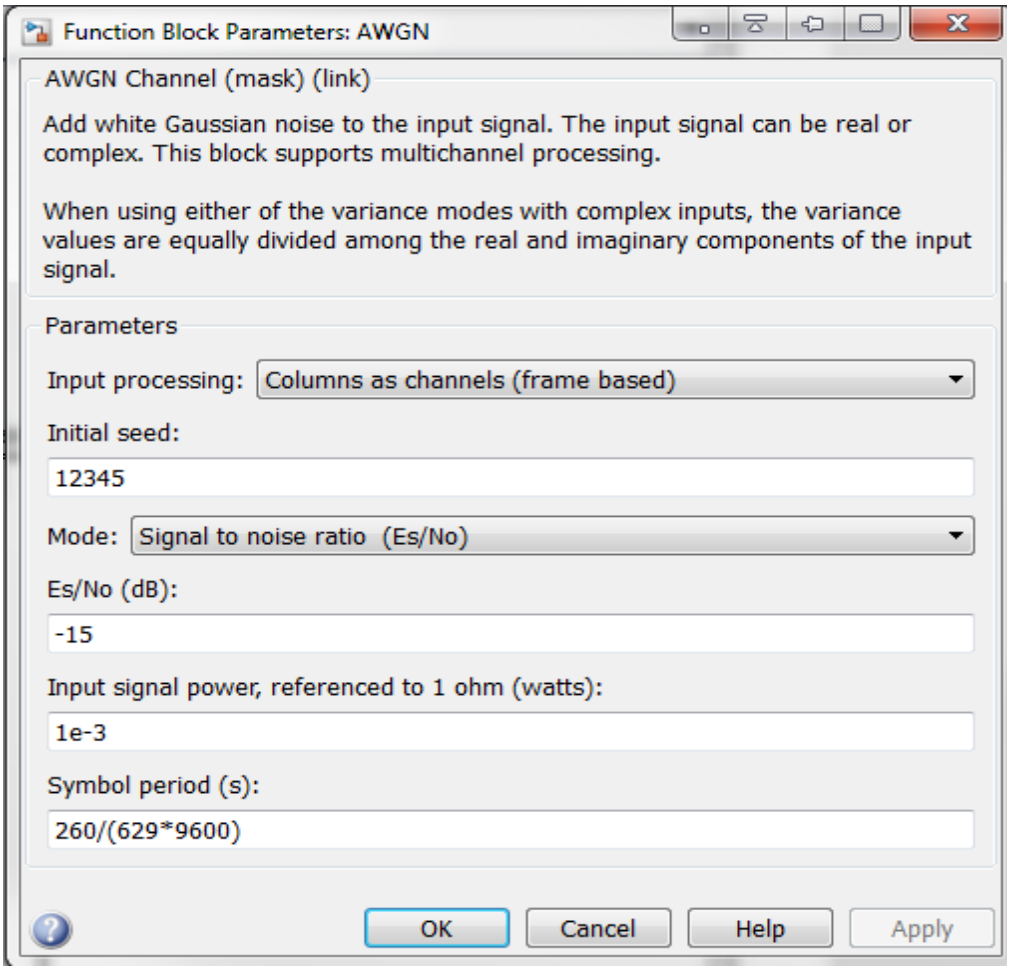


Рис. 3.9. Изменение отношения сигнал/шум.

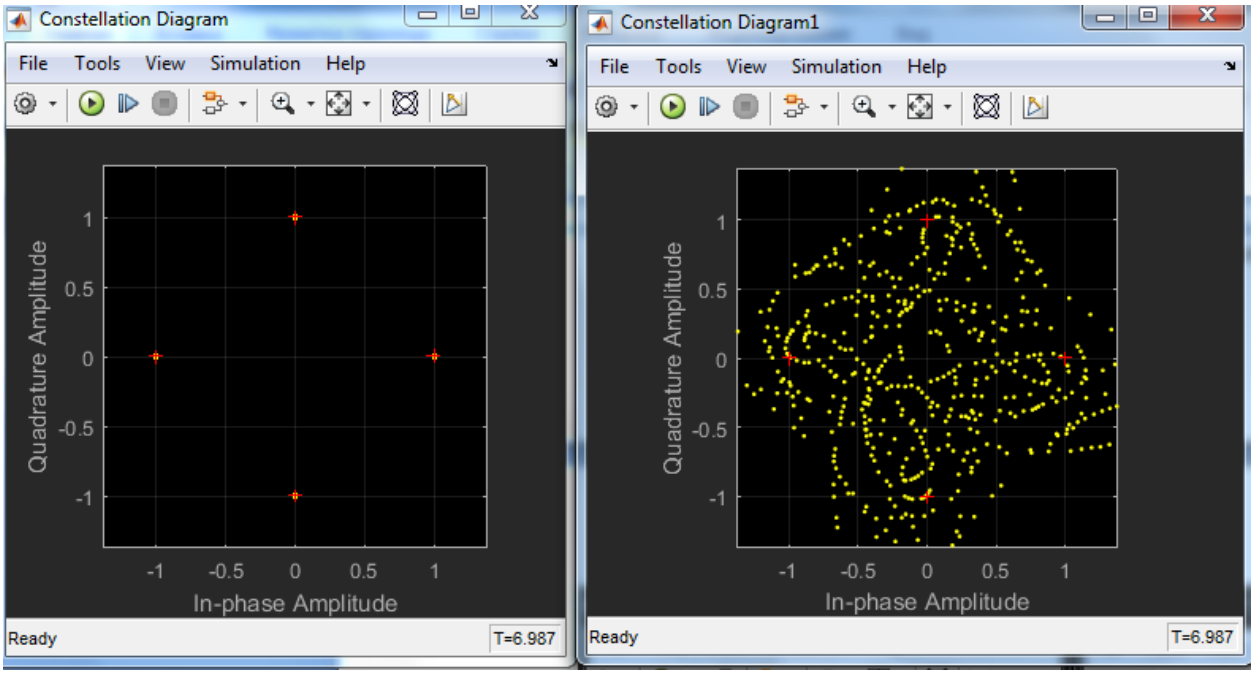


Рис. 3.10. Сравнение передаваеваемого созвездия и принятого, при отношении С/Ш – 20 Дб.

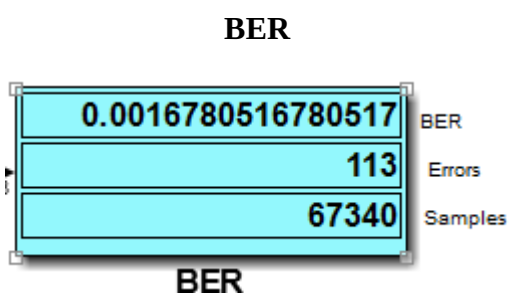


Рис. 3.11. BER при отношении С/Ш 15 Дб.

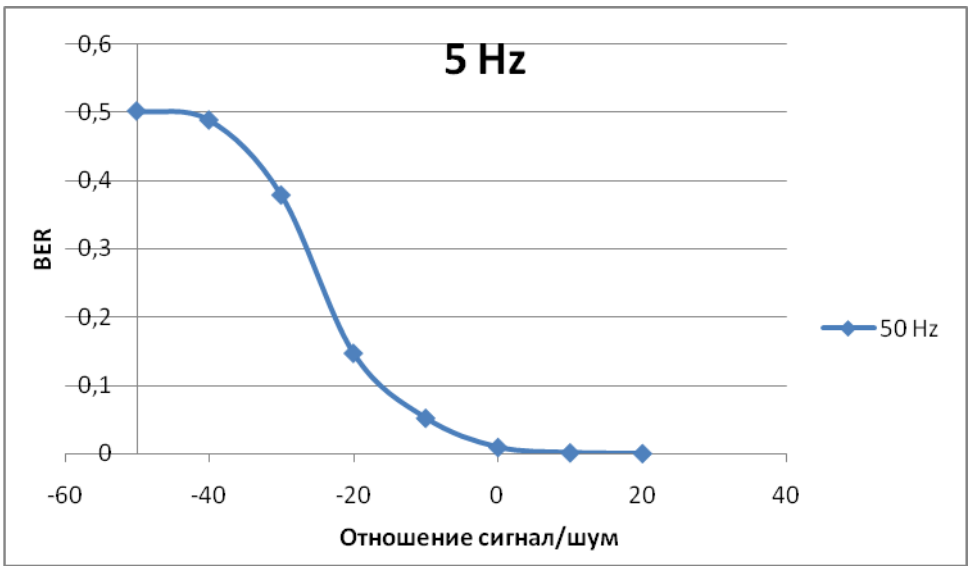


Рис. 3.12. Зависимость BER от отношения сигнал/шум при доплеровском сдвиге 5 Гц

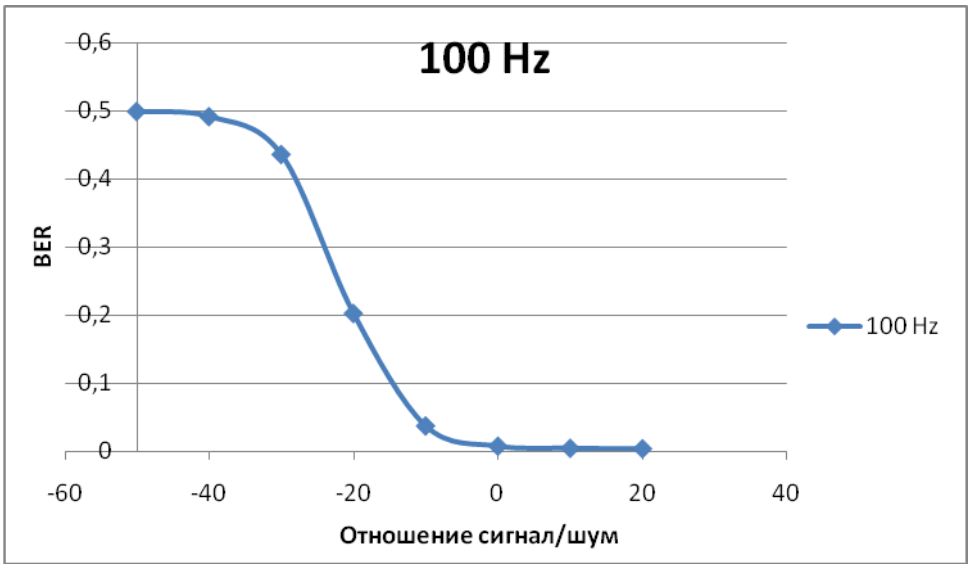


Рис. 3.13. Зависимость BER от отношения сигнал/шум при доплеровском сдвиге 100 Гц

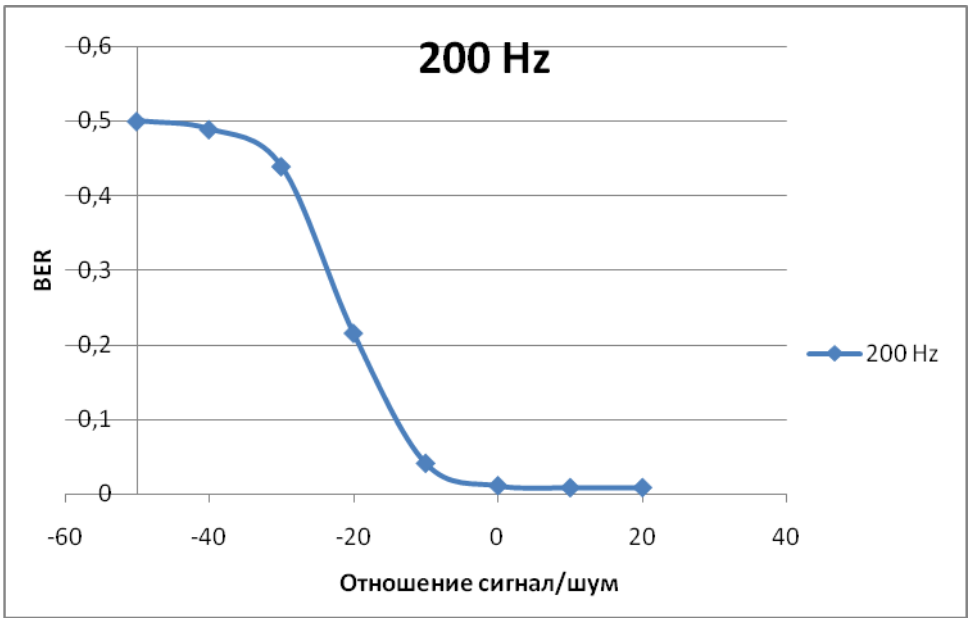


Рис. 3.14. Зависимость BER от отношения сигнал/шум при доплеровском сдвиге 200 Гц

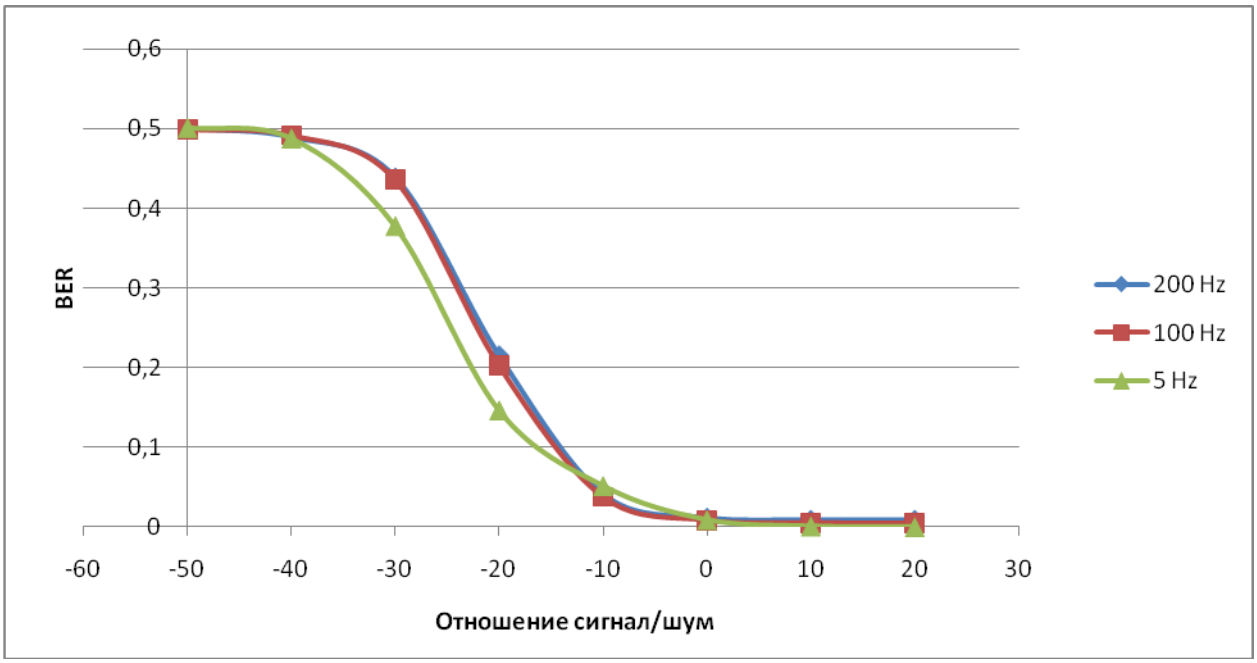


Рис. 3.15. Зависимость BER от отношения сигнал/шум при доплеровском сдвиге 5, 100, 200 Гц

В ходе данной работы мы исследовали стандарт GSM. Он позволяет производить эффективную передачу сигнала при довольном малом соотношении Сигнал Шум. Сигнал GSM зависим от Доплеровского эффекта, но учитывая, что скорость ЭМ волн крайне большая, по сравнению со скоростью обьектов связи, то этот эффект нормализуется.

3.2. Проектирование защтщенной системы мобильной связи стандарта CDMA [17-20]

В настоящее время развиваются системы мобильной связи, так как каждый год осуществляется рост числа абонентов, что приводит к загруженности сети, необходимости улучшения качества связи, улучшения емкости базовых станций, а также увеличения зоны покрытия сот. Но необходимо улучшать и безопасность мобильной связи, так как злоумышленники могут осуществить перехват информационного сигнала.

Новые поколения сотовой связи появляются достаточно быстро, но их внедрение требует значительных временных ресурсов, поэтому до сих пор основополагающими считаются технологии CDMA и GSM, но технология CDMA работает не только как отдельный стандарт, эта технология используется, например, в LTE.

CDMA - система множественного доступа с кодовым разделением - стала, возможно, самой многообещающей системой, появившейся на мировом рынке. Десятилетия назад эта технология использовалась в военной связи (США), а сегодня известна всем как глобальный цифровой стандарт для коммерческих систем коммуникаций. Технология использования CDMA была протестирована, стандартизирована, лицензирована и запущена в производство большинством поставщиков беспроводного оборудования и применяется во всем мире. В отличие от других методов доступа абонентов к сети, где энергия сигнала концентрируется на выбранных частотах или временных интервалах, сигналы CDMA распределены в непрерывном частотно-временном пространстве. Фактически метод манипулирует и частотой, и временем, и энергией.

CDMA применяется в 32 странах Азии и Океании, 2 странах Северной Америки, 14 странах Европы и 45 странах Африки.

История технологии CDMA берёт своё начало в 30-е годы прошлого (XX) столетия. В 1935 году в СССР академик Агеев Дмитрий Васильевич издал небольшим тиражом брошюру под странным названием "Кодовое разделение каналов". В ней были определены основы ортогонального разделения сигналов, разделения сигналов по форме. В то время реально существовал только один способ разделения каналов связи – частотный. И относилось это, в основном, к каналам радиосвязи. При таком методе каждый канал занимает некоторую свою полосу в общем спектре частот. Эти полосы относительно узки и разделены между собой защитными интервалами. Частотный диапазон ещё не был так перегружен как сегодня, поэтому использование такого способа разделения каналов связи считалось достаточно простым и логичным, поскольку осуществлялась манипуляция только одним параметром сигнала – частотой. Однако учёные, работавшие в области разработок новейших систем

связи, в общем, и радиосвязи, в частности, понимали, что такая идиллия не будет долгой. Кроме того, узкополосные радиосигналы очень чувствительны к селективным замираниям. Требовалось разработать методику, минимизирующую потери полезного сигнала за счёт селективных замираний и позволяющую бережнее относится к используемому диапазону частот.

Несколько позже, примерно в одно и то же время, появляются работы «Математическая теория связи» Клода Шеннона (США) и «Теория потенциальной помехоустойчивости» Владимира Александровича Котельникова (СССР).

Впервые радиооборудование, использующее кодовое разделение каналов, появилось в США где-то в конце 50-х годов. Технология CDMA нашла применение в военных системах, где успешно отработала более двух десятков лет. Во второй половине 80-х годов военное ведомство США рассекретило данную технологию и разрешило ее использование в гражданских средствах радиосвязи (диапазон 800 МГц).

В сентябре 1995 года в Гонконге фирма HUTCHISON начала развертывание первой в мире коммерческой сети CDMA, используя базовое оборудование Motorola (базовые станции SC 9600 и коммутирующее оборудование EMX 2500) и мобильные телефоны Qualcomm. На конец 1996 года эта сеть насчитывала 113 сот, работала на одном частотном канале с полосой 1,25 МГц и обслуживала более 40.000 абонентов. Правда, соты CDMA были наложены на существующую сеть AMPS и мобильные терминалы работали в дуалмодовом режиме, т.е. при сбое в CDMA-сети абонентский терминал автоматически переключался в сеть AMPS (FDMA). В Корее в январе 1996 года фирма KMT, используя оборудование Gold Star, начала коммерческую эксплуатацию CDMA-сети. А в апреле Shinsengi Telecom начала создавать новую сеть на базе оборудования Samsung, Sony, Qualcomm. На конец 1996 года эти сети обслуживали более 200.000 клиентов. Корея приняла IS-95 в качестве национального стандарта сотовой связи. В США развертыванием CDMA-сетей занимаются такие фирмы, как Air Touch (Сан-Диего, Лос-Анджелес), BANM (Трентон, Нью-Джерси), 360-Communications (Лас-Вегас, Невада). Они используют базовое оборудование Qualcomm, Lucent Technologies, Motorola, а также абонентские терминалы фирм Qualcomm, Sony, Nortel. В Австралии, в канун Олимпийских игр, были построены сети сотовой мобильной радиотелефонной связи в Сиднее и Мельбурне на базе оборудования CDMA-one (IS-95) производства фирмы Samsung.

Кроме вышеназванного стандарта (IS-95) в 1999 году был разработан и широкополосный вариант - W-CDMA (Ericsson, Швеция), функционирующий в диапазоне 1800 МГц. Он предназначался для использования в районах с высокой плотностью населения, так как обладал ещё большей пропускной способностью.

Стандарты CDMA

В CDMA системах каждый голосовой поток отмечен своим уникальным кодом и передается на одном канале одновременно со многими другими кодированными голосовыми потоками. Принимающая сторона использует тот же код для выделения сигнала из шума. Единственное отличие между множественными голосовыми потоками это уникальный код. Канал, как правило, очень широк и каждый голосовой поток занимает целиком всю ширину диапазона. Эта система использует наборы каналов шириной 1.23МГц. Голос кодируется на скорости 8.55кбит/с, но определение голосовой активности и различные скорости кодирования могут урезать поток данных до 1200бит/с. В системах CDMA могут устанавливаться очень прочные и защищенные соединения, несмотря на экстремально низкую величину мощности сигнала, теоретически - сигнал может быть слабее, чем уровень шума

Стандарт CDMAOne

Стандарт cdmaOne, существует в вариациях IS-95a, IS-95b (cellular по американской терминологии, 800 МГц) и J-STD-008 (PCS, диапазон 1900). Аббревиатура IS (interim standard - временной стандарт) используется для учета в Ассоциации телекоммуникационной промышленности TIA (Telecommunications Industry Association). Как правило, в сетях cdmaOne используется IS-95a, он обеспечивают передачу сигнала со скоростью 9,6 кбит/с (с кодированием) и 14,4 кбит/с (без кодирования). Версия IS-95b основана на объединении нескольких каналов CDMA, организуемых в прямом направлении (от базовой станции к мобильной). Скорость может увеличиваться до 28,8 кбит/с (при объединении двух каналов по 14,4 кбит/с) или до 115,2 кбит/с (8 каналов по 14,4 кбит/с). Собственно, кроме IS-95 сети cdmaOne используют еще целый набор протоколов и стандартов, их список можно найти в любой достаточно глубокой статье по этой теме. Прямой и обратный каналы располагаются соответственно в диапазонах 869,040-893,970 и 824,040-848,860 МГц. Используются 64 кода Уолша и несущие в 1.25 МГц.

Стандарт WCDMA

WCDMA (Wideband Code Division Multiple Access - широкополосный CDMA) - технология радиоинтерфейса избранная большинством операторов сотовой связи Японии и (в январе 1988 года) институтом ETSI (European Telecommunications Standards Institute) для обеспечения широкополосного радиодоступа с целью поддержки услуг третьего поколения.

Технология оптимизирована для предоставления высокоскоростных мультимедийных услуг типа видео, доступа в Интернет и видеоконференций; обеспечивает скорости доступа вплоть до 2 Мбит/с на коротких расстояниях и 384 Кбит/с на больших с полной мобильностью. Такие величины скорости передачи данных требуют широкую полосу частот, посему ширина полосы WCDMA составляет5 Мгц. Технология может быть добавлена к существующим сетям GSM и PDC, что делает стандарт WCDMA наиболее перспективным с точки зрения использования сетевых ресурсов и глобальной совместимости.

WCDMA (широкополосный множественный доступ с кодовым разделением каналов) представляет собой технологию, использующую расширенную полосу пропускания и разновидность принципа DMA. Это технология мобильной радиосвязи третьего поколения, обеспечивающая значительно более высокие скорости передачи данных, чем стандарт GSM. WCDMA поддерживает передачу голоса, изображений, данных и видео в сетях мобильной связи на скорости до 2 Мбит/с (локальный доступ) или 384 кбит/с (глобальный доступ). WCDMA используется в основном в Европе при переходе от стандарта GSM к стандарту UMTS.

Стандарт CDMA2000

Стандарт cdma2000 является дальнейшим развитием стандарта 2 поколения cdmaOne. Дальнейшим развитием cdmaOne должен был стать IS-95c, и именно это обозначение очень часто используется производителями. Официальным обновлением стандарта, разработанным компанией Qualcomm и утвержденным ITU (Международный союз электросвязи, International Telecommunication Union), является cdma2000. В документах Lucent Technologies встречается обозначение IS-2000. Наконец, международный союз электросвязи (МСЭ) отобрал из десяти предложенных проектов пять радиоинтерфейсов третьего поколения IMT-2000 (International Mobile Telecommunications System - 2000 - Международная система мобильной связи - 2000), в их числе - IMT-MC (Multi Carrier), который представляет собой модификацию многочастотной системы cdma2000, в которой обеспечивается обратная совместимость с оборудованием стандарта cdmaOne (IS-95).

Еще один из пяти стандартов IMT-2000 - IMT-DS (Direct Spread) - построен на базе проектов W-CDMA и взят за основу европейской системы UMTS.

На начало 2003г. из 127 миллионов пользователей CDMA почти 15 миллионов использовали технологию cdma2000. В течение первых семи месяцев 2002 года, в Азии и Америке было запущено 11 сетей CDMA2000 и общее количество этих сетей составляло 18. Это - 99% рынка 3G, на IMT-MC приходилось 14.8 миллионов абонентов, на UMTS - 0.13

миллиона. Однако, стоит отметить, что реализованная фаза cdma2000 1X все же не является полноценным 3G, ибо не дотягивает до обязательных двух мегабит. Поэтому ее чаще называют 2.5G.

Изначально cdma2000 (IMT-MC) разделили на две фазы - 1X и 3X. Именно к первой фазе применяется название IS-95C. А вторую позже назвали 1X-EV (evolution), разделив ее на две фазы - cdma2000 1X EV-DO (data only) и cdma2000 1X EV-DV (data & voice).

И именно стандарт cdma2000 1X EV-DO подразумевается под 3G IMT-MC. Стандарт 1x-EV-DO был принят TIA в октябре 2000 года и предусматривает следующую схему функционирования: аппарат одновременно производит поиск сети 1x и 1xEV, передачу данных осуществляет с помощью 1xEV, голоса - с помощью 1x. Стандарт 1xEV-DV полностью соответствует всем требованиям 3G.

Следует отметить, что стандарты семейства cdma2000 не требуют организации отдельной полосы частот и в ходе их эволюционного развития от cdmaOne могут быть реализованы во всех частотных диапазонах, используемых системами сотовой подвижной связи (450, 700, 800, 900, 1700, 1800, 1900, 2100 МГц).

Структура и формирование сигналов

Схема кодирования в прямом канале (от базовой станции к абоненту).

Базовая скорость передачи данных в канале составляет 9,6 кбит/с, что достигается добавлением дополнительных корректирующих двоичных символов к цифровому потоку вокодера 8,55 кбит/с.

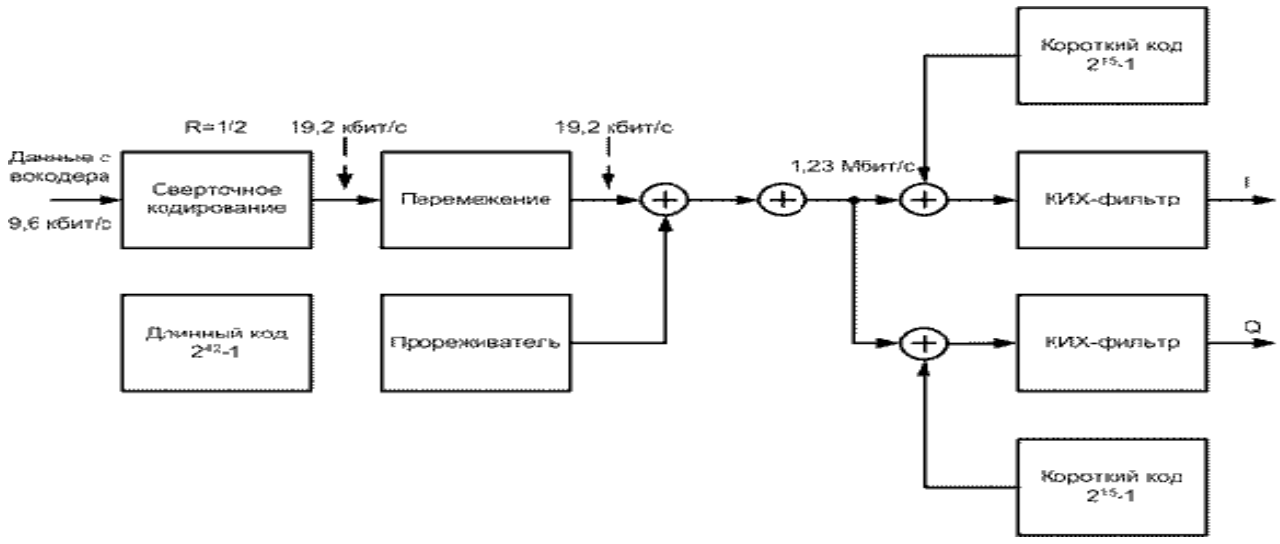


Рис. 3.16. Схема кодирования в прямом канале

Для реализации на приемной стороне прямой коррекции ошибок (без повторной передачи сообщения) в канале используется избыточное кодирование. Для этого базовый цифровой поток разбивается на пакеты длительностью по 20 мс и подается на сверточный кодер с половинной скоростью. На его выходе число битов удваивается. Затем данные перемежаются, т. е. перемешиваются во временном интервале 20 мс. Это делается для того, чтобы равномерно распределить в потоке данных (после обратного перемежения) потерянные во время передачи биты. Известно, что ошибочно принятые символы обычно формируют группы. В то же время, схема прямой коррекции ошибок работает наилучшим образом, когда ошибки распределены равномерно во времени. Это происходит после осуществления на приемной стороне процедуры, обратной перемежению при передаче. После перемежения цифровой поток преобразуется с помощью длинного кода и логической операции "исключающее ИЛИ" (сложение по модулю два). По определению, длинными кодами (кодами максимальной длины - М-последовательностями) являются коды, которые могут быть получены с помощью регистра сдвига или элемента задержки заданной длины.

Максимальная длина двоичной последовательности, которая может быть получена с помощью генератора, построенного на основе регистра сдвига, равна 2^n-1 двоичных символов, где n - число разрядов регистра сдвига. В аппаратуре стандарта CDMA длинный код формируется в результате нескольких последовательных логических операций с псевдослучайной двоичной последовательностью, генерируемой в 42-разрядном регистре сдвига, и двоичной 32-битовой маской, которая определяется индивидуально для каждого абонента. Такой регистр сдвига применяется во всех базовых станциях этого стандарта для обеспечения режима синхронизации всей сети. Длина М-последовательности при этом составляет 4 398 046 511 103 бит и если ее элементы формируются с тактовой частотой, например, 450 МГц, то период повторения будет составлять 9773,44 с= 2 ч 43 мин. Это значит, что если даже удастся засинхронизировать приемник в случае несанкционированного перехвата, то чтобы определить структуру сигнала-носителя необходимо вести наблюдение в течение почти 3-х часов, а с применением индивидуальной 32-битовой маски 'подслушивание" практически исключено. Так как информационный поток имеет скорость 19,2 Кбит/с, то в прямом канале используется только каждый 64-й символ длинного кода. Следующий этап преобразования сообщения - кодирование с помощью кодов Уолша. Любая строка матрицы Уолша ортогональна другой строке. Матрица Уолша размером 2 имеет вид:

$$W_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Матрицы больших размеров образуются следующим образом:

$$W_{2N} = \begin{pmatrix} W_N & W_N \\ W_N & -W_N \end{pmatrix}$$

т.е., например,

$$W_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Можно показать, что строки матрицы Уолша ортогональны. Ортогональность строк x и y длиной N определяется следующим условием:

$$\sum_{i=1}^{N} x_i y_i = 0$$

По сути в этом случае вычисляется значение ВКФ двух различных строк при временном сдвиге равном нулю.

Один ряд матрицы Уолша ставится в соответствие каналу связи между абонентом и базовой станцией. Если на входе кодера "0", то посылается соответствующий ряд матрицы (код Уолша), если "1" - посылается последовательность, сформированная путем логического отрицания соответствующего ряда матрицы (кода Уолша). При точном совпадении начала пришедшей последовательности и имеющейся (строка матрицы W_{64}) наблюдаются пики корреляционной функции положительной и отрицательной полярностей - в зависимости от передаваемого бита. В случае обработки "чужого" сигнала на выходе в момент окончания сигнала не будет ничего, т.е. происходит разделение каналов при приеме абонентской станцией. Кодирование по Уолшу повышает скорость информационного потока с 19,2 Кбит/с до 1,2288 Мбит/с. Соответственно расширяется и спектр сигнала. На заключительном этапе двоичный поток разделяется между синфазным и квадратурным каналами (I- и Q-каналами) для последующей передачи с использованием квадратурной фазовой манипуляции (QPSK). До подачи на смесители цифровой поток в каждом из каналов преобразуется с помощью короткого кода и операции сложения по модулю два.

Короткий код представляет собой псевдослучайную двоичную последовательность длиной 32768 двоичных символов, генерируемую со скоростью 1,3288 Мбит/с. Эта

последовательность является общей для всех базовых и подвижных станций в сети. Короткий код формируется в 15-разрядном регистре сдвига с линейной обратной связью. Результирующий двоичный поток в каждом канале проходит через цифровой фильтр с конечной импульсной характеристикой (КИХ-фильтр), что позволяет ограничить полосу излучаемого сигнала. Частота среза фильтра составляет около 615 кГц. Полученные аналоговые сигналы поступают на соответствующие входы I/Q-модулятора. Ряд информационных сигналов образуется путем слияния I- и Q-каналов.

Поскольку все пользователи получают объединенный сигнал, то для выделения информации необходимо передавать опорный сигнал по каналу, получившему название пилотного. В пилотном канале передается нулевой информационный сигнал, код Уолша для этого канала формируется из нулевого ряда матрицы Уолша (все единицы). Другими словами, в пилотном канале передается только короткий код. Обычно на нем излучается около 20% общей мощности. Опорный сигнал необходим для последующей фазовой демодуляции. Короткий код позволяет многократно использовать в каждой ячейке один и тот же набор кодов Уолша. Каждая базовая станция имеет свой временной сдвиг при формировании кода и поэтому может быть однозначно определена в сети. Основано это на уже описанном свойстве псевдослучайных двоичных последовательностей: значение АКФ близко к нулю для всех временных смещений более одной длины бита.

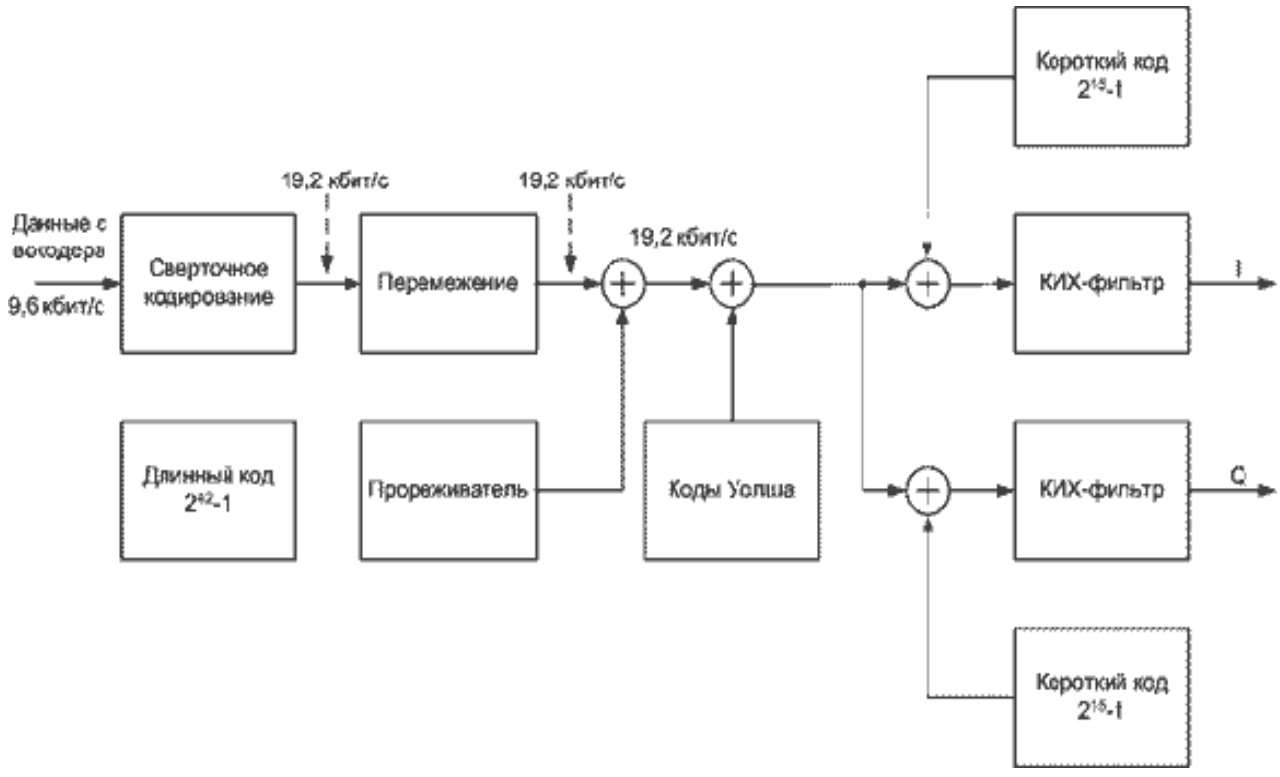


Рис. 3.17. Схема кодирования в обратном канале.

В обратном канале (от абонента к базовой станции) применяется другая схема кодирования. Подвижная станция не может использовать преимуществ трансляции опорного сигнала. В этом случае необходимо было бы передавать два сигнала, что значительно усложнило бы демодуляцию в приемнике базовой станции. В обратном канале применяется такой же, как и в прямом, вокодер и сверточное кодирование со скоростью 1/3, что повышает скорость передачи данных с базовой 9,6 до 28,8 кбит/с, и перемежение в пакете длительностью 20 мс. После перемежения выходной поток разбивается на слова по шесть битов в каждом. Шестибитовому слову можно поставить в соответствие один из 64 кодов Уолша. Таким образом, каждый абонентский терминал использует весь их набор. После этой операции скорость потока данных повышается до 307,2 Кбит/с. Далее поток преобразуется с помощью длинного кода, аналогичного используемому базовой станцией. На этом этапе происходит разделение пользователей. Абонентская емкость системы определяется обратным каналом. Для ее увеличения применяется регулирование мощности в обратном канале, методы пространственного разнесения приема на базовой станции и др. Окончательное формирование потоков данных происходит таким же образом, как и в базовой станции, за исключением дополнительного элемента задержки на 1/2 длительности символа в Q-канале для реализации, смещенной QPSK.

В системе CDMA применяются квадратурная фазовая манипуляция (QPSK) в базовой и смещенная QPSK в подвижных станциях. При этом информация извлекается путем анализа изменения фазы сигнала, поэтому фазовая стабильность системы - критичный фактор при обеспечении минимальной вероятности появления ошибки в сообщениях. Применение смещенной QPSK позволяет снизить требования к линейности усилителя мощности подвижной станции, так как амплитуда выходного сигнала при этом виде модуляции изменяется значительно меньше. До того, как интерференционные помехи будут подавлены методами цифровой обработки сигналов, они должны пройти через высокочастотный тракт приемника и не вызвать насыщения малошумящего широкополосного усилителя (МШУ) и смесителя. Это заставляет разработчиков системы искать баланс между динамическими и шумовыми характеристиками приемника.

Рис. 3.18. Структурная схема CDMA

Моделирование CDMA2000 1xRTT

Модель состоит из трех основных блоков:

1. Базовая станция (передатчик);
2. Канал;
3. Мобильная станция (приемник).

Канал имеет три режима работы:

1. Нет канала;
2. Канал с шумами;

Канал с многолучевым распространением.

Мобильный приемник состоит из декодера и приемника, которые выполняют все операции необходимые декодирования сигнала [25].

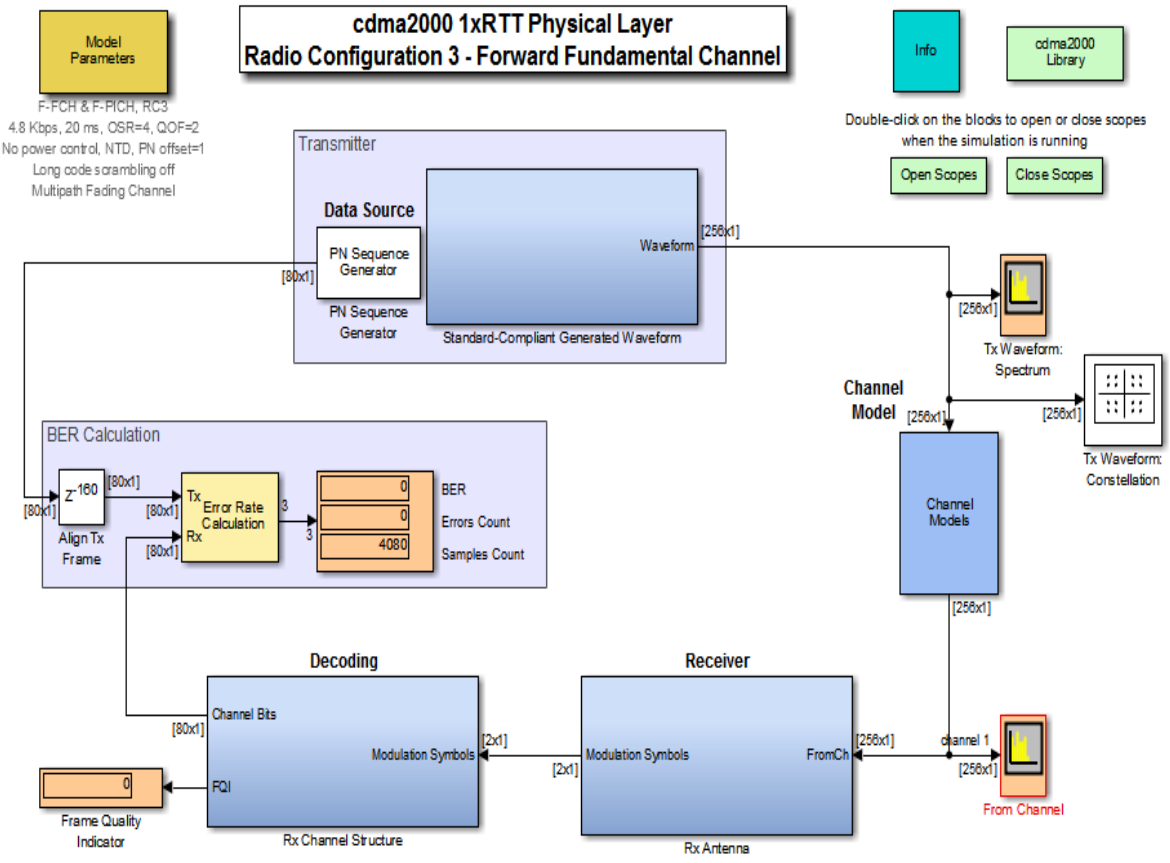


Рис.3.19. Модель CDMA2000 1xRTT в MATLAB R2015b

Развернутая модель передатчика представлена на рисунке 5.20.

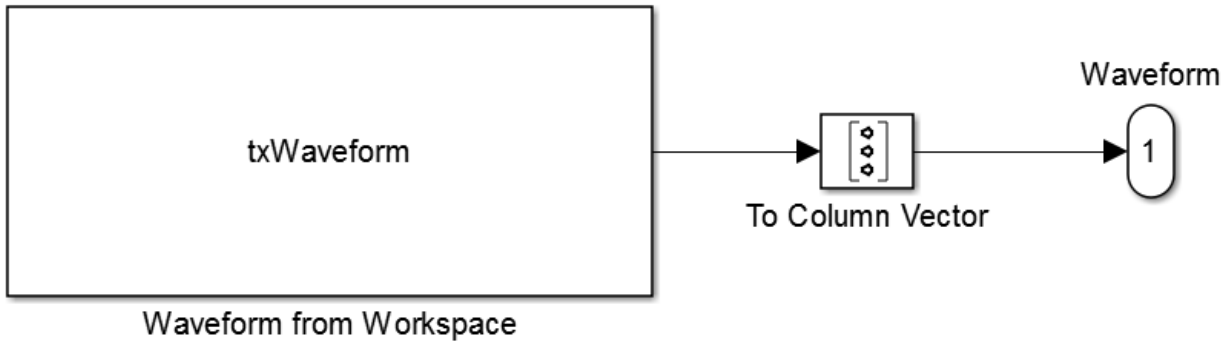


Рис. 3.20. Модель передатчика

Блок txWaveform содержит в себе длинный программный код посредством которого и генерируется сигнал, далее этот сигнал формируется в вектор с помощью блока To Column Vector. Этот вектор передается по каналу и затем поступает в приемник. Развернутая модель приемника представлена на рисунке 5.21.

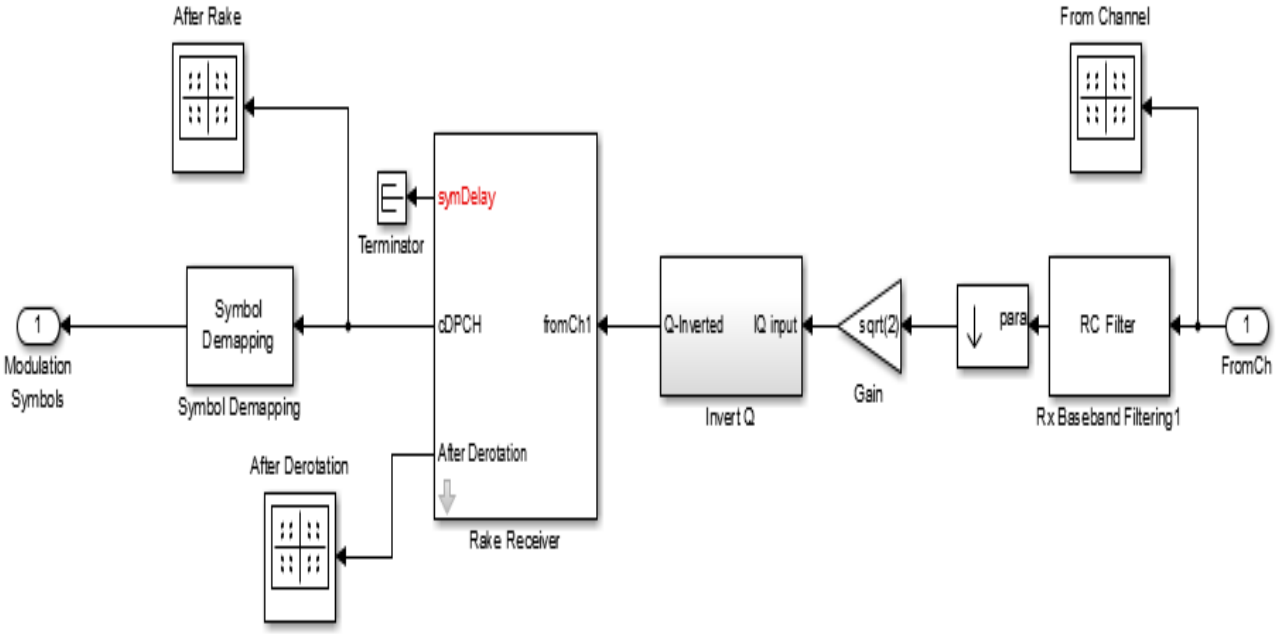


Рис. 3.21. Модель приемника.

Принятый сигнал поступает на фильтр RC Filter, АЧХ которого представлена на рисунке 6, и затем усиливается с помощью блока Gain в корень из двух раз, после чего сигнал поступает в блок Invert Q, который разделяет его на реальную и мнимую части, умножает мнимую часть на -1 и затем объединяет реальную и мнимую части обратно. Далее восстанавливается созвездие с помощью блока Rake Reciever, после чего сигнал поступает в блок Symbol Demapping для демодуляции. Полученные символы модуляции поступают на декодер, развернутая модель которого представлена на рисунке 5.22.

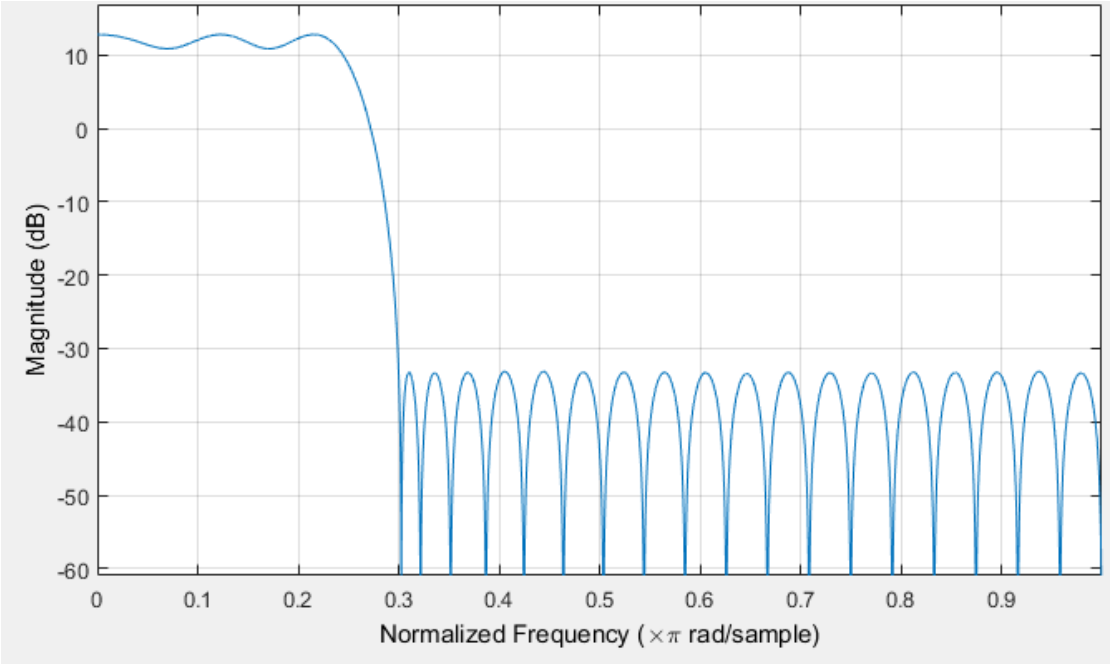


Рис. 3.22. АЧХ фильтра приемника

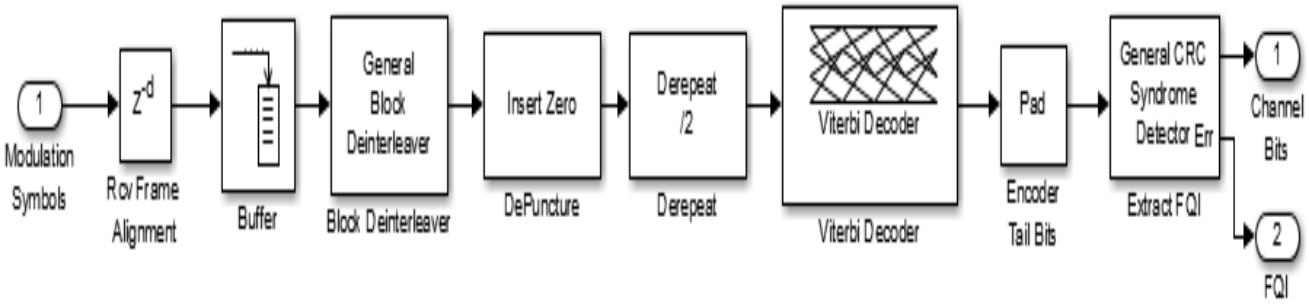


Рис. 3.23. Модель декодера.

Полученные символы модуляции поступают в блок Rcv Frame Alignment, который представляет собой задержку на 768 тактов, далее символы поступают в блок Buffer для накопления 768 символов. Накопленные символы поступают в блок Block Deinterleaver для обратного перемежения, далее данные поступают в блок Insert Zero, который возвращает последовательности нулей, замененных на специальные символы, далее данные поступают в блок Derepeat, обратное преобразование кодов с повторением с коэффициентом повторения 2, далее данные поступают на декодер Витерби и наконец в блок Encoder Tail Bits, который добавляет нули или урезает число бит если оно не равно 80.

Параметры модели

Модель позволяет изменять такие настройки как скорость потока и вид канала. В зависимости от вида канала можно задавать значение отношения сигнал/шум, а также параметры многолучевого распространения сигнала: максимальное Доплеровское отклонение частоты, вектор задержки и вектор ослабления/усиления. Длины векторов определяют количество лучей в канале.

Результаты моделирования

Компонент расчета BER сравнивает декодированный сигнал и сигнал, сгенерированный базовой станцией. Если BER равен нулю, то сигнал не подвергся каким-либо изменениям либо ошибки удалось исправить. Сигнал с базовой станции перед попаданием в блок расчета BER проходит через задержку для того что бы выровнять фреймы.

Для того что бы отобразить все возможные графики необходимо два раза кликнуть по кнопке Open Scopes в правом верхнем углу. В результате чего отобразятся следующие графики:

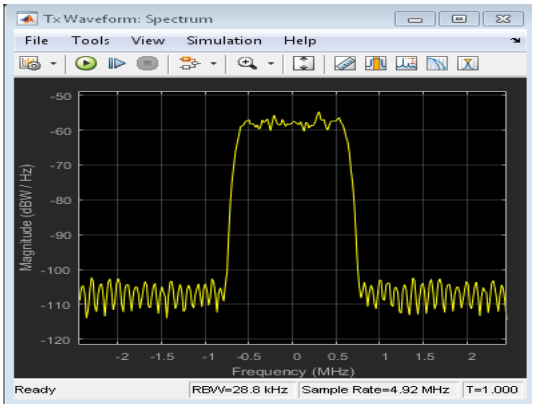


Рис. 3.24. Спектр сигнала сгенерированного базовой станцией.

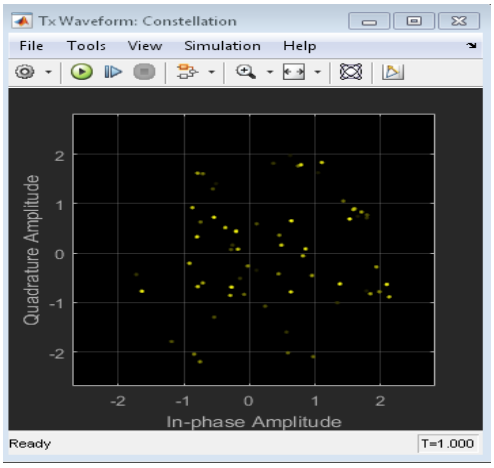


Рис. 3.25. Сгенерированный базовой станцией сигнал на I-Q диаграмме

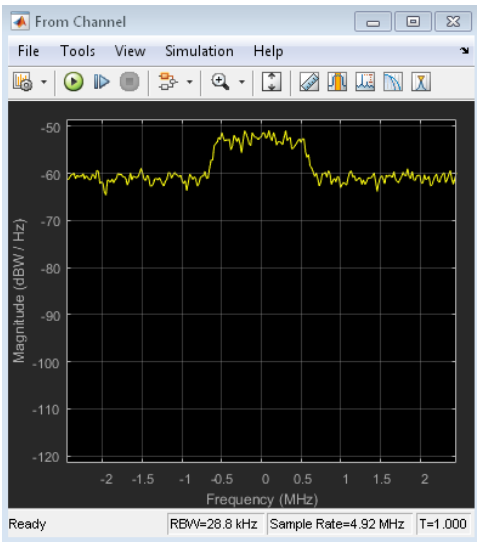


Рис. 3.26. Спектр принимаемого мобильной станцией сигнала после прохождения через канал.

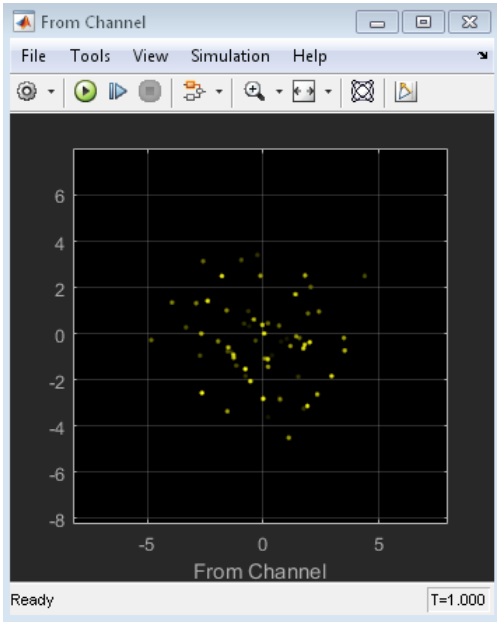


Рис. 3.27. Сигнал принимаемый мобильной станцией после прохождения через канал на I-Q диаграмме.

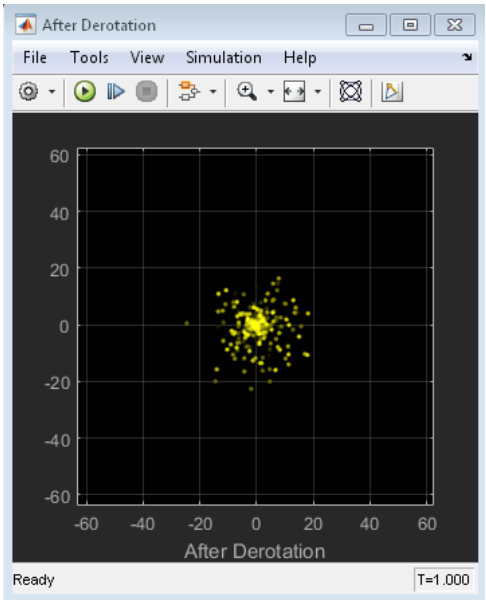


Рис. 3.28. Сигнал, принятый мобильной станцией

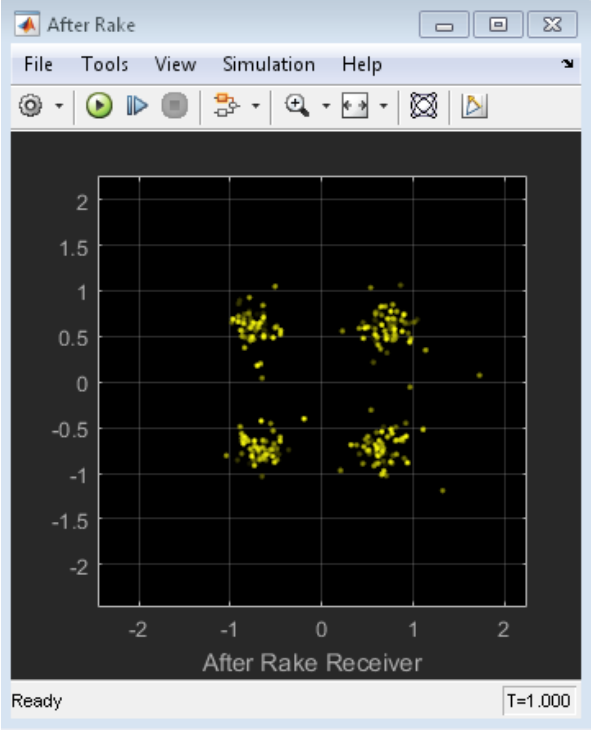


Рис. 3.29. Сигнал, декодированный мобильной станцией, на I-Q диаграмме.

Исследование модели

В блоке Model Parameters во вкладке Channel Settings выберем Channel Model: No Channel.

Результат моделирования:

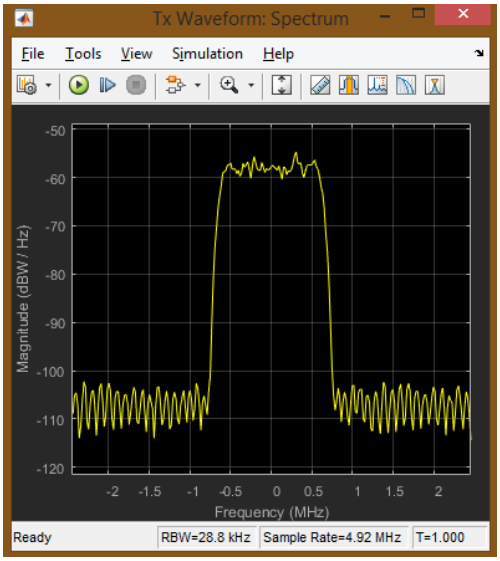


Рис. 3.30. Спектр сигнала сгенерированного базовой станцией

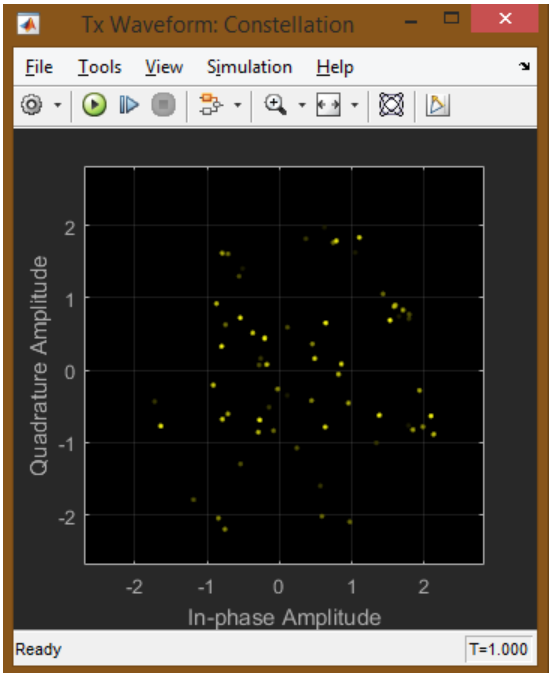


Рис. 3.31. Сгенерированный базовой станцией сигнал на I-Q диаграмме.

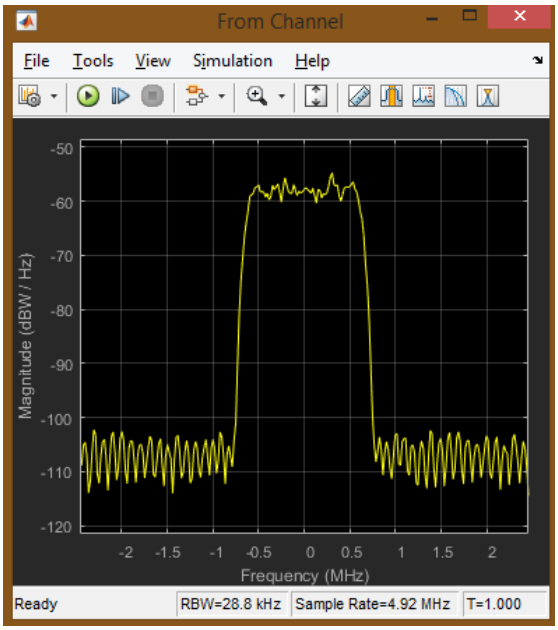


Рис. 3.32. Спектр сигнала после канала

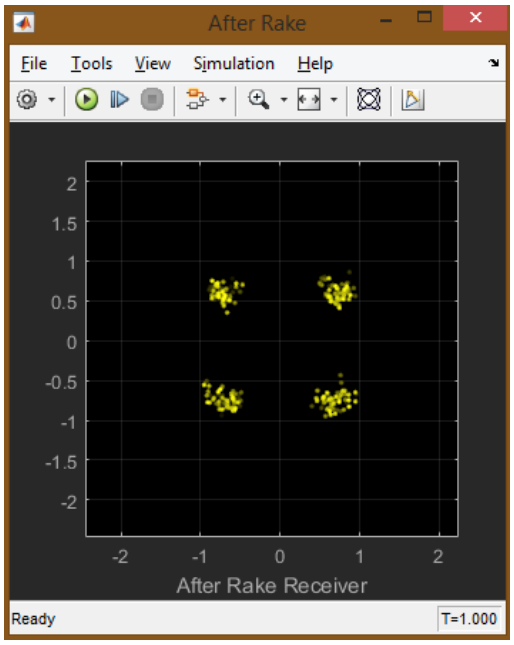


Рис. 3.33. Сигнал, декодированный мобильной станцией, на I-Q диаграмме

Видно, что спектр сигнала не изменился, так как в канале не было потерь. По результатам моделирования BER равен нулю.

В блоке Model Parameters во вкладке Channel Settings выберем Channel Model: AWGN Channel.

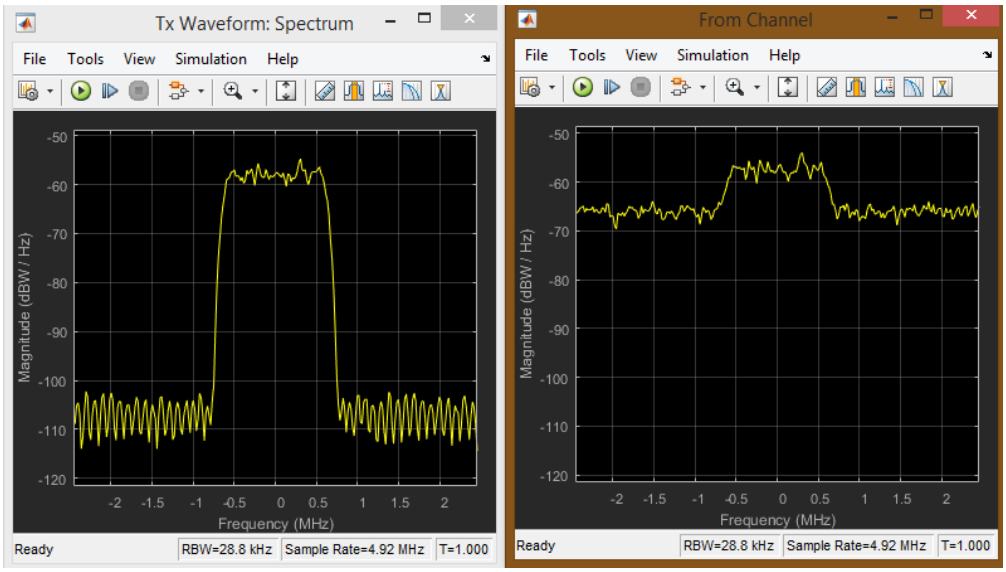


Рис. 3.34. Спектр сигнала до и после канала при отношении сигнал/шум 5 дБ

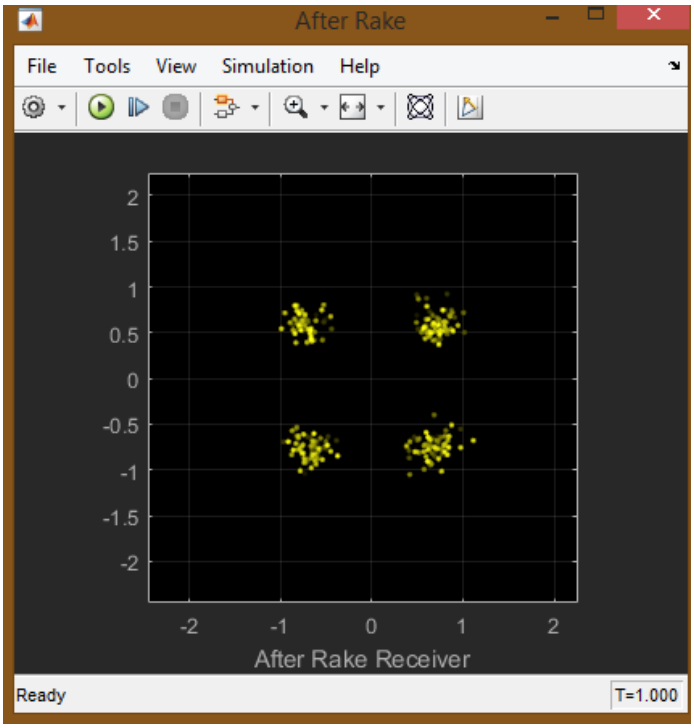


Рис. 3.35. Сигнал, декодированный мобильной станцией, на I-Q диаграмме.

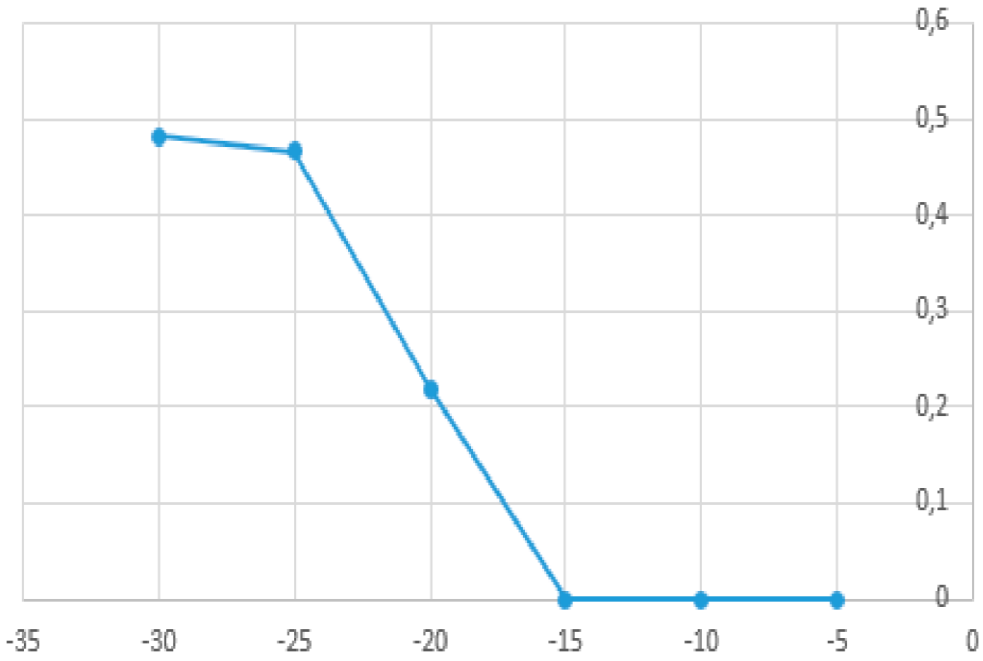


Рис. 3.36. Зависимость BER от SNR в канале с шумами.

Таблица 3.1. Зависимость BER от SNR в канале с шумами.

SNR	-30	-25	-20	-15	-10	-5
BER	0,4814	0,4662	0,2186	0	0	0

В блоке Model Parameters во вкладке Channel Settings выберем Channel Model: Multipath Fading Channel.

И установим следующие параметры

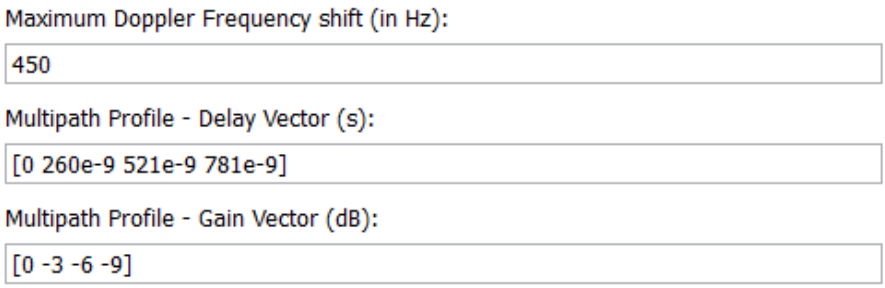


Рис. 3.37. Заданные параметры канала с многолучевым распространением.

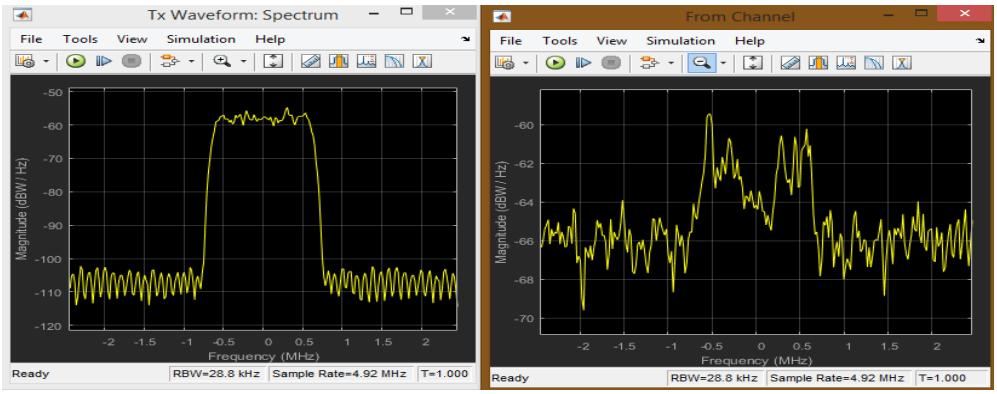


Рис. 3.38. Спектры сигнала до и после канала при отношении сигнал/шум 5 дБ.

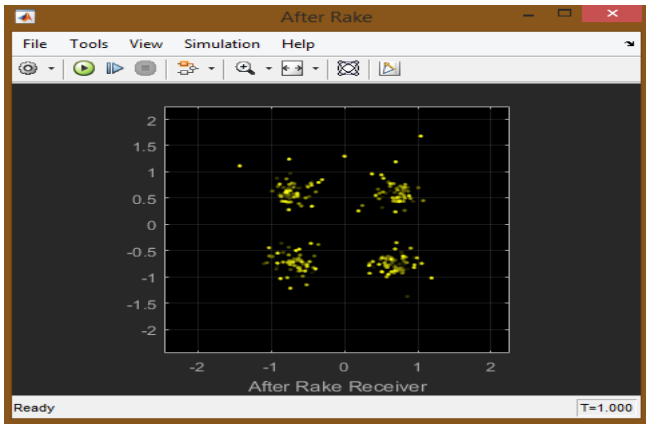


Рис. 3.39. Сигнал, декодированный мобильной станцией, на I-Q диаграмме.

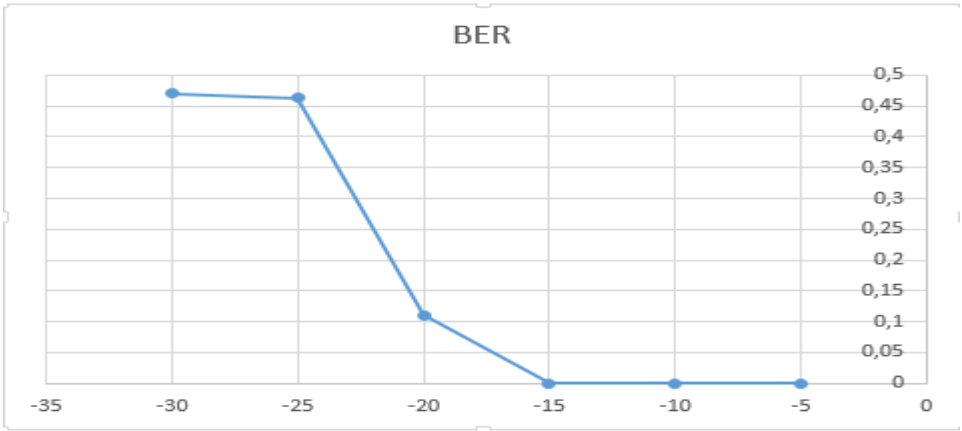


Рис. 3.40. Зависимость BER от SNR в канале с многолучевым распространением.

Таблица 3.2. Зависимость BER от SNR в канале с многолучевым распространением

SNR	-30	-25	-20	-15	-10	-5
BER	0,4708	0,4637	0,1105	0	0	0

В блоке Model Parameters во вкладк*е Channel Settings выберем Channel Model: Multipath Fading Channel.

И установим следующие параметры

Maximum Doppler Frequency shift (in Hz):

600

Multipath Profile - Delay Vector (s):

[0 280e-9 541e-9 801e-9]

Multipath Profile - Gain Vector (dB):

[0 -4 -7 -10]

Рис. 3.41. Заданные параметры канала с многолучевым распространением

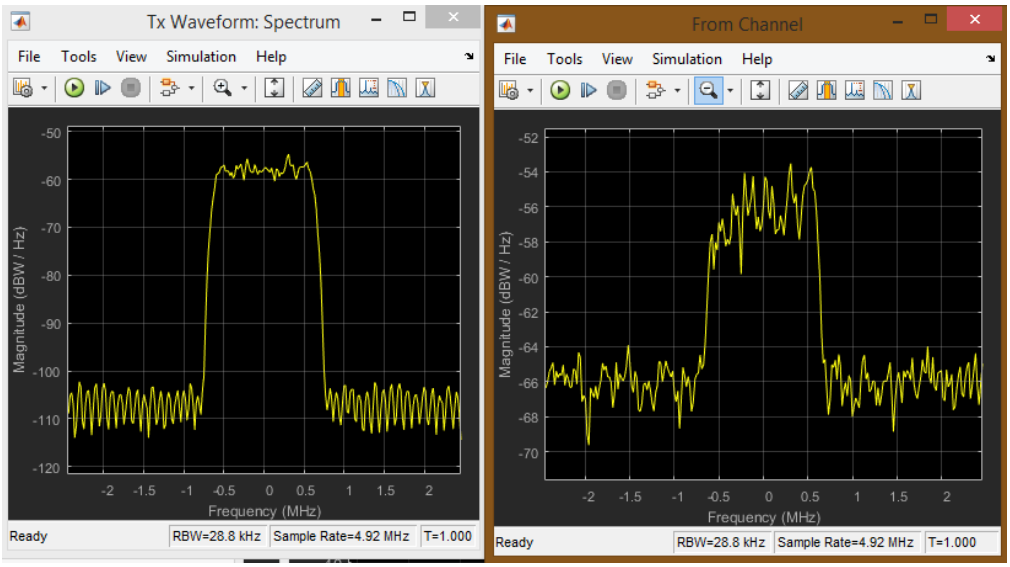


Рис. 3.42. Спектры сигнала до и после канала при отношении сигнал/шум 5 дБ

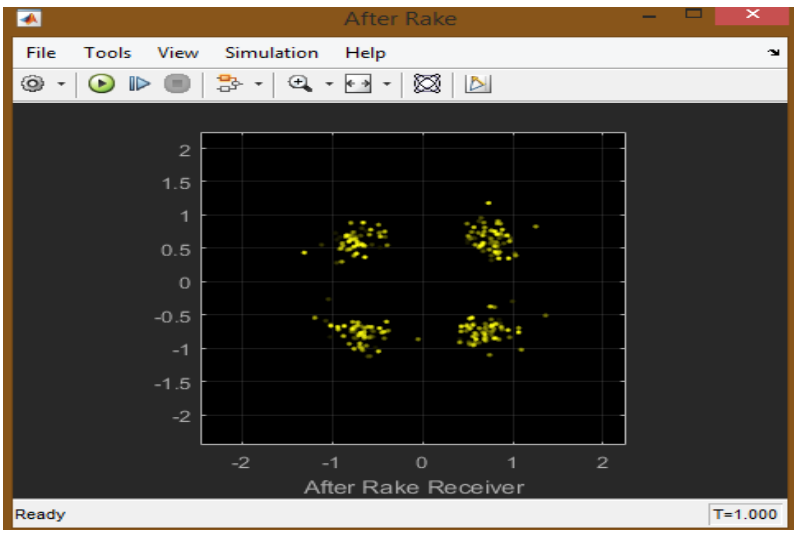


Рис. 3.43. Сигнал, декодированный мобильной станцией, на I-Q диаграмме

Таблица 3.3. Зависимость BER от SNR в канале с многолучевым распространением

SNR	-30	-25	-20	-15	-10	-5
BER	0,5007	0,4657	0,1532	0	0	0

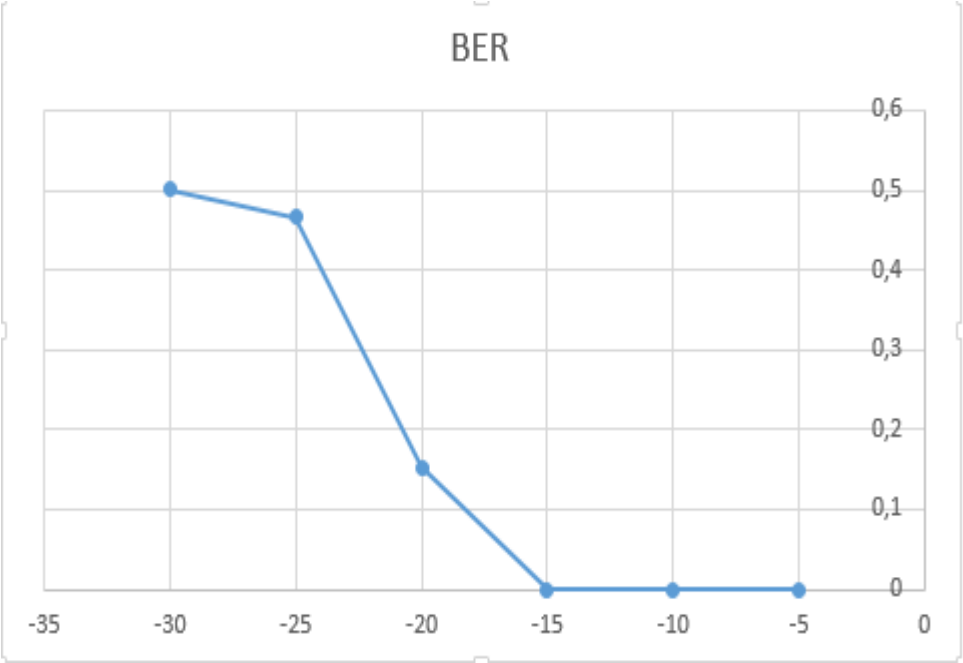


Рис. 3.44**.** Зависимость BER от SNR в канале с многолучевым распространением

Таким образом, в разделе было сделано:

1. Проведен аналитический обзор существующих методов и средств систем мобильной связи с кодовым разделением канала CDMA;
2. Разработана структурная схема DownLink канала CDMA2000 и приведена в приложении Б;
3. Приведена модель DownLink канала CDMA2000 реализованная в MATLAB R2015b;
4. Приведено исследование данной модели, а также методика проведения исследования, представленная в приложении А. Данную методику можно использовать для проведения учебных лабораторных работ.

На основе проведенного исследования можно сделать следующие выводы:

1. Система мобильной связи CDMA2000 обладает рядом преимуществ: возможность декодировать сигналы при отношении сигнал/шум меньше единицы, т.е. уровень передаваемого сигнала ниже уровня шума, что делает сигнал скрытным, а значит более защищенным.

2. Формируемый сигнал возможно принять и декодировать без ошибок даже при наличии многолучевости, однако при большом Доплеровском отклонении частоты и больших задержках, например, 1МГц и 1 мкс ошибки будут даже при высоком отношении сигнал/шум, например, 40 дБ. Но такие плохие характеристики канала довольно редки.

3. Для большей защищенности в аппаратуре стандарта CDMA длинный код формируется в результате нескольких последовательных логических операций с псевдослучайной двоичной последовательностью, генерируемой в 42-разрядном регистре сдвига, и двоичной 32-битовой маской, которая определяется индивидуально для каждого абонента. Такой регистр сдвига применяется во всех базовых станциях этого стандарта для обеспечения режима синхронизации всей сети. Длина М-последовательности при этом составляет 4 398 046 511 103 бит и если ее элементы формируются с тактовой частотой, например, 450 МГц, то период повторения будет составлять 9773,44 с= 2 ч 43 мин. Это значит, что если даже удастся засинхронизировать приемник в случае несанкционированного перехвата, то чтобы определить структуру сигнала-носителя необходимо вести наблюдение в течение почти 3-х часов, а с применением индивидуальной 32-битовой маски 'подслушивание" практически исключено.

Таблица 3.4. Характеристики CDMA2000

Характеристика	Значение
Базовая скорость передачи данных в канале	9.6 кбит/с
Длительность пакетов, на которые разбивается базовый поток	20 мс
Цифровая модуляция DownLink	QPSK
Цифровая модуляция UpLink	OQPSK
Размер матрицы Адамара	64x64
Разрядность регистра сдвига для формирования длинного кода	42
Длина М-последовательности длинного кода	4 398 046 511 103
Количество бит в индивидуальной	32

маске пользователя	
Разрядность регистра сдвига для формирования короткого кода	15
Длина М-последовательности короткого кода	32768
Частота среза КИХ-фильтра	615 кГц

Методика проведения измерений работы:

1. Запустить MATLAB R2015b от имени администратора;
2. В командной строке ввести команду «cdma2000SimulinkExample»;
3. Два раза кликнуть левой кнопкой мыши по блоку Model Parameters;
4. Во вкладке Channel Settings выбрать Channel Model: No Channel;
5. Два раза кликнуть левой кнопкой мыши по блоку Open Scopes;
6. Запустить моделирование;
7. После отображения всех графиков сохранить полученные данные и убедиться, что спектр сигнала, до и после канала, не изменился;
8. Не закрывая окна с графиками два раза кликнуть левой кнопкой мыши по блоку Model Parameters;
9. Во вкладке Channel Settings выбрать Channel Model: AWGN Channel и изменяя значение отношения сигнал/шум построить зависимость BER от SNR, и сохранить полученные диаграммы хотя бы для одного измерения;
10. Не закрывая окна с графиками два раза кликнуть левой кнопкой мыши по блоку Model Parameters;
11. Во вкладке Channel Settings выбрать Channel Model: Multipath Fading Channel и изменяя значение отношения сигнал/шум построить зависимость BER от SNR, и сохранить полученные диаграммы хотя бы для одного измерения;
12. Не закрывая окна с графиками два раза кликнуть левой кнопкой мыши по блоку Model Parameters;
13. Во вкладке Channel Settings изменить параметры доплеровского отклонения частоты (Maximum Doppler Frequency shift), вектора задержки (Multipath Profile – Delay Vector), вектора усиления (Multipath Profile – Gain Vector) и повторить пункт 11. Длины векторов задержки и усиления должны совпадать!

3.3. Проектирование защищенной системы мобильной связи стандарта IEEE 802.11 (WiFi) [25]

На современном этапе развития сетевых технологий, технология беспроводных сетей Wi-Fi является наиболее удобной в условиях, требующих мобильность, простоту установки и использования. Как правило, технология Wi-Fi используется для организации беспроводных локальных компьютерных сетей, а также создания так называемых горячих точек высокоскоростного доступа в Интернет.

Беспроводные сети обладают, по сравнению с традиционными проводными сетями, немалыми преимуществами, главным из которых, конечно же, является:

- Простота развёртывания;
- Гибкость архитектуры сети, когда обеспечивается возможность динамического изменения топологии сети при подключении, передвижении и отключении мобильных пользователей без значительных потерь времени;
- Быстрота проектирования и реализации, что критично при жестких требованиях к времени построения сети;

В то же время беспроводные сети на современном этапе их развития не лишены серьёзных недостатков. Прежде всего, это зависимость скорости соединения и радиуса действия от наличия преград и от расстояния между приёмником и передатчиком. Один из способов увеличения радиуса действия беспроводной сети заключается в создании распределённой сети на основе нескольких точек беспроводного доступа. При создании таких сетей появляется возможность превратить здание в единую беспроводную зону и увеличить скорость соединения вне зависимости от количества стен (преград). Аналогично решается и проблема масштабируемости сети, а использование внешних направленных антенн позволяет эффективно решать проблему препятствий, ограничивающих сигнал.

В соответствии с техническим заданием основными задачами данной работы являлись:

1. Аналитический обзор существующих методов и средств;
2. Разработка структурной схемы программного комплекса;
3. Разработка алгоритма программы;
4. Разработка программного интерфейса для исследования характеристик и визуализации основных преобразований;
5. Разработка методики и проведение исследования основных технических характеристик, анализ результатов исследования.

Полученная в результате разработка позволяет исследовать беспроводные сети на базе стандарта 802.11b.

История развития

В 1990 г. Комитет по стандартам IEEE 802 (Institute of Electrical and Electronic Engineers) сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11. Это группа занялась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2.4 ГГц со скоростями 1 и 2 Мбит/с. Работа по созданию стандарта были завершены через семь лет, и в июне 1997 г. была ратифицирована первая спецификация 802.11 [1].

Стандарт IEEE 802.11 стал первым стандартом для продуктов WLAN от независимой международной организации. Однако к моменту выхода стандарта в свет первоначально заложенная в нем скорость передачи данных оказалась недостаточной. Это послужило причиной последующих доработок, поэтому сегодня можно говорить о группе стандартов.

Методы построения радиосигнала в WiFi-сетях

В настоящее время при разработке аппаратуры для беспроводных сетей используются два метода построения сигнала:

1. С непосредственной модуляцией несущей частоты (Direct-Sequence Spread Spectrum – DSSS).

Информационный сигнал домножается на псевдослучайный код (Pncode – Pseudo Random Noise Code). Полученный результат используют для модуляции несущей. В приемнике полученный сигнал умножают на тот же код и выделяют полезный сигнал.

Основной проблемой, возникающей при использовании метода прямой последовательности, является эффект близко расположенного передатчика, т.е. уровень сигнала мешающего передатчика гораздо выше уровня нужного передатчика, что может привести к потери связи.

2. Со скачкообразной перестройкой частоты (Frequency-Hopping Spread Spectrum – FHSS).

Частота несущей изменяется согласно уникальной последовательности. Для реализации этого метода необходим скоростной синтезатор частот.

Недостаток: сложность получения высокого значения базы сигнала, что необходимо для увеличения числа пользователей, помехоустойчивости, повышения конфиденциальности.

Достоинство: меньшая подверженность эффекту близкого передатчика.

Оба метода основаны на принципе приемопередачи с «расширенным спектром», который обеспечивает защиту от помех и конфиденциальность передаваемой информации. Обычно при выборе сетевого продукта учитывают следующие факторы: скорость передачи данных, дальность устойчивой связи, соответствие стандартам, эксплуатационные характеристики и стоимость. Выбор типа аппаратуры для беспроводной сети определяется как условиями

эксплуатации, так и стоимостью изделия. Следует отметить, что устройства, работающие по методу FHSS, можно получить миниатюрный и недорогой адаптер для портативного ПК [2].

Описание стандарта

Из всех существующих стандартов беспроводной передачи данных IEEE 802.11 на практике чаще всего используются всего три стандарта, определенные Инженерным институтом электротехники и радиоэлектроники (IEEE): 802.11b, 802.11a и 802.11g.

В стандарте IEEE 802.11b благодаря высокой скорости передачи данных (до 11 Мбит/с), практически эквивалентной пропускной способности обычных проводных локальных сетей Ethernet, а также ориентации на диапазон 2,4 ГГц, этот стандарт завоевал наибольшую популярность у производителей оборудования для беспроводных сетей.

Поскольку оборудование, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, стандартом 802.11b предусмотрено автоматическое снижение скорости при ухудшении качества сигнала.

Стандарт IEEE 802.11a имеет большую ширину полосы из семейства стандартов 802.11 при скорости передачи данных до 54 Мбит/с.

В отличие от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями 802.11a предусмотрена работа в диапазоне 5 ГГц. В качестве метода модуляции сигнала выбрано ортогональное частотное мультиплексирование (OFDM).

К недостаткам 802.11a относятся более высокая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия.

Стандарт IEEE 802.11g является логическим развитием 802.11b и предполагает передачу данных в том же частотном диапазоне. Кроме того, стандарт 802.11g полностью совместим с 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с, поэтому на сегодня это наиболее перспективный стандарт беспроводной связи.

При разработке стандарта 802.11g рассматривались две отчасти конкурирующие технологии: метод ортогонального частотного разделения OFDM и метод двоичного пакетного сверточного кодирования PBCC, опционально реализованный в стандарте 802.11b. В результате стандарт 802.11g содержит компромиссное решение: в качестве базовых применяются технологии OFDM и CCK, а опционально предусмотрено использование технологии PBCC.

Физические уровни стандарта

Основное назначение физических уровней стандарта 802.11 - обеспечить механизмы беспроводной передачи для подуровня MAC, а также поддерживать выполнение вторичных функций, таких как оценка состояния беспроводной среды и сообщение о нем подуровню MAC. Уровни MAC и PHY разрабатывались так, чтобы они были независимыми. Именно независимость между MAC и подуровнем PHY и позволила использовать дополнительные высокоскоростные физические уровни, описанные в стандартах802.11b, 802.11a и 802.11g.

Каждый из физических уровней стандарта 802.11 имеет два подуровня:

- Physical Layer Convergence Procedure (PLCP). Процедура определения состояния физического уровня.
- Physical Medium Dependent (PMD). Подуровень физического уровня, зависящий от среды передачи.

На рис.1 показано, как эти подуровни соотносятся между собой и с вышестоящими уровнями в модели взаимодействия открытых систем (Open System Interconnection - OSI).

Подуровень PLCP по существу является уровнем обеспечения взаимодействия, на котором осуществляется перемещение элементов данных протокола MAC (MAC Protocol Data Units - MPDU) между MAC-станциями с использованием подуровня PMD, на котором реализуется тот или иной метод передачи и приема данных через беспроводную среду. Подуровни PLCP и PMD отличаются для разных вариантов стандарта 802.11.

Перед тем как приступить к изучению физических уровней, рассмотрим одну из составляющих физического уровня, до сих пор не упомянутую, а именно - скрэмблирование.

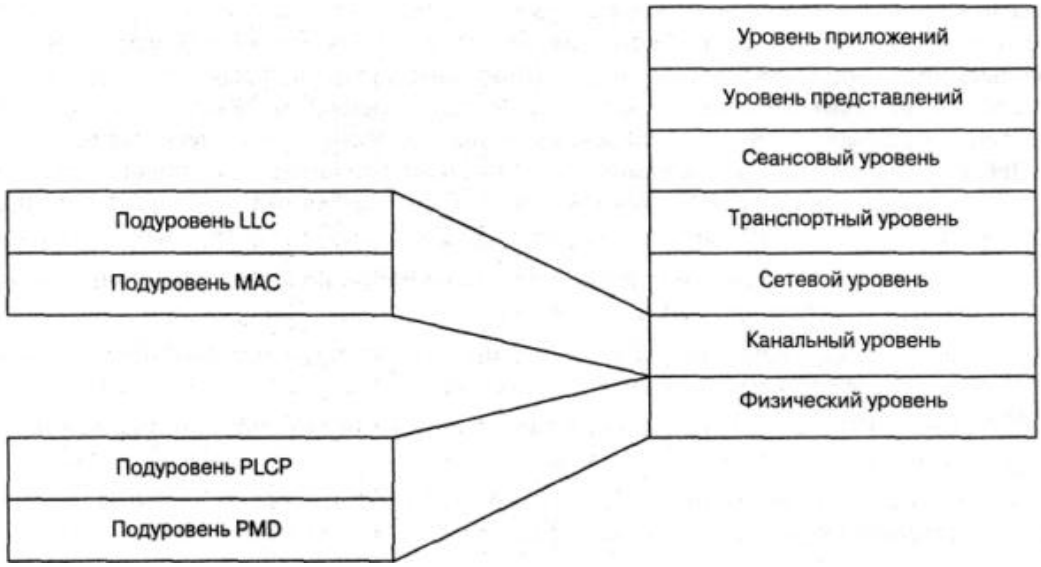


Рис. 3.45. Подуровни уровня PHY

Одна из особенностей, лежащих в основе современных передатчиков, благодаря которой данные можно передавать с высокой скоростью, - это предположение о том, что данные, которые предлагаются для передачи, поступают, с точки зрения передатчика, случайным образом. Без этого предположения многие преимущества, получаемые за счет применения остальных составляющих физического уровня, остались бы нереализованными.

Однако бывает, что принимаемые данные не вполне случайны и на самом деле могут содержать повторяющиеся наборы и длинные последовательности нулей и единиц.

Скрэмблирование (перестановка элементов) - это метод, посредством которого принимаемые данные делаются более похожими на случайные; достигается это путем перестановки битов последовательности таким образом, чтобы превратить ее из структурированной в похожую на случайную. Эту процедуру иногда называют "отбеливанием потока данных". Дескрэмблер приемника затем выполняет обратное преобразование этой случайной последовательности с целью получения исходной структурированной последовательности. Большинство способов скрэмблирования относится к числу самосинхронизирующихся; это означает, что дескрэмблер способен самостоятельно синхронизироваться со скрэмблером.

IEEE 802.11

Исходный стандарт 802.11 определяет три метода передачи на физическом уровне:

- Передача в диапазоне инфракрасных волн.
- Технология расширения спектра путем скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц.
- Технология широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.

Передача в диапазоне инфракрасных волн

Средой передачи являются инфракрасные волны диапазона 850 нм, которые генерируются либо полупроводниковым лазерным диодом, либо светодиодом (LED). Так как инфракрасные волны не проникают через стены, область покрытия LAN ограничивается зоной прямой видимости. Стандарт предусматривает три варианта распространения излучения: ненаправленную антенну, отражение от потолка и фокусное направленное излучение. В первом случае узкий луч рассеивается с помощью системы линз. Фокусное направленное излучение предназначено для организации двухточечной связи, например между двумя зданиями.

Беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS)

Беспроводные локальные сети FHSS поддерживают скорости передачи 1 и 2 Мбит/с. Устройства FHSS делят предназначенную для их работы полосу частот от 2,402 до 2,480 ГГц

на 79 неперекрывающихся каналов (это справедливо для Северной Америки и большей части Европы). Ширина каждого из 79 каналов составляет 1 МГц, поэтому беспроводные локальные сети FHSS используют относительно высокую скорость передачи символов - 1 МГц - и намного меньшую скорость перестройки с канала на канал.

Последовательность перестройки частоты должна иметь следующие параметры: частота перескоков не менее 2,5 раз в секунду как минимум между шестью (6 МГц) каналами. Чтобы минимизировать число коллизий между перекрывающимися зонами покрытия, возможные последовательности перескоков должны быть разбиты на три набора последовательностей, длина которых для Северной Америки и большей части Европы составляет 26. В таблице 1 представлены схемы скачкообразной перестройки частоты, обеспечивающие минимальное перекрытие.

По сути, схема скачкообразной перестройки частоты обеспечивает неторопливый переход с одного возможного канала на другой таким образом, что после каждого скачка покрывается полоса частот, равная как минимум 6 МГц, благодаря чему в многосотовых сетях минимизируется возможность возникновения коллизий.

Таблица 3.5 - Схема FHSS для Северной Америки и Европы

Набор	Схема скачкообразной перестройки частоты
1	{0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75}
2	{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76}
3	{2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,74,77}

После того как уровень MAC пропускает MAC-фрейм, который в локальных беспроводных сетях FHSS называется также служебным элементом данных PLCP, или PSDU (PLCP Service Data Unit), подуровень PLCP добавляет два поля в начало фрейма, чтобы сформировать таким образом фрейм PPDU (PPDU - элемент данных протокола PLCP). На рис.2 представлен формат фрейма FHSS подуровня PLCP.

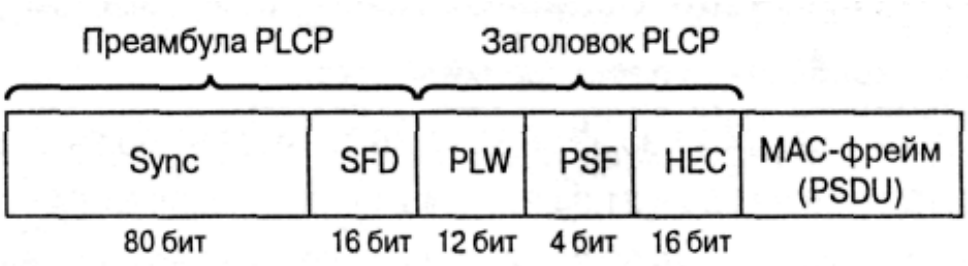


Рис. 3.46. Формат фрейма FHSS подуровня PLCP

Преамбула PLCP состоит из двух подполей:

- Подполе Sync размером 80 бит. Строка, состоящая из чередующихся 0 и 1, начинается с 0. Приемная станция использует это поле, чтобы принять решение о выборе антенны при наличии такой возможности, откорректировать уход частоты (frequency offset) и синхронизировать распределение пакетов (packet timing).
- Подполе флага начала фрейма (Start of Frame Delimiter, SFD) размером 16 бит. Состоит из специфической строки (0000 1100 1011 1101, крайний слева бит первый) в обеспечение синхронизации фреймов (frame timing) для приемной станции.

Заголовок фрейма PLCP состоит из трех подполей:

- Слово длины служебного элемента данных PLCP (PSDU), PSDU Length Word (PLW) размером 12 бит. Указывает размер фрейма MAC (PSDU) в октетах.
- Сигнальное поле PLCP (Signaling Field PLCP - PSF) размером 4 бит. Указывает скорость передачи данных конкретного фрейма.
- HEC (Header Error Check). Контрольная сумма фрейма.

Служебный элемент данных PLCP (PSDU) проходит через операцию скрэмблирования с целью отбеливания (рандомизации) последовательности входных битов. Получившийся в результате PSDU представлен на рис.3. Заполняющие символы вставляются между всеми 32-символьными блоками. Эти заполняющие символы устраняют любые систематические отклонения в данных, например, когда единиц больше, чем нулей, или наоборот, которые могли бы привести к нежелательным эффектам при дальнейшей обработке.

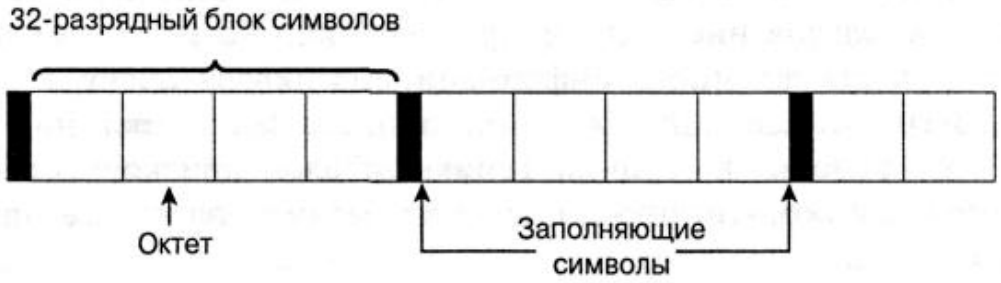


Рис. 3.47. Скрэмблированный PSDU в технологии FHSS

Подуровень PLCP преобразует фрейм в поток битов и передает его на подуровень PMD. Подуровень PMD технологии FHSS модулирует поток данных с использованием модуляции, основанной на гауссовой частотной модуляции (Gaussian Frequency Shift Keying - GFSK).

Беспроводные локальные сети, использующие широкополосную модуляцию DSSS с расширением спектра методом прямой последовательности

В спецификации стандарта 802.11 оговорено использование и другого физического уровня - на основе технологии широкополосной модуляции с расширением спектра методом

прямой последовательности (DSSS). Как было указано в стандарте 802.11 разработки 1997 года, технология DSSS поддерживает скорости передачи 1 и 2 Мбит/с.

Аналогично подуровню PLCP, используемому в технологии FHSS, подуровень PLCP технологии DSSS стандарта 802.11 добавляет два поля во фрейм MAC, чтобы сформировать PPDU: преамбулу PLCP и заголовок PLCP Формат фрейма представлен на рис.3.48.

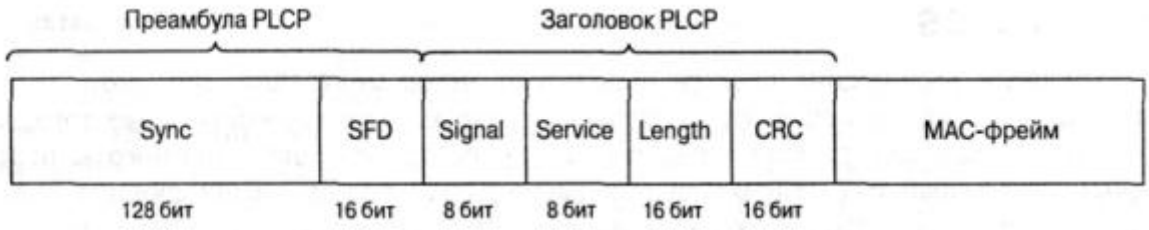


Рис. 3.48. Формат фрейма DSSS подуровня PLCP

Преамбула PLCP состоит из двух подполей:

- Подполе Sync шириной 128 бит, представляющее собой строку, состоящую из единиц. Задача этого подполя - обеспечить синхронизацию для приемной станции.
- Подполе SFD шириной 16 бит ; в нем содержится специфичная строка OxF3A0; его задача - обеспечить тайминг (timing) для приемной станции.

Заголовок PLCP состоит из четырех подполей:

- Подполе Signal шириной 8 бит, указывающее тип модуляции и скорость передачи для данного фрейма.
- Подполе Service шириной 8 бит зарезервировано. Это означает, что во время разработки спецификации стандарта оно осталось неопределенным; предполагается, что оно пригодится в будущих модификациях стандарта.
- Подполе Length шириной 16 бит, указывающее количество микросекунд (из диапазона 16-216), необходимое для передачи части MAC-фрейма.
- Подполе CRC. 16-битная контрольная сумма.

Подуровень PLCP преобразует фрейм в поток битов и передает данные на подуровень PMD. Весь PPDU проходит через процесс скрэмблирования с целью рандомизации данных.

Скрэмблированная преамбула PLCP всегда передается со скоростью 1 Мбит/с, в то время как скрэмблированный фрейм MPDU передается со скоростью, указанной в подполе Signal. Подуровень PMD модулирует отбеленный поток битов, используя следующиеметоды модуляции:

- Двоичная относительная фазовая модуляция (Differential Binary Phase Shift Keying - DBPSK) для скорости передачи 1 Мбит/с.

- Квадратурная относительная фазовая модуляция (Differential Quadrature Phase Shift Key - DQPSK) для скорости передачи 2 Мбит/с.

IEEE 802.11b

На физическом уровне к MAC-кадрам (MPDU) добавляется заголовок физического уровня, состоящий из преамбулы и собственно PLCP-заголовка (рис.5.5).

Преамбула содержит стартовую синхропоследовательность (SYNC) для настройки приемника и 16-битный код начала кадра (SFD) - число F3A016. PLCP-заголовок включает поля SIGNAL (информация о скорости и типе модуляции), SERVICE (дополнительная информация, в том числе о применении высокоскоростных расширений и PBCC-модуляции) и LENGTH (время в микросекундах, необходимое для передачи следующей за заголовком части кадра). Все три поля заголовка защищены 16-битной контрольной суммой CRC.

Рис. 3.49. Структура кадров сети IEEE 802.11b физического уровня

В стандарте IEEE 802.11b предусмотрено два типа заголовков: длинный и короткий (51).

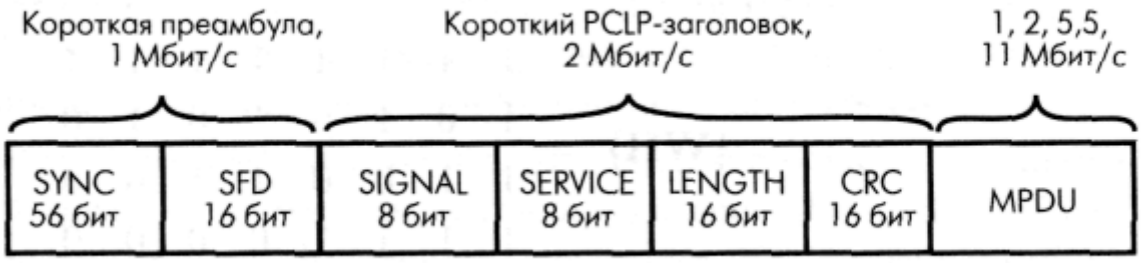


Рис. 3.50. Короткий заголовок кадров сети 802.11b

Они отличаются длиной синхропоследовательности (128 и 56 бит), способом ее генерации, а также тем, что символ начала кадра в коротком заголовке передается в обратном порядке. Кроме того, если все поля длинного заголовка передаются со скоростью 1 Мбит/с, то при коротком заголовке преамбула транслируется на скорости 1 Мбит/с, другие поля заголовка - со скоростью 2 Мбит/с. Остальную часть кадра можно передавать на любой

из допустимых стандартом скоростей передачи, указанных в полях SIGNAL и SERVICE. Короткие заголовки физического уровня предусмотрены спецификацией IEEE 802.11b для увеличения пропускной способности сети.

Из описания процедур связи сети IEEE 802.11 видно, что "накладные расходы" в этом стандарте выше, чем в проводной сети Ethernet. Поэтому крайне важно обеспечить высокую скорость передачи данных в канале. Повысить пропускную способность канала с заданной шириной полосы частот можно, разрабатывая и применяя новые методы модуляции. По этому пути пошла группа разработчиков IEEE 802.11b.

Напомним, что изначально стандарт IEEE 802.11 предусматривал работу в режиме DSSS с использованием так называемой Баркеровской последовательности (Barker) длиной 11 бит: B1 = (10110111000). Каждый информационный бит замещается своим произведением по модулю 2 (операция "исключающее ИЛИ") с данной последовательностью, т. е. каждая информационная единица заменяется на B1, каждый ноль - на инверсию B1. В результате бит заменяется последовательностью 11 чипов. Далее сигнал кодируется посредством дифференциальной двух- или четырехпозиционной фазовой модуляции (DBPSK или DQPSK, один или два чипа на символ соответственно). При частоте модуляции несущей 11 МГц общая скорость составляет в зависимости от типа модуляции 1 и 2 Мбит/с.

Стандарт IEEE 802.11b дополнительно предусматривает скорости передачи 11 и 5,5 Мбит/с. Для этого используется так называемая ССК-модуляция (Complementary Code Keying - кодирование комплементарным кодом).

Хотя механизм расширения спектра, используемый для получения скоростей 5,5 и 11 Мбит/с с применением ССК, относится к методам, которые применяются для скоростей 1 и 2 Мбит/с, он по-своему уникален. В обоих случаях применяется метод расширения, но при использовании модуляции ССК расширяющий код представляет собой код из 8 комплексных чипов, в то время как при работе со скоростями 1 и 2 Мбит/с применяется 11-разрядный код. 8-чиповый код определяется или 4, или 8 битами - в зависимости от скорости передачи данных. Скорость передачи чипов составляет 11 Мчип/с, т.е. при 8 комплексных чипах на символ и 4 или 8 битов на символ можно добиться скорости передачи данных 5,5 и 11 Мбит/с.

Для того чтобы передавать данные со скоростью 5,5 Мбит/с, нужно сгруппировать скрэмблированный поток битов в символы по 4 бита (b0, b1, b2 и b3). Последние два бита (b2 и b3) используются для определения 8 последовательностей комплексных чипов, как показано в таблице 6, где {cl, c2, c3, c4, c5, c6, c7, c8} представляют чипы

последовательности. В таблицн 6 j представляет мнимое число, корень квадратный из -1, и откладывается по мнимой, или квадратурной, оси комплексной плоскости.

Таблица 3.6. Последовательность чипов ССК

(b2, b3)	1	2	3	4	5	6	7	C8
00				1			1	1
01	j	1	j				j	1
10	j		j	1	j			1
11		1			j			1

Теперь, имея последовательность чипов, определенную битами (b2, b3), можно использовать первые два бита (b0, b1) для определения поворота фазы, осуществляемого при модуляции по методу DQPSK, который будет применен к последовательности (таблица 3). Вы должны также пронумеровать каждый 4-битовый символ PSDU, начиная с 0, чтобы можно было определить, преобразуете вы четный либо нечетный символ в соответствии с этой таблицей. Следует помнить, что речь идет об использовании DQPSK, а не QPSK, и поэтому представленные в таблице изменения фазы отсчитываются по отношению к предыдущему символу или, в случае первого символа PSDU, по отношению к последнему символу предыдущего DQPSK-символа, передаваемого со скоростью 2 Мбит/с.

Таблица 3.7. Поворот фазы при модуляции ССК

(b0,b1)	**Изменение фазы четных символов**	**Изменение фазы нечетных символов**
00	0	π
01	$\pi/2$	$-\pi/2$
11	π	0
10	$-\pi/2$	$\pi/2$

Это вращение фазы применяется по отношению к 8 комплексным чипам символа, затем осуществляется модуляция на подходящей несущей частоте.

Чтобы передавать данные со скоростью 11 Мбит/с, скрэмблированная последовательность битов PSDU разбивается на группы по 8 символов. Последние 6 битов выбирают одну последовательность, состоящую из 8 комплексных чипов, из числа 64 возможных последовательностей, почти так же, как использовались биты (b2, b3) для выбора одной из четырех возможных последовательностей. Биты (b0,b1) используются таким же образом, как при модуляции ССК на скорости 5,5 Мбит/с для вращения фазы последовательности и дальнейшей модуляции на подходящей несущей частоте.

В чем достоинство ССК-модуляции? Дело в том, что чипы символа определяются на основе последовательностей Уолша-Адамара. Последовательности Уолша-Адамара хорошо изучены, обладают отличными автокорреляционными свойствами. Что немаловажно, каждая такая последовательность мало коррелирует сама с собой при фазовом сдвиге - очень полезное свойство при борьбе с переотраженными сигналами. Нетрудно заметить, что теоретическое операционное усиление ССК-модуляции - 3 дБ (в два раза), поскольку без кодирования QPSK-модулированный с частотой 11 Мбит/с сигнал может транслировать 22 Мбит/с. Как видно, ССК-модуляция представляет собой вид блочного кода, а потому достаточно проста при аппаратной реализации. Совокупность этих свойств и обеспечила ССК место в стандарте IEEE 802.11b в качестве обязательного вида модуляции.

На практике важно не только операционное усиление. Существенную роль играет и равномерность распределения символов в фазовом пространстве - они должны как можно дальше отстоять друг от друга, чтобы минимизировать ошибки их детектирования. И с этой точки зрения ССК-модуляция не выглядит оптимальной, ее реальное операционное усиление не превышает 2 дБ. Поэтому изначально прорабатывался другой способ модуляции - пакетное бинарное сверточное кодирование PBCC (Packet BinaryConvolutional Coding). Этот метод вошел в стандарт IEEE 802.11b как дополнительная (необязательная) опция. Механизм PBCC (5.51) позволяет добиваться в сетях IEEE 802.11b пропускной способности 5,5, 11 и 22 Мбит/с.

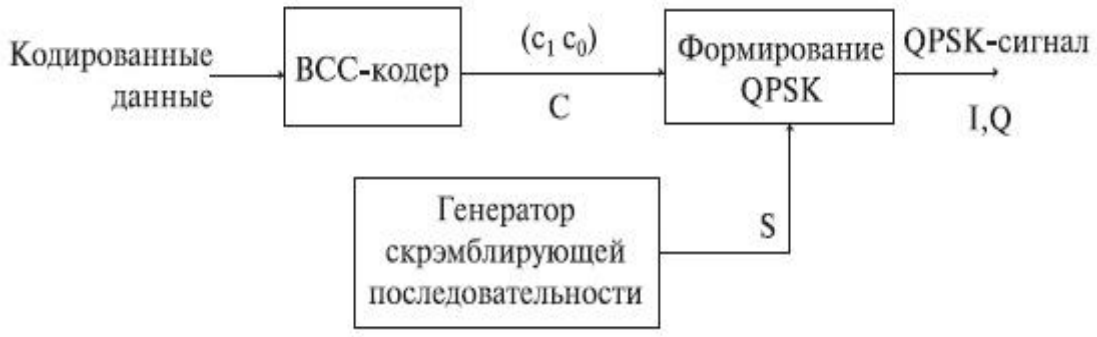


Рис. 3.51. Общая схема PBCC-модуляции

Как следует из названия, метод основан на сверточном кодировании. Для скоростей 5,5 и 11 Мбит/с поток информационных битов поступает в шестиразрядный сдвиговый регистр с сумматорами (5.52). В начальный момент времени все триггеры сдвигового регистра инициализируют нулем. В результате каждый исходный бит d заменяется двумя битами кодовой последовательности (c0, c1). При скорости 11 Мбит/с c0 и c1 задают один символ четырехпозиционной QPSK-модуляции. Для скорости 5,5 Мбит/с используют двухпозиционную BPSK-модуляцию, последовательно передавая кодовые биты c0 и c1. Если же нужна скорость 22 Мбит/с, схема кодирования усложняется (рис.5.9): три кодовых бита (c0-c2) определяют один символ в 8-позиционной 8-PSK-модуляции.

После формирования PSK-символов происходит скрэмблирование. В зависимости от сигнала s (5.51) символ остается без изменений (s = 0), либо его фаза увеличивается на $\pi/2$ (s = 1). Значение s определяет 256-битовая циклически повторяющаяся последовательность S. Она формируется на основе начального вектора U = 338Bh, в котором равное число нулей и единиц.

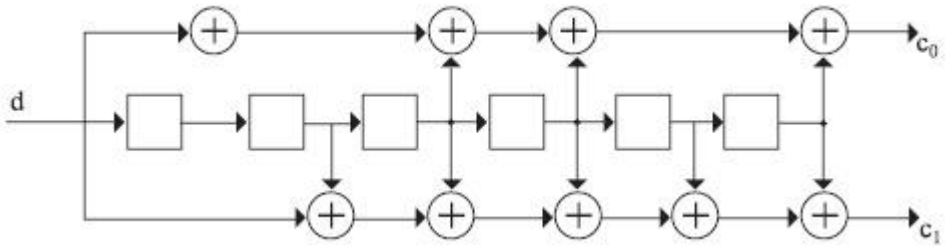


Рис. 3.52. Сверточное кодирование с двумя битами кодовой последовательности

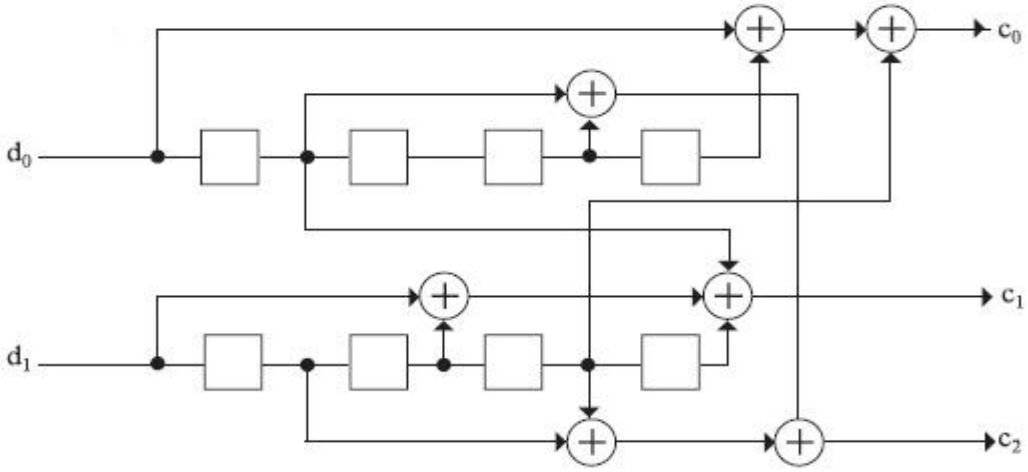


Рис. 3.53. Сверточное кодирование с тремя битами кодовой последовательности

У шестиразрядного сдвигового регистра, применяемого в PBCC для скоростей 11 и 5,5 Мбит/с, 64 возможных выходных состояния. Так что при модуляции PBCC информационные биты в фазовом пространстве оказываются гораздо дальше друг от друга, чем при CCK-модуляции. Поэтому PBCC и позволяет при одном и том же соотношении "сигнал-шум" и уровне ошибок вести передачу с большей скоростью, чем в случае CCK. Однако плата за более эффективное кодирование - сложность аппаратной реализации данного алгоритма.

IEEE 802.11a

Стандарт IEEE 802.11a появился практически одновременно с IEEE 802.11b, в сентябре 1999 года. Эта спецификация была ориентирована на работу в диапазоне 5 ГГц и основана на принципиально ином, чем описано выше, механизме кодирования данных - на частотном мультиплексировании посредством ортогональных несущих (OFDM).

Стандарт 802.11a определяет характеристики оборудования, применяемого в офисных или городских условиях, когда распространение сигнала происходит по многолучевым каналам из-за множества отражений.

В IEEE 802.11a каждый кадр передается посредством 52 ортогональных несущих, каждая с шириной полосы порядка 300 КГц (20 МГц/64). Ширина одного канала - 20 МГц. Несущие модулируют посредством BPSK, QPSK, а также 16- и 64-позиционной квадратурной амплитудной модуляции (QAM). В совокупности с различными скоростями кодирования (1/2 и 3/4, для 64-QAM - 2/3 и 3/4) образуется набор скоростей передачи 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с. В таблице 5.8показано, как необходимая скорость передачи данных преобразуется в соответствующие параметры узлов передатчика OFDM.

Таблица 5.8. Параметры передатчика стандарта 802.11a

Скорость передачи данных (Мбит/с)	**Модуляция**	**Скорость сверточного кодирования**	**Число канальных битов на поднесущую**	**Число канальных битов на символ**	**Число битов данных на символ OFDM**
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192

54	64-QAM	3/4	6	288	216

Из 52 несущих 48 предназначены для передачи информационных символов, остальные 4 - служебные. Структура заголовков физического уровня отличается от принятого в спецификации IEEE 802.11b, но незначительно (рис.3.54).

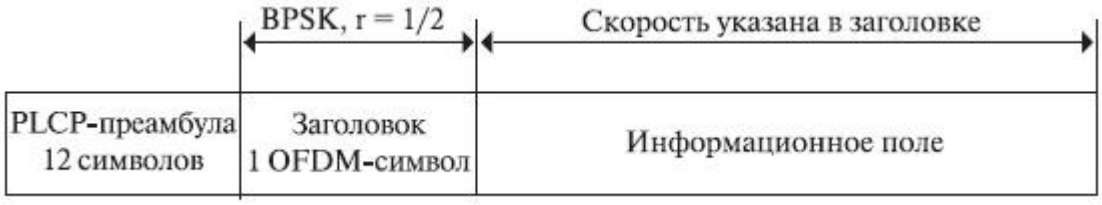


Рис. 3.54. Структура заголовка физического уровня стандарта IEEE 802.11a

Кадр включает преамбулу (12 символов синхропоследовательности), заголовок физического уровня (PLCP-заголовок) и собственно информационное поле, сформированное на MAC-уровне. В заголовке передается информация о скорости кодирования, типе модуляции и длине кадра. Преамбула и заголовок транслируются с минимально возможной скоростью (BPSK, скорость кодирования r = 1/2), а информационное поле - с указанной в заголовке, как правило, максимальной, скоростью, в зависимости от условий обмена. OFDM-символы передаются через каждые 4 мкс, причем каждому символу длительностью 3,2 мкс предшествует защитный интервал 0,8 мкс (повторяющаяся часть символа). Последний необходим для борьбы с многолучевым распространением сигнала - отраженный и пришедший с задержкой символ попадет в защитный интервал и не повредит следующий символ.

Естественно, формирование/декодирование OFDM-символов происходит посредством быстрого преобразования Фурье (обратного/прямого, ОБПФ/БПФ). Функциональная схема трактов приема/передачи (рис. 5.54) достаточно стандартна для данного метода и включает сверточный кодер, механизм перемежения/перераспределения (защита от пакетных ошибок) и процессор ОБПФ. Фурье-процессор, собственно, и формирует суммарный сигнал, после чего к символу добавляется защитный интервал, окончательно формируется OFDM-символ и посредством квадратурного модулятора/конвертера переносится в заданную частотную область. При приеме все происходит в обратном порядке.

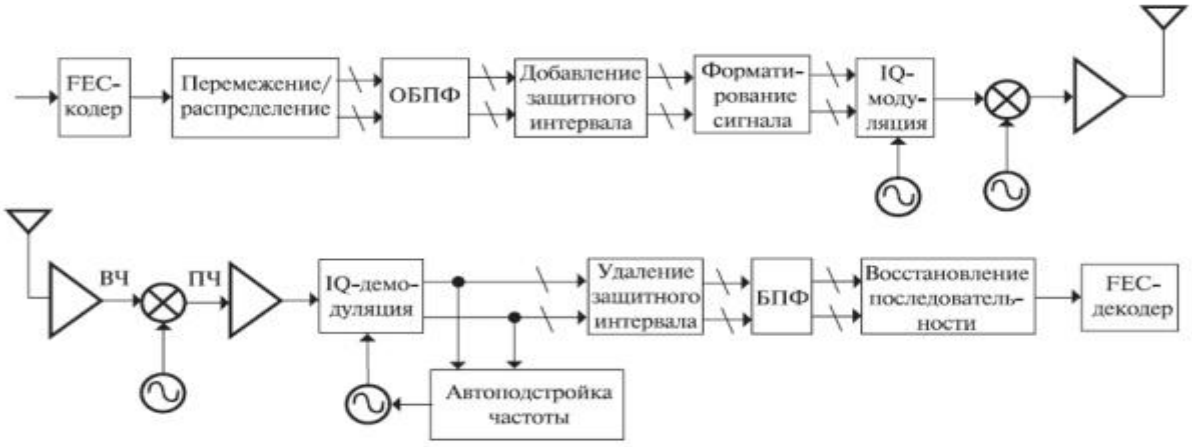


Рис. 3.55. Функциональная схема трактов приема/передачи стандарта IEEE 802.11a

IEEE 802.11g

Стандарт IEEE 802.11g по сути представляет собой перенесение схемы модуляции OFDM, прекрасно зарекомендовавшей себя в 802.11a, из диапазона 5 ГГц в область 2,4 ГГц при сохранении функциональности устройств стандарта 802.11b. Это возможно, поскольку в стандартах 802.11 ширина одного канала в диапазонах 2,4 и 5 ГГц схожа - 22 МГц.

Одним из основных требований к спецификации 802.11g была обратная совместимость с устройствами 802.11b. Действительно, в стандарте 802.11b в качестве основного способа модуляции принята схема ССК (Complementary Code Keying), а в качестве дополнительной возможности допускается модуляция PBCC (Pocket Binary Convolutional Coding).

Разработчики 802.11g предусмотрели ССК-модуляцию для скоростей до 11 Мбит/с и OFDM для более высоких скоростей. Но сети стандарта 802.11 при работе используют принцип CSMA/CA - множественный доступ к каналу связи с контролем несущей и предотвращением коллизий. Ни одно устройство 802.11 не должно начинать передачу, пока не убедится, что эфир в его диапазоне свободен от других устройств. Если в зоне слышимости окажутся устройства 802.11b и 802.11g, причем обмен будет происходить между устройствами 802.11g посредством OFDM, то оборудование 802.11b просто не поймет, что другие устройства сети ведут передачу, и попытается начать трансляцию. Последствия очевидны.

Чтобы не допустить подобной ситуации, предусмотрена возможность работы в смешанном режиме - CCK-OFDM. Информация в сетях 802.11 передается кадрами. Каждый информационный кадр включает два основных поля: преамбулу с заголовком и информационное поле (рис.5.56).

Рис. 3.56. Кадры IEEE 802.11g в различных режимах модуляции

Преамбула содержит синхропоследовательность и код начала кадра, заголовок - служебную информацию, в том числе о типе модуляции, скорости и продолжительности передачи кадра. В режиме CCK-OFDM преамбула и заголовок модулируются методом CCK (реально - путем прямого расширения спектра DSSS посредством последовательности Баркера, поэтому в стандарте 802.11g этот режим именуется DSSS-OFDM), а информационное поле - методом OFDM. Таким образом, все устройства 802.11b, постоянно "прослушивающие" эфир, принимают заголовки кадров и узнают, сколько времени будет транслироваться кадр 802.11g. В этот период они "молчат". Естественно, пропускная способность сети падает, поскольку скорость передачи преамбулы и заголовка - 1 Мбит/с.

Видимо, данный подход не устраивал лагерь сторонников технологии PBCC, и для достижения компромисса в стандарт 802.11g в качестве дополнительной возможности ввели, так же как и в 802.11b, необязательный режим - PBCC, в котором заголовок и преамбула передаются так же, как и при CCK, а информационное поле модулируется по схеме PBCC и передается на скорости 22 или 33 Мбит/с. В результате устройства стандарта 802.11g должны оказаться совместимыми со всеми модификациями оборудования 802.11b и не создавать взаимных помех. Диапазон поддерживаемых им скоростей отражен в таблице 3.9, зависимость скорости от типа модуляции - на рис.3.57.

Таблица 3.9. Возможные скорости и тип модуляции в спецификации IEEE 802.11g

Скорость, Мбит/с	Тип модуляции	
	Обязательно	Допустимо
1	Последовательность Баркера	

2	Последовательность Баркера	
5,5	CCK	PBCC
6	OFDM	OFDM
9		OFDM, CCK-OFDM
11	CCK	PBCC
12	OFDM	CCK-OFDM
18		OFDM, CCK-OFDM
22		PBCC
24	OFDM	CCK-OFDM
33		PBCC
36		OFDM, CCK-OFDM
48		OFDM, CCK-OFDM
54		OFDM, CCK-OFDM

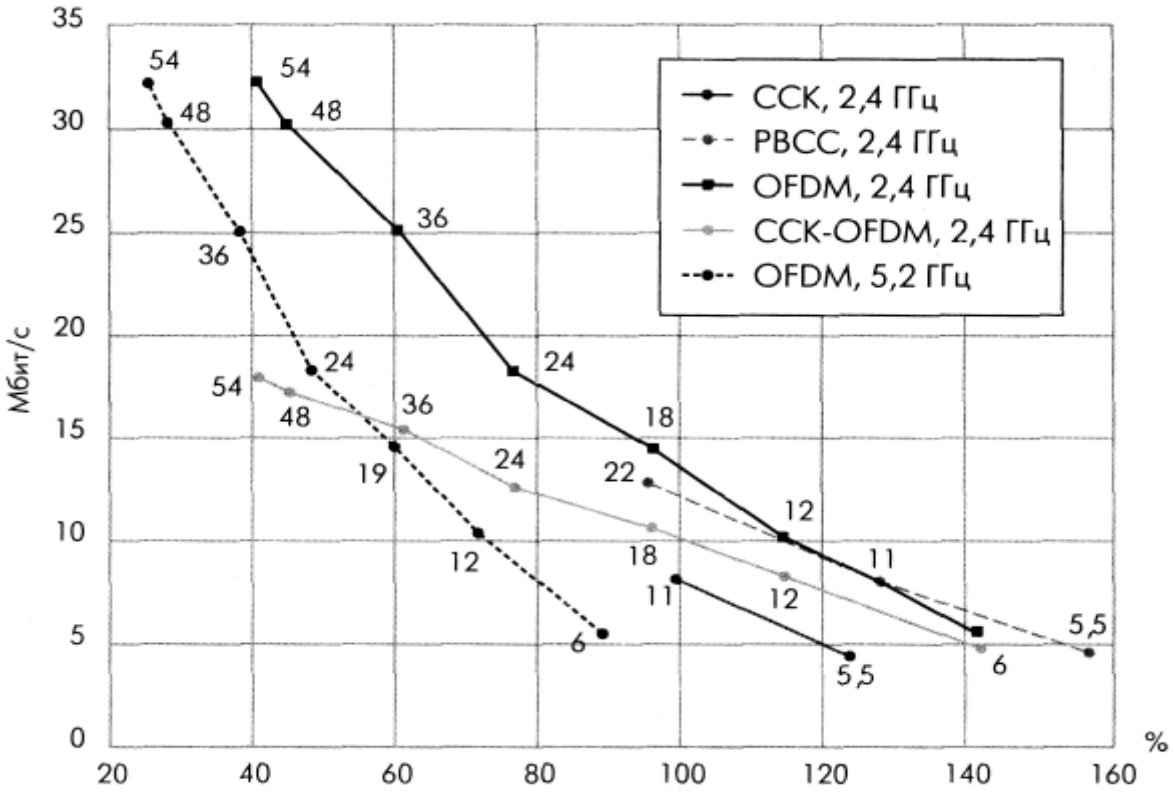


Рис. 3.57. Зависимость скорости передачи от расстояния для различных технологий передачи. Расстояние приведено в процентах, 100% - дальность передачи с модуляцией ССК на скорости 11 Мбит/с

Очевидно, что устройствам стандарта IEEE 802.11g достаточно долго придется работать в одних сетях с оборудованием 802.11b. Также очевидно, что производители в массе своей не будут поддерживать режимы CCK-OFDM и PBCC в силу их необязательности, ведь почти все решает цена устройства. Поэтому одна из основных проблем данного стандарта - как обеспечить бесконфликтную работу смешанных сетей 802.11b/g.

Основной принцип работы в сетях 802.11 - "слушать, прежде чем вещать". Но устройства 802.11b не способны услышать устройства802.11g в OFDM-режиме. Ситуация аналогична проблеме скрытых станций: два устройства удалены настолько, что не слышат друг друга и пытаются обратиться к третьему, которое находится в зоне слышимости обоих. Для предотвращения конфликтов в подобной ситуации в 802.11 введен защитный механизм, предусматривающий перед началом информационного обмена передачу короткого кадра "запрос на передачу" (RTS) и получение кадра подтверждения "можно передавать" (CTS). Механизм RTS/CTSприменим и к смешанным сетям 802.11b/g. Естественно, эти кадры должны транслироваться в режиме ССК, который обязаны понимать все устройства. Однако защитный механизм существенно снижает пропускную способность сети.

Таблица 3.10. Стандарты физического уровня

Параметр	802.11 DSSS	802.11 FHSS	802.11b	802.11a	802.11g
Частотный диапазон (ГГц)	2,4	2,4	2,4	5	2,4
Максимальная скорость передачи данных (Мбит/с)	2	2	11	54	54
Технология	DSSS	FHSS	CCK	OFDM	OFDM
Тип модуляции (для максимальной скорости передачи)	QPSK	GFSK	QPSK	64-QAM	64-QAM
Число неперекрывающихся каналов	3	3	3	15	3

Создание модели радиоинтерфейса WiFi 802.11 [21]

IEEE 802.11b

Чтобы открыть модель необходимо в командном окне ввести (Command Window): commwlan80211b. Появится модель, изображенная на рис.3.58.

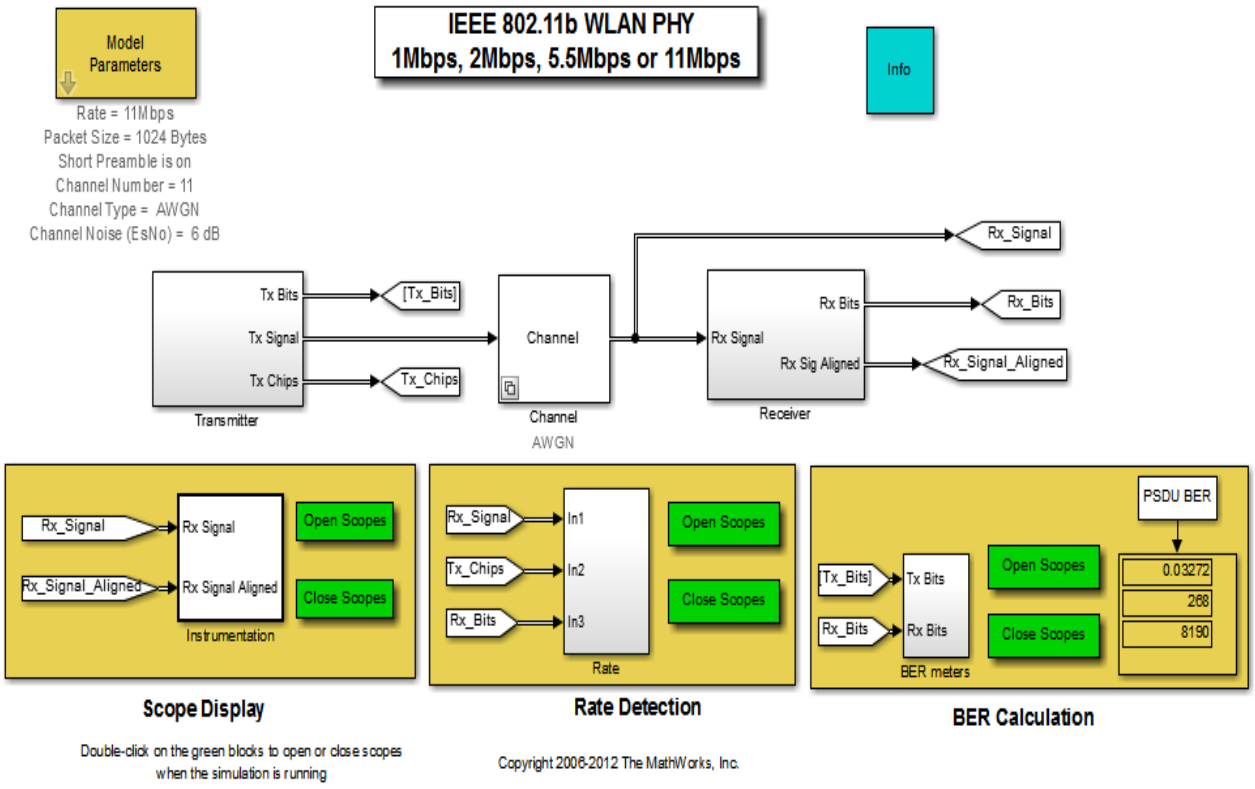


Рис. 3.58. Модель радиоинтерфейса 802.11b Simulink MATLAB 2015b

С помощью двойного щелчка на элемент Model Parameters можно устанавливать желаемые параметры моделируемой сети:

- скорость передачи данных (Rate),
- размер пакета (Packet Size),
- число каналов (Channel Number),
- тип канала (Channel Type),
- уровень шумов в канале (Channel EsNo).

Двойным щелчком по передатчику, приемнику или каналу передачи можно посмотреть их структурные схемы. Они представлены на рис.5.59, рис.5.60, рис.5.61.

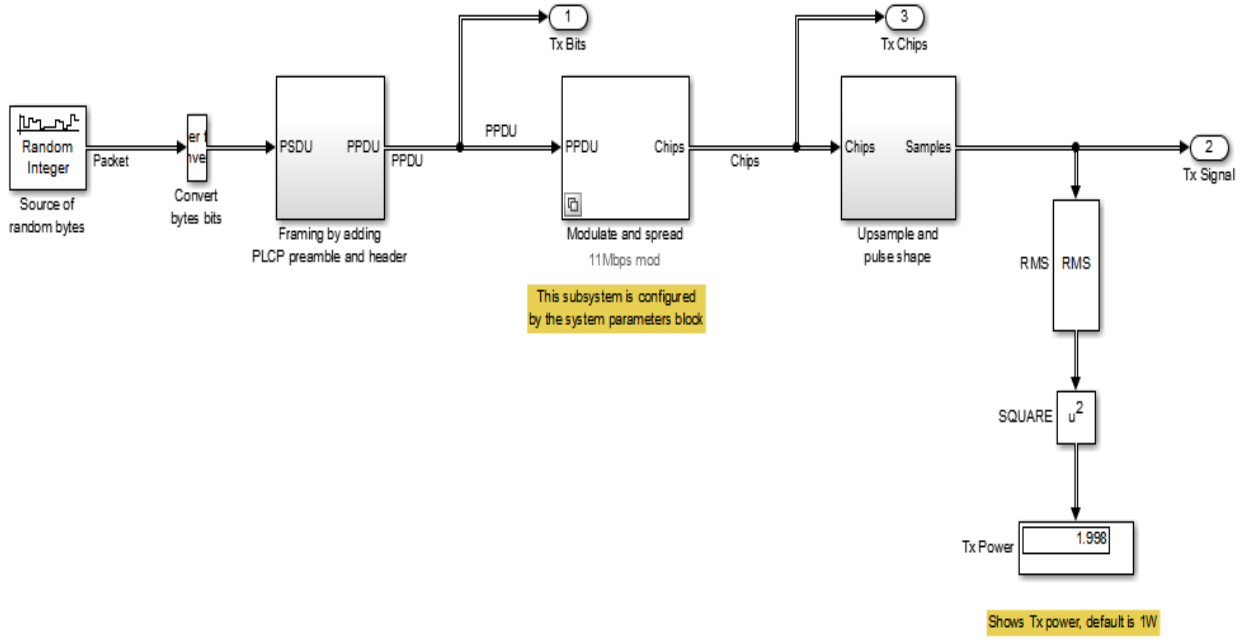


Рис. 3.59. Структурная схема передатчика IEEE 802.11b

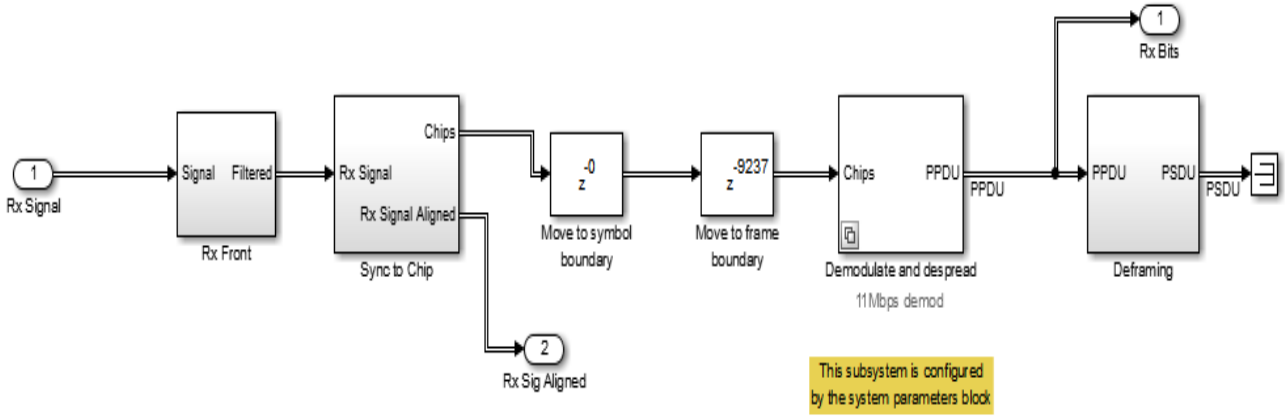


Рис. 3.60. Структурная схема приемника IEEE 802.11b

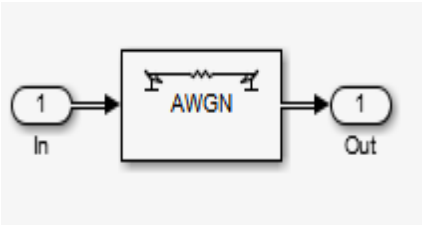


Рис. 3.61. Структурная схема канала передачи IEEE 802.11b

Пример частотной характеристика представлен на рис.3.62, а диаграмма созвездий на рис.3.63.

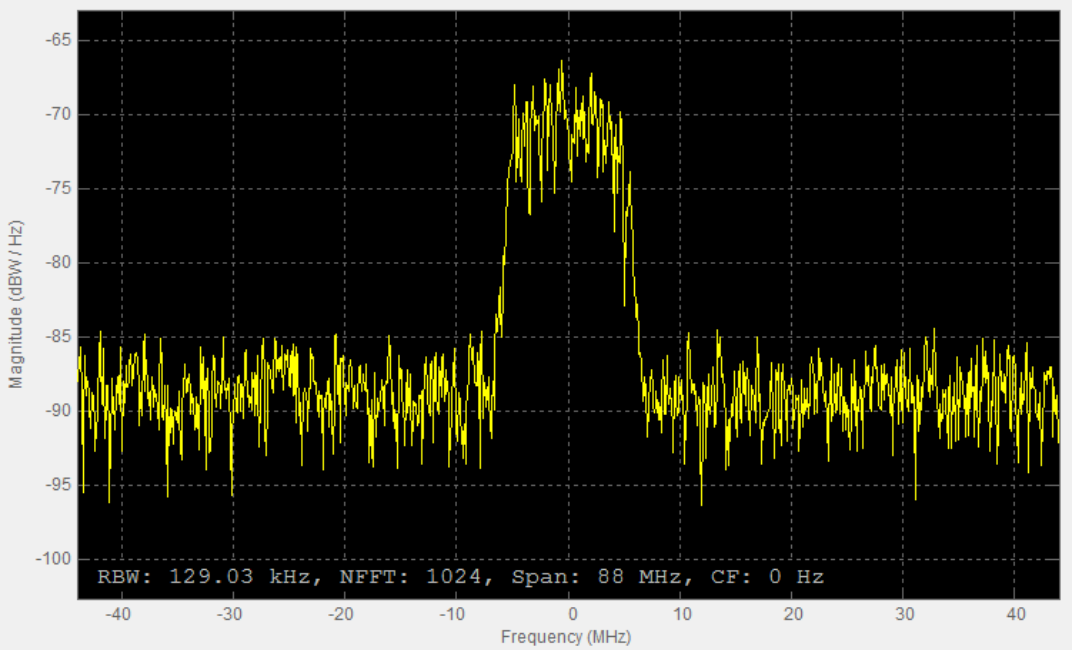


Рис. 3.62. Частотная характеристика для скорости передачи 11 Мбит/с

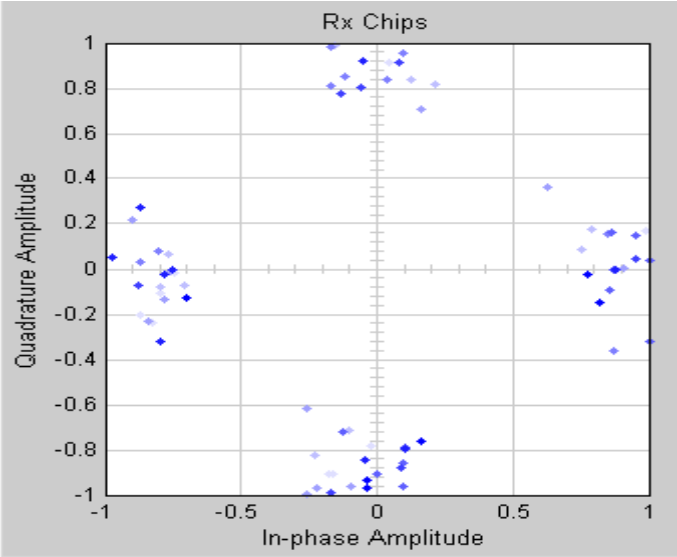


Рис. 3.63. Диаграмма созвездий для скорости передачи 11 Мбит/с

Исследование влияния ошибок BER

BitErrorRate (BER) - коэффициент ошибок, отношение числа неверно принятых битов (0 вместо 1 и наоборот) к полному числу переданных битов при передаче по каналу связи.

Чтобы получить зависимость BER от отношения сигнал/шум необходимо визменять уровень шумов в канале (0-14) и снимать показания в блоке BER Calculation в верхнем дисплее.

Протестировав систему таким образом, были получены зависимости, представленные на рис.3.64.

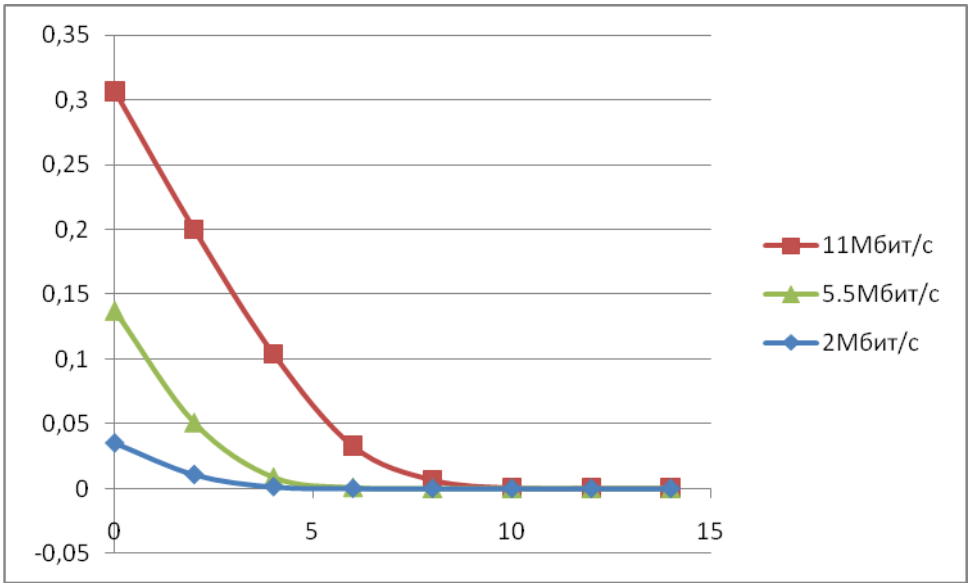


Рис. 3.64. Зависимость ошибки BER от отношения сигнал/шум для различных скоростей IEEE 802.11b

По полученным результатам можно сделать следующие выводы:

1) Большим скоростям соответствует большая вероятность появления ошибки

2) Для уменьшения ошибки необходимо увеличивать отношение сигнал/шум

3) Большим скоростям необходимо более высокое значение отношения сигнал шум для устранения возможных ошибок.

В результате работы изучены стандарты IEEE 802.11.

Рассмотрены и протестированы модели данных стандартов, реализованные в среде Simulink Matlab. Получены графики зависимостей вероятности ошибки (BER) от отношения сигнал/шум для разных скоростей.

Методические указания к моделированию [25]

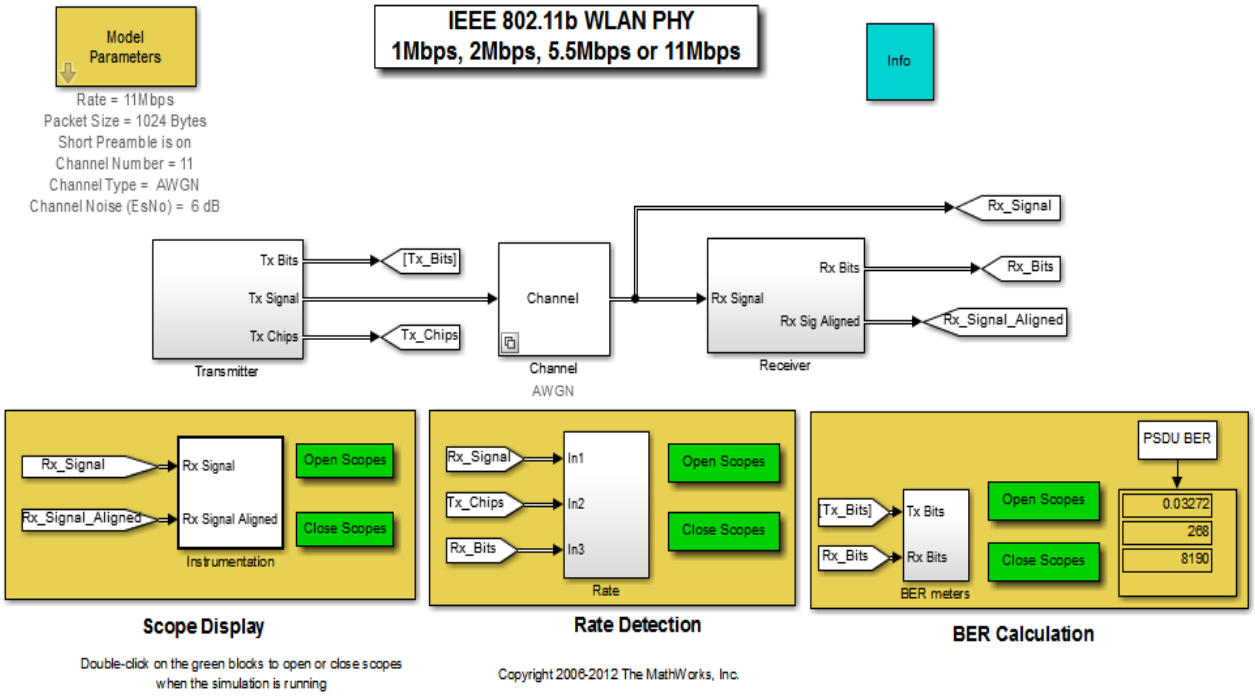


Рис. 3.65. Схем сети IEEE 802.11b MATLAB

1. Запустить модель командой commwlan80211b и изучить ее параметры. Сделать скриншоты полной схемы, а также передатчика, приёмника и канала.

2. Снять частотную характеристику, а также диаграмму созвездий для 4-х вариантов максимальной скорости передачи (1, 2, 5, 11 Мбит/с). Параметр «тип канала» (Channel Type) – none.

3. Для каждой скорости изменяя отношение сигнал/шум в канале от 0 до 14дБ снять зависимость BER от Channel EsNo. Параметр «тип канала» (Channel Type) – AWGN.

5. Сделать выводы по проделанной работе.

3.4. Имитационное моделирование системы мобильной связи стандарта IEEE 802.15.4 ZigBee [25]

Среди наиболее известных беспроводных технологий можно выделить: Wi-Fi, Wi-Max, Bluetooth, Wireless USB и относительно новую технологию — ZigBee, которая изначально разрабатывалась с ориентацией на промышленные применения.

Каждая из этих технологий имеет свои уникальные характеристики, которые определяют соответствующие области применения.

Стандарт	802.15.4 ZigBee™			802.15.1 Bluetooth	802.15.3 High Rate WPAN, WiMedia	802.15.3a* UWB	802.11b Wi-Fi
Приложения	Мониторинг, управление, сети датчиков, домашняя/промышленная автоматика			Голос, данные, замена кабелей	Потоковое мультимедиа, замена кабелей аудио/видеосистем		Данные, видео, ЛВС
Преимущества	Цена, энергосбережение, размеры сети, менее загруженные диапазоны		Цена, энерго-сбережение, размеры сети, глобальный диапазон	Цена, энерго-сбережение, передача голоса, перескоки частоты	Высокая скорость, энергосбережение		Скорость, гибкость
Частота, ГГц	0,868	0,915	2,4			3,1 – 10,6	2,4
Макс. скорость	20 Кбит/с	40 Кбит/с	250 Кбит/с	1 Мбит/с	22 Мбит/с (доп. 11, 33, 44, 55 Мбит/с)	110 Мбит/с (10 м), 200 Мбит/с (4 м) (доп. 480 Мбит/с)	11 Мбит/с
Выходная мощность (ном.), дБм	0			0 (класс 3) 4 (класс 2) 20 (класс 1)	0	< 20 (110 Мбит/с) < 24 (200 Мбит/с)	20
Дальность, м	10 – 100			10 (класс 3) 100 (класс 1)	5 – 50	10 (110 Мбит/с) 4 (200 Мбит/с)	100
Чувствительность (спецификация, дБм)	-92		-85	-70	-75	-	-76
Размер стека, Кбайт	4 – 32			> 250	-		> 1000
Срок службы батареи, дней	100 – 1000+			1 – 7	теоретически более 1000		0,5 – 5
Размер сети	65536 (16-битные адреса), 2^{64} (64-битные адреса)			мастер +7	до 127 на хост		32

Рис. 3.66. Основные характеристики популярных стандартов беспроводной связи

Рис. 3.67. Внешний вид микросхемы ZigBee

Анализ беспроводных технологий показывает, что высокоскоростные технологии Wi-Fi, Wi-Max, Bluetooth, Wireless USB предназначены в первую очередь для обслуживания компьютерной периферии и устройств мультимедиа. Они оптимизированы для передачи больших объемов информации на высоких скоростях, работают в основном по топологии

«точка-точка» или «звезда» и малопригодны для реализации сложных разветвленных промышленных сетей с большим количеством узлов. Напротив, технология ZigBee имеет достаточно скромные показатели скорости передачи данных и расстояния между узлами, но обладает следующими важными, с точки зрения применения в промышленности, преимуществами:

- Она ориентирована на преимущественное использование в системах распределенного мульти-микропроцессорного управления со сбором информации с интеллектуальных датчиков, где вопросы минимизации энергопотребления и процессорных ресурсов являются определяющими.
- Предоставляет возможность организации самоконфигурируемых сетей со сложной топологией, в которых маршрут сообщения автоматически определяется не только числом исправных или включенных/выключенных на текущий момент устройств (узлов), но и качеством связи между ними, которое автоматически определяется на аппаратном уровне.
- Обеспечивает масштабируемость — автоматический ввод в работу узла или группы узлов сразу после подачи питания на узел.
- Гарантирует высокую надежность сети за счет выбора альтернативного маршрута передачи сообщений при отключениях/сбоях в отдельных узлах.
- Поддерживает встроенные аппаратные механизмы шифрации сообщений AES-128, исключая возможность несанкционированного доступа в сеть.

Организация сети ZigBee

ZigBee — относительно новый стандарт беспроводной связи, который изначально разрабатывался как средство для передачи небольших объемов информации на малые расстояния с минимальным энергопотреблением. Фактически этот стандарт описывает правила работы программно-аппаратного комплекса, реализующего беспроводное взаимодействие устройств друг с другом.

Стек протоколов ZigBee представляет собой иерархическую модель, построенную по принципу семиуровневой модели протоколов передачи данных в открытых системах OSI (OpenSystemInterconnection). Стек включает в себя уровни стандарта IEEE 802.15.4, отвечающие за реализацию канала связи, и программные сетевые уровни и уровни поддержки приложений, определенные спецификацией ZigBee. Модель реализации стандарта связи ZigBee представлена на рисунке 3.69.

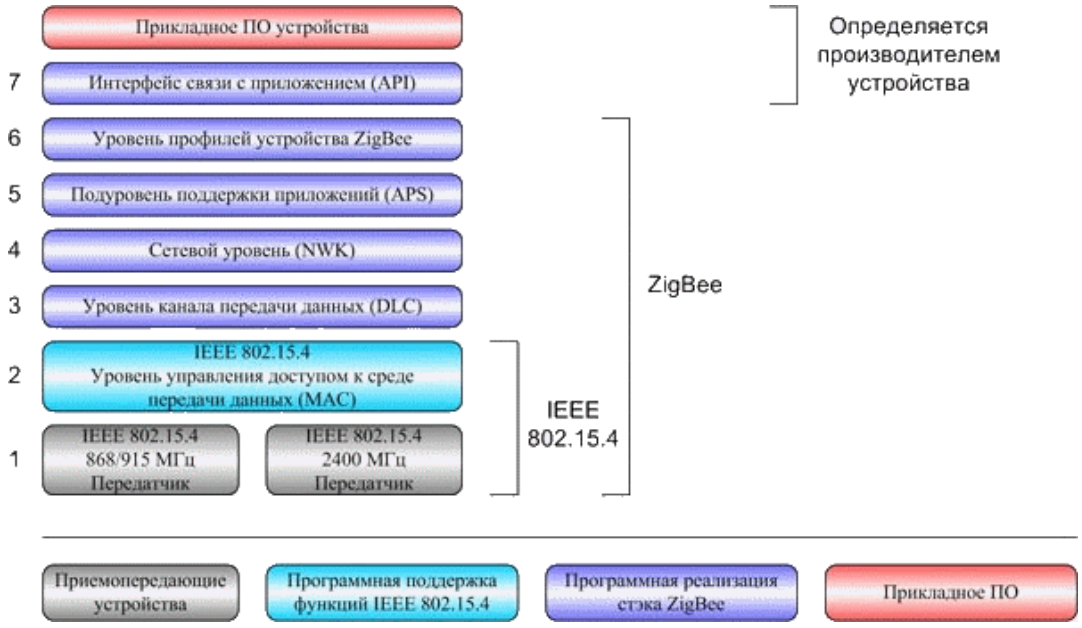


Рис. 3.68. Многоуровневая модель стандарта связи ZigBee

Стандарт IEEE 802.15.4 определяет два нижних уровня стека: уровень доступа к среде (MAC) и физический уровень передачи данных в среде распространения (PHY), то есть нижние уровни протокола беспроводной передачи данных. Альянс определяет программные уровни стека ZigBee от уровня канала передачи данных (DataLinkControl) до уровня профилей устройств (ZigBeeProfiles). Прием и передача данных по радиоканалу осуществляется на физическом уровне PHY, определяющем рабочий частотный диапазон, тип модуляции, максимальную скорость, число каналов. Уровень PHY осуществляет активацию-дезактивацию приемопередатчика, детектирование энергии принимаемого сигнала на рабочем канале, выбор физического частотного канала, индикацию качества связи при получении пакета данных и оценку свободного канала. Важно понимать, что стандарт 802.15.4 — это физическое радио (микросхема радио-приемопередатчика), а ZigBee — это логическая сеть и программный стек, обеспечивающие функции безопасности и маршрутизации.

Далее в структуре стека ZigBee следует уровень контроля доступа к среде IEEE 802.15.4 MAC, осуществляющий вход и выход из сети устройств, организацию сети, формирование пакетов данных, реализацию различных режимов безопасности (включая 128-битное шифрование AES), 16- и 64-битную адресацию.

Уровень MAC обеспечивает различные механизмы доступа в сеть, поддержку сетевых топологий от «точка-точка» до «многоячейковая сеть», гарантированный обмен данными (ACK, CRC), поддерживает потоковую и пакетную передачи данных.

Для предотвращения нежелательных взаимодействий возможно использование временного разделения на основе протокола CSMA-CA (протокол множественного доступа к среде с контролем несущей и предотвращением коллизий).

Временное разделение ZigBee базируется на использовании режима синхронизации, при котором подчиненные сетевые устройства, большую часть времени находящиеся в «спящем» состоянии, периодически «просыпаются» для приема сигнала синхронизации от сетевого координатора, что позволяет устройствам внутри локальной сетевой ячейки знать, в какой момент времени осуществлять передачу данных. Данный механизм, основанный на определении состояния канала связи перед началом передачи, позволяет существенно сократить (но не устранить) столкновения, вызванные передачей данных одновременно несколькими устройствами. Стандарт 802.15.4 основывается на полудуплексной передаче данных (устройство может либо передавать, либо принимать данные), что не позволяет использовать метод CSMA-CA для обнаружения коллизий — только для их предотвращения.

В спецификации стека предусмотрены три типа устройств: координатор, маршрутизатор и конечное устройство.

Координатор инициализирует сеть, управляет ее узлами, хранит информацию о настройках каждого узла, задает номер частотного канала и идентификатор сети PAN ID, а в процессе работы может являться источником, приемником и ретранслятором сообщений.

Маршрутизатор отвечает за выбор пути доставки сообщения, передаваемого по сети от одного узла к другому, и в процессе работы также может являться источником, приемником или ретранслятором сообщений. Если маршрутизаторы имеют соответствующие возможности, они могут определять оптимизированные маршруты к определенной точке и хранить их для последующего использования в таблицах маршрутизации.

Оконечное устройство не участвует в управлении сетью и ретрансляции сообщений, являясь только источником/приемником сообщений.

Среди свойств ZigBee следует особо выделить поддержку сложных топологий сетей. Именно за счет этого, при относительно малой максимальной дальности связи двух близлежащих устройств, возможно расширить зону покрытия сети в целом. Также этому способствует 16-битная адресация, позволяющая объединять в одну сеть более 65 тыс. устройств.

Спецификация стандарта IEEE 802.15.4

Спецификация ZigBee-стека определяет сетевой уровень, уровни безопасности и доступа к приложению и может использоваться совместно с решениями на базе стандарта 802.15.4 для обеспечения совместимости устройств.

Таблица 3.11. Спецификация стандарта IEEE 802.15.4

Стандарт	802.15.4 ZigBee™		
Частота	868 МГц	915 МГц	2,4 ГГц
Число каналов/шаг	1/–	10/2 МГц	16/5 МГц
География распространения	Европа	Америка	Весь мир
Макс. скорость, модуляция	20 кбит/с, BPSK	40 кбит/с, BPSK	250 кбит/с, O-QPSK
Выходная мошность, ном.	0 dBm (1 мВт)	0 dBm (1 мВт)	0 dBm (1 мВт)
Дальность	10–100м		
Чувствительность (спецификация)	–92dBm	–92dBm	–85dBm
Размер стека	4–32 кбайт		
Срок службы батареи	От 100 до 1000 и более дней		
Размер сети	65536 (16-битные адреса), 2^{64} (64-битные адреса)		

Практическая часть

Задание:

1. Собрать схему
2. Подготовить схемы для реализации Стандарта ZigBee 802.15.4 основываясь на примере, представленном в отчете.
3. Изменять SNR в пределах от 1 до 100 (не менее 4-х точек)
4. Построить графики зависимости SNR от BER
5. Все поэтапное исследование представить в отчете.

В рабочем поле необходимо собрать схему для работы стандарта ZigBee 802.15.4. Схема представлена на рисунке 3.70.

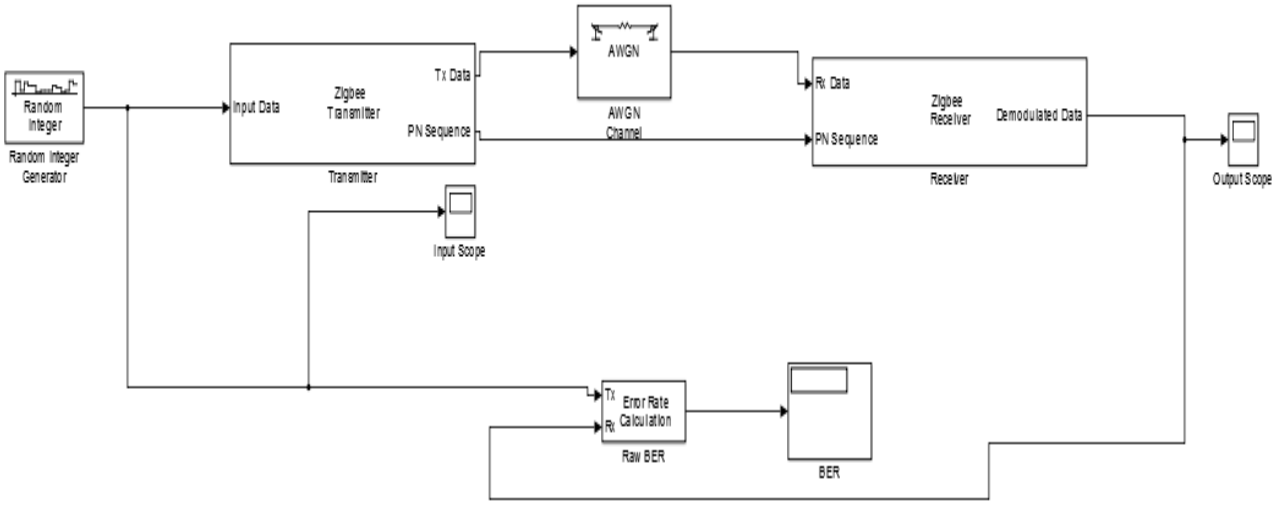


Рис. 3.69. Схема стандарта ZigBee 802.15.4 Simulink MATLAB 2015b

В состав схемы входят:

1. RandomIntegerGenerator
2. ZigBeeTransmitter
3. AWGN Channel (каналпередачи)
4. ZigBeeReciever
5. ErrorRateCalculation (анализаторошибок)
6. Display

Рассмотрим каждый блок отдельно. Все значения, заданные в блоках, помимо отношения Сигнал/шум в канале, остаются неизменными.

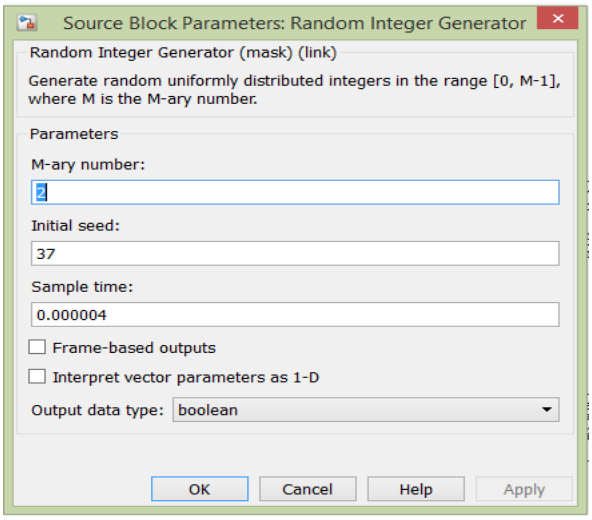


Рис. 3.70. Параметры блока Random Integer Generator

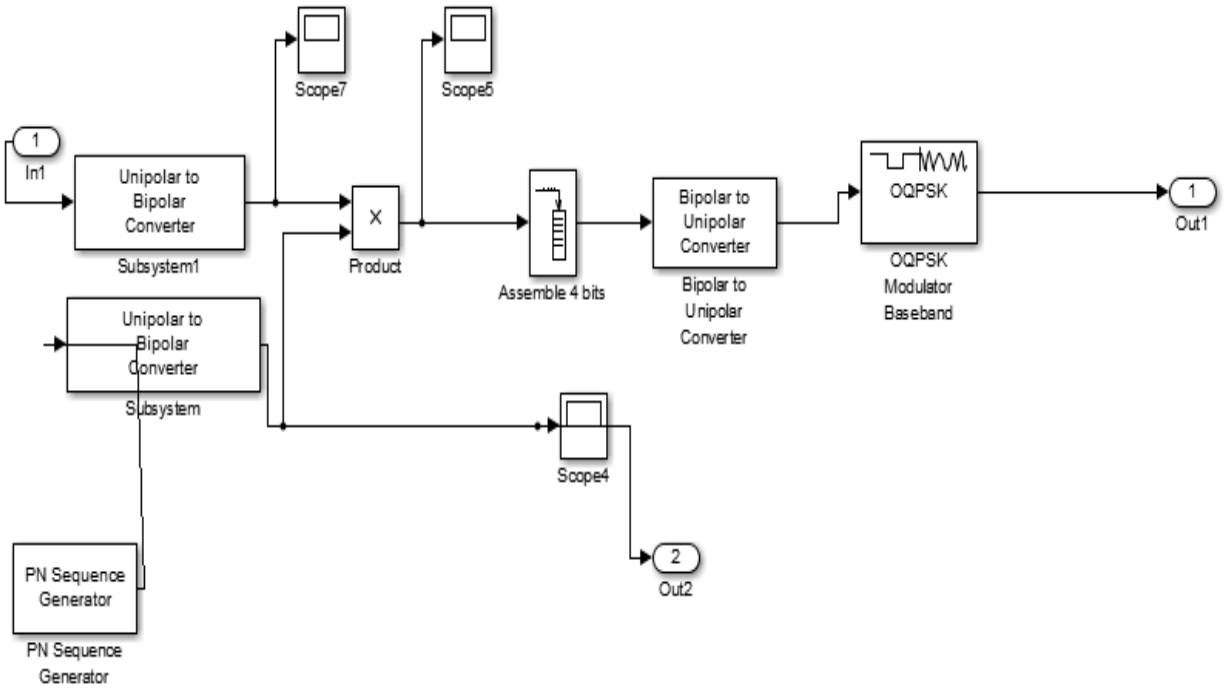


Рис. 3.71. Схема ZigBeeTransmitter

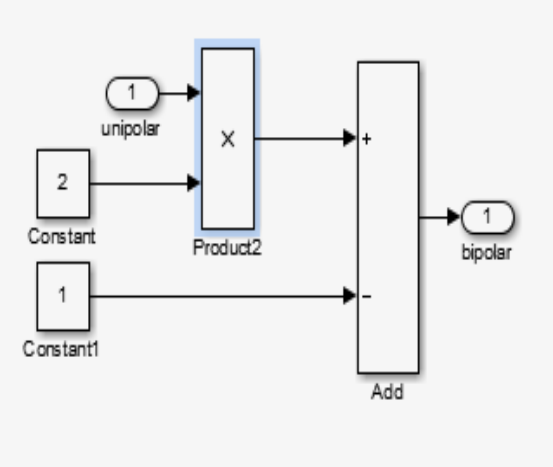


Рис. 3.72. Unipolar to bipolar converter

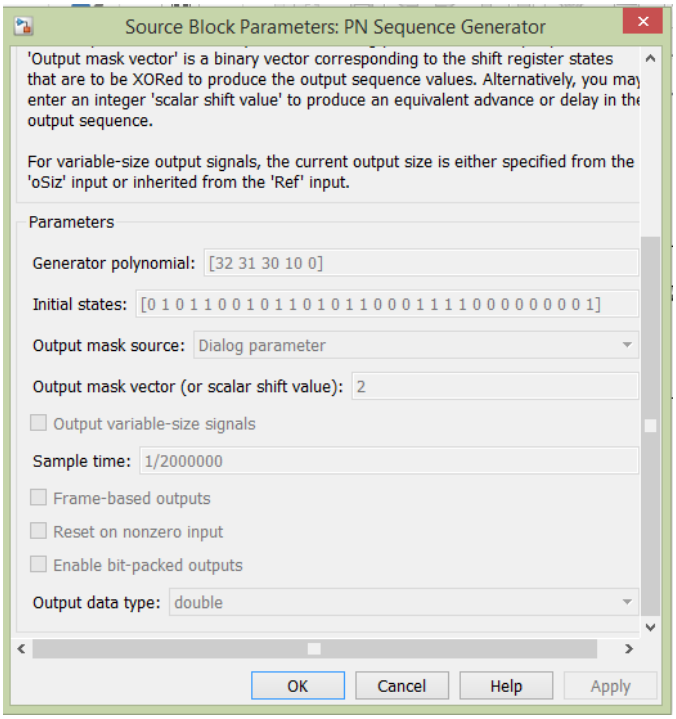


Рис. 3.73. Параметры блока PN sequence generator

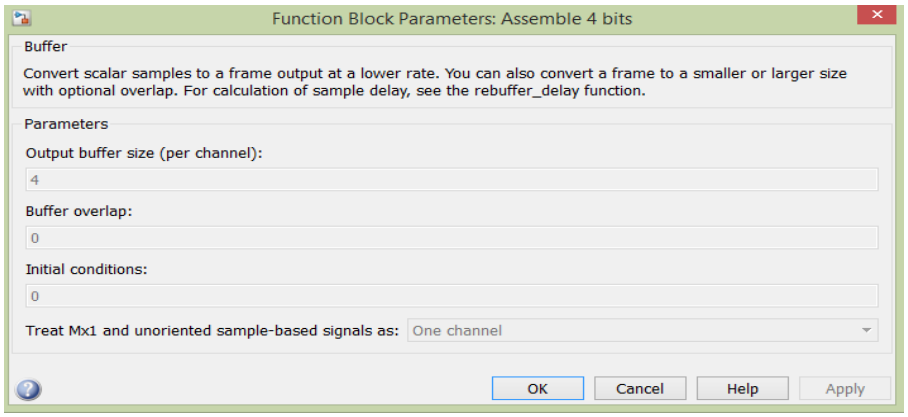


Рис. 3.74. Параметры блока Function block parameters: Assemble 4 bits

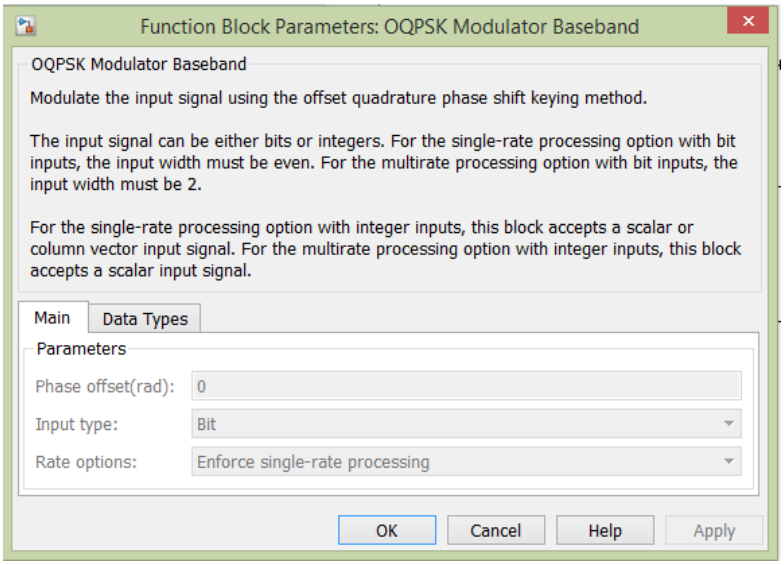


Рис. 3.75. Параметры блока OQPSK modulator baseband

OQPSK - четырехпозиционная фазовая модуляции со сдвигом квадратур (**OQPSK**), где битовые потоки, подаваемые на модуляторы квадратур I и Q, сдвинуты друг относительно друга на длительность одного бита (половина символьного интервала).

Рассмотрим блок канала с БГШ. В данном блоке необходимо изменять значения в строчке Eb\No от 1 до 100.

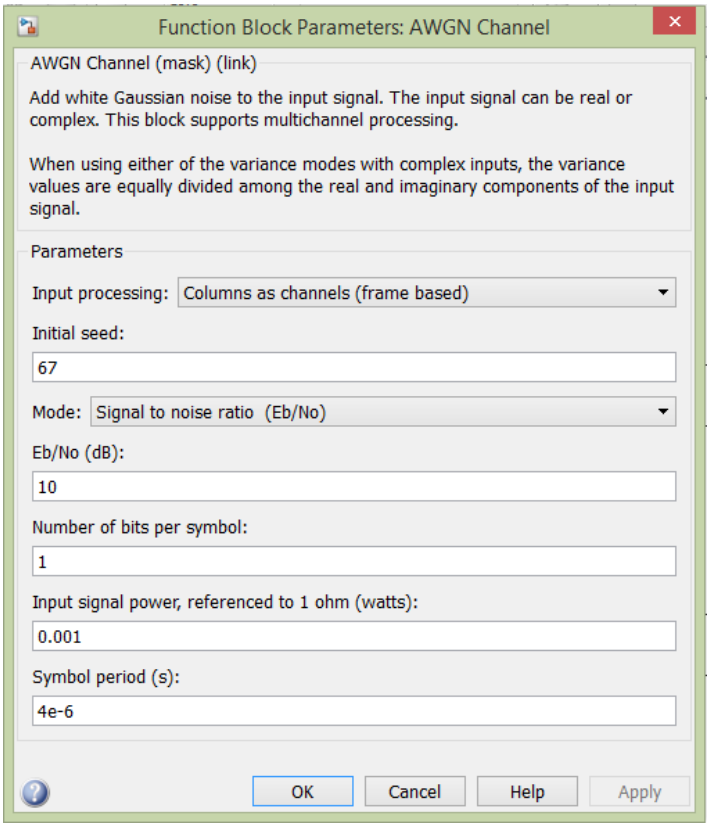


Рис. 3.76. Параметры блока AWGNchannel

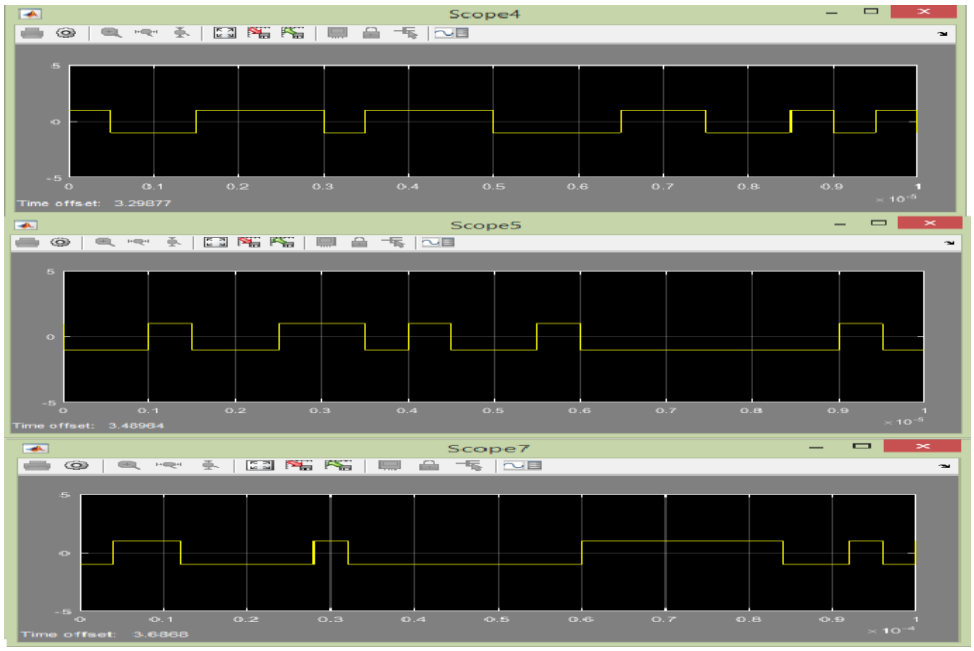


Рис. 3.77. Вид сигнала на осциллографах 4, 5, 7

Рассмотрим подробнее блок ZigBee Receiver.

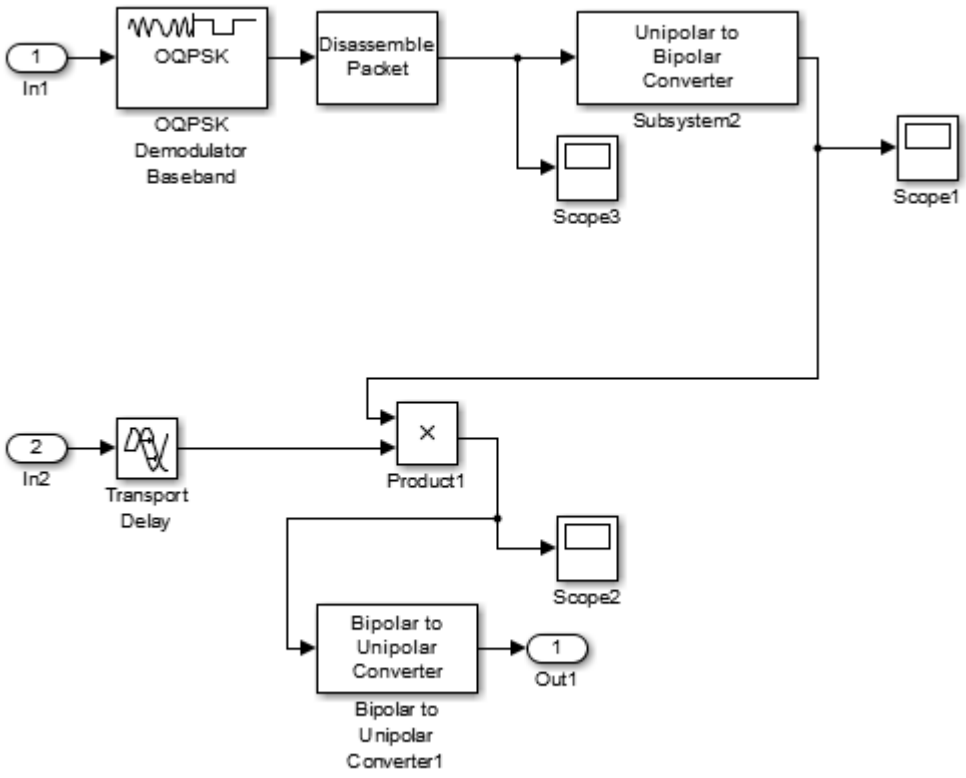


Рис. 3.78. Схема приемника стандарта ZigBee

Рассмотрим каждый блок отдельно. Единственным незнакомым элементом является блок TransportDelay.

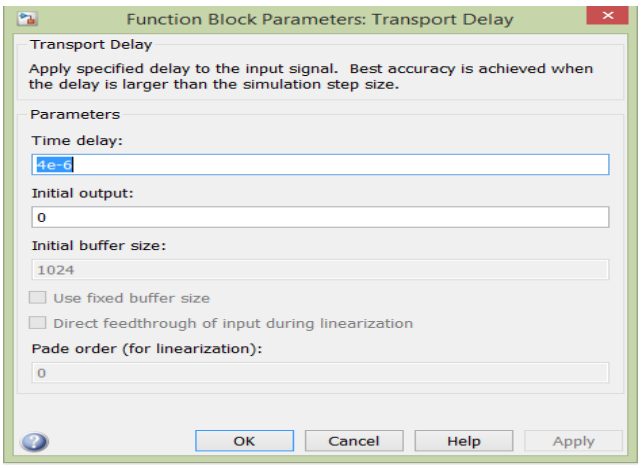


Рис. 3.79. Параметры блока TransportDelay

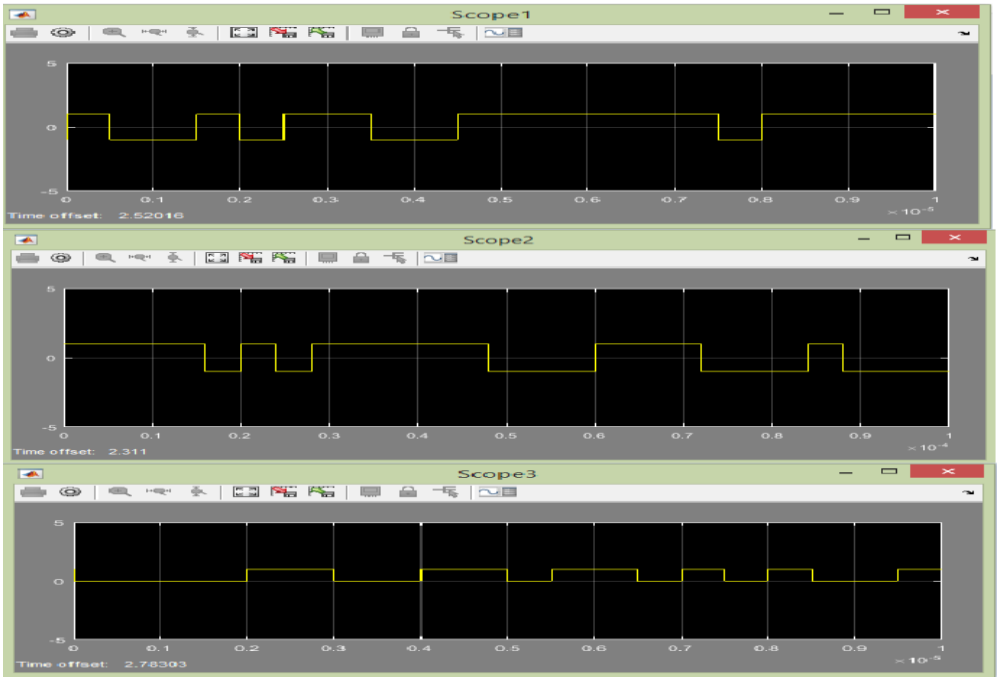


Рис. 3.80. Вид сигнала на осциллографах 1, 2, 3

Вернемся к общей схеме стандарта ZigBee.

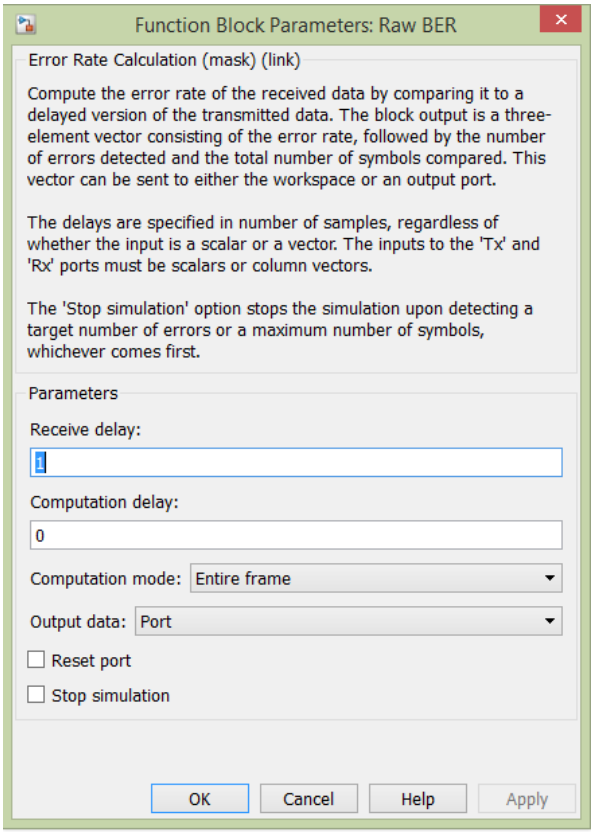


Рис. 3.81. Параметры блока RawBER

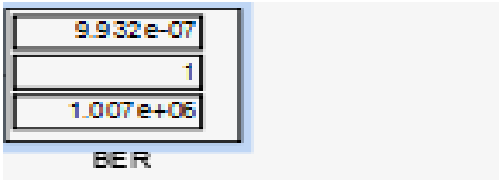


Рис. 3.82. Счетчик ошибок

Для построения графика зависимости BER от SNR, необходимо из счетчика брать первую строку.

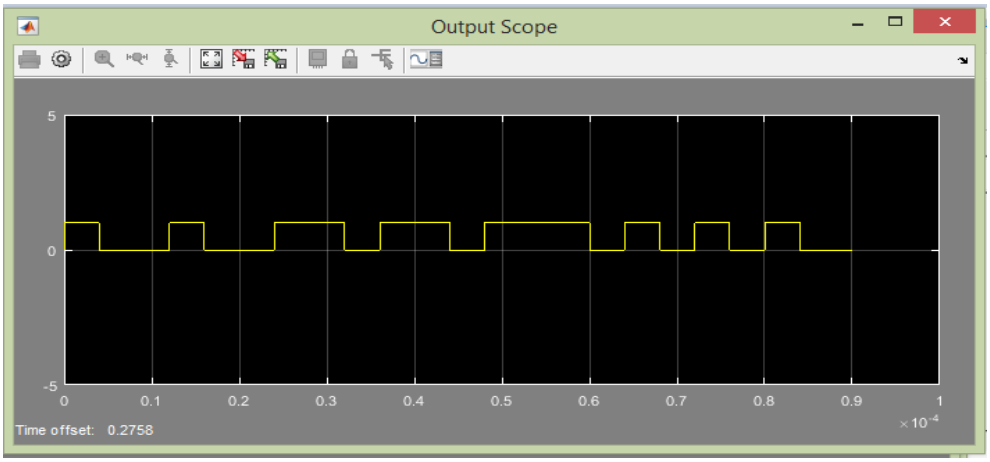


Рис. 3.83. Вид сигнала на выходе

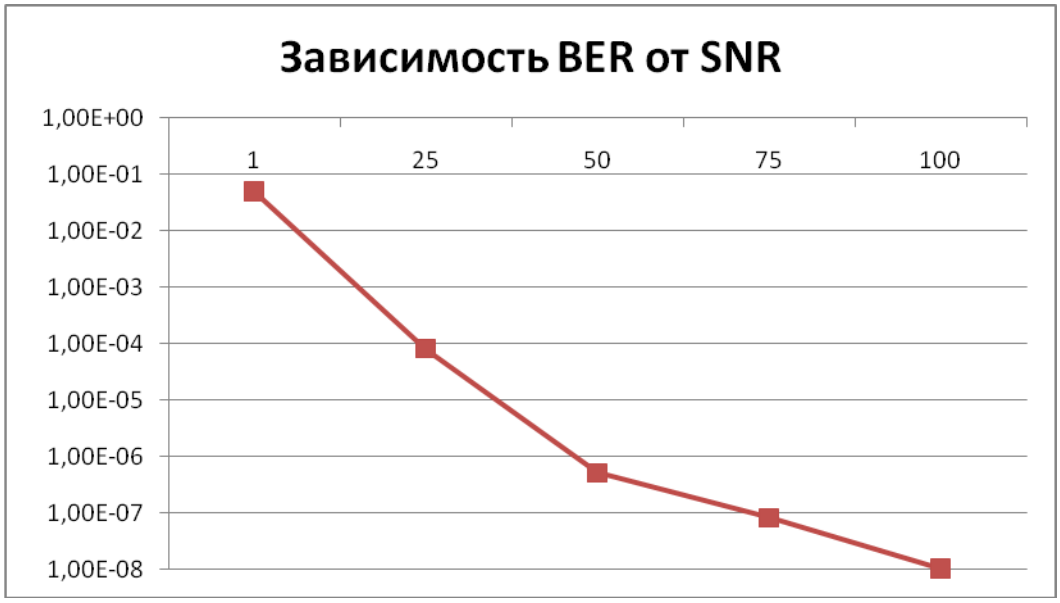


Рис. 3.84. График зависимости BER от SNR

В разделе построена схема стандарта ZigBee 802.15.4 в среде Simulink. Построен график зависимостей зависимости BER от SNR. Из графика (рисунок 5.85) видно, что при увеличении значения сигнал/шум, снижается количество ошибок.

3.5. Проектирование защищенной системы мобильной связи стандарта IEEE 802.15.1 (Bluetooth) [17-25]

Bluetooth

Стандарт Bluetooth является компромиссным с точки зрения соотношения параметров экономичность/дальность/скорость. По своей функциональности и возможности применения в различных приложениях он имеет наибольшее число пересечений с другими стандартами группы Short Range RF. Поэтому для начала рассмотрим именно его.

Основная идея Bluetooth заключалась в создании универсального, надежного и очень дешевого радиоинтерфейса беспроводного доступа. Технология Bluetooth позволяет обеспечить сопряжение с различным профессиональным и бытовым оборудованием в режимах передачи речи, данных и мультимедиа, при этом гарантируется его электромагнитная совместимость с другим домашним или офисным оборудованием. Как было указано в таблице, существует всего три класса устройств Bluetooth, если градировать их по излучаемой мощности: 1-й — до 100 метров (до 100 мВт); 2-й — до 10 метров (до 2,5 мВт); 3-й — до 1 метра (до 1 мВт).

Для определения модели поведения при установлении соединения между различными типами устройств в технологии Bluetooth введено понятие профиль. Этим термином обозначается набор функций и возможностей, которые использует Bluetooth в качестве механизма транспортировки. Профили гарантируют возможность обмена информацией между устройствами разных производителей. Bluetooth SIG определяет 15 стандартных профилей:

- Generic Access Profile (GAP);
- Service Discover Application Profile (SDAP);
- Serial Port Profile (SPP);
- Dial-up Networking Profile (DUNP);
- Generic Object Exchange Profile (GOEP);
- Object Push Profile (OPP);
- File Transfer Profile (FTP);
- Synchronization Profile (SP);
- AV Control, Headset Profile (HSP);
- Advanced Audio Distribution Profile (A2DP);
- Basic Imaging Profile (BIP);

- Handsfree Profile (HFP);
- Human Interface Device Profile (HID);
- LAN Access Profile (LAP);
- Sim-Card Access Profile (SAP).

По характеру взаимодействия со внешними устройствами и приложениями архитектура всех существующих модулей Bluetooth может быть разделена на три вида (рис. 1). Модули с двухпроцессорной архитектурой (рис. 1а) не содержат в себе программного высокоуровневого стека Bluetooth с поддержкой стандартных профилей. Это значит, что необходимые профили Bluetooth должны быть реализованы на внешнем процессоре. Взаимодействие внешнего процессора с модулем происходит через виртуальный интерфейс HCI (Host Controller Interface). В частном случае HCI может быть реализован через аппаратный интерфейс SPI или UART.

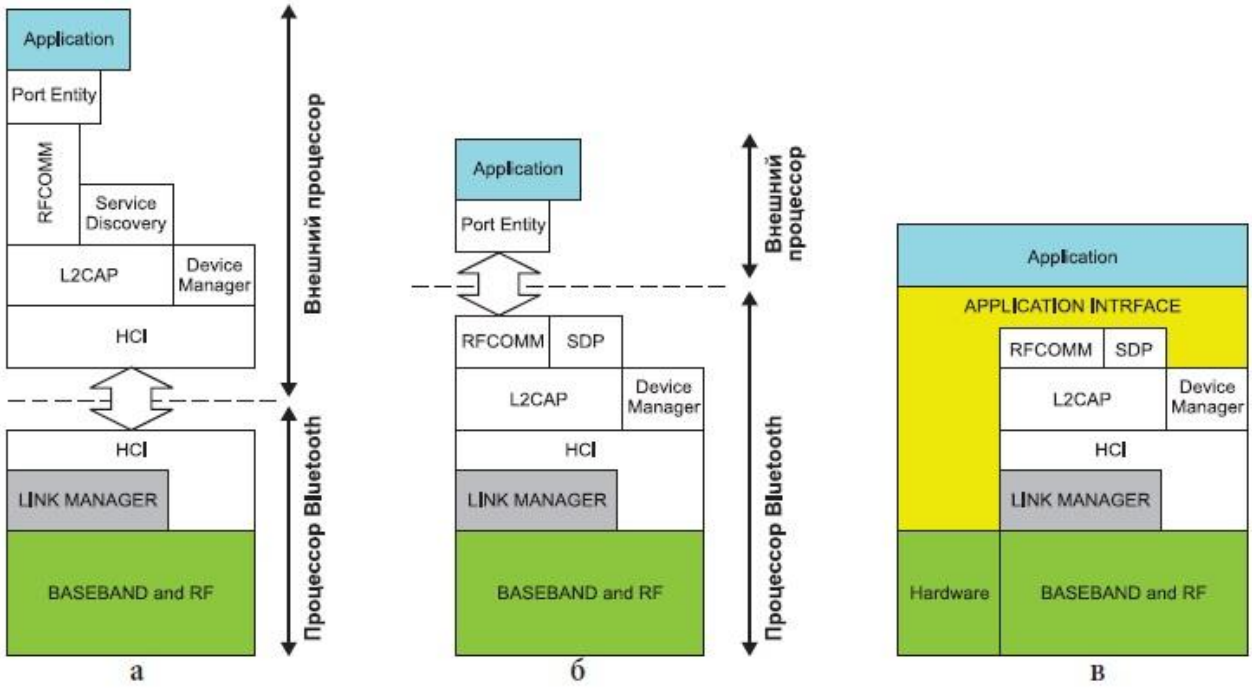


Рис. 3.85. Разновидности архитектуры модулей стандарта Bluetooth: а) двухпроцессорная; б) встроенная двухпроцессорная; в) однопроцессорная

Модули Bluetooth со встроенной двухпроцессорной архитектурой (рис. 3.85б) являются наиболее распространенными. Данная разновидность архитектуры подразумевает наличие стека Bluetooth высокого уровня с поддержкой стандартных профилей непосредственно во внутреннем процессоре модуля. В этом случае приложение, работающее на внешнем процессоре, взаимодействует с модулем Bluetooth через аппаратные интерфейсы.

Однопроцессорная архитектура (рис. 3.85в) является наименее распространенной. Для ее реализации разработчик должен создать специальное приложение, которое будет работать на внутреннем процессоре модуля Bluetooth. В этом случае модуль превращается в автономное устройство, доступ к которому через внешние аппаратные интерфейсы закрыт.

Принадлежность модуля к той или иной архитектуре может определяться как его аппаратной реализацией, так и внутренним программным обеспечением. Например, в частном случае один и тот же модуль Bluetooth может быть отнесен к любой из трех разновидностей архитектуры в зависимости от типа прошивки, загруженной во внутренний процессор модуля. Такой подход пользуется наибольшей популярностью среди зарубежных производителей.

Чтобы получить наиболее полное представление о роли Bluetooth среди других представителей группы Short Range RF, обратимся к истории (рис. 5.86). Развитие Bluetooth с самого начала шло по пути увеличения скорости обмена данными, снижения энергопотребления, повышения безопасности и надежности соединения. Вплоть до версии 3.0 сохранялась обратная совместимость всех версий Bluetooth между собой. До сих пор в эксплуатации встречаются устройства Bluetooth версий 1.1 и 1.2, которые успешно используются совместно с 2.0 и 2.1.

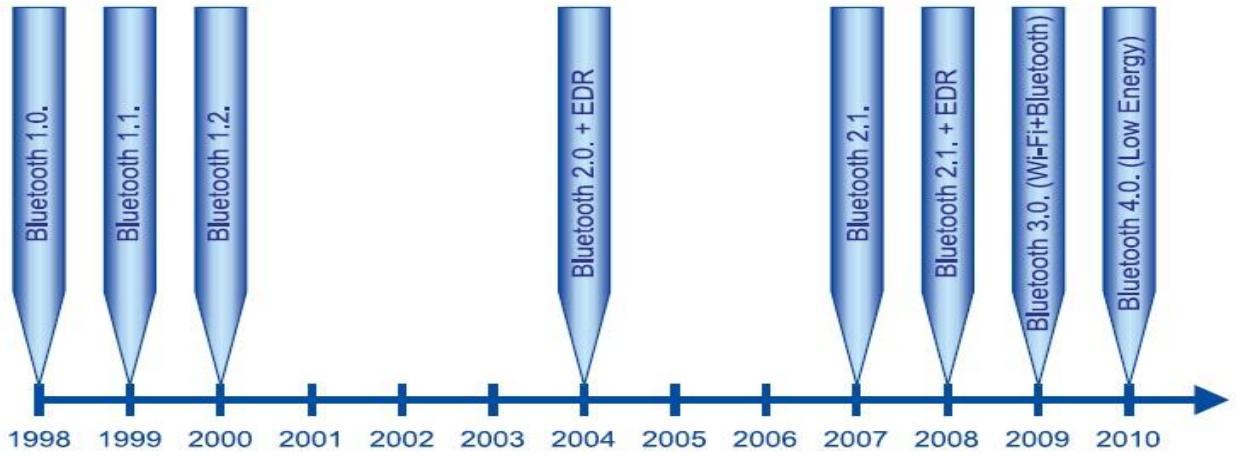


Рис. 3.86. Хронология развития стандарта Bluetooth

Bluetooth 3.0 является чем-то средним между Bluetooth и Wi-Fi. Модули с ее поддержкой соединяют в себе две радиосистемы: первая обеспечивает передачу данных в 3 Мбит/с (стандартная для Bluetooth 2.0) и имеет низкое энергопотребление; вторая совместима со стандартом 802.11 (Wi-Fi) и обеспечивает возможность передачи данных со скоростью до 24 Мбит/с (сравнима со скоростью сетей Wi-Fi). Выбор радиосистемы для передачи данных зависит от размера передаваемого файла. Это один из наиболее ярких примеров объединения

двух разных технологий для завоевания новых сегментов рынка. Правда, успеха эта попытка не имела: распространения Bluetooth 3.0 не получил.

Bluetooth 4.0 не имеет обратной совместимости с предыдущими версиями. Сверхнизкое энергопотребление достигается за счет использования специального алгоритма работы. Передатчик включается только на время отправки данных, что обеспечивает возможность работы от одной батарейки типа CR2032 в течение нескольких лет. Стандарт предоставляет скорость передачи данных в 1 Мбит/с при размере пакета 8–27 байт. В новой версии два Bluetooth-устройства смогут устанавливать соединение менее чем за 5 мс и поддерживать его на расстоянии до 100 м. Для этого используется усовершенствованная коррекция ошибок, а необходимый уровень безопасности обеспечивает 128-битное шифрование.

Предполагается, что Bluetooth 4.0 будет конкурировать и вытеснять ZigBee в классе малопотребляющих радиочастотных устройств с поддержкой сложных сетей. Это также является ярким примером пересечения двух разных технологий, в данном случае — ZigBee и Bluetooth.

Проанализировав современное состояние технологии Bluetooth, можно обозначить плюсы и минусы. К достоинствам стандарта относятся:

- высокий уровень стандартизации и совместимость между устройствами Bluetooth разных производителей;
- защита передаваемых данных;
- низкая стоимость;
- высокая дальность действия (до 1000 м);
- универсальность и большое разнообразие модулей под разные задачи.

Среди недостатков отметим:

- Относительно высокое энергопотребление (работа от автономных источников питания не всегда возможна). Предполагается, что этого недостатка будет лишена новая версия спецификации Bluetooth 4.0.
- Относительно невысокая скорость обмена данными (до 1 Мбит/с). Как правило, реальная скорость обмена данными ограничивается пропускной способностью внешних аппаратных интерфейсов модуля.

Одно из основных преимуществ стандарта Bluetooth заключается в его высоком уровне стандартизации и широчайшем распространении в составе пользовательских электронных устройств. Это позволяет в ряде случаев практически в два раза сэкономить время и затраты на разработку при проектировании некоторой системы сбора данных, телеметрии или

управления на основе Bluetooth, поскольку в качестве одной из сторон беспроводного обмена данными может выступать, например, обычный серийно выпускаемый ноутбук или коммуникатор с поддержкой данной технологии.

Исходя из характерных особенностей модулей Bluetooth, сформировались их области применения в России и за рубежом:

- Автомобильная электроника. Модули Bluetooth могут использоваться в бортовых автомобильных системах контроля и управления. Эта область применения характерна для России.

- Системы удаленного управления и телеметрии. Здесь устройства Bluetooth могут использоваться наряду с модулями технологий Wi-Fi, ZigBee, Short Range RF 434/868 МГц. Данная область применения в равной степени актуальна как для России, так и для зарубежных стран.

Bluetooth

Ноутбуки, сотовые телефоны, смартфоны, торговые терминалы со встроенной функцией Bluetooth. Bluetooth - это современная технология беспроводной передачи данных, позволяющая соединять друг с другом практически любые устройства: мобильные телефоны, ноутбуки, принтеры, цифровые фотоаппараты и даже холодильники, микроволновые печи, кондиционеры. Соединить можно все, что соединяется (то есть имеет встроенный микрочип Bluetooth). Технология стандартизирована, следовательно, проблемы несовместимости устройств от конкурирующих фирм быть не должно.

Bluetooth - это маленький чип, представляющий собой высокочастотный (2.4 - 2.48 ГГц) приёмопередатчик, работающий в диапазоне ISM (Industry, Science and Medicine; промышленный, научный и медицинский). Для использования этих частот не требуется лицензия (исключения рассмотрим ниже). Скорость передачи данных, предусматриваемая стандартом, составляет порядка 720 Кбит/с в асимметричном режиме и 420 Кбит/с в полнодуплексном режиме. Обеспечивается передача трех голосовых каналов, но не видеосигнала. Энергопотребление (мощность передатчика) не должно превышать 10 мВт. Изначально технология предполагала возможность связи на расстоянии не более 10 метров. Сегодня некоторые фирмы предлагают микросхемы Bluetooth, способные поддерживать связь на расстоянии до 100 метров. Как радиотехнология, Bluetooth способна "обходить" препятствия, поэтому соединяемые устройства могут находиться вне зоны прямой видимости. Соединение происходит автоматически, как только Bluetooth-устройства оказываются в пределах досягаемости, причем не только по принципу точка - точка (два устройства), но и по принципу точка - много точек (одно устройство работает с несколькими

другими). Естественно, для реализации технологии Bluetooth на практике необходимо определенное программное обеспечение (ПО). Кстати, в новую версию операционной системы MS Windows Whistler встроена поддержка Bluetooth [17].

Передача данных Bluetooth

В стандарте Bluetooth предусмотрена дуплексная передача на основе разделения времени (Time Division Duplexing - TDD). Основное устройство передает пакеты в нечетные временные сегменты, а подчиненное устройство – в четные.

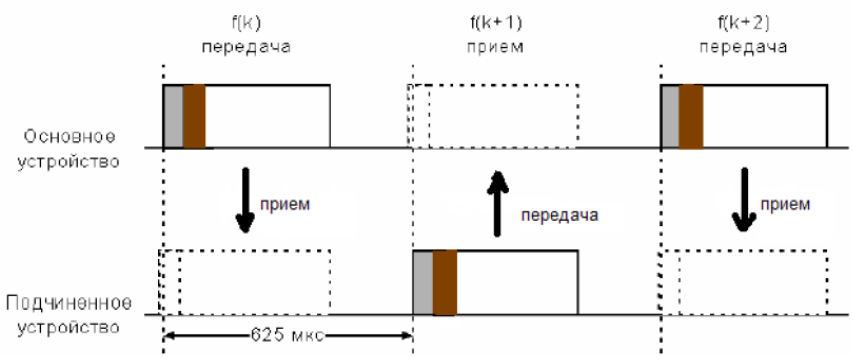


Рис. 3.87. Дуплексная передача с временным разделением

Пакеты в зависимости от длины могут занимать до пяти временных сегментов. При этом частота канала не меняется до окончания передачи пакета.

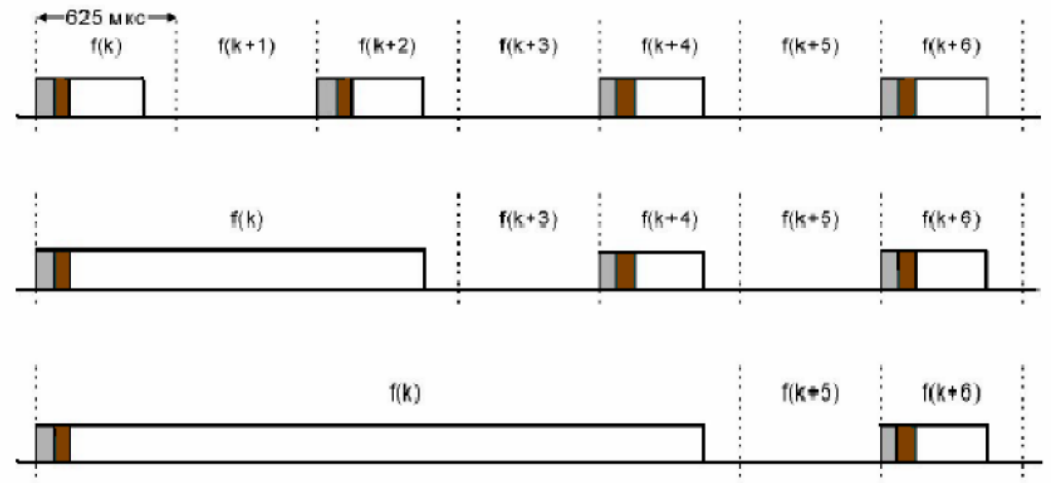


Рис. 3.88. Передача пакетов различной длины

Протокол Bluetooth может поддерживать асинхронный канал данных, до трех синхронных (с постоянной скоростью) голосовых каналов или канал с одновременной асинхронной передачей данных и синхронной передачей голоса. Скорость каждого голосового канала – 64 Кбит/с в каждом направлении, асинхронного в асимметричном режиме – до 723,2 Кбит/с в прямом и 57,6 кбит/с в обратном направлениях или до 433,9 Кбит/с в каждом направлении в симметричном режиме.

Структура пакета

Стандартный пакет Bluetooth содержит код доступа длиной 72 бита, 54-битный заголовок и информационное поле длиной не более 2745 бит. Однако пакеты могут быть различных типов. Так, пакет может состоять только из кода доступа (в этом случае его длина равна 68 битам) или кода доступа и заголовка.

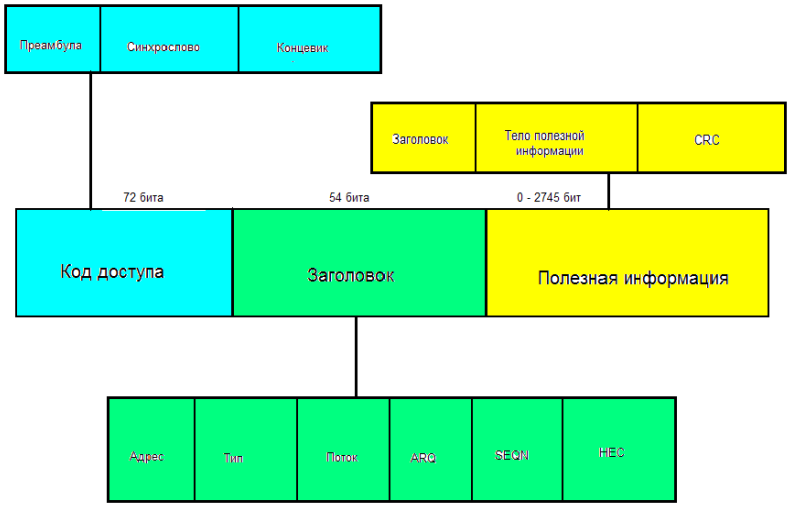


Рис. 3.89. Структура пакета

Код доступа идентифицирует пакеты, принадлежащие одной пикосети, а также используется для синхронизации и процедуры запросов. Он включает преамбулу (4 бита), синхрослово (64 бита) и концевик – 4 бита контрольной суммы.

Заголовок содержит информацию для управления связью и состоит из шести полей:

- Адрес (3 бита) - адрес активного элемента;
- Тип (4 бита) - код типа данных;
- Поток (1 бит) - управление потоком данных, показывает готовность устройства к
- приему;
- ARQ (1 бит) - подтверждение правильного приема;
- SEQN (1 бит) - служит для определения последовательности пакетов;
- HEC (8 бит) - контрольная сумма.

Заключительной частью общего формата пакета является **полезная информация**. В этой части есть два типа полей: поле голоса (синхронное) и поле данных (асинхронное). ACL пакеты имеют только поле данных, а SCO пакеты – только поле голоса. Исключением является пакет данных и голоса (Data Voice - DV), который имеет оба поля. Поле данных состоит из трех сегментов: заголовок полезной информации, тело полезной информации и возможно, CRC (Cyclic Redundancy Check) код.

- Заголовок полезной информации (8 бит). Только поля данных имеют заголовокполезной информации. Он определяет логический канал, управление потоком в логических каналах, а также имеет указатель длины полезной информации.
- Тело полезной информации (0-2721 бит). Тело полезной информации включает пользовательскую информацию. Длина этого сегмента указана в поле длины заголовка полезной информации.
- CRC (16 бит). От передаваемой информации вычисляется 16-битный циклический избыточный код (CRC), после чего он прикрепляется к информации.

Существует 4 типа контрольных пакетов: NULL, POLL, FHS, ID. Они одинаковые как для ACL, так и для SCO.

- ID-пакеты имеют длину 68 бит и применяются для пейджинга и запросов. Состоит из поля Код Доступа .
- NULL-пакеты (126 бит) состоят только из полей Код Доступа и Заголовок, играя роль подтверждений установления соединения или получения данных
- Тип POLL (126 бит) аналогичен предыдущему за исключением того, что POLL-пакеты обязывают получателя ответить.
- Пакеты FHS (366 бит) содержат информацию об адресе, классе устройства и тактовой частоте его передатчика

Работа Bluetooth

Есть два основных состояния для устройств Bluetooth: Соединение (Connection) и Режим ожидания (Standby). Предусмотрено семь субсостояний, которые используются для добавления клиента или подключения к пикосети: **page, page scan, inquiry, inquiry scan, master response, slave response** и **inquiry response**.

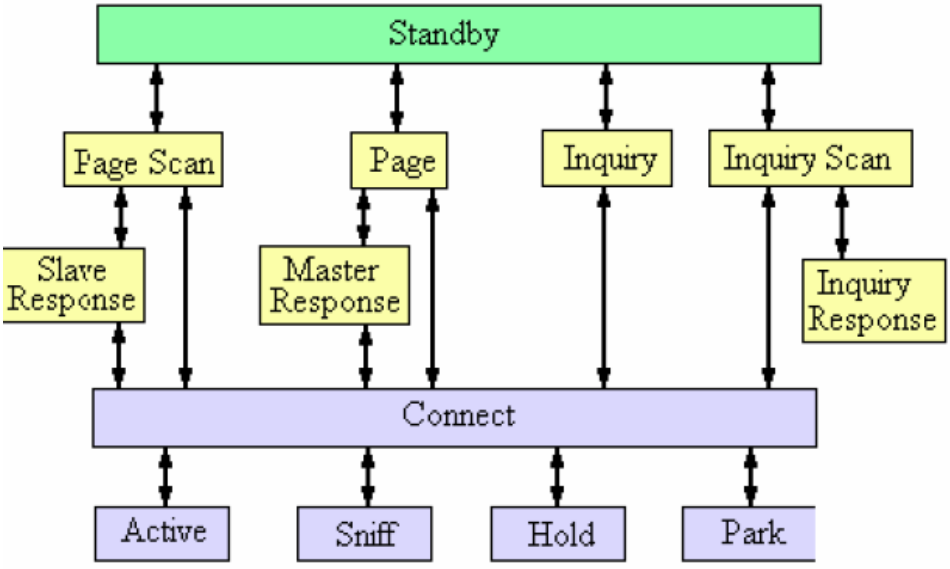


Рис. 3.60. Состояние соединений

Состояние Standby по умолчанию является режимом с пониженным энергопотреблением, работает только внутренний задающий генератор. В состоянии Соединения основной узел (master) и подчиненный (slave) могут обмениваться пакетами, используя код доступа к каналу.

Соединение между устройствами присходит так - если об удаленном устройстве ничего не известно, то используются процедуры inquiry и page. Если некоторая информация о устройстве все-таки есть, то достаточно процедуры page.

Этап 1

Процедура **inquiry** позволяет устройству определить, какие приборы доступны, выяснить адреса и осуществить синхронизацию.

1.1 Посылаются пакеты inquiry и получаются отклики.

1.2 Если адресат, получивший пакет inquiry, находится в состоянии inquiry scan , тогда он способен принимать такие пакеты

1.3 Получатель переходит в состояние inquiry response и посылает отправителю пакет-отклик.

После того как процедура inquiry завершена, соединение может быть установлено с помощью процедуры paging.

Этап 2

Процедура **paging** реализует соединение. Для осуществления этой процедуры необходим адрес. Устройство, выполняющее процедуру paging, атоматически становится хозяином этого соединения.

2.1 Посылается пакет paging

2.2 Адресат получет этот пакет (находится в состоянии page Scan)

2.3 Получатель посылает отправителю пакет-отклик (находится в состоянии Slave Response)

2.4 Инициатор посылает адресату пакет FHS (находится в состоянии Master Response).

2.5 Получатель посылает отправителю второй пакет-отклик (находится в состоянии Slave Response)

2.6 Получатель и отправитель устанавливают параметры канала заданные инициатором (находятся в состоянии Master Response & Slave Response)

После установления соединения основной узел (master) посылает пакет POLL, чтобы проверить, синхронизовал ли клиент свои часы и настроился ли на коммутацию частот. Клиент при этом может откликнуться любым пакетом. После успешного обнаружения устройств новое Bluetooth устройство получает набор адресов доступных Bluetooth устройств, после чего выясняет имена всех доступных Bluetooth устройств из списка. У

каждого Bluetooth устройства есть свой глобально уникальный адрес, но на уровне пользователя обычно используется не этот адрес, а имя устройства, которое может быть любым, и ему не обязательно быть глобально уникальным. Имя Bluetooth устройства может быть длиной до 248 байт, и использовать кодовую страницу в соответствии с Unicode UTF-8 (при использовании UCS-2, имя может быть укорочено до 82 символов). Также у Bluetooth есть возможность автоматического подключения Bluetooth устройств к службам, предоставляемым другими Bluetooth устройствами. Поэтому, после того как имеется список имён и адресов, выполняется поиск доступных услуг, предоставляемых различными устройствами. Для поиска возможных услуг используется специальный протокол обнаружения услуг (Service Discovery Protocol - SDP).

Устройство Bluetooth при установлении соединения может работать в четырех режимах: **Active** (активный), **Hold** (удержание)**, Sniff** (прослушивание) и **Park** (пассивный).

Таблица 3.12. Режимы работы Bluetooth

Название режима	Описание
Active	В активном режиме устройство Bluetooth участвует в работе канала. Основной узел (master) диспетчеризует обмены на основе запросов трафика, поступающих от участников. Кроме того, этот режим предусматривает регулярные обмены с целью синхронизации клиентов. Активные клиенты прослушивают домены master-to-slave пакетов. Если к активному клиенту нет обращений, он может пребывать в пассивном состоянии (sleep) до очередной передачи со стороны главного узла
Sniff	Устройства синхронизованные в рамках пикосети могут перейти в режим экономного расходования энергии, когда их активность понижается. В режиме **SNIFF**, подчиненное устройство прослушивает пикосеть с пониженной частотой. Этот режим имеет наивысшую скважность рабочего цикла (наименьшая экономия энергии) из 3 экономичных режимов (**sniff, hold** и **park**)
Hold	Устройства синхронизованные в рамках пикосети могут перейти в режим экономного расходования энергии, когда их активность понижается. Основной узел пикосети может перевести клиента в режим HOLD, когда работает только внутренний таймер. Подчиненное устройство может запросить перевода в режим HOLD. Передача данных возобновляется мгновенно, когда

	устройство выходит из режима HOLD. Клиент имеет промежуточную скважность (промежуточный уровень экономии энергии) из указанных 3 режимов (sniff, hold и park)
Park	В режиме PARK, устройство еще синхронизовано в рамках пикосети, но не принимает участия в обменах. Пассивные устройства отказываются от своих MAC-адресов, прослушивают трафик главного модуля с целью ресинхронизации и отслеживают широковещательные сообщения. Данный режим имеет минимально возможную скважность (максимальная экономия энергии) из указанных 3 режимов (sniff, hold и park). Устройства, находящиеся в режиме park, должны посылать пакеты широковещательно, так как лишены собственного активного адреса.

"Частотный конфликт"

Тот факт, что частотный диапазон 2.4 ГГц свободен от лицензирования, вносит определенные сложности в использование Bluetooth-устройств. В этом диапазоне работают также различные медицинские приборы, бытовая техника, беспроводные телефоны, беспроводные локальные сети стандарта IEEE. Вполне логично предположить, что они могут "конфликтовать" друг с другом. Во избежание интерференции с другими беспроводными устройствами Bluetooth работает по принципу скачкообразной перестройки частоты (1600 скачков в секунду). Переход с одной частоты на другую происходит по псевдослучайному алгоритму. Это позволяет "освободить" нужные другим устройствам частоты[3].

Моделирование Bluetooth

Модель состоит из трех основных блоков:

1 Передатчик;

2 Канал;

3 Приемник.

Канал имеет три режима работы:

1 Нет канала;

2 AWGN канал;

Также имеется генератор сигнала стандарта 802.11, который как раз может конфликтовать с сигналами Bluetooth, для чего и применяется скачкообразная перестройка частоты.

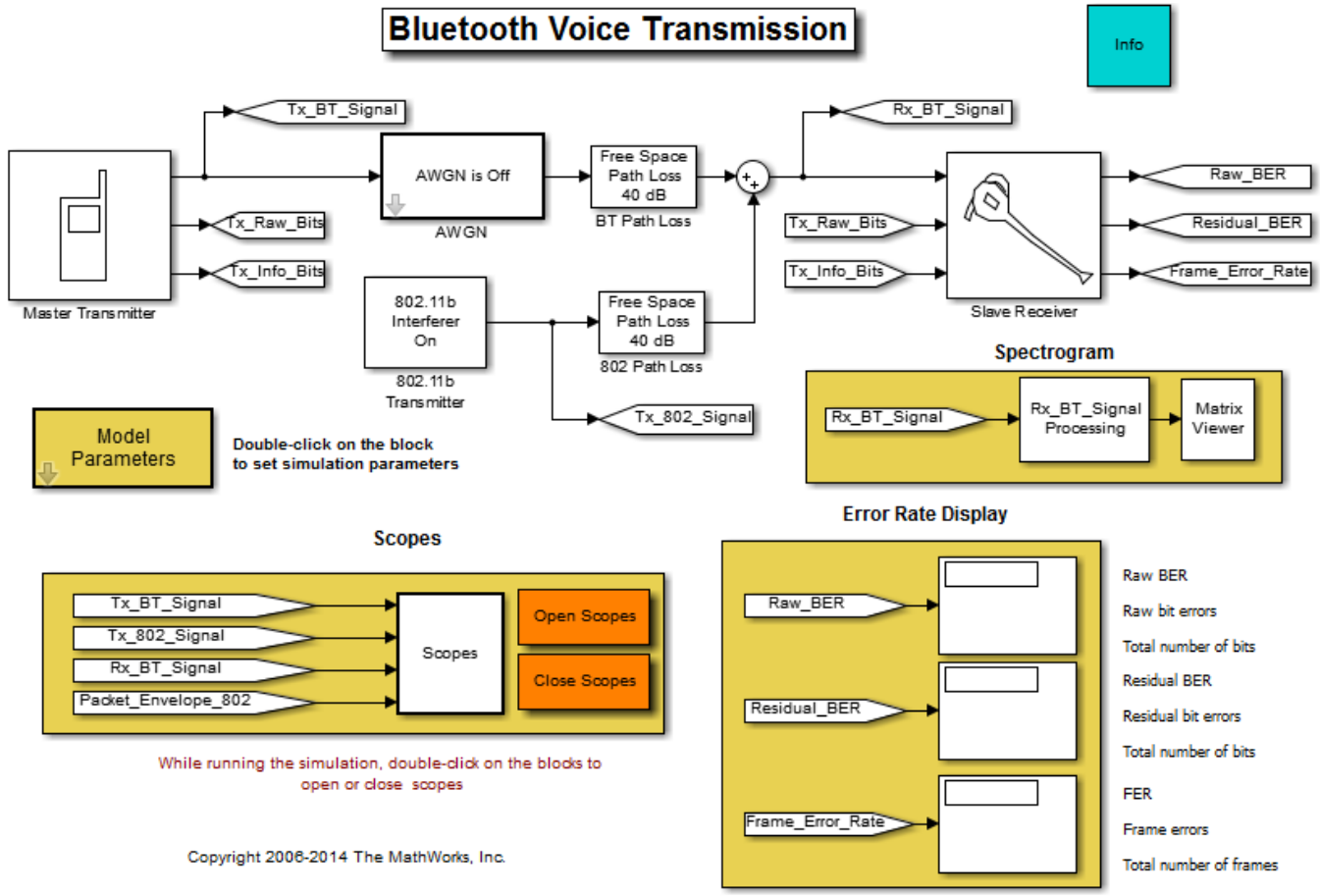


Рис. 3.61. Модель Bluetooth в MATLAB R2015b

Результаты моделирования.

В результате моделирования данной схемы система строит три графика: спектр сигнала, временную форму сигнала и зависимость изменения рабочей частоты во времени(скачкообразная перестройка). На графике ниже представлен спектр Bluetooth сигнала в один из моментов времени. Одним из минусов метода перестройки частоты в системе Bluetooth являются задержки, которые хорошо видны на данной диаграмме при моделировании, также о них будет сказано ниже.

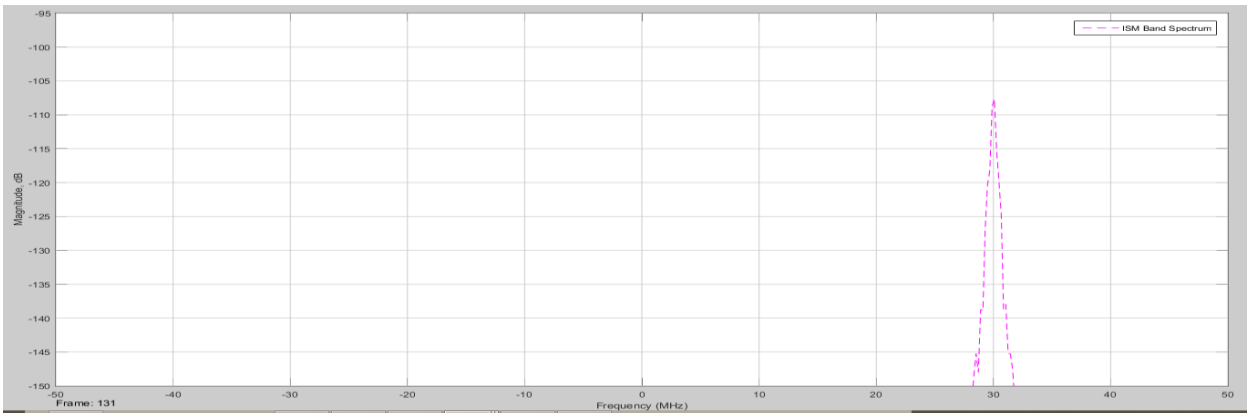


Рис. 3.61. Спектр Bluetooth без мешающего сигнала 802.11

Временная форма сигнала представляет просто набор битов, как и во многих современных системах связи. О значениях каждого бита(структуре кадра) была сказано ранее.

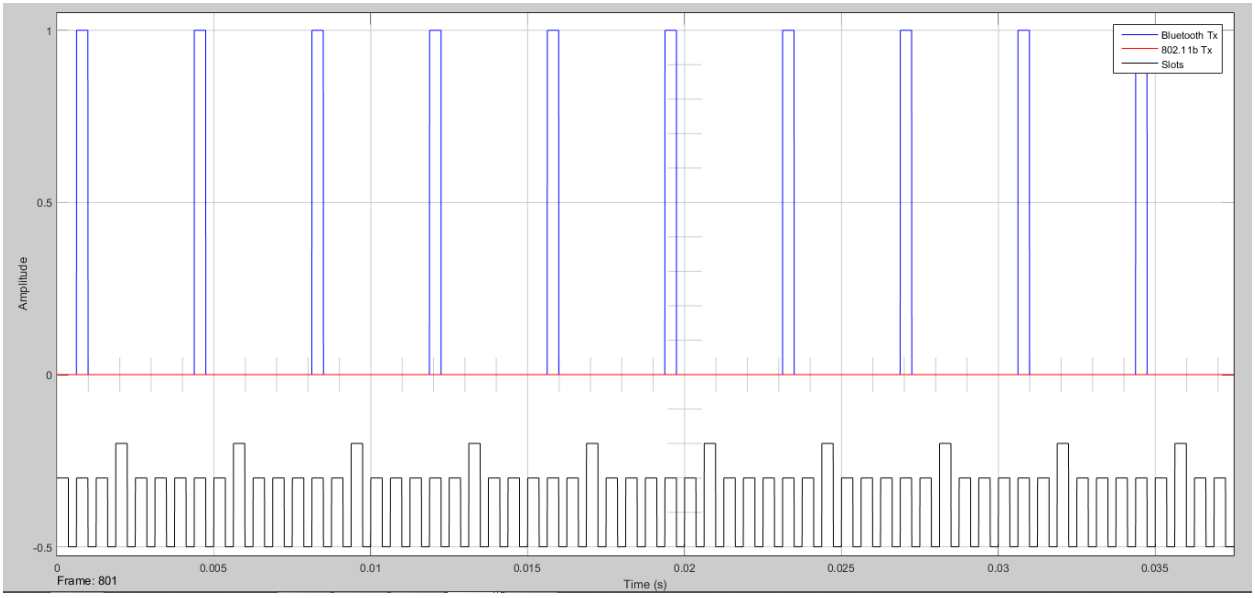


Рис. 3.62. Временная диаграмма Bluetooth без мешающего сигнала 802.11

На рисунке 3.63 хорошо видно изменение частоты от времени. На рисунке на оси абсцисс представлена частота, а на оси ординат время. Видно, что по оси времени перестройка с одной частоты на другую занимает определенное время, что относят к недостаткам системы Bluetooth.

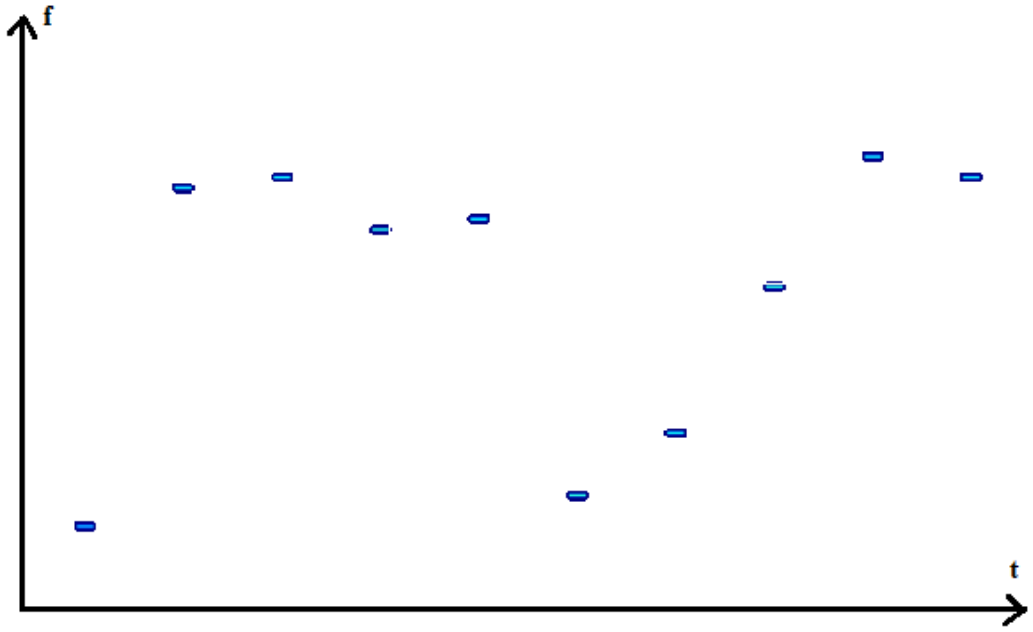


Рис. 3.63. Пример скачков частоты Bluetooth во времени без мешающего сигнала 802.11(WiFi)

На рисунке 3.64 представлен спектр вместе с мешающим сигналам. Здесь прекрасно видно, почему для построения системы Bluetooth был выбран алгоритм FHSS, который позволяет ему работать в одном диапазоне частот со стандартом 802.11 не мешая друг другу.

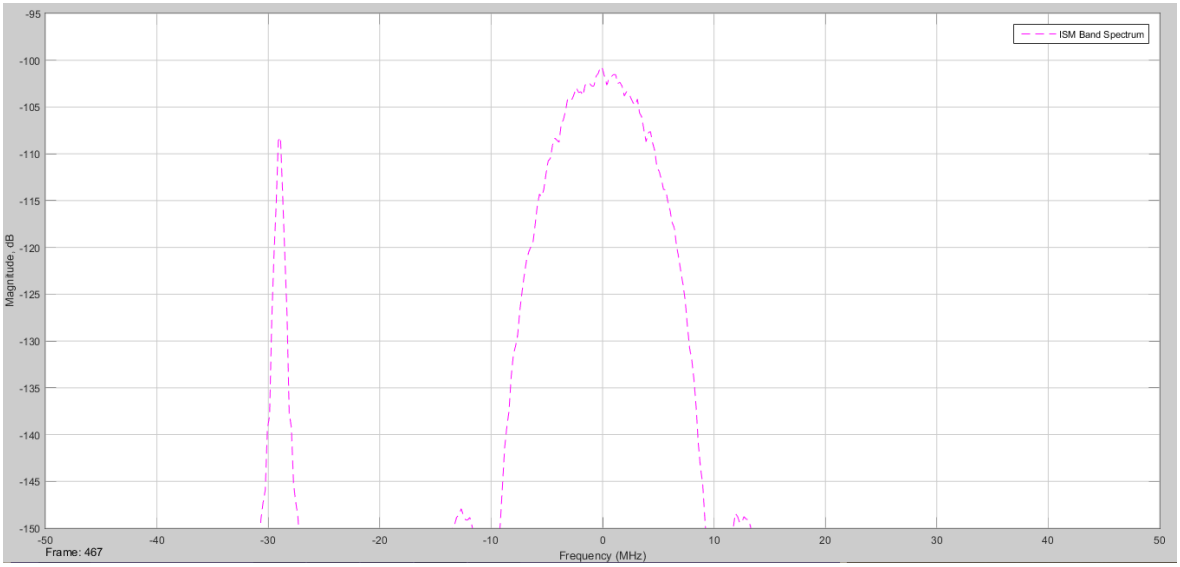


Рис. 3.64. Спектр Bluetooth с мешающим сигналом 802.11

Благодаря тому, что спектры сигналов разнесены в частотной области перекрытие их во временной, не играет большой роли, т.к. сигналы можно без проблем разделить.

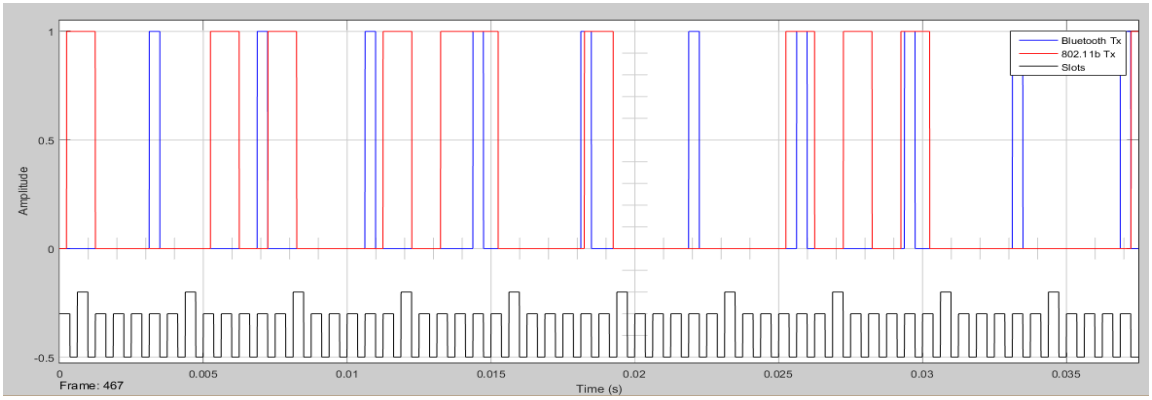


Рис. 3.65. Временная диаграмма Bluetooth с мешающим сигналом 802.11

Из рисунка ниже прекрасно видно, что во время работы устройства стандарта 802.11 рабочая частота системы Bluetooth находится достаточно далеко по спектру, а в некоторые моменты занимает свободный диапазон стандарта 802.11

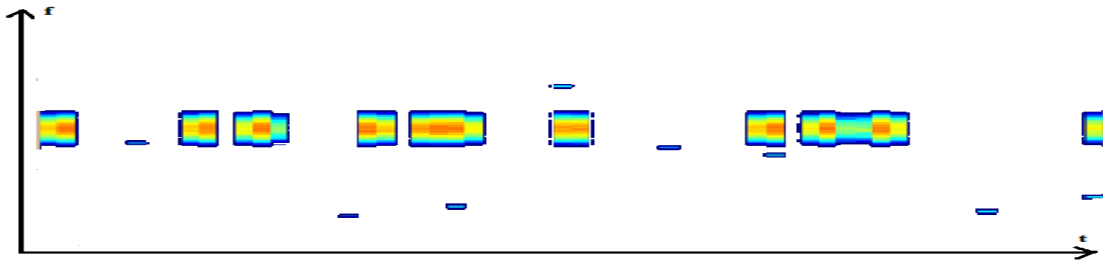


Рис. 3.66. Пример скачков частоты Bluetooth во времени с мешающим сигналом 802.11

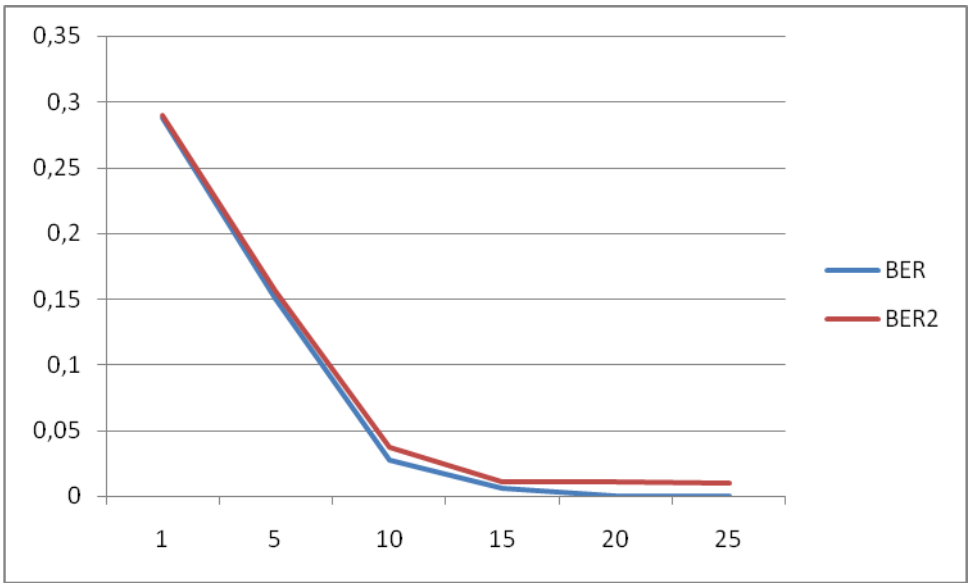


Рис. 3.67. Зависимость BER от SNR. Красным цветом (верхняя кривая) выделен график при включенном мешающем сигнале 802.11

Благодаря алгоритму FHSS система не сильно подвержена влиянию других стандартов передачи данных, работающих в том же диапазоне частот.

В разделе покана технология передачи данных 802.15.1 Bluetooth, а также использована модель передачи звука по такой системе в системе Simulink.

С помощью модели были построены временная диаграмма сигнала, спектр и FHSS спектр сигнала BLUETOTH при воздействии мешающего сигнала и без него. Также была построена зависимость BER от SNR.

На основе графиков зависимости BER от SNR (рисунок 5.67) видно,что мешающий сигнал 802.11 оказывает незначительное влияние на передачу данных. На рисунке 5.66 видно, что во время передачи сигнала 802.11, сигнал Bluetooth совершает скачок на другую частоту, что также хорошо видно на рисунке 3.64.

3.6. Имитационное моделирование системы мобильной связи стандарта IEEE 802.16 (WiMAX)

Существующие системы проводной цифровой связи уже не могут в полной мере удовлетворять растущим потребностям высокоскоростного широкополосного доступа. Важнейшими их недостатками являются длительные сроки прокладки, сложности расширения, высокие затраты, проблема "последней мили". Основной и является так называемая проблема "последней мили". Высокоскоростные цифровые соединительные линии DSL (Digital Subscriber Line) не снимают этой проблемы.

Технология WiMAX позволяет разрешить эту проблему в кратчайшие сроки, так как не требует прокладки соединительных линий к зданиям. Значительно проще развернуть по

городу сеть базовых станций (наподобие сети станций сотовой связи). Каждая базовая станция в типовом варианте покрывает зону радиусом 6—8 км (возможны зоны радиусом до 30—50 км). В этой зоне каждая базовая станция (BS) по схеме "точка-многоточка" способна передавать/принимать сигналы от сотен зданий, внутри которых находится телекоммуникационное оборудование пользователей.

Под аббревиатурой WiMAX (Worldwide Interoperability for Microwave Access) понимается технология операторского класса с высоким качеством сервиса, которая основана на семействе стандартов IEEE 802.16, разработанных международным институтом инженеров по электротехнике и электронике (IEEE). Обеспечивает мультисервисность, гибкое распределение частот, задание приоритетов различным видам трафика, возможность обеспечения разного уровня качества (QoS), поддержка интерфейсов IP. Эта технология позволяет параллельно передавать голос, мультимедийную информацию и цифровые данные по одному каналу связи. Важным преимуществом является возможность быстро наращивать емкость и расширять территорию связи.

Технология WiMAX представляет прекрасную возможность обеспечивать беспроводной доступ всем пользователям цифрового оборудования, включая оборудование беспроводных локальных сетей, технологии Wi-Fi, к глобальным сетям, являясь связующим звеном между локальными сетями и глобальными сетями.

2 Теоретическая часть. Общие принципы построения сетей WiMAX

2.1 Стандарты IEEE 802.16. Форум WiMAX.

При переходе к созданию систем широкополосного радиодоступа с интеграцией услуг стало понятно, что основополагающие принципы, заложенные в беспроводные системы на предыдущих этапах, нуждаются в существенной корректировке. На сигнальном уровне первостепенное значение приобрело оптимальное использование спектрального ресурса радиоканала при любых соотношениях “скорость - помехоустойчивость”. На уровне протоколов стало необходимым обеспечивать заданный уровень качества обслуживания каждому абоненту сети.

Основным преимуществом сетей WiMAX по сравнению с другими технологиями, призванными решать аналогичные задачи, является относительно быстрое развертывание систем на достаточно больших территориях без проведения работ по прокладке кабеля и предоставление конечным пользователям каналов связи в единицы Мбит/с, что особенно актуально для мест с неразвитой сетевой инфраструктурой. Основным конкурентом сетей WiMAX являются системы связи четвертого поколения LTE E UTRA.

На сегодняшний день беспроводные сети городского масштаба представлены следующими стандартами:

- IEEE 802.16e-2005, 2009 (WiMAX);
- ETSI HiperMAN;
- IEEE 802.20 (WBWA).

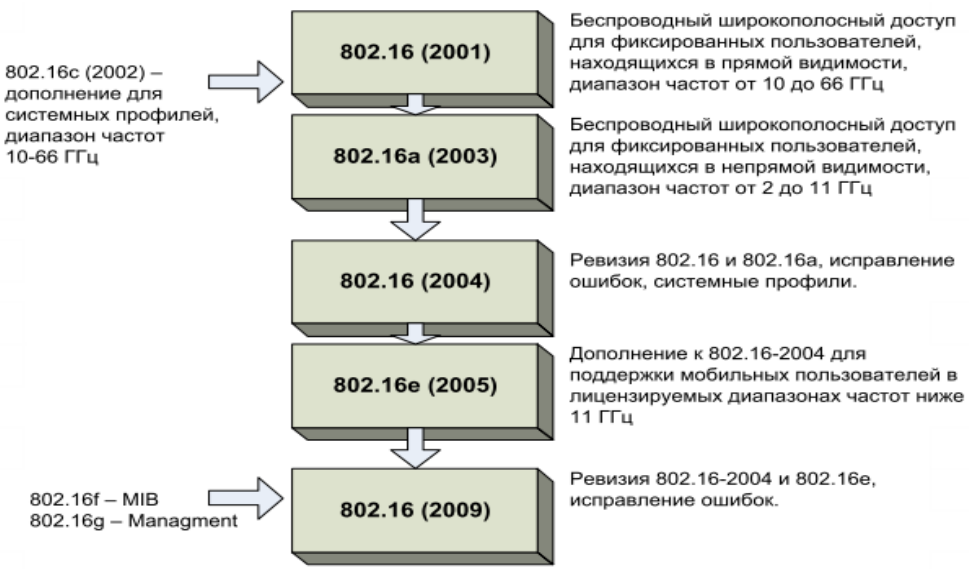


Рисунок 3.1 – Эволюция стандартов IEEE 802.16

Таблица 3.1 – Краткие характеристики стандартов, входящих в семейство IEEE 802.16

Название стандарта	**IEEE 802.16**	**IEEE 802.16a**	**IEEE 802.16e**
Частотный диапазон	10-66 ГГц	2-11 ГГц	2-6 ГГц
Скорость передачи информации	32-135 Мбит/с	до 75 Мбит/с	до 15 Мбит/с
Модуляция	QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM
Ширина полосы частот	20, 25 и 28 МГц	Регулируемая 1,5 – 20 МГц	Регулируемая 1,5 – 20 МГц
Радиус действия	2-5 км	7-10 км, макс. радиус 50 км	2-5 км
Условия работы	Прямая видимость	Работа на отраженных лучах	Работа на отраженных лучах

Для обеспечения работоспособности систем в диапазоне 10-66 ГГц, вследствие относительно малой длины волны, требуется наличие прямой видимости между передатчиком и приемником. В таких условиях при анализе канала связи многолучевостью среды можно пренебречь. Данные передаются на одной несущей. Ширина полосы частот одного канала составляет 20, 25 или 28 МГц, что позволяет достигать скорости передачи данных до 135 Мбит/с.

В диапазоне частот 2-11 ГГц за счет увеличения длины волны возможен сценарий взаимодействия передатчика и приемника в условиях отсутствия прямой видимости. При этом необходимо применять более сложные (по сравнению с системами, функционирующими в диапазоне частот 10-66 ГГц) методы регулировки мощности, различные способы борьбы с межсимвольной интерференцией. Для передачи данных используется одна или множество несущих (сигналы с OFDM).

Необходимо различать стандарты связи серии IEEE 802.16 (рисунок 2.1) и форум WiMAX (рисунок 2.2). Стандарты серии IEEE 802.16 — это множество стандартов, определяющих беспроводные сети городского масштаба (WMAN — Wireless Metropolitan Area Network), разработаны для обеспечения беспроводным широкополосным доступом стационарных и мобильных пользователей. Форум WiMAX является некоммерческой организацией для продвижения и сертификации устройств беспроводного широкополосного доступа, основанных на согласованном стандарте IEEE 802.16/ETSI HiperMAN. Сотрудничает с поставщиками услуг, производителями оборудования, производителями тестового оборудования, сертификационными лабораториями и поставщиками программно-аппаратных ресурсов для обеспечения соответствия ожиданиям заказчика и государственным стандартам.

Стандарты серии IEEE 802.16 определяет радиоинтерфейс для систем широкополосного беспроводного доступа (уровни MAC и PHY) с фиксированными и мобильными абонентами в диапазоне частот 1-66 ГГц, рассчитанных на внедрение в городских распределенных беспроводных сетях операторского класса. Сети, построенные на основе этих стандартов, займут промежуточной положение между локальными сетями (IEEE 802.11x) и региональными сетями (WAN), где планируется применение разрабатываемого стандарта IEEE 802.20. Указанные стандарты совместно со стандартом IEEE 802.15 (PAN — Personal Area Network) и IEEE 802.17 (мосты уровня MAC) образуют иерархию стандартов беспроводной связи.

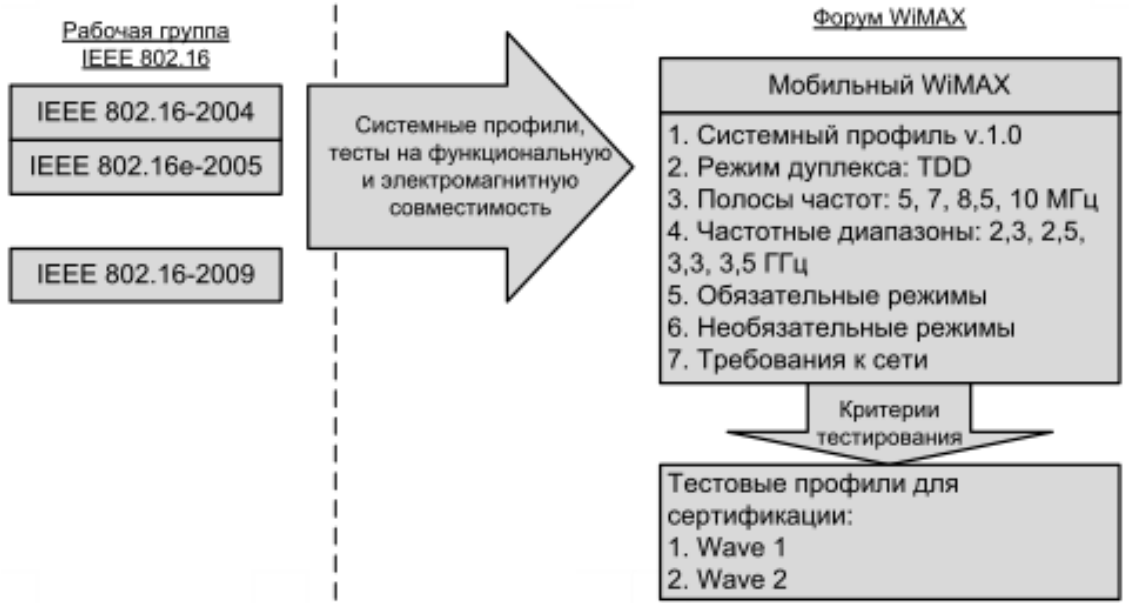


Рисунок 3.2 – Стандарты серии IEEE 802.16 и форум WiMAX

Структура стандартов IEEE 802.16 представлена на рисунке 2.3. Стандарты описывают MAC- и PHY- уровни семиуровневой эталонной модели взаимодействия открытых систем (ЭМВОС). При этом уровень MAC делится на подуровни конвергенции, общей части и безопасности.

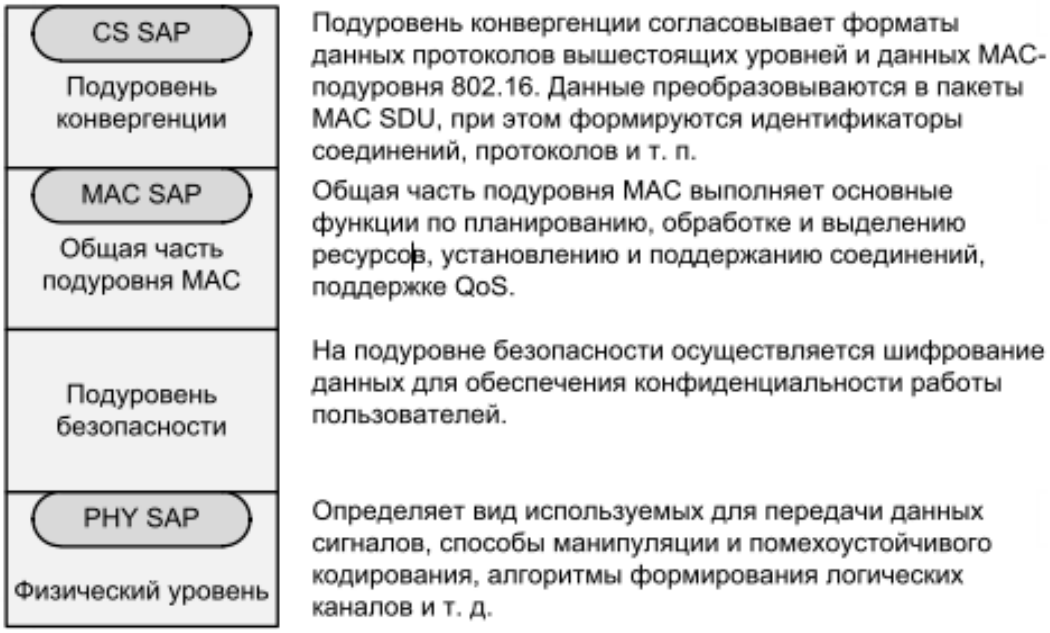


Рисунок 3.3 – Структура стандартов IEEE 802.16

Архитектура сетей WiMAX IEEE 802.16. Сетевой уровень

Базовая станция (БС, BS — Base Station) размещается в здании или на вышке и осуществляет связь с абонентскими станциями (АС, SS —Subscriber Station) по схеме — «точка – мультиточка» (Point to Multipoint —PMP). Возможен сеточный режим связи (Mesh — сетка связей — «точка – точка» — PTP), когда любые клиенты (АС) могут осуществлять связь между собой непосредственно, а антенные системы, как правило, являются

ненаправленными. БС предоставляет соединение с основной сетью и радиоканалы к другим станциям. Радиус действия БС может достигать 30 км (в случае прямой видимости) при типовом радиусе сети 6–8 км. АС может быть радиотерминалом или повторителем, который используется для организации локального трафика. Трафик может проходить через несколько повторителей, прежде чем достигнет клиента. Антенны в этом случае являются направленными.

Канал связи предполагает наличие двух направлений передачи: восходящий канал (АС – БС, uplink) и нисходящий (БС – АС, downlink). Эти два канала используют разные неперекрывающиеся частотные диапазоны при частотном дуплексе и различные интервалы времени при временном дуплексе.

Простейший способ представления архитектуры сетей WiMAX заключается в их описании как совокупности БС, которые располагаются на крышах высотных зданий или вышках, и клиентских приемо-передатчиков (рисунок 3.4).

Рисунок 3.4 – Схематичное изображение сети WiMAX

Радиосеть обмена данными между БС и АС работает в СВЧ-диапазоне от 2 до 11 ГГц. Такая сеть в идеальных условиях может обеспечить техническую скорость передачи информации до 75 Мбит/с и не требует того, чтобы БС находилась на расстоянии прямой видимости от пользователя.

Диапазон частот от 10 до 66 ГГц используется для установления соединения между соседними базовыми станциями при условии, что они располагаются в зоне прямой видимости друг от друга. Так как в городской среде это условие может оказаться

невыполнимым, связь между базовыми станциями иногда организуют посредством прокладки кабелей.

При более детальном рассмотрении сеть WiMAX можно описать как совокупность беспроводного и базового (опорного) сегментов. Первый описывается в стандарте IEEE 802.16, второй определяется спецификациями WiMAX Forum. Базовый сегмент объединяет все аспекты, не относящиеся к абонентской радиосети, то есть связь базовых станций друг с другом, связь с локальными сетями. Базовый сегмент основывается на IP-протоколе и стандарте IEEE 802.3-2005 (Ethernet). Однако само описание архитектуры в части, не относящейся к беспроводной клиентской сети, содержится в документах WiMAX Forum, объединенных под общим названием – "Network Architecture".

Таблица 3.2 – Основные режимы для стандарта IEEE 802.16 в РФ

Диапазон частот, ГГц	Разрешенные полосы частот, МГц	Общая ширина выделенных полос, МГц	Тип беспроводного доступа
2,5	2500 – 2530 2560 – 2570 2620 – 2630 2660 – 2670 2680 – 2690	70	мобильный
3,5	3400 – 3450 3500 – 3550	100	фиксированный
5	5150 – 5350 5650 – 5725 5725 – 6425	975	фиксированный

В этих спецификациях к сетям WiMAX предъявляются такие требования, как независимость архитектуры от функций и структуры транспортной IP-сети. В то же время, должны обеспечиваться услуги, основанные на применении IP-протокола, а также мобильная телефония на основе VoIP и мультимедийные услуги. Обязательным является условие поддержки архитектурой протоколов IPv4 и IPv6. Сети WiMAX должны быть легко масштабируемыми и гибко изменяемыми и основываться на принципе декомпозиции (строиться на основе стандартных логических модулей, объединяемых через стандартные интерфейсы). Свойства масштабируемости и гибкости необходимо обеспечивать по таким эксплуатационным характеристикам, как плотность абонентов, географическая протяженность зоны покрытия, частотные диапазоны, топология сети, мобильность абонентов. Сети WiMAX должны поддерживать взаимодействие с другими беспроводными

или проводными сетями. Большое значение имеет способность обеспечивать различные уровни качества обслуживания QoS.

Физический уровень WiMAX

На физическом уровне систем WiMAX над передаваемыми битами осуществляются следующие канальные процедуры (рисунок 2.5): скремблирование (рандомизация), помехоустойчивое кодирование, перемежение, кодирование повторением и модуляция.

Полученные модуляционные символы делятся на логические подканалы, и с использованием ОБПФ формируется отсчет передаваемого OFDMA-символа.

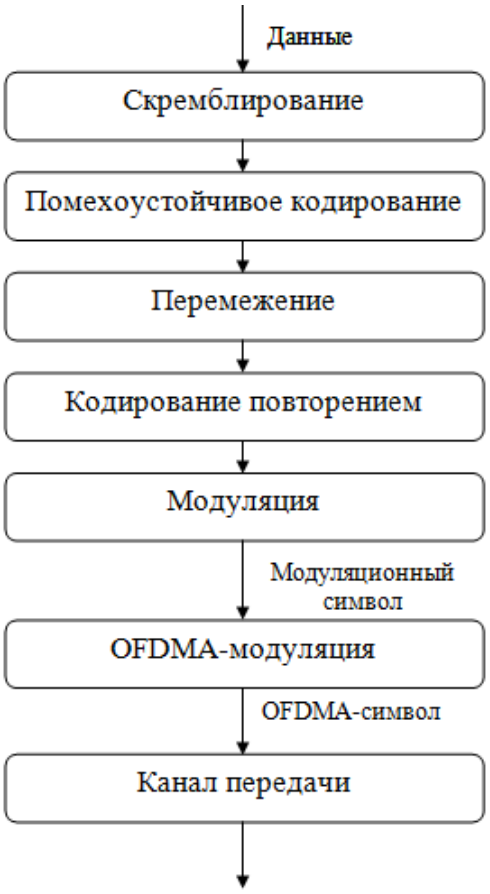


Рисунок 3.5 – Преобразования данных на физическом уровне WiMAX

На физическом уровне в стандарте IEEE 802.16-2004 определены три метода передачи данных: метод модуляции одной несущей (SC), метод ортогонального частотного мультиплексирования (OFDM) и метод множественного доступа на основе такого мультиплексирования (OFDMA) [2].

Спецификация физического уровня WirelessMAN-OFDM является наиболее интересной с точки зрения практической реализации. Она базируется на технологии OFDM, что значительно расширяет возможности оборудования, в частности, позволяет работать на относительно высоких частотах в условиях отсутствия прямой видимости. Кроме того, в нее включена поддержка топологии «каждый с каждым» (mesh) [3], при которой абонентские

устройства могут одновременно функционировать и как базовые станции, что сильно упрощает развертывание сети и помогает преодолеть проблемы прямой видимости.

Скремблирование

Скремблирование — это сложение по модулю два передаваемых битов с элементами ПСП, которую формирует генератор ПСП с задающим полиномом вида $x^{15} + x^{14} + 1$. Генератор ПСП инициализируется вектором 011011100010101.

Скремблирование осуществляется только над информационными битами Причем при скремблировании каждого блока данных, подлежащих помехоустойчивому кодированию, сдвигающий регистр скремблера инициализируется заново. Байты данных поступают на вход скремблера начиная со старшего значащего разряда.

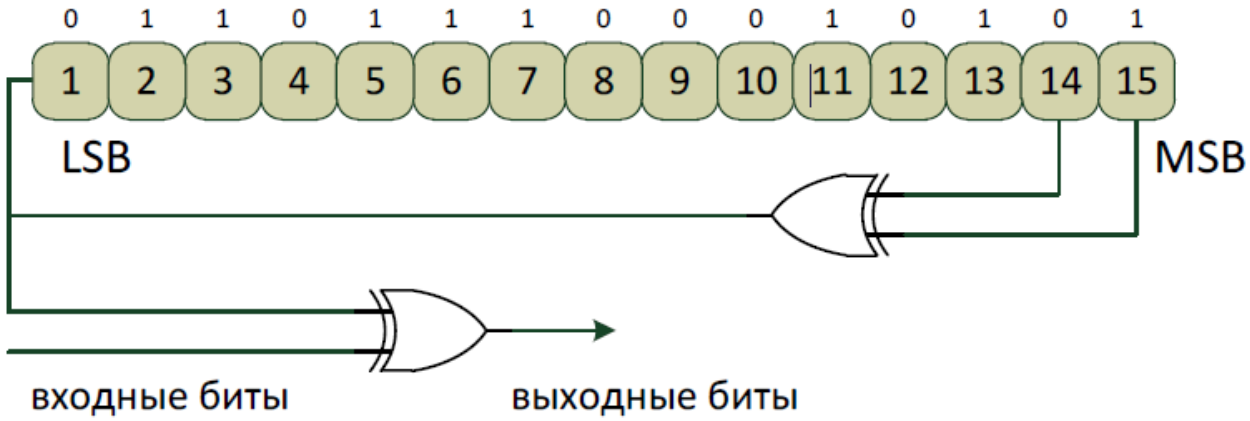


Рисунок 3.6 – Схема скремблера

Помехоустойчивое кодирование

Многолучевое распространение радиосигнала может приводить к ослаблению и даже полному подавлению некоторых поднесущих вследствие интерференции прямого и задержанного сигналов. Для решения этой проблемы используется помехоустойчивое кодирование. В стандарте IEEE 802.16-2004 предусмотрены как традиционные технологии помехоустойчивого кодирования, так и относительно новые методы. К традиционным относится сверточное кодирование с декодированием по алгоритму Витерби и коды Рида-Соломона. К относительно новым — блочные и сверточные турбокоды.

Перемежение

После осуществления скремблирования и помехоустойчивого кодиро-вания, над битами каждого блока должно быть выполнено двухэтапное пе-ремежение. Первый этап гарантирует, что соседние в исходной последова-тельности биты будут распределены не в соседние поднесущие. Второй этап обеспечивает распределение соседних битов или в наиболее, или в наименее значимые биты сигнального созвездия, что предотвратит дли-тельные последовательности наименее надежных битов.

Модуляция

В системах беспроводного широкополосного доступа используют сигналы как двоичной (ФМ-2), так и многопозиционной (ФМ-4, КАМ-16, КАМ-64 и т. п.) модуляции. Сигналы многопозиционной фазовой модуляции (МФМ) характеризуются высокой частотной эффективностью, однако при этом вследствие уменьшения евклидовых расстояний между сигнальными точками существенно снижается помехоустойчивость приема, что при фиксированной вероятности ошибки эквивалентно ухудшению энергетической эффективности. Сигналы КАМ являются некоторым компромиссом, выигрывая у МФМ по энергетической эффективности, но уступая по спектральной, что может компенсироваться применением помехоустойчивого кода. По этой причине в сетях WiMAX IEEE 802.16e-2005, 2009 применяются методы модуляции ФМ-2, ФМ-4, КАМ-16 и КАМ-64.

При отображении бит на сигнальную плоскость применяется манипуляционный код Грея. Соответствующие сигнальные созвездия представлены на рисунке 3.7.

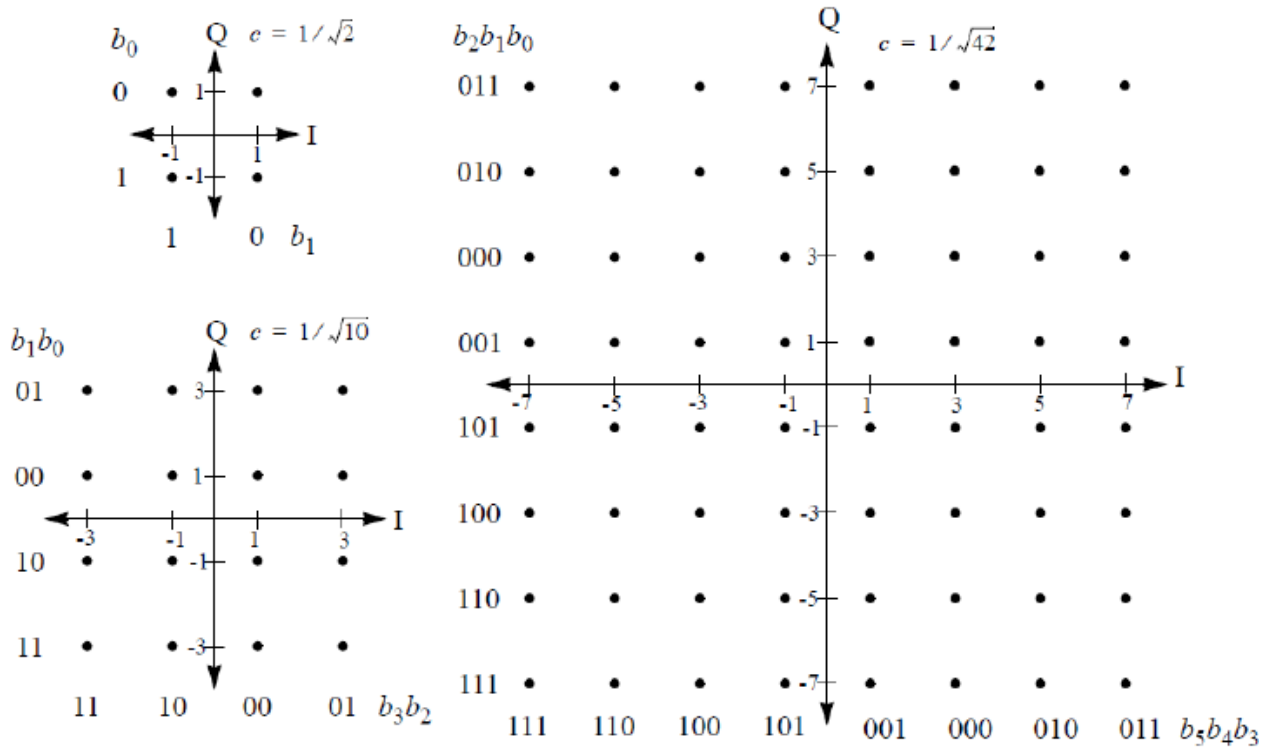


Рисунок 3.7 – Сигнальные созвездия, соответствующие методам модуляции ФМ-4, КАМ-16 и КАМ-64, IEEE 802.16e-2005

Модуляция OFDM

При формировании OFDM-сигнала [4] цифровой поток данных делится на несколько подпотоков, и каждая поднесущая связывается со своим подпотоком данных. Амплитуда и фаза поднесущей вычисляются на основе выбранной схемы модуляции. Согласно стандарту, отдельные поднесущие могут модулироваться с использованием бинарной фазовой манипуляции (BPSK), квадратурной фазовой манипуляции (QPSK) или квадратурной

амплитудной манипуляции (QAM) порядка 16 или 64. В передатчике амплитуда как функция фазы преобразуется в функцию от времени с помощью обратного быстрого преобразования Фурье (ОБПФ). В приемнике с помощью быстрого преобразования Фурье (БПФ) осуществляется преобразование амплитуды сигналов как функции от времени в функцию от частоты.

Применение преобразования Фурье позволяет разделить частотный диапазон на поднесущие, спектры которых перекрываются, но остаются ортогональными. Ортогональность поднесущих означает, что каждая из них содержит целое число колебаний на период передачи символа. Как видно на рисунке 2.8, спектральная кривая любой из поднесущих имеет нулевое значение для «центральной» частоты смежной кривой. Именно эта особенность спектра поднесущих и обеспечивает отсутствие между ними интерференции.

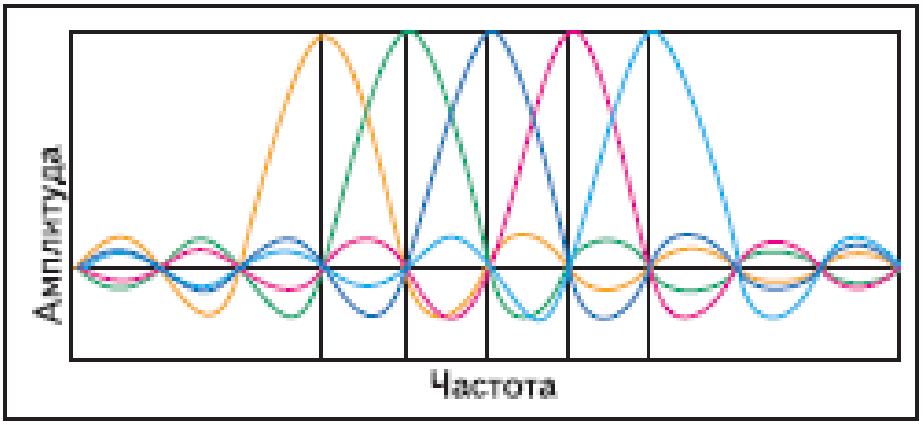


Рисунок 3.8 – Ортогональные поднесущие

Одним из главных преимуществ метода OFDM является его устойчивость к эффекту многолучевого распространения. Эффект вызывается тем, что излученный сигнал, отражаясь от препятствий, приходит к приемной антенне разными путями, вызывая межсимвольные искажения. Этот вид помех характерен для городов с разноэтажной застройкой из-за многократных отражений радиосигнала от зданий и других сооружений. Для того чтобы избежать межсимвольных искажений, перед каждым OFDM-символом вводится защитный интервал, называемый циклическим префиксом. Циклический префикс представляет собой фрагмент полезного сигнала, что гарантирует сохранение ортогональности поднесущих (но только в том случае, если отраженный сигнал при многолучевом распространении задержан не больше, чем на длительность циклического префикса). Кроме того, циклический префикс позволяет выбрать окно для преобразования Фурье в любом месте временного интервала символа (рисунок 3.9).

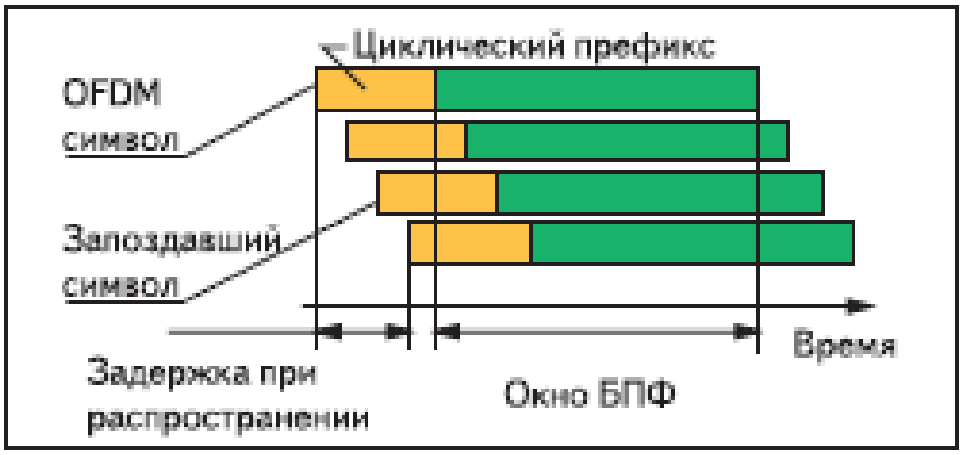


Рисунок 3.9– Обработка OFDM-символа при многолучевом распространении

Защита информации

В соответствии со стандартом, для предотвращения несанкционированного доступа и защиты пользовательских данных осуществляется шифрование всего передаваемого по сети трафика. Базовая станция (БС) WiMAX представляет собой модульный конструктив, в который при необходимости можно установить несколько модулей со своими типами интерфейсов, но при этом должно поддерживаться административное программное обеспечение для управления сетью. Данное программное обеспечение обеспечивает централизованное управление всей сетью. Логическое добавление в существующую сеть абонентских комплектов осуществляется также через эту административную функцию.

Абонентская станция (АС) представляет собой устройство, имеющее уникальный серийный номер, MAC-адрес, а также цифровую подпись X.509, на основании которой происходит аутентификация АС на БС. При этом, согласно стандарту, срок действительности цифровой подписи АС составляет 10 лет. После установки АС у клиента и подачи питания АС авторизуется на базовой станции, используя определенную частоту радиосигнала, после чего базовая станция, основываясь на перечисленных выше идентификационных данных, передает абоненту конфигурационный файл по TFTP-протоколу. В этом конфигурационном файле находится информация о поддиапазоне передачи (приема) данных, типе трафика и доступной полосе, расписание рассылки ключей для шифрования трафика и прочая необходимая для работы АС информация. Необходимый файл с конфигурационными данными создается автоматически, после занесения администратором системы АС в базу абонентов, с назначением последнему определенных параметров доступа.

После процедуры конфигурирования аутентификация АС на базовой станции происходит следующим образом:

1. Абонентская станция посылает запрос на авторизацию, в котором содержится сертификат X.509, описание поддерживаемых методов шифрования и дополнительная информация.

2. Базовая станция в ответ на запрос на авторизацию (в случае достоверности запроса) присылает ответ, в котором содержится ключ на аутентификацию, зашифрованный открытым ключом абонента, 4-битный ключ для определения последовательности, необходимый для определения следующего ключа на авторизацию, а также время жизни ключа.

3. В процессе работы АС через промежуток времени, определяемый администратором системы, происходит повторная авторизация и аутентификация, и в случае успешного прохождения аутентификации и авторизации поток данных не прерывается.

В стандарте используется протокол PKM (Privacy Key Management), в соответствии с которым определено несколько видов ключей для шифрования передаваемой информации:

- Authorization Key (АК) — ключ, используемый для авторизации АК на базовой станции;
- Traffi c Encryption Key (ТЕК) — ключ, используемый для криптозащиты трафика;
- Key Encryption Key (КЕК) — ключ, используемый для криптозащиты передаваемых в эфире ключей.

Согласно стандарту, в каждый момент времени используются два ключа одновременно, с перекрывающимися временами жизни. Данная мера необходима в среде с потерями пакетов (а в эфире они неизбежны) и обеспечивает бесперебойность работы сети. Имеется большое количество динамически меняющихся ключей, достаточно длинных, при этом установление безопасных соединений происходит с помощью цифровой подписи. Согласно стандарту, криптозащита выполняется в соответствии с алгоритмом 3-DES, при этом отключить шифрование нельзя. Опционально предусмотрено шифрование по более надежному алгоритму AES

Практическая часть. Описание экспериментальной установки и методики измерений

Работа выполняется с использованием симулятора физического уровня стандарта IEEE 802.16-2004 в программной среде Simulink. Для запуска программы, в командную строку MATLAB необходимо ввести "commwman80216dstbc" и нажать Enter.

Схема исследуемой системы приведена на рисунке 3.10.

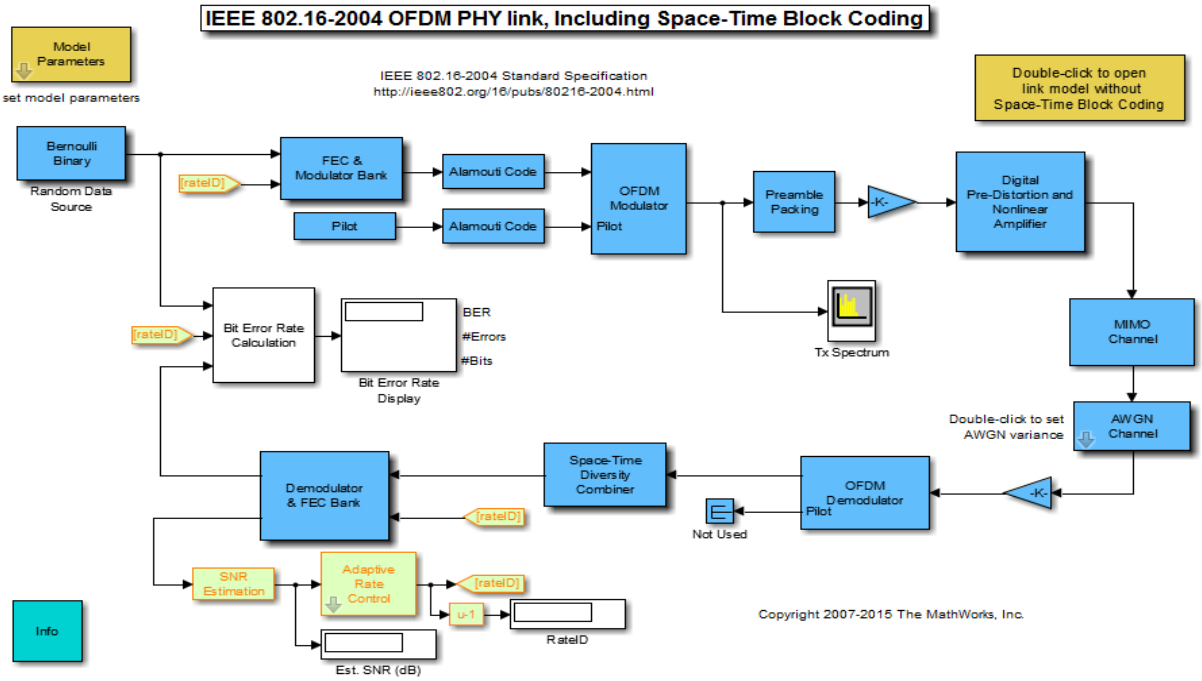


Рисунок 3.10 – Модель IEEE 802.16-2004 OFDM в MATLAB 2015b

Параметры источника случайной последовательности Bernulli Binary

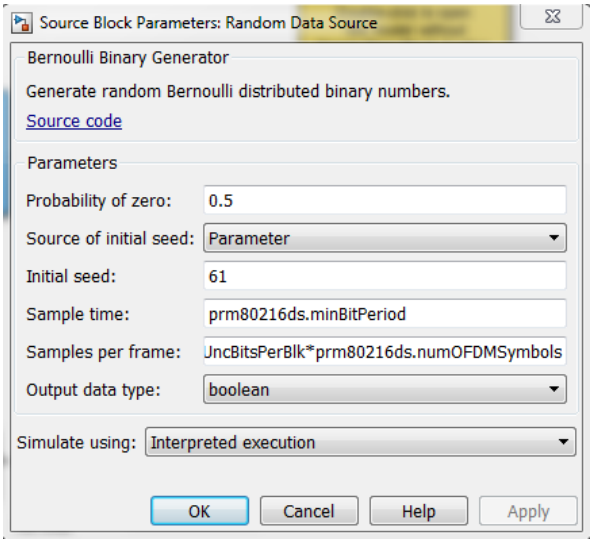


Рисунок 3.11 – Параметры блока Bernulli Binary

При проведении симуляции существует возможность изменения ряда параметров системы в следующих блоках:

Общие параметры модели (блок «Model Parameters», рисунок 3.12).

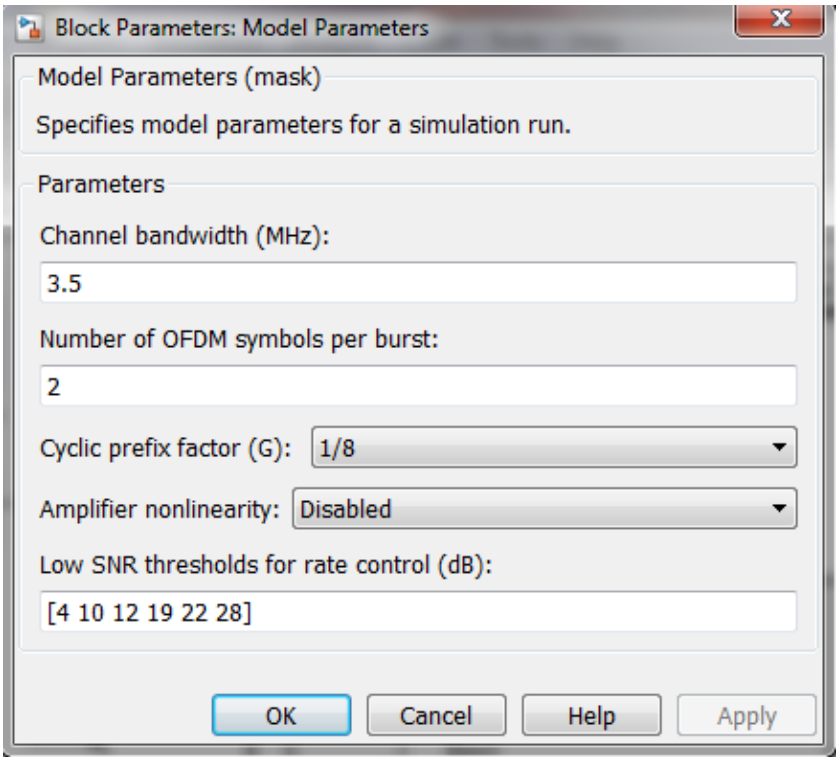


Рисунок 3.13 – Параметры системы, изменяемые в блоке «Model Parameters»

Блок помехоустойчивого кодирования и модуляции («FEC & Modulator Bank», рисунок 3.5) производит формирование сигнально-кодовой конструкции (СКК) определенного вида в зависимости от условий передачи.

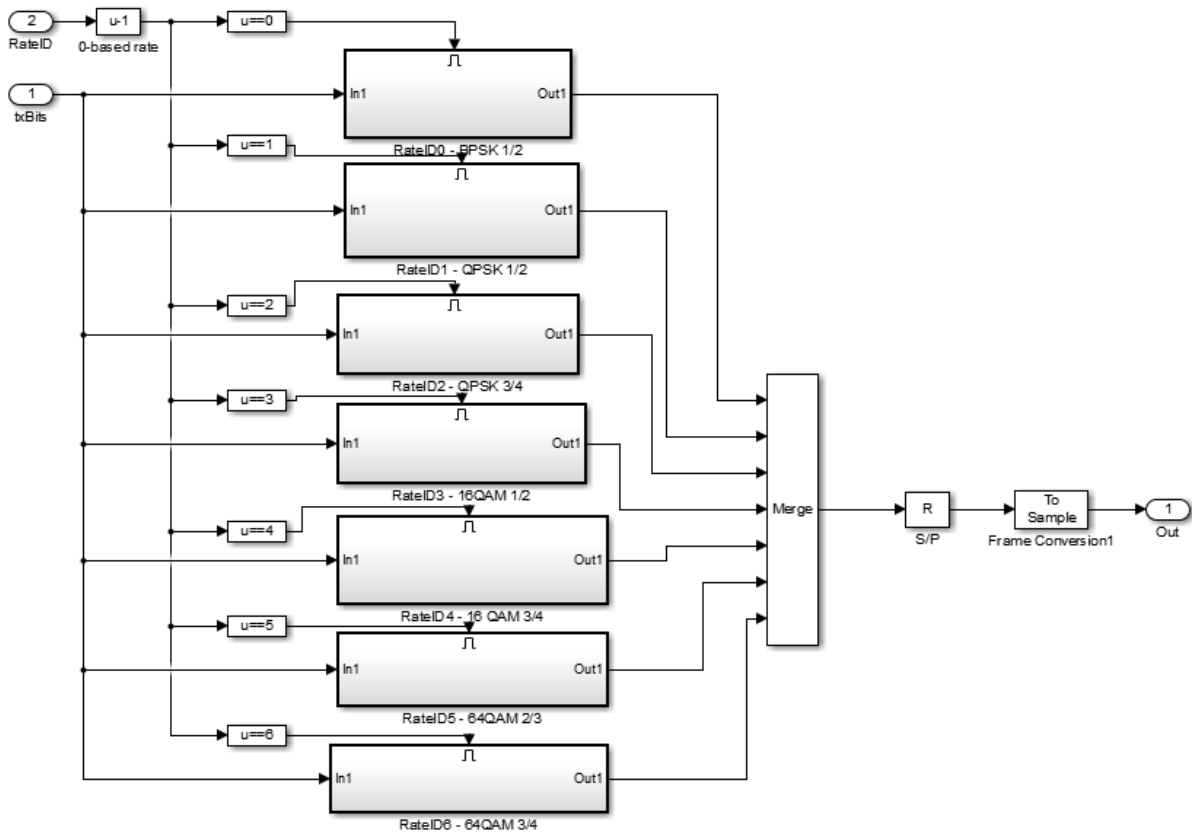


Рисунок 3.14 – Состав блока «FEC & Modulator Bank»

Рассмотрим состав каждого входящего блока:

Состав блока модулятора BPSK 1/2:

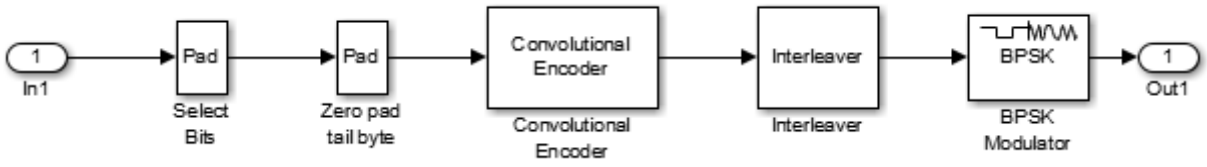


Рисунок 3.15 – Состав блока модулятора «BPSK 1/2»

Состав блока модулятора QPSK 1/2:

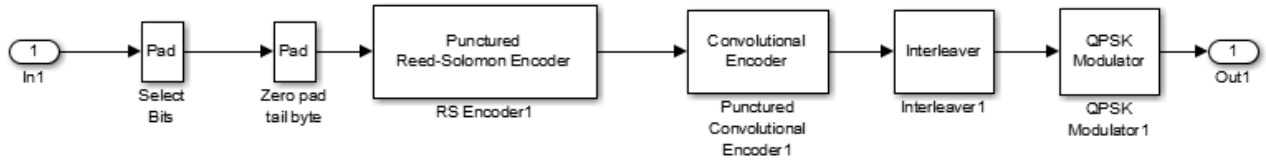


Рисунок 3.16 – Состав блока модулятора «QPSK 1/2»

Состав блока модулятора QPSK 3/4:

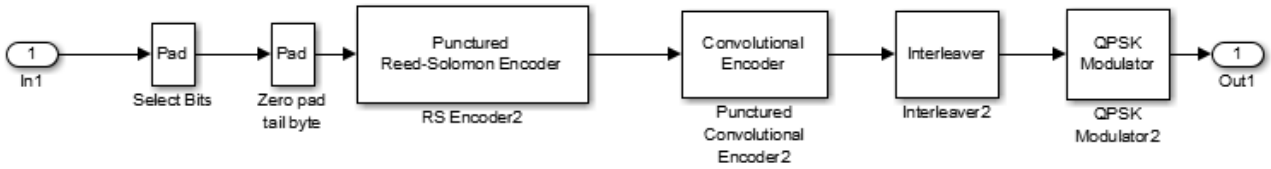


Рисунок 3.17 – Состав блока модулятора «QPSK 3/4»

Состав блока модулятора 16QAM 1/2:

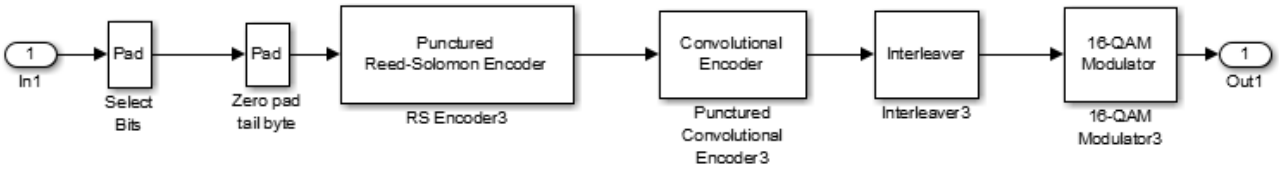


Рисунок 3.18 – Состав блока модулятора «16QAM 1/2»

Состав блока модулятора 16QAM 3/4:

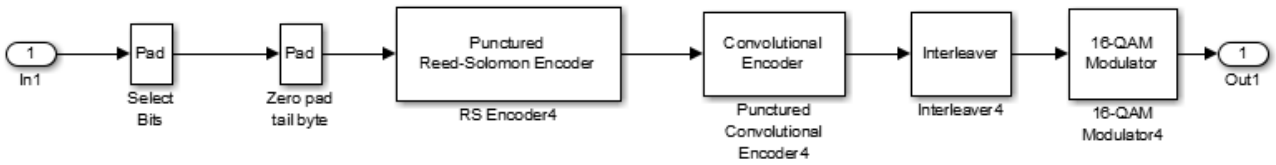


Рисунок 3.19 – Состав блока модулятора «16QAM 3/4»

Состав блока модулятора 64QAM 2/3:

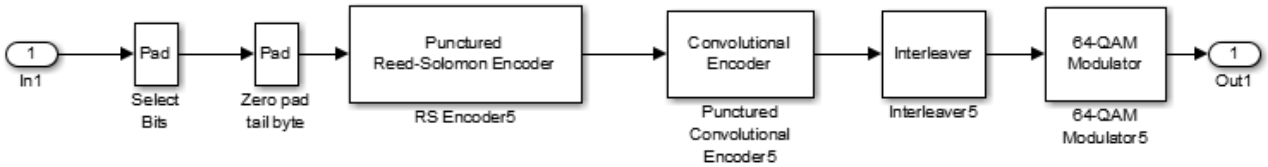


Рисунок 3.20 – Состав блока модулятора «64QAM 2/3»

Состав блока модулятора 64QAM 3/4:

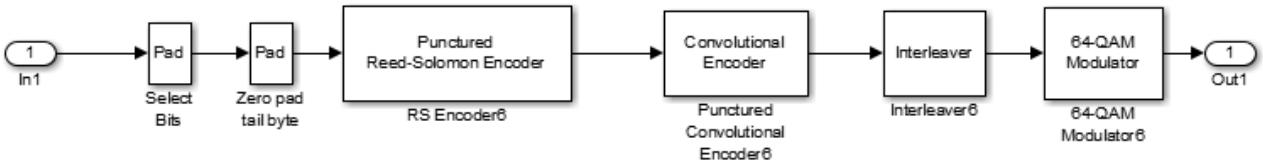


Рисунок 3.21 – Состав блока модулятора «64QAM 3/4»

Формирование сигнально-кодовых конструкций в каждом блоке происходит следующим образом: к поступающим информационным битам добавляется определяется «хвост» из нулевых бит, полученная последовательность кодируется блочным циклическим кодом Рида-Соломона. Следующий этап кодирования – сверточный код с использованием Треллис-структуры, затем, после перемежения, последовательность бит модулируется определенным образом для передачи по каналу.

В каждом из блоков на рисунках используется одинаковая последовательность блоков, отличающихся своими параметрами. Например для блока «16QAM 1/2» блоки имеют параметры.

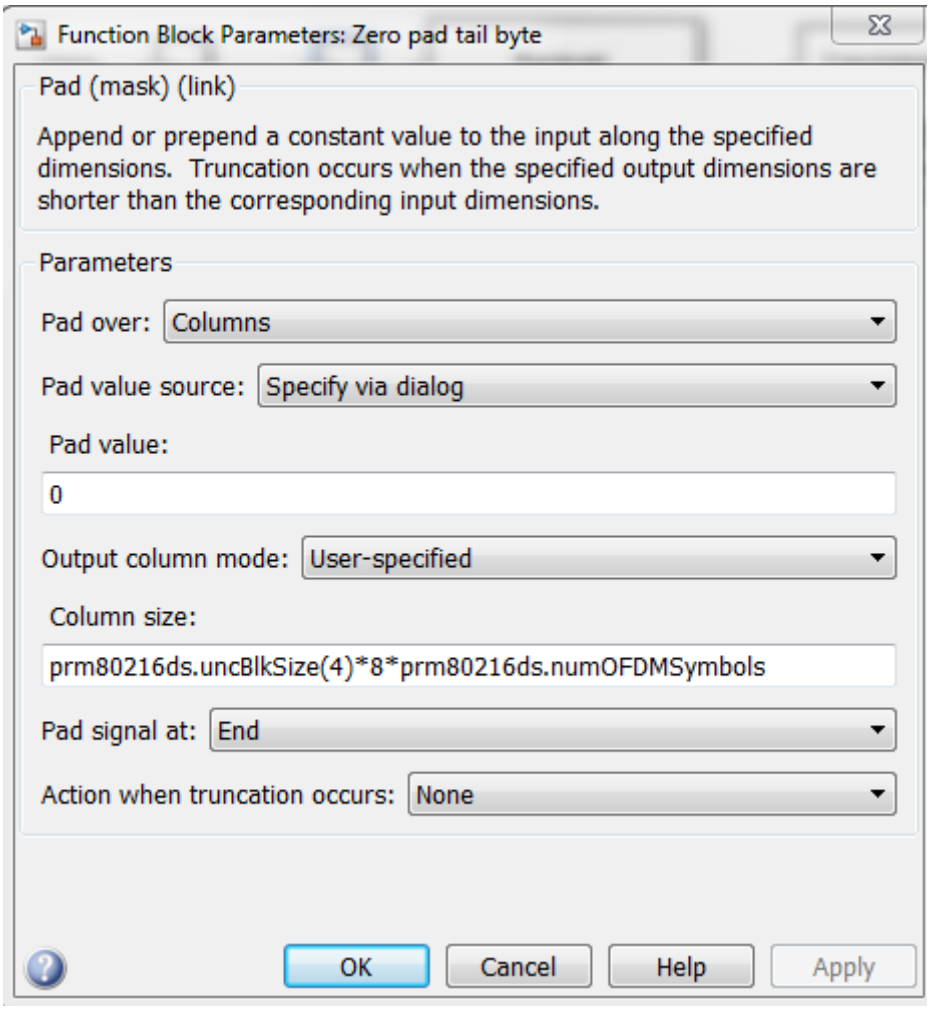


Рисунок 3.22 – Состав блока «Zero pad tail byte 16QAM 1/2»

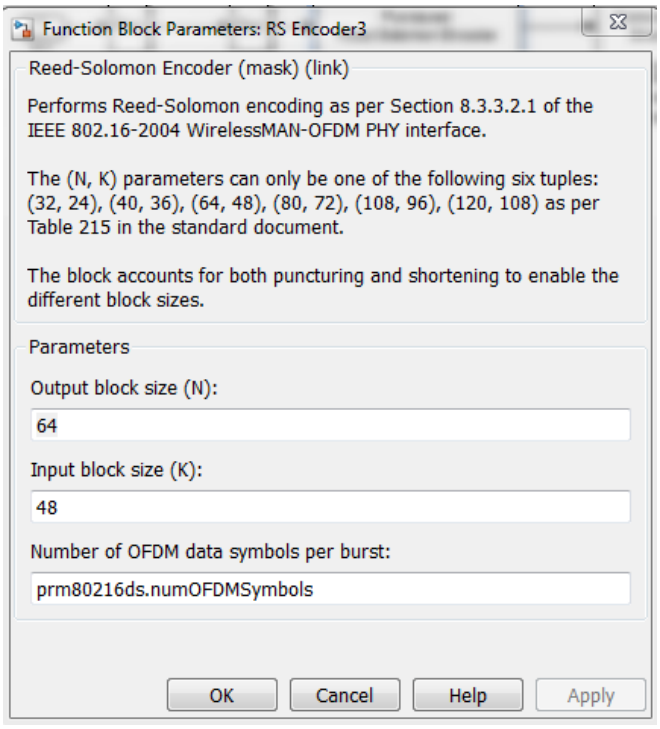


Рисунок 3.23 – Состав блока кодера Рида-Соломона «Puncured Reed-Solomon Encoder 16QAM 1/2»

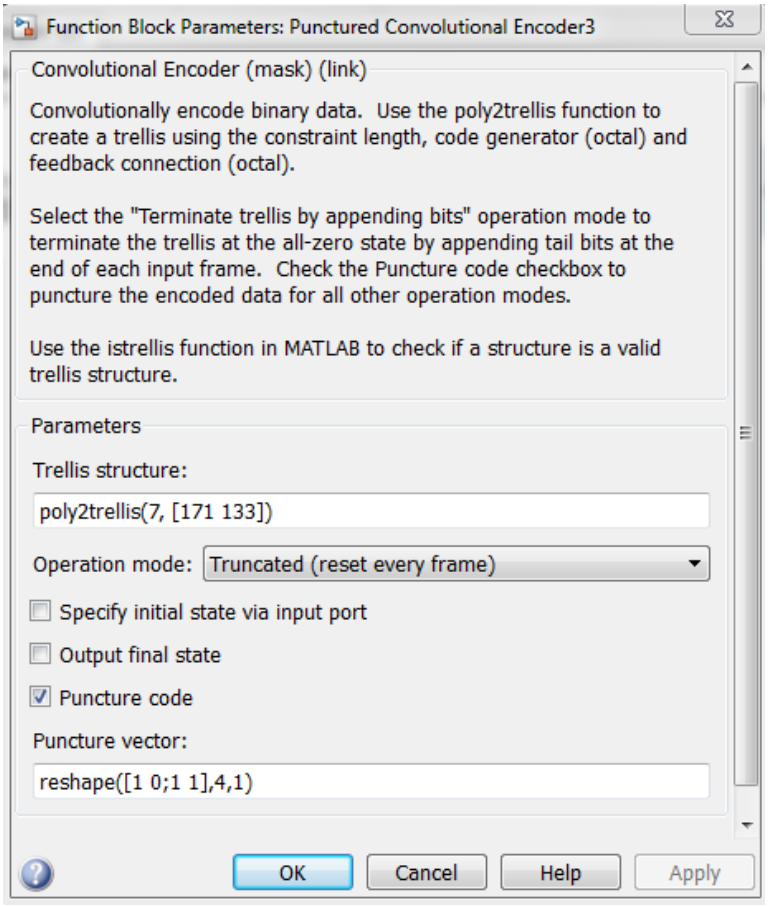


Рисунок 3.24 – Состав блока сверточного кодера«Convolutinal Encoder 16QAM 1/2»

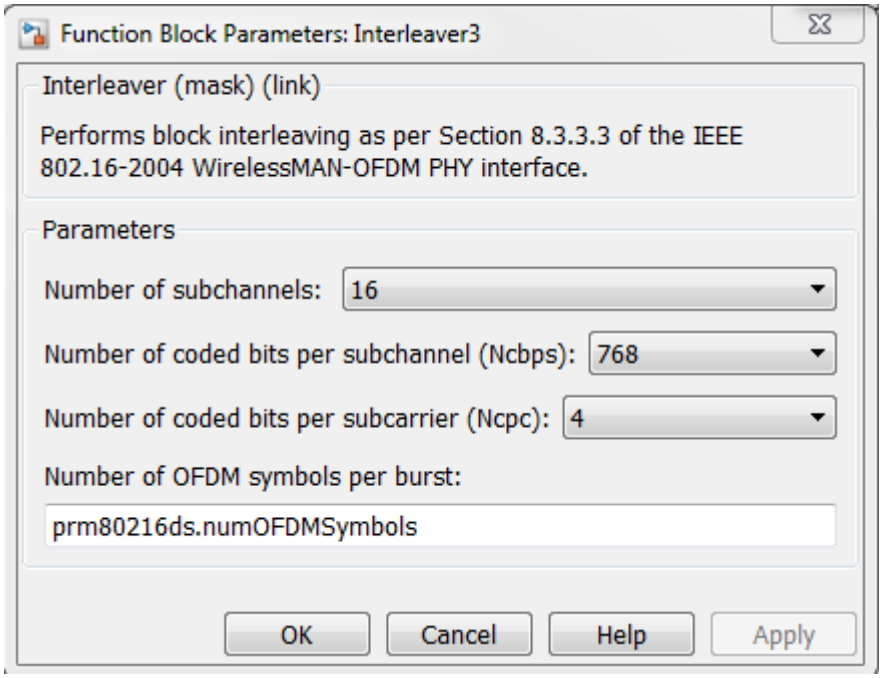


Рисунок 3.25 – Состав блока перемежителя «Interleaver 16QAM 1/2»

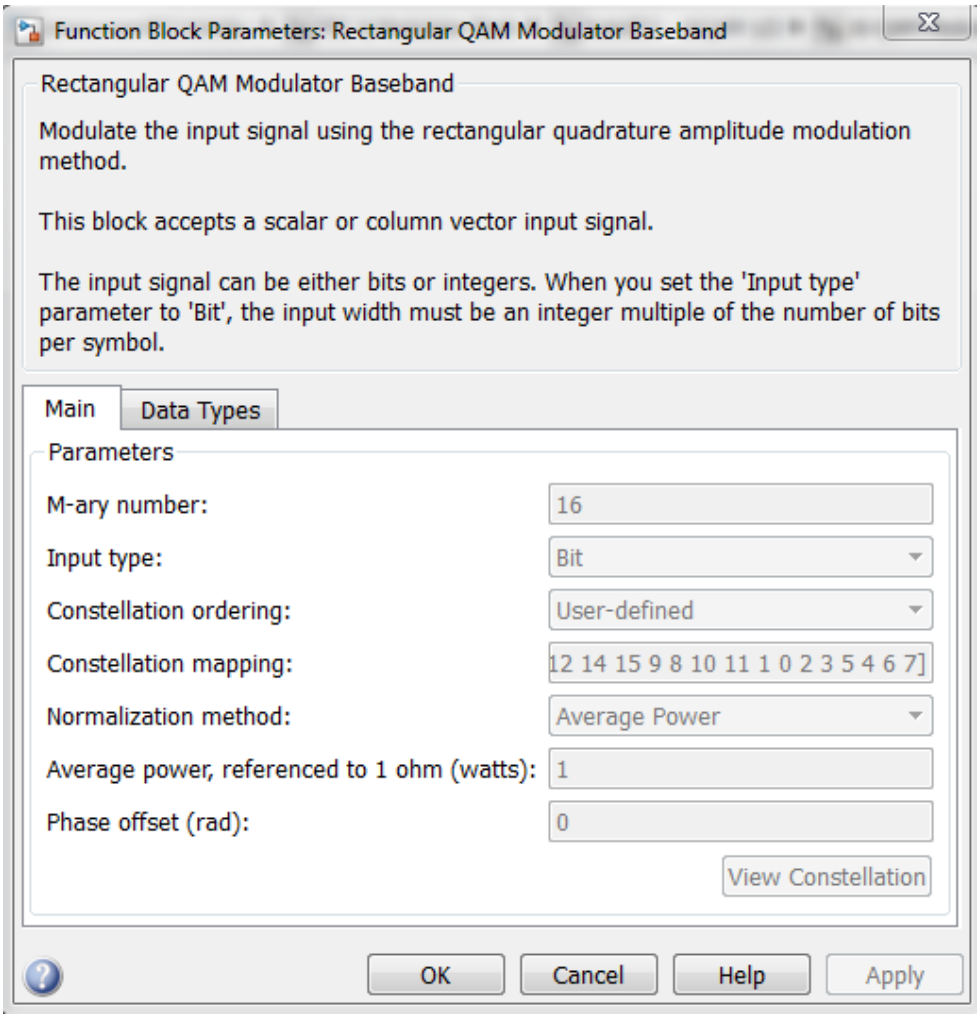


Рисунок 3.26 – Состав блока модулятора «16-QAM Modulator 16QAM 1/2»

Таблица 3.1 – Параметры кода Рида-Соломона для различных сигнально-кодовых конструкций

Вид модуляции	Общая скорость кодирования	Длина входной последовательности, бит	Длина выходной (кодированной) последовательности, бит	Параметры кода Рида-Соломона, (n, k, d)
BPSK	1/2	12	24	(12,12,0)
QPSK	1/2	24	48	(32,24,4)
QPSK	3/4	36	48	(40,36,2)
16-QAM	1/2	48	96	(64,48,8)
16-QAM	3/4	72	96	(80,70,4)
64-QAM	2/3	96	144	(108,96,6)
64-QAM	3/4	108	144	(120,108,6)

Состав блока помехоустойчивого декодирования и демодуляции («Demodulator & FEC Bank»)

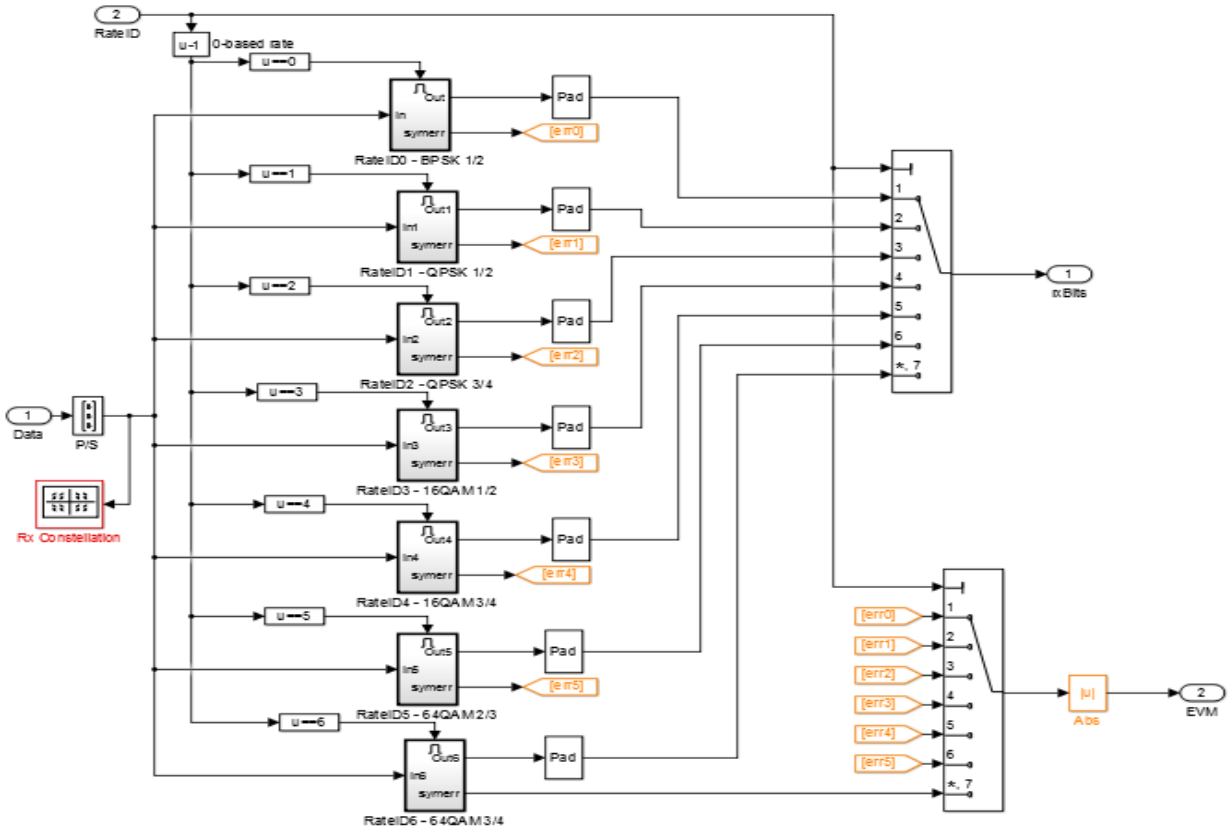


Рисунок 3.27 – Состав блока декодирования и демодуляции («Demodulator & FEC Bank»)

Состав блока BPSK 1/2 демодулятора

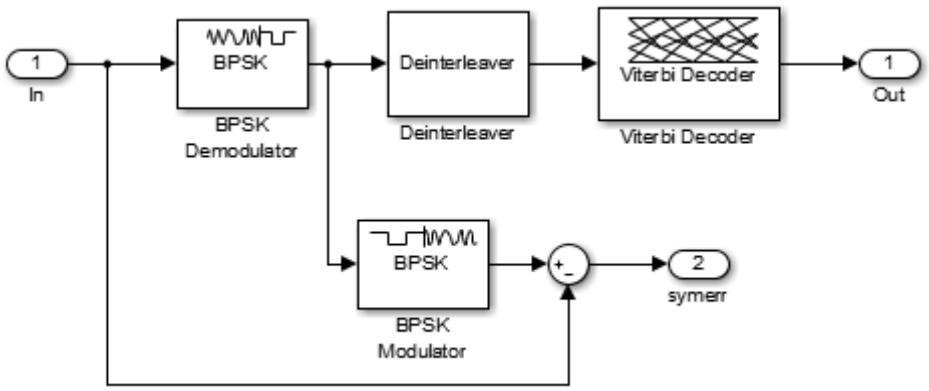


Рисунок 3.28 – Состав блока демодулятора «BPSK»

Состав блока QPSK 1/2 демодулятора

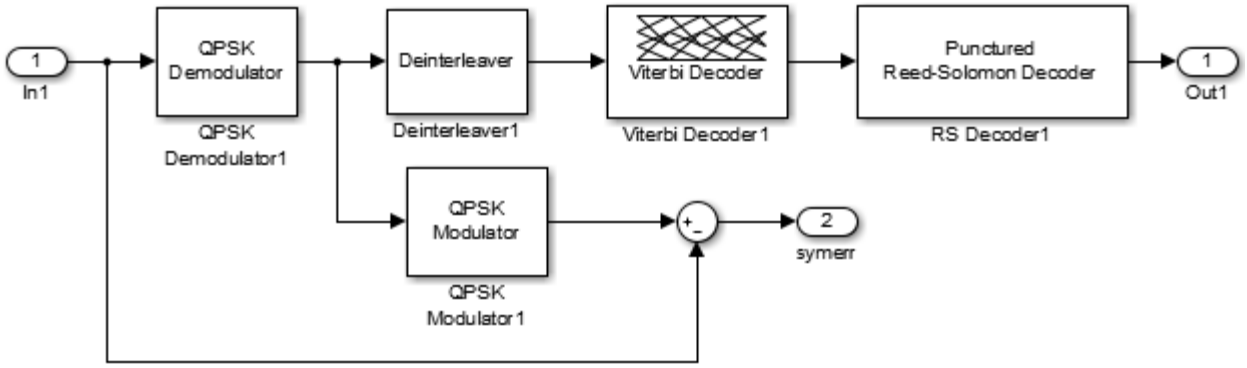


Рисунок 3.29 – Состав блока демодулятора «QPSK 1/2»

Состав блока QPSK 3/4 демодулятора

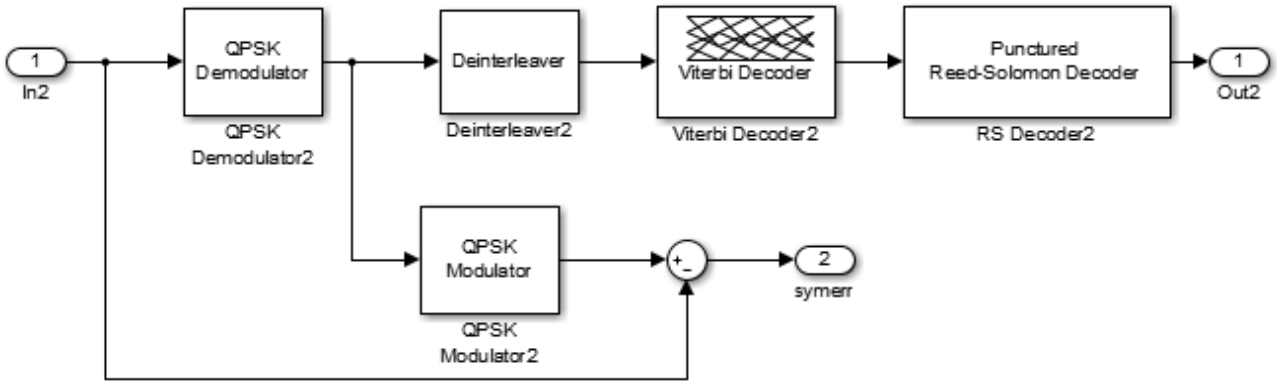


Рисунок 3.30 – Состав блока демодулятора «QPSK 3/4»

Состав блока 16QAM 1/2 демодулятора

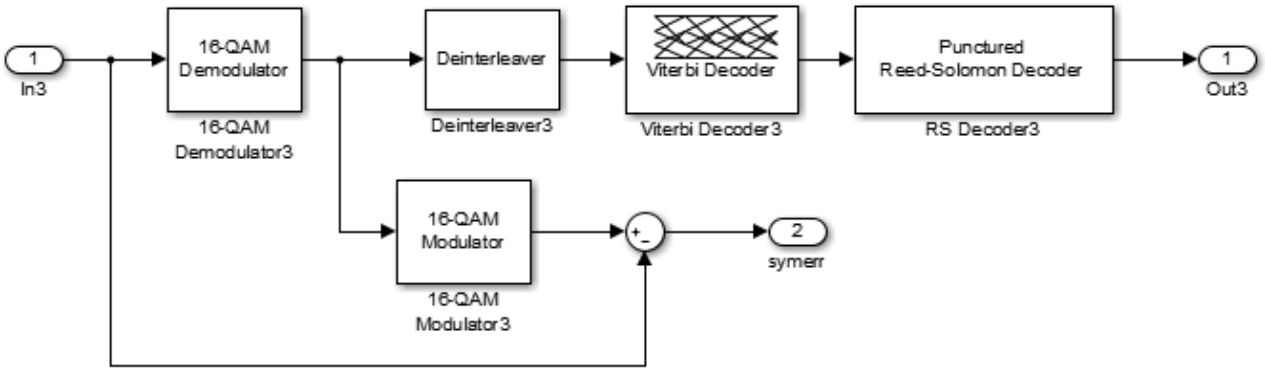


Рисунок 3.31 – Состав блока демодулятора «16QAM 1/2»

Состав блока 16QAM 3/4 демодулятора

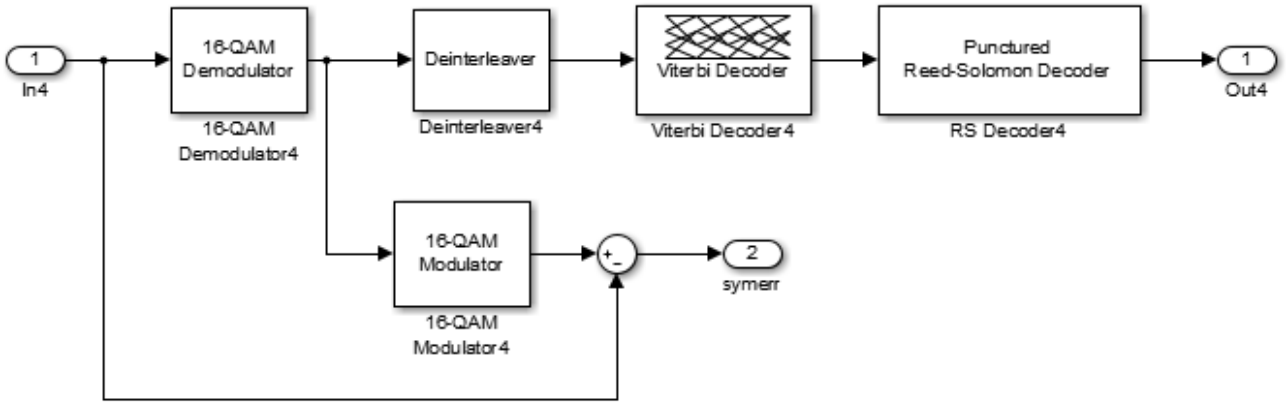


Рисунок 3.32 – Состав блока демодулятора «16QAM 3/4»

Состав блока 64QAM 2/3 демодулятора

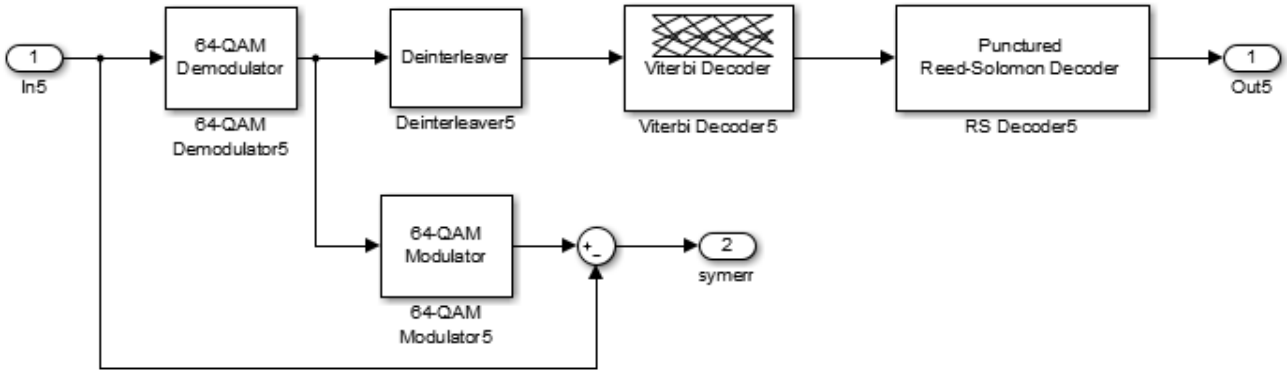


Рисунок 3.33 – Состав блока демодулятора «64QAM 2/3»

Состав блока 64QAM 3/4 демодулятора

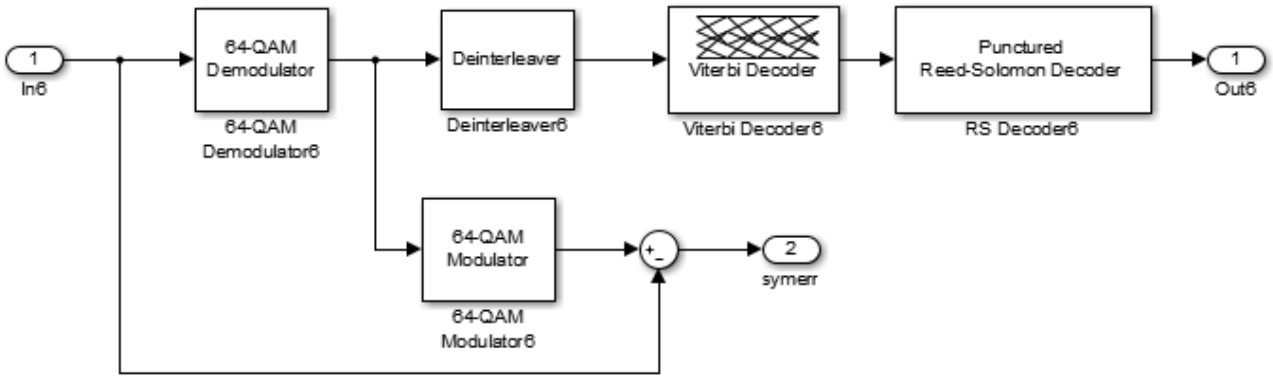


Рисунок 3.34 – Состав блока демодулятора «64QAM 3/4»

В процессе демодуляции и декодирования, описанные выше процессы, производятся в обратном порядке: демодуляция, деперемежение, декодирование сверточного кода по алгоритму Витерби, декодирования циклического блочного кода Рида-Соломона.

В каждом из блоков используется одинаковая последовательность блоков, отличающихся своими параметрами. Например для блока «16QAM 1/2» блоки имеют параметры.

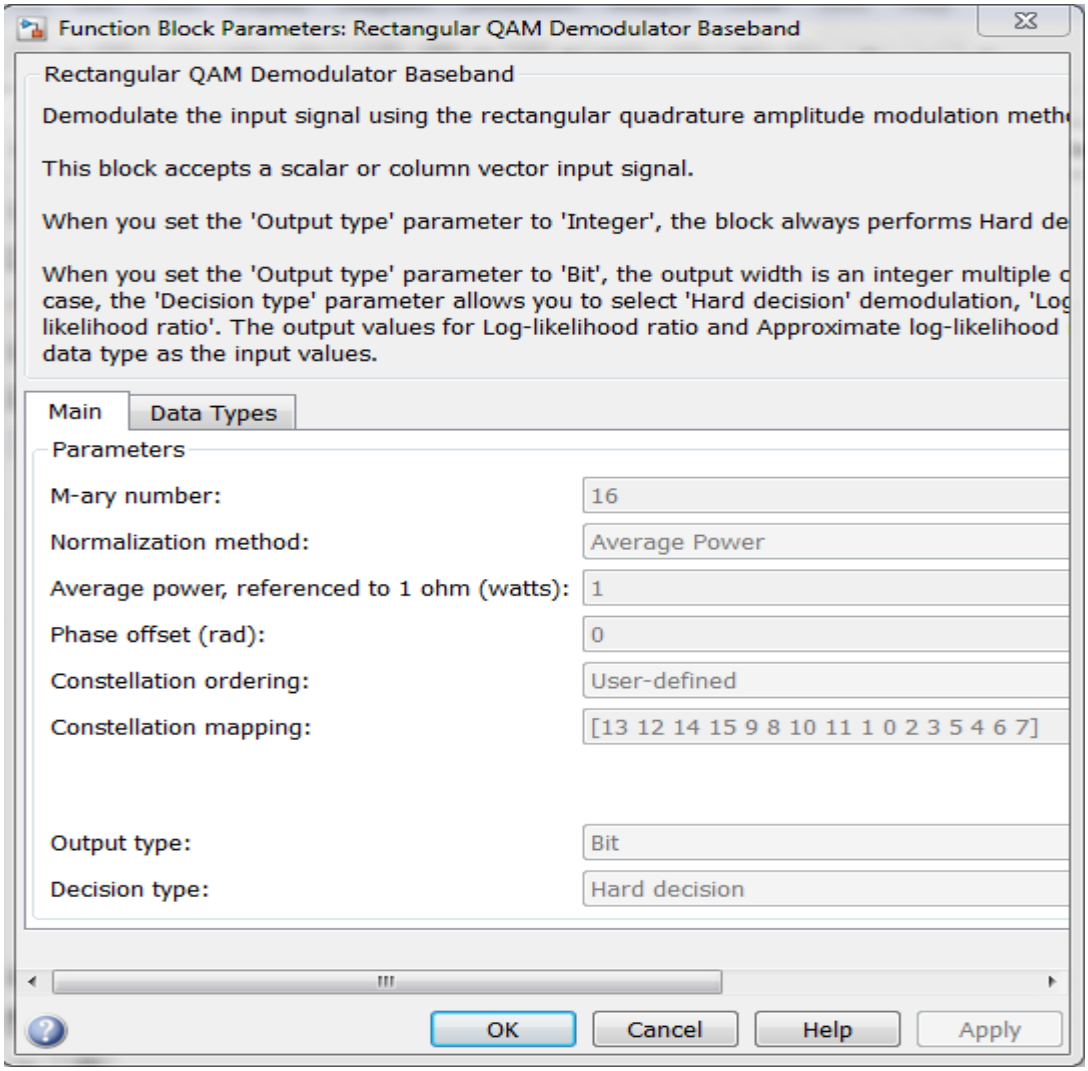


Рисунок 3.35 – Состав блока демодулятора «16-QAM Modulator 16QAM 1/2»

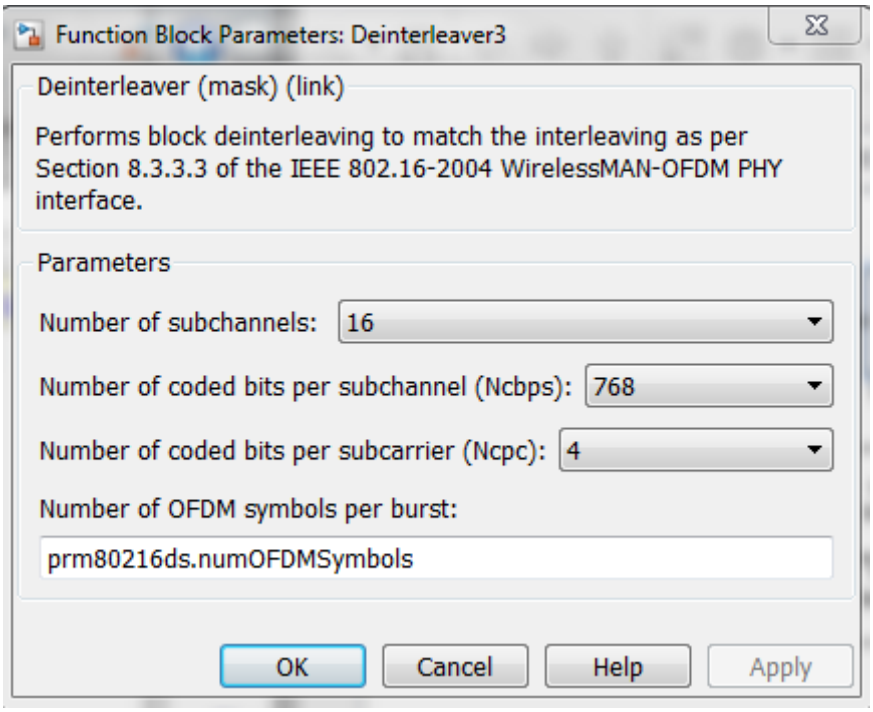


Рисунок 3.36 – Состав блока деперемежителя « Deinterleaver 16QAM 1/2»

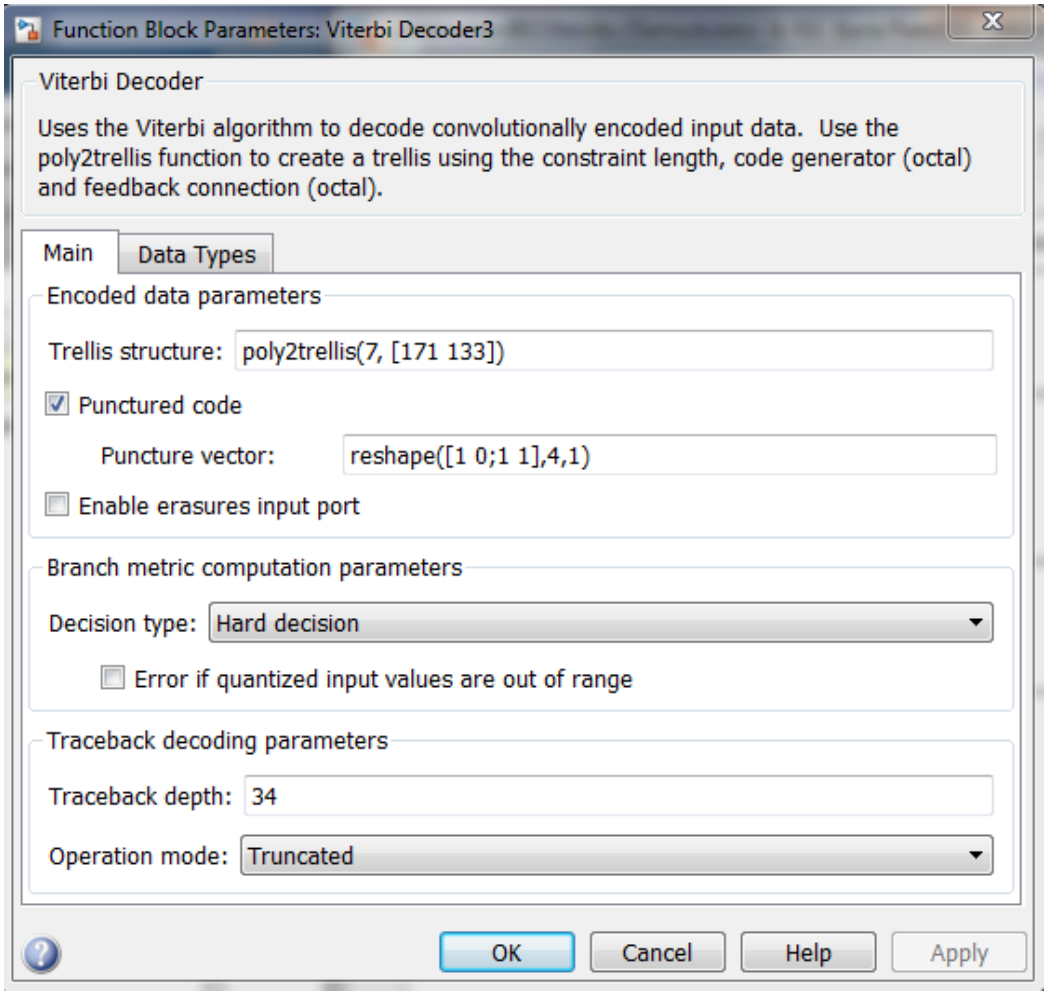


Рисунок 3.37 – Состав блока декодера Витерби «Viterbi Decoder 16QAM 1/2»

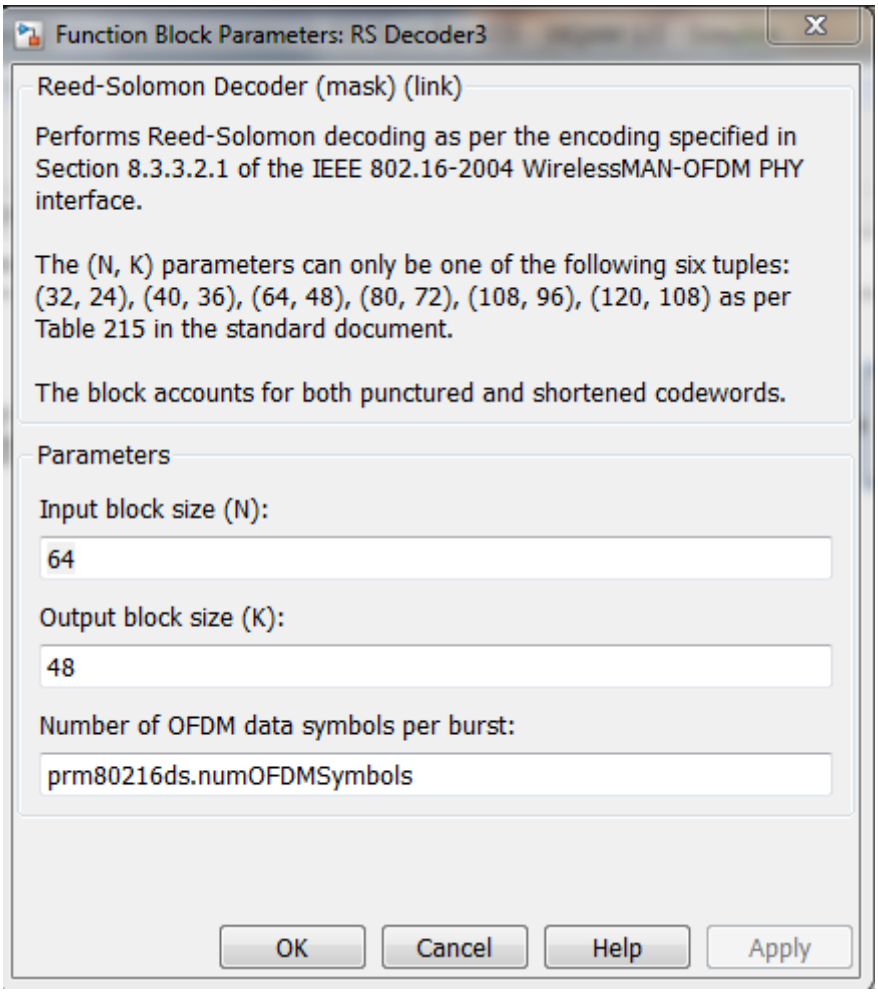


Рисунок 3.38 – Состав блока декодера Рида-Соломона «RS Decoder 16QAM 1/2»

В каждый момент времени, используемый вид модуляции и скорость кодирования (R) адаптируются под условия передачи. Блок «Adaptive Rate Control» анализирует уровень SNR в приемном устройстве и устанавливает параметры в соответствии с таблицей 3.2:

Таблица 3.2 – Изменение параметров модуляции и кодирования в зависимости от SNR

Вид модуляции и скорость кодирования	Отношение сигнал/шум в приемнике
BPSK	SNR < 4 дБ
QPSK, R=1/2	4 дБ < SNR < 10 дБ
QPSK, R=3/4	10 дБ < SNR < 12 дБ
16-QAM, R=1/2	12 дБ < SNR < 19 дБ
16-QAM, R=3/4	19 дБ < SNR < 22 дБ
64-QAM, R=1/2	22 дБ < SNR < 28 дБ
64-QAM, R=3/4	SNR > 28 дБ

Параметры OFDM-модулятора (блок «OFDM Modulator», рисунок 3.39).

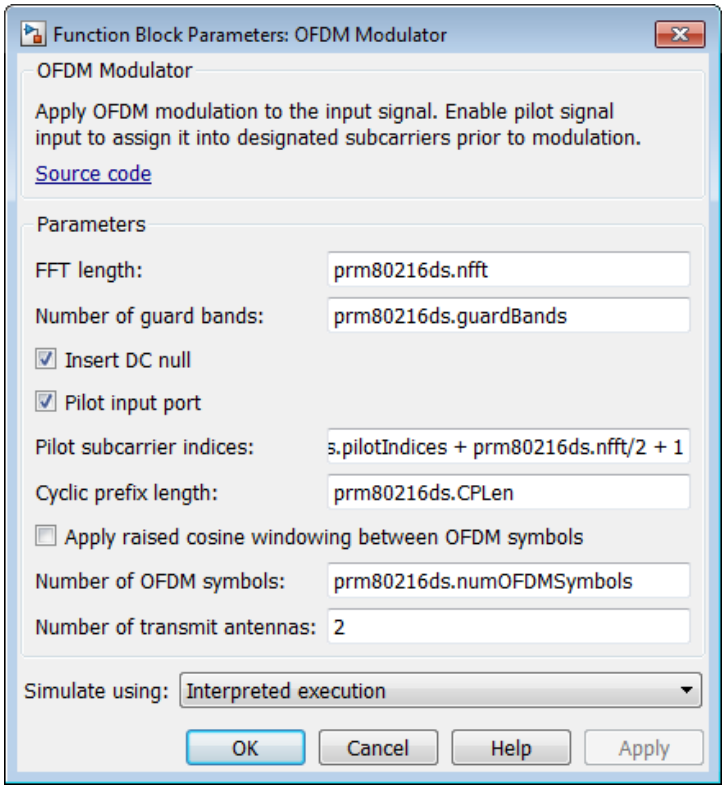


Рисунок 3.40 – Параметры системы, изменяемые в блоке «OFDM Modulator»

Параметры OFDM-демодулятора (блок «OFDM Demodulator», рисунок 3.41).

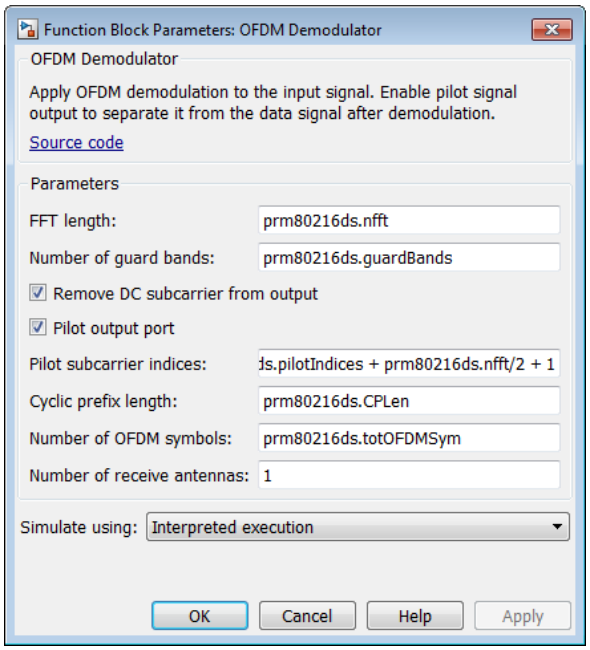


Рисунок 3.42 – Параметры системы, изменяемые в блоке «OFDM Demodulator»

Параметры канала MIMO (блок «MIMO Channel», рисунок 3.43).

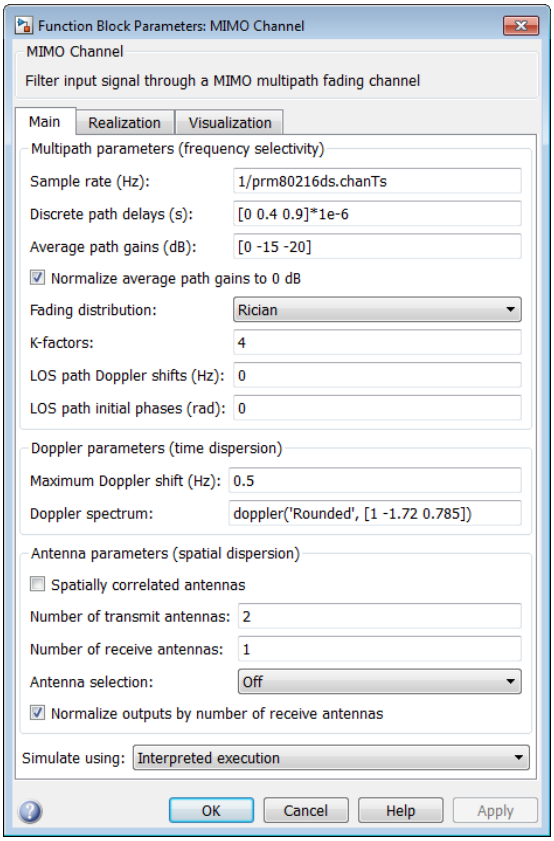


Рисунок 3.44 – Параметры системы, изменяемые в блоке «MIMO Channel»

Параметры канала AWGN (блок «AWGN Channel», рисунок 3.42).

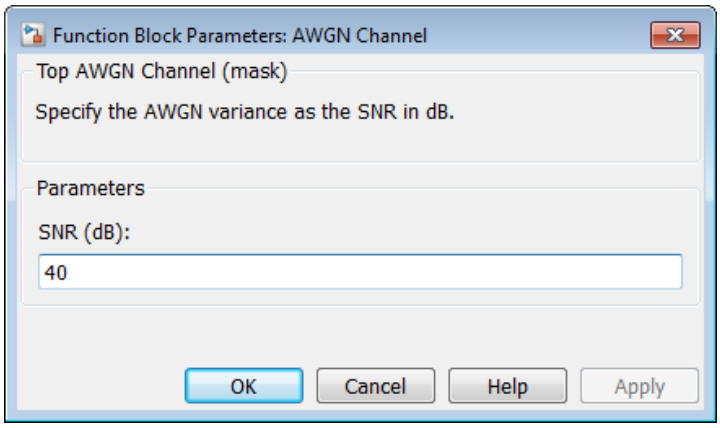


Рисунок 3.46 – Параметры системы, изменяемые в блоке «AWGN Channel»

Результаты работы и их анализ

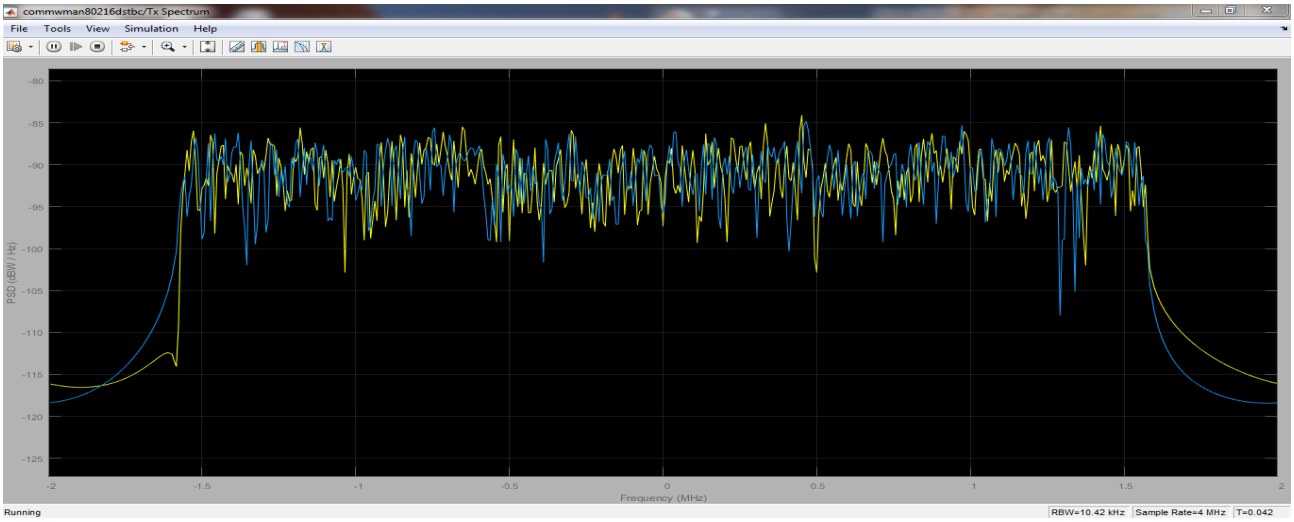


Рисунок 3.47 – Спектр передаваемых сигналов, поступающих на соответствующую передающую антенну

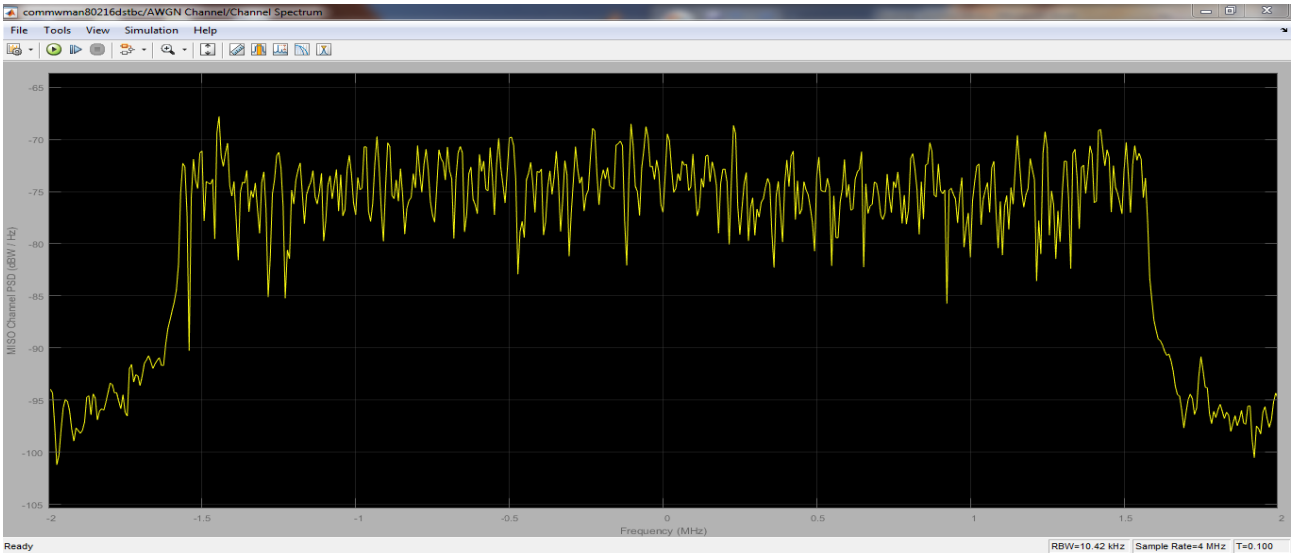


Рисунок 3.48 – Спектр принимаемого сигнала

Как было описано ранее, система адаптируется к условиям передачи, изменяя вид сигнально-кодовой конструкции сигнала (таблица 3.2). Необходимо исследовать поведение системы в зависимости от SNR в канале передачи (блок AWGN Channel), оформить полученные значения в виде графиков.

Созвездие принимаемого сигнала (BPSK):

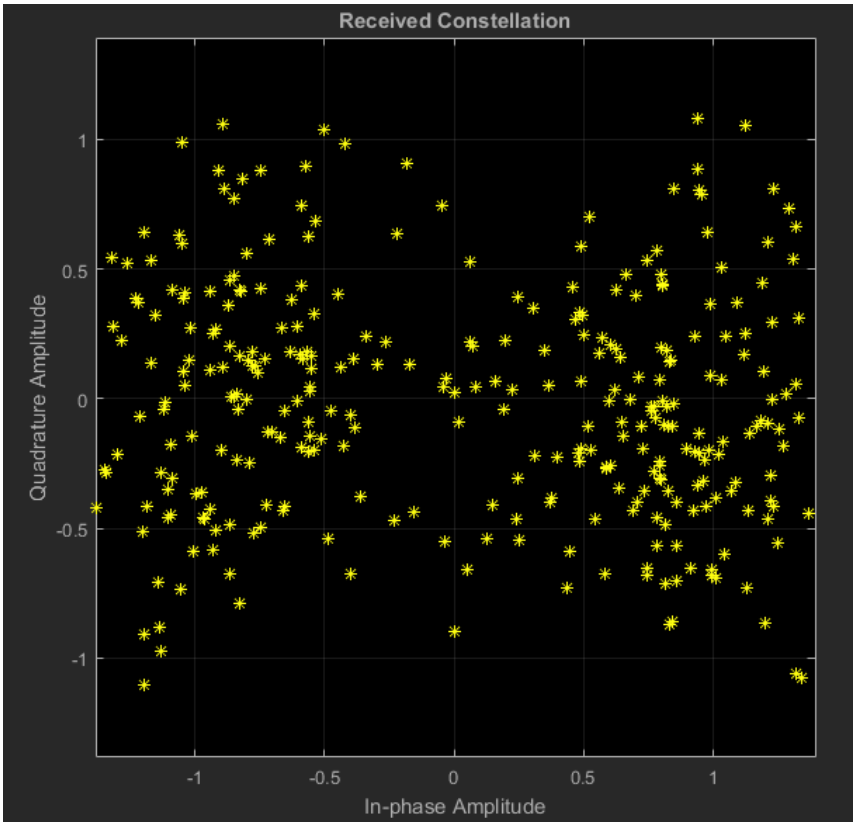


Рисунок 3.49 – Созвездие принимаемого сигнала (SNR = 2)

Созвездие принимаемого сигнала (QAM-4):

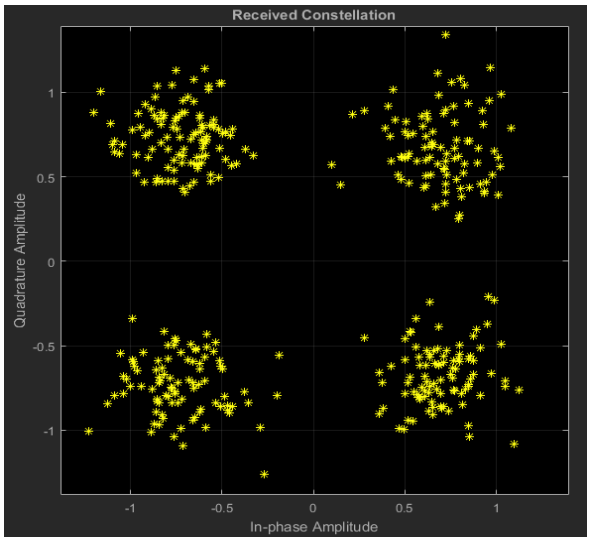


Рисунок 3.50 – Созвездие принимаемого сигнала (SNR = 11)

Созвездие принимаемого сигнала (QAM-16):

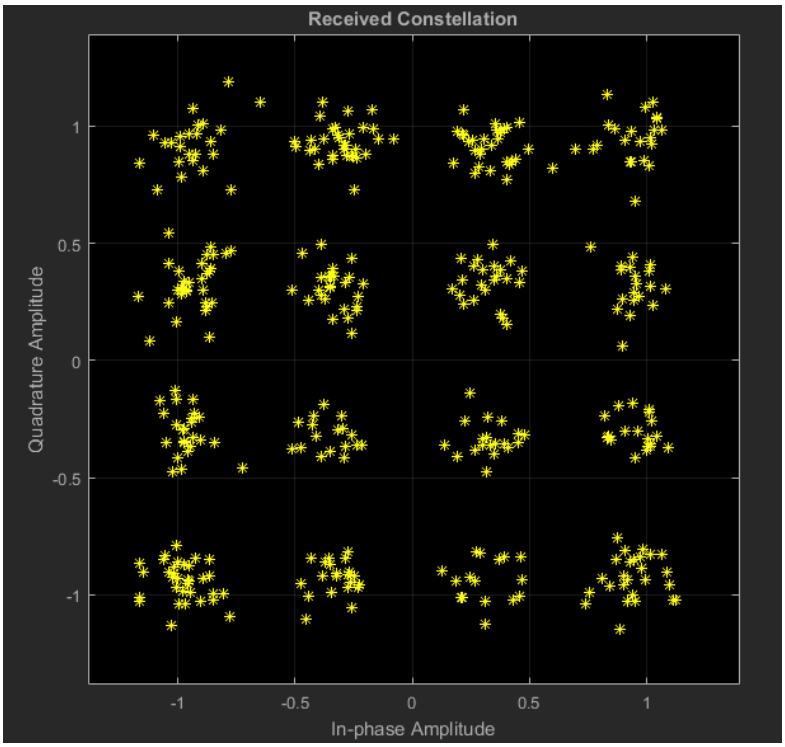


Рисунок 3.51 – Созвездие принимаемого сигнала (SNR = 18)

Созвездие принимаемого сигнала (QAM-64):

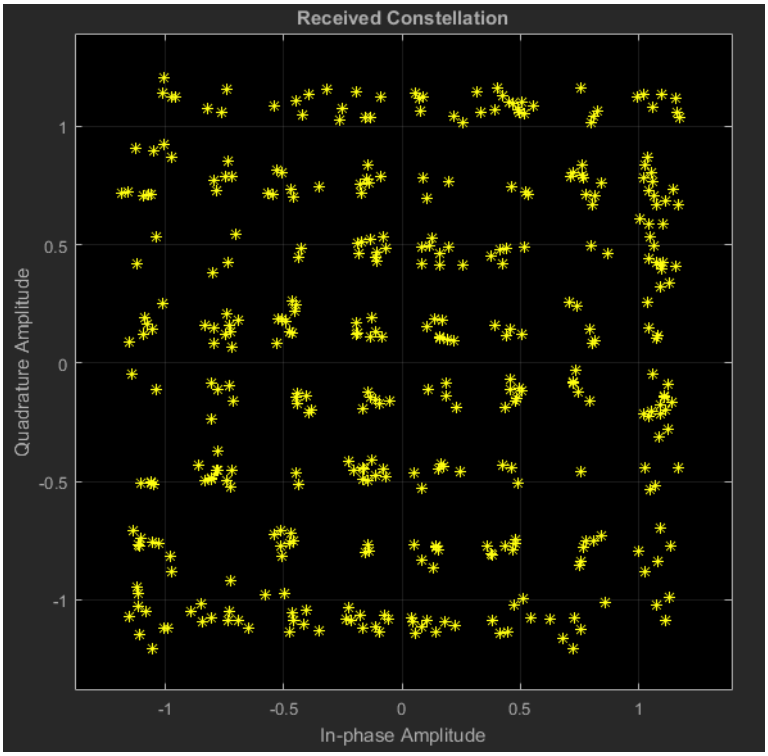


Рисунок 3.52 – Созвездие принимаемого сигнала (SNR = 22)

По данным блока «Bit Error Rate Display» можно построить график зависимости битовой вероятности ошибки (BER) от отношения сигнал/шум в канале (рисунок 3.53).

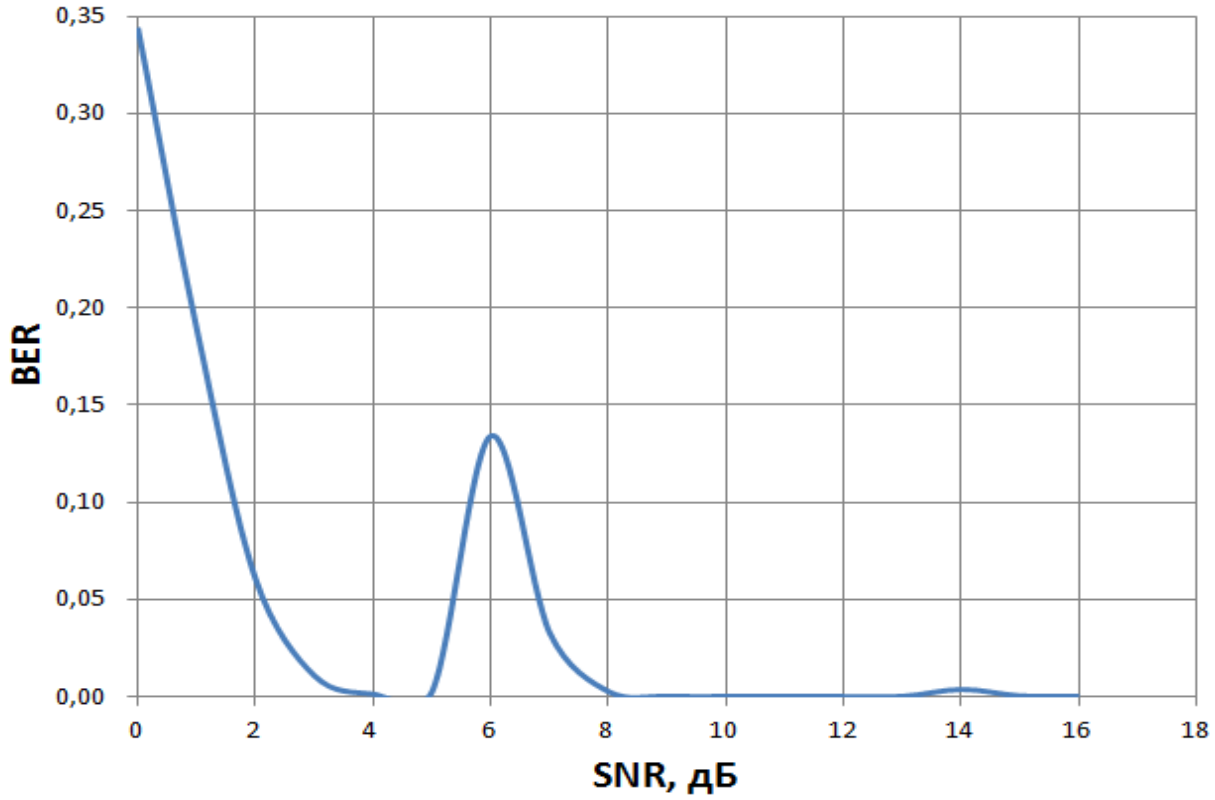


Рисунок 3.53 – Зависимость BER от SNR при использовании адаптивного изменения параметров

Зависимости BER от SNR для каждого конкретного вида модуляции и скорости кодирования представлены на рисунке 3.39

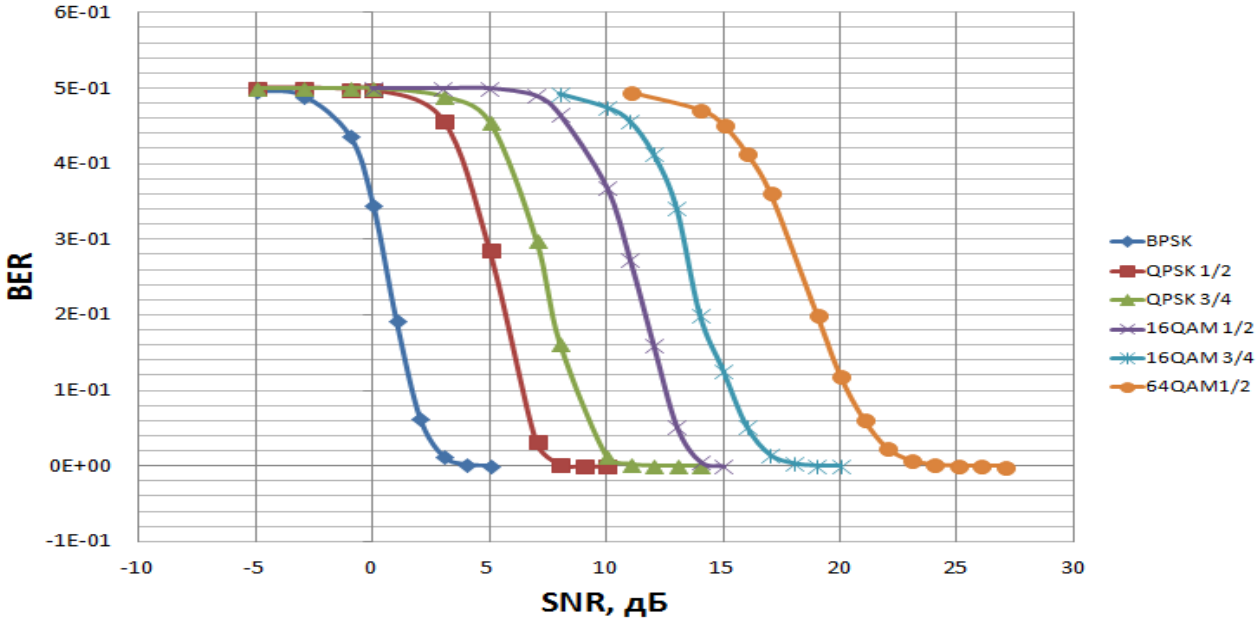


Рисунок 3.54 – Графики зависимости BER от SNR для отдельных видов модуляции и скорости кодирования.

Та же зависимость в логарифмическом масштабе:

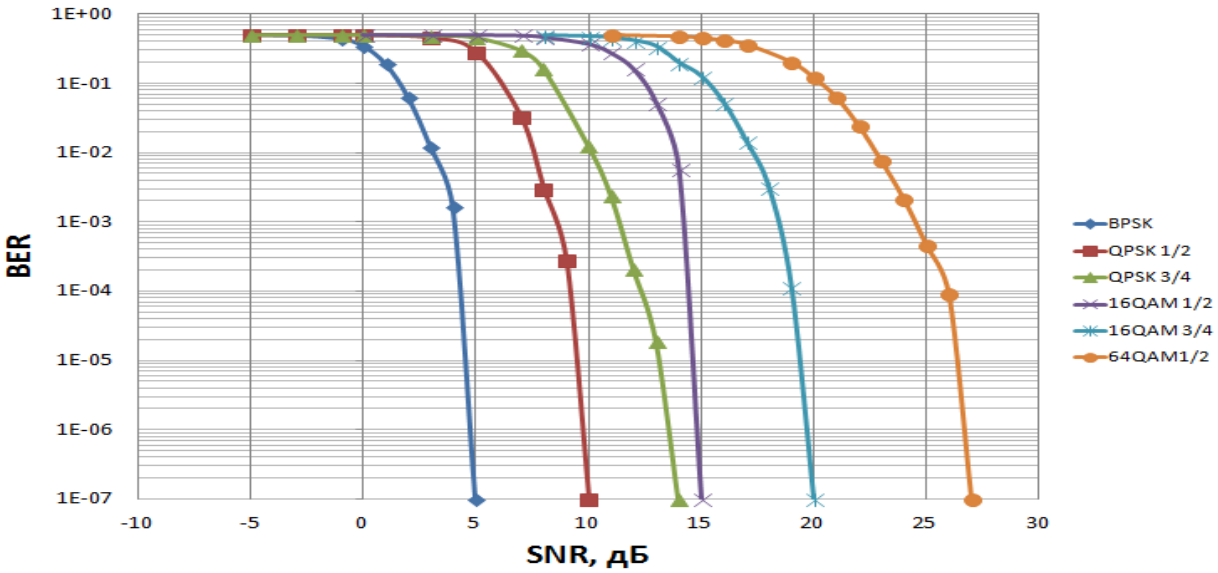


Рисунок 3.55 – Графики зависимости BER от SNR для отдельных видов модуляции и скорости кодирования. Логарифмическая шкала

Переход с одного вида модуляции на другой требует большей энергетики сигнала, но взамен происходит значительное увеличение скорости передачи. На рисунке 3.56 представлена зависимость принятого количества бит за 1 секунду (скорость передачи в Мбит/с) от SNR в канале.

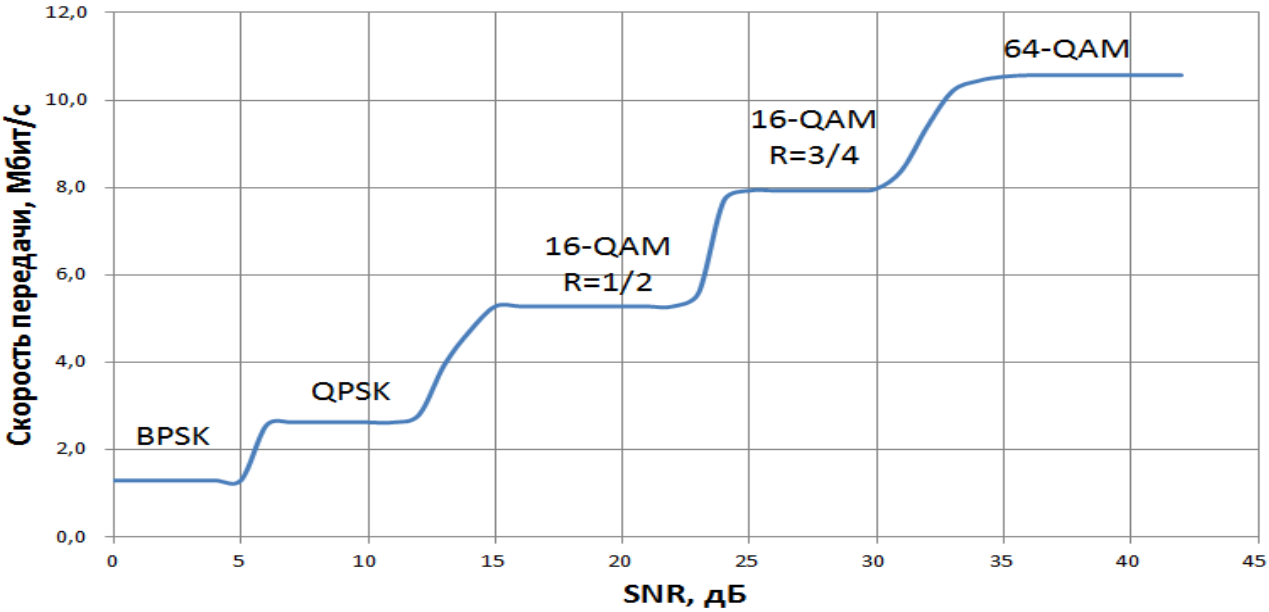


Рисунок 3.57 – График зависимости скорости передачи от SNR

После демодуляции и декодирования производится оценка SNR для принятых данных (блок «SNR Estimation»). Зависимость оцененного SNR от SNR в канале передачи приведена на рисунке 3.58

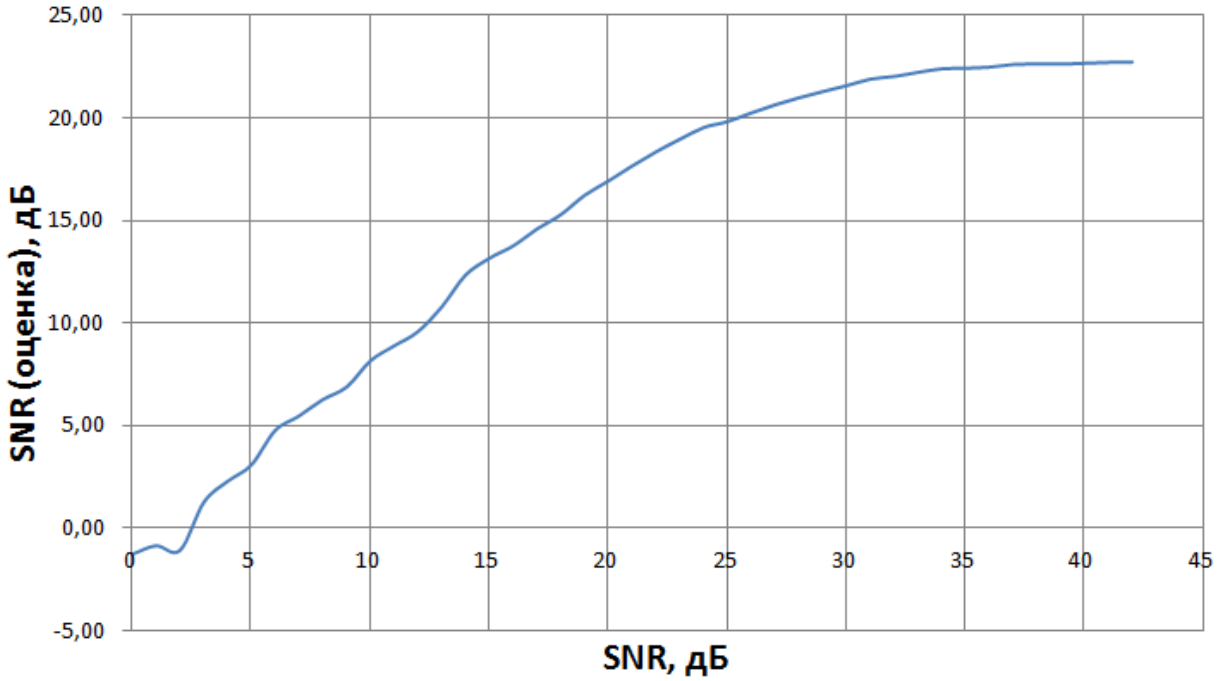


Рисунок 3.58 – График зависимости оценки SNR от SNR в канале передачи

В результате проделанной работы были получены теоретические знания об основах построения беспроводных сетей WiMAX на основе протокола IEEE 802.16-2004. Изучены сетевой, канальный и физический уровни данного протокола.

По результатам практического исследования модели физического уровня IEEE 802.16-2004 были сделаны следующие выводы:

1. Сравнивая рисунки 3.38 и 3.39 видно, что адаптивное изменение параметров системы в зависимости от SNR в канале приводит к уменьшению вероятности ошибок. Выбросы значений BER при SNR = 6 и 14 дБ происходят из-за перехода на менее помехозащищенные, но более скоростные виды модуляции.

2. Одновременно с этим происходит увеличение скорости передачи (рисунок 3.41). Скорость передачи изменяется от 1.25 Мбит/с при использовании BPSK до 11 Мбит/с при использовании 64-QAM.

3. По графику зависимости оценки SNR от реального SNR (рисунок 3.42), можно сделать вывод, что система работает наиболее стабильно (зависимость линейна) на участке 5…24 дБ. При SNR > 24 дБ более точная оценка канала не требуется (выбирается наименее помехоустойчивый метод модуляции – QAM-64 (в рамках стандарта)). При SNR < 6 дБ выбирается наиболее помехоустойчивый метод модуляции – BPSK.

3.7. Проектирование защищенной системы мобильной связи стандарта IEEE 802. 20 (LTE) на базе ПО MATLAB

Целью раздела является приобретение и закрепление навыков организации и реализации в программной среде системы мобильной связи стандарта LTE, подробное изучение схем входящих в состав стандарта и программного обеспечения с которыми предстоит работать при выполнении курсового проекта, умения выбрать необходимые решения на основе требований технического задания.

Помимо теоритической части, задачей курсового проектирования является построение в программной среде схемы передачи информации от базовой станции (БС) к мобильной станции (МС) и ее анализ. Схема будет включать в свой состав: генератор бинарной последовательности, кодек, модулятор/демодулятор, канал связи, анализатор ошибок и т.д.

Основным отличием стандарта LTE от предыдущих стандартов сетей связи является применение «плоской» более упрощённой IP-архитектуры, которая способствует уменьшению задержек при установленной Интернет-сессии. В стандарте LTE использовано два принципиально новых метода увеличения пропускной способности. Первый заключается в применении технологии MIMO (Multiple Input Multiple Output), где передача и приём сигнала осуществляется одновременно через несколько передающих и приёмных антенн. Таким образом, повышается скорость передачи данных в беспроводных сетях. Второй метод заключается в применении OFDM (Orthogonal frequency division multiplexing) модуляции, использующей несколько поднесущих. Преимущество данного метода заключается также в том, что системы связи с LTE могут работать в отсутствии прямой видимости.

Стандарты 2G и 3G

Стандарт 2G (GSM)

Разработка стандарта GSM началась еще в 1982 году организацией по стандартизации CEPT (European Conference of Postal and Telecommunications Administrations) . В 1991 году в Финляндии была введена в эксплуатацию первая в мире сеть GSM. Уже к концу 1993 года число абонентов, использующих этот стандарт, перевалило за миллион. К этому времени сети GSM были развернуты в 73 странах мира.

Сети стандарта GSM позволяют предоставлять широкий перечень услуг:

- Голосовые соединения
- Услуги передачи данных (до 384 кбит/сек благодаря технологии EDGE (дополнение технологии GPRS, в результате появилась передача данных с пакетной коммутацией, т.е. пакетный трафик отделяется от голосового))
- Передача коротких текстовых сообщений (SMS)

- Передача факсов
- Голосовая почта
- Конференцсвязь и мн. др.

Итак, рассмотрим основные элементы, входящие в состав системы GSM:

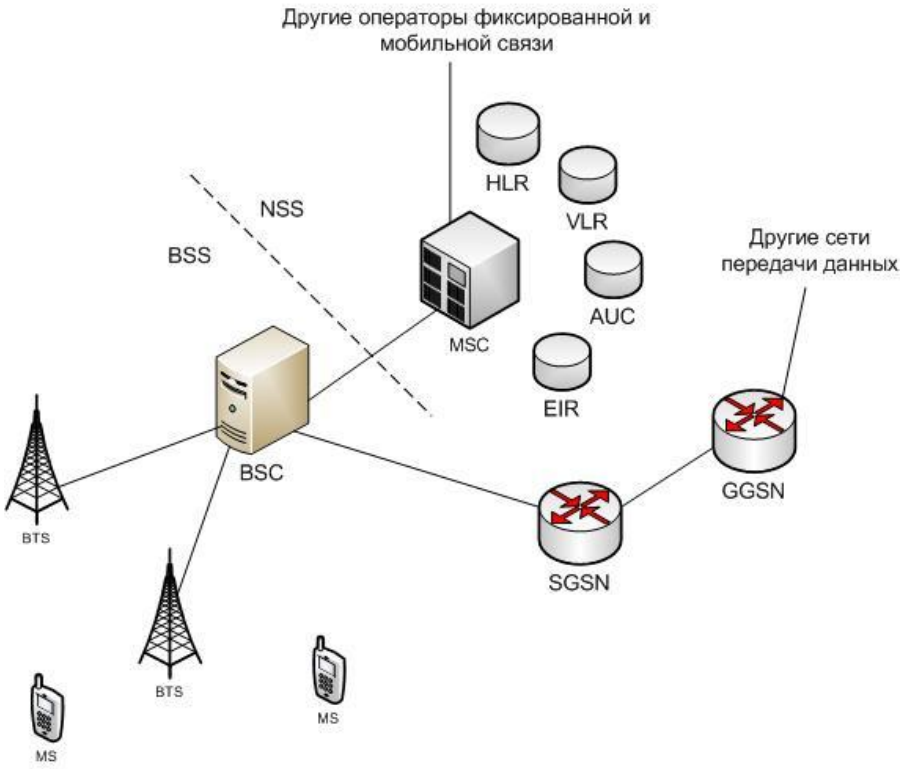


Рис. 3.94. Структура сети стандарта 2G (GSM)

Сеть GSM делится на 2 системы. Каждая из этих систем включает в себя ряд функциональных устройств, которые, в свою очередь являются компонентами сети мобильной радиосвязи.

Данными системами являются:

- Система коммутации – Network Switching System (NSS).
- Система базовых станций - Base Station System (BSS).

Система NSS выполняет функции обслуживания вызовов и установления соединений, а также отвечает за реализацию всех назначенных абоненту услуг. NSS включает в себя следующие функциональные устройства:

- Центр коммутации мобильной связи (MSC).
- Домашний регистр местоположения (HLR).
- Визитный регистр местоположения (VLR).
- Центр аутентификации (AUC).
- Регистр идентификация абонентского оборудования (EIR).

Система BSS отвечает за все функции, относящиеся к радиоинтерфейсу. Эта система включает в себя следующие функциональные блоки:

- Контроллер базовых станций (BSC).
- Базовую станцию (BTS).

MS (т.е. телефон абонента (мобильная станция)) не принадлежит ни к одной из этих систем, но рассматривается как элемент сети.

Элементы сети, относящиеся к пакетной передачи данных:

- SGSN – узел обслуживания абонентов.
- GGSN – шлюзовой узел.

Стандарт 3G (UMTS)[2]

Разработка стандарта UMTS началась в 1992 году организацией по стандартизации IMT-2000. Впоследствии разработка этого стандарта была поручена 3GPP. Первая сеть UMTS была запущена в коммерческую эксплуатацию 1 декабря 2001 года в Норвегии. К маю 2010 года число абонентов переваливает за 540 миллионов по всему миру.

Скорость передачи данных для сетей UMTS может достигать 2Мбит/сек. Благодаря технологии HSDPA-High Speed Downlink Packet Access (3.5G), которая была внедрена в 2006 году максимальная скорость возросла до 14 Мбит/сек. Эти и другие преимущества UMTS позволяют предоставлять абонентам широкий перечень услуг: видеозвонки, видеоконференции, высококачественные голосовые звонки, загрузка файлов с высокой скоростью, сетевые игры, мобильная коммерция и мн. др.

Рассмотрим структуру системы UMTS и ее основные отличия от стандарта второго поколения GSM.

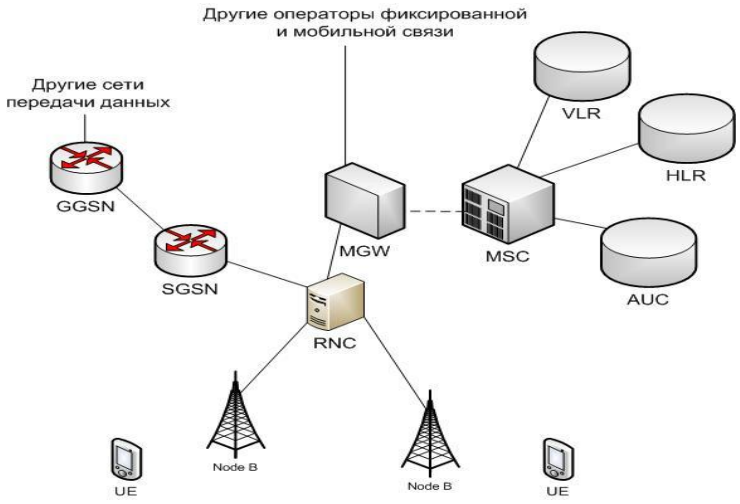


Рис. 3.95. Структура сети стандарта 3G (UMTS)

Подсистема коммутации:

В первых релизах стандарта UMTS (R99, R4) подсистема коммутации не отличалась по своей структуре от той же подсистемы сетей второго поколения. В нее входили MSC – Mobile Switching Centre, который выполнял функции коммутации, установления соединения, тарификации и др., а также ряд регистров HLR, VLR, AUC, которые предназначены для хранения абонентских данных. В более поздних релизах (R5, R6, R7,R8) функции MSC были разделены между двумя устройствами: MSC-Server и MGW (Media gateway). MSC-Server отвечает за установление соединений, тарификацию, выполняет некоторые функции аутентификации. MGW представляет собой коммутационное поле, подчиненное MSC-Server.

Подсистема базовых станций:

В сети UMTS по сравнению с сетью GSM наибольшие изменения претерпела подсистема базовых станций. Отмеченные выше преимущества достигаются в первую очередь за счет новой технологии передачи информации между базовой станцией и телефоном абонента.

Итак, рассмотрим основные элементы, входящие в подсистему базовых станций:

RNC (Radio Network Controller) – контроллер сети радиодоступа системы UMTS. Он является центральным элементом подсистемы базовых станций и выполняет большую часть функций: контроль радиоресурсов, шифрование, установление соединений через подсистему базовых станций, распределение ресурсов между абонентами и др. В сети UMTS контроллер выполняет гораздо больше функций, нежели в системах сотовой связи второго поколения.

NodeB – базовая станция системы сотовой связи стандарта UMTS. Основной функцией NodeB является преобразование сигнала, полученного от RNC в широкополосный радиосигнал, передаваемый к телефону. Базовая станция не принимает решений о выделении ресурсов, об изменении скорости к абоненту, а лишь служит мостом между контроллером и оборудованием абонента, и она полностью подчинена RNC.

Оборудование абонента получило название UE (User Equipment (мобильная станция)). Тем самым подчеркивается, что в отличие от предшествующих стандартов в UMTS может быть не только обычный телефон, но и смартфон, ноутбук, стационарный компьютер и т.п.

Пакетные данные в сети UMTS передаются от MGW к известному нам по системе GSM элементу SGSN (узел обслуживания абонентов), после чего через GGSN (шлюзовой узел) поступают к другим внешним сетям передачи данных, например Internet. Как правило, SGSN и GGSN сети GSM применяются для тех же целей и в сети UMTS. Производится только коррекция программного обеспечения данных элементов.

Стандарт LTE и его отличие от предыдущих стандартов

Стандарты третьего поколения позволяют предоставить широкий перечень мультимедийных услуг и поддерживают скорости передачи данных до 14Мбит/сек. Это

вполне соответствует запросам абонентов в настоящее время. Однако, объемы передаваемой информации в телекоммуникационных сетях растут с каждым днем. Чтобы удовлетворить потребности пользователей по скорости передачи данных и набору услуг, хотя бы на 20 лет вперед необходим новый стандарт, уже четвертого поколения.

Работа над первым стандартом четвертого поколения - LTE (Long Term Evolution) началась в 2004 году организацией 3GPP. Главными требованиями, которые предъявлялись в процессе работы над стандартом были следующие:

- Скорость передачи данных выше 100 Мбит/сек.
- Высокий уровень безопасности системы.
- Высокая энергоэффективность.
- Низкие задержки в работе системы.
- Совместимость со стандартами второго и третьего поколений.

В конце 2009 года в Швеции была запущена в коммерческую эксплуатацию первая сеть стандарта LTE.

Сети LTE поддерживают скорости передачи данных до 326,4 Мбит/сек. К примеру, загрузка фильма в хорошем качестве займет менее одной минуты. Таким образом, верхняя планка по скорости передачи данных практически снимается.

Рассмотрим структуру сети LTE:

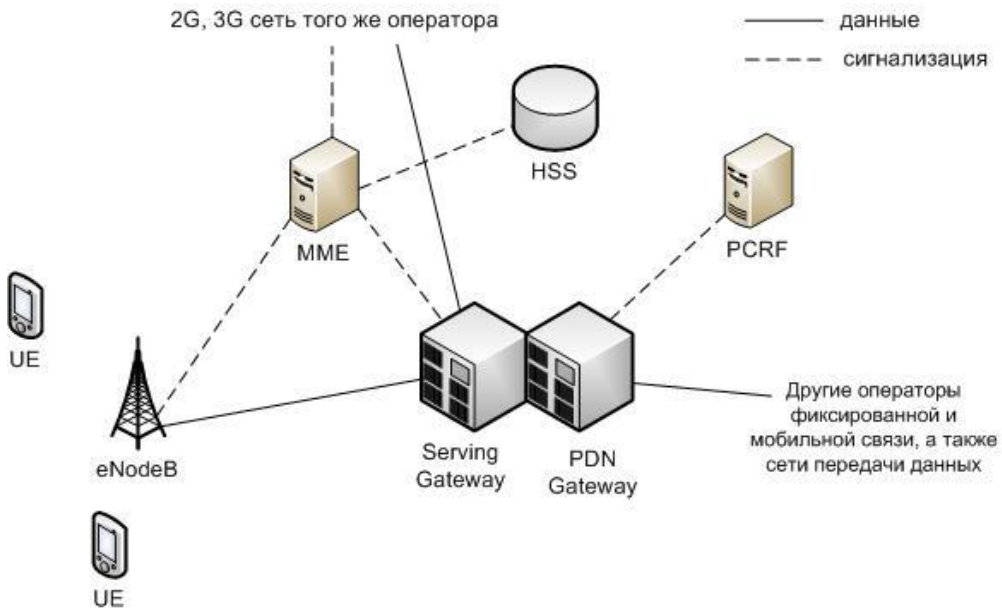


Рис. 3.96. Структура сети стандарта LTE

Из схемы сети LTE, представленной выше, уже видно, что структура сети сильно отличается от сетей стандартов 2G и 3G. Существенные изменения претерпела и подсистема базовых станций, и подсистема коммутации. Была изменена технология передачи данных между оборудованием пользователя и базовой станцией. Также подверглись изменению и

протоколы передачи данных между сетевыми элементами. Вся информация (голос, данные) передается в виде пакетов. Таким образом, уже нет разделения на части обрабатывающие либо только голосовую информацию, либо только пакетные данные.

Можно выделить следующие основные элементы сети стандарта LTE:

Serving SAE Gateway или просто Serving Gateway (SGW) – обслуживающий шлюз сети LTE. Предназначен для обработки и маршрутизации пакетных данных поступающих из/в подсистему базовых станций. По сути, заменяет MSC (выполняет функции коммутации, установления соединения, тарификации), MGW (представляет собой коммутационное поле) и SGSN (узел обслуживания абонентов пакетной сети передачи данных) сети UMTS (3G). SGW имеет прямое соединение с сетями второго и третьего поколений того же оператора, что упрощает передачу соединения в/из них по причинам ухудшения зоны покрытия, перегрузок и т.п.

Public Data Network (PDN) SAE Gateway или просто PDN Gateway (PGW) – шлюз к/от сетей других операторов. Если информация (голос, данные) передаются из/в сети данного оператора, то они маршрутизируются именно через PGW.

Mobility Management Entity (MME) – узел управления мобильностью. Предназначен для управления мобильностью абонетов сети LTE.

Home Subscriber Server (HSS) – сервер абонентских данных. HSS представляет собой объединение VLR (гостевой регистр местоположения), HLR (домашний регистр местоположения), AUC (центр аутентификации абонентов) выполненных в одном устройстве.

Policy and Charging Rules Function (PCRF) – узел выставления счетов абонентам за оказанные услуги связи.

Все перечисленные выше элементы относятся к системе коммутации сети LTE. В системе базовых станций остался лишь один знакомый нам элемент – базовая станция, которая получила название **eNodeB**. Этот элемент выполняет функции и базовой станции, и контроллера базовых станций сети LTE. За счет этого упрощается расширение сети, т.к. не требуется расширение емкости контроллеров или добавления новых. Мобильная станция представлена – **UE.**

Интерфейсы между узловыми элементами в сетях стандарта LTE

Структура сети стандарта LTE претерпела значительные изменения по сравнению с сетями предыдущих поколений. Это повлияло также и на изменение интерфейсов между узлами сети. На рисунке ниже представлена общая модель сети стандарта LTE и ее основные интерфейсы.

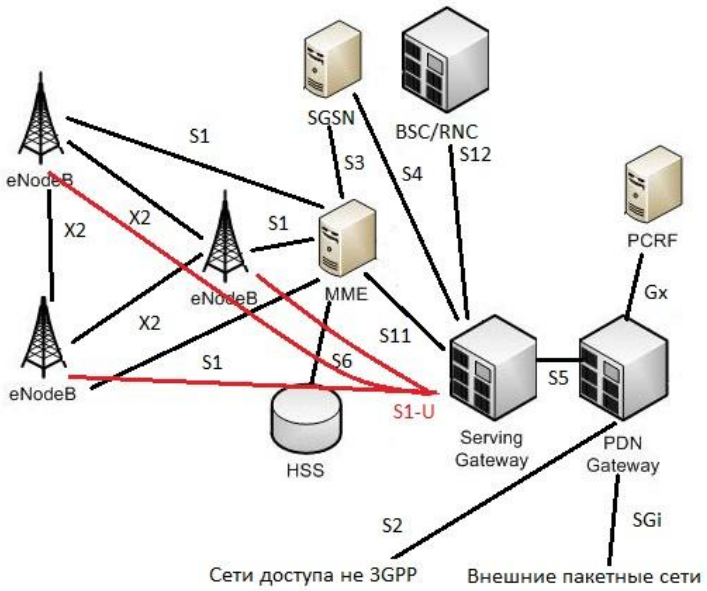


Рис. 3.97. Интерфейсы сети стандарта LTE

Рассмотрим основные интерфейсы сети LTE:

- X2 - интерфейс между eNodeB. Базовые станции в сети LTE соединены по принципу «каждый с каждым».
- S1 – интерфейс связывающий подсистему базовых станций E-UTRAN и MME. По данному интерфейсу передаются данные управления.
- S1-U – интерфейс между E-UTRAN и SAE, по которому передаются пользовательские данные.
- S2 – интерфейс для организации соединения между PDN-Gateway и сетями доступа, которые не разрабатывались 3GPP.
- S3 – интерфейс, предоставляющий прямое соединение SGSN и MME. Он служит для передачи данных управления для обеспечения мобильности между LTE и 2G/3G сетями.
- S4 – интерфейс, связывающий SAE и SGSN. Он служит для передачи пользовательских данных для обеспечения мобильности между LTE и 2G/3G сетями.
- S5 – интерфейс между SAE и PDN-Gateway. S5 предназначен для передачи пользовательских данных между SAE и PDN-Gateway.
- S6 – интерфейс между MME и HSS. Он используется для передачи данных абонентского профиля, а также осуществления процедур аутентификации в сети LTE.
- Gx – интерфейс между PDN-Gateway и PCRF. Gx предназначен для передачи правил тарификации от PCRF к PDN-Gateway.
- SGi - интерфейс между PDN-Gateway и внешними IP-сетями.

Принципы построения радиоинтерфейса LTE в Downlink (от БС к МС)

Одной из главных отличительных особенностей стандарта LTE, которая позволяет достигать высоких скоростей передачи данных является изменение принципов построения интерфейса от eNodeB (БС) до UE (МС) на линии «вниз». Рассмотрим главные особенности этого интерфейса и постараемся выделить основные качественные отличия, которые отличают этот стандарт от других.

В сетях связи стандарта LTE в Downlink (DL) используется модуляция OFDM – Orthogonal Frequency Devision Multiplexing– ортогональная частотная модуляция. Этот тип модуляции определяет и принцип доступа OFDMA - Orthogonal Frequency Devision Multiple Access – множественный доступ с ортогональным частотным разделением каналов. Суть его заключается в том, что все частотно-временное поле, выделенное для работы оператора, разделяется на небольшие блоки. Причем они небольшие как по частоте (15 кГц), так и по времени (0,5 мс). Сеть распределяет эти блоки между абонентами в зависимости от их потребностей и возможностей сети. Таким образом, обеспечивается максимально эффективное использование ресурсов.

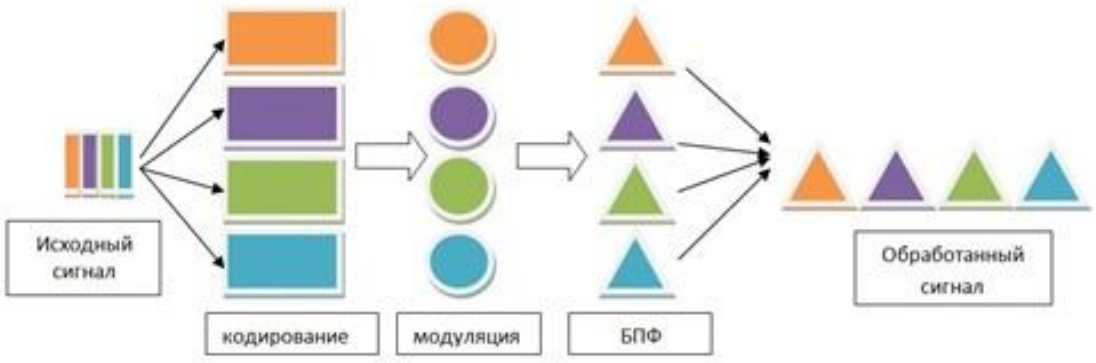


Рис. 3.98. OFDM – модулятор

Ниже перечислены главные шаги преобразования сигнала в OFDM модуляторе.

1) Разделение исходного потока бит на параллельные потоки.

2) Кодирование помехоустойчивым кодом, в процессе которого значительно увеличивается число символов в отдельных потоках.

3) Манипуляция выбранным в данный конкретный момент способом модуляции: QPSK, 16QAM, 64QAM.

4) Перемножение полученной последовательности каждого потока на свою поднесущую. Эта операция является ключевой и будет рассмотрена ниже.

5) Объединение сигналов и передача в эфир.

Умножение сигнала на свою поднесущую перемещает сигнал в нужное частотное пространство. Также на этом этапе происходит преобразование сигнала из временной области в частотную. Это выполняется благодаря БПФ – быстрому преобразованию Фурье. Эти две процедуры позволяют добиться максимально близкого размещения сигналов в частотной области и сократить до минимума защитные интервалы. Это достигается благодаря тому, что поднесущие выбираются ортогональными (на практике квазиортогональными), и отдельные потоки относительно легко выделить на приемной стороне.

Кроме использования OFDMA в LTE – есть еще одно важное новшество: обязательное (в отличие от UMTS) использование MIMO - Multiple Input Multiple Output – множественный вход множественный выход. При этом информационный поток направляется между сторонами обмена информации несколькими «путями», что обеспечивает более эффективное использование частотно-временного ресурса.

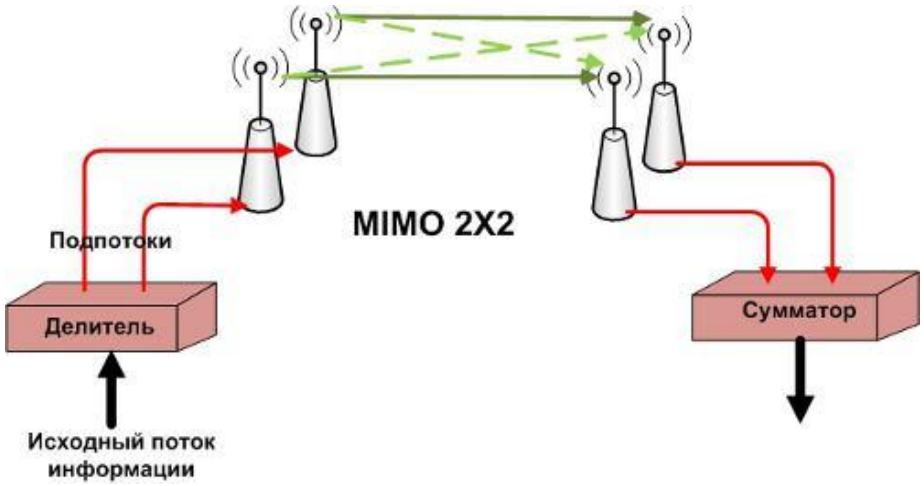


Рис. 3.99. MIMO 2x2

Эти два важных изменения позволяют добиться скорости передачи данных в Downlink свыше 100 Мбит/сек. Задержки передачи данных не превышают 20 мс. Для сравнения в UMTS скорости передачи данных редко поднимаются свыше 20 Мбит/сек, а задержки могут колебаться от 40 до 100 мс.

Принципы построения радиоинтерфейса LTE в Uplink (от МС к БС)

В сетях связи стандарта LTE скорость передачи данных в направлении от UE (МС) к eNodeB (БС) может достигать 50 Мбит/сек, а задержки не превышают 10мс. Эти показатели на много превышают значения в сетях третьего поколения и практически сравнялись с проводными выделенными каналами связи. Рассмотрим главные особенности построения радиоинтерфейса Uplink в стандарте LTE.

В отличие от радиоинтерфейса Downlink, где информация одного пользователя может передаваться на разных поднесущих, в Uplink данные каждого пользователя передаются в одной полосе частот, причем в одно и то же время. Однако это не означает, что информационные потоки накладываются друг на друга и необратимо искажаются. Это обеспечивается благодаря использованию множественного доступа с частотным разделением с единственной несущей частотой SC-FDMA (Single Carrier Frequency Devision Multiple Access). Рассмотрим основные принципы работы SC-FDMA – модулятора.

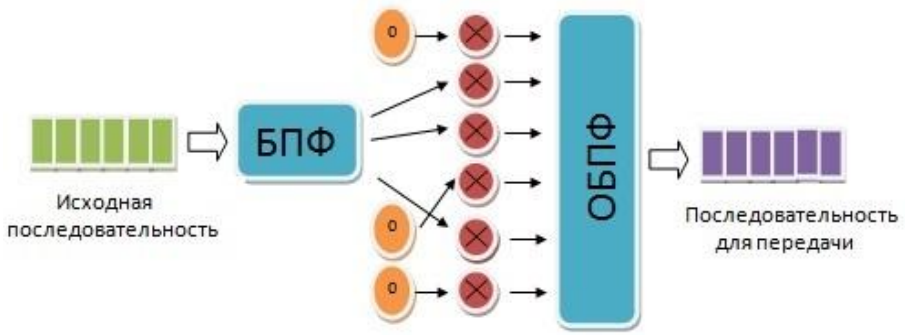


Рис. 3.100. SC-FDMA – модулятор

Первым этапом исходная информационная последовательность, предназначенная для передачи от абонента, преобразуется в частное представление с помощью быстрого преобразования Фурье (БПФ). Далее, в зависимости от скорости потока от данного абонента, сеть выделяет UE (MC) несколько поднесущих, среди которых распределяются преобразованный поток. Те поднесущие, которые используют другие пользователи не занимаются в данном абонентском терминале, а соответствующие поднесущие перемножаются с «0». После обратного быстрого преобразования Фурье (ОБПФ) модулированные потоки объединяются и переводятся обратно во временную область. Не смотря на то, что данные передаются от разных устройств в сети в одно и то же время в одной и той же полосе частот, на приемной стороне после обратных сказанным выше процедур, можно выделить информационные потоки от отдельных UE (MC).

Благодаря использованию SC-FDMA в системе LTE удалось достигнуть трехкратного увеличения спектральной эффективности на линии «вверх», по сравнению с сетями 3G.

Логические каналы на радиоинтерфейсе в LTE

Одной из важнейших составляющих радиоинтерфейса любой подвижной системы связи, которая обеспечивает заданные характеристики ее работы, является структура логических, транспортных и физических каналов. Рассмотрим логические параметры сети связи LTE.

Рис. 3.101. Логические каналы LTE

Логические каналы подразделяются по типам передаваемой информации на каналы управления и на трафиковые каналы.

К каналам управления относятся:

 BCCH (Broadcast Control Channel) – вещательный канал управления – служит для передачи системной служебной информации в Downlink.

 PCCH (Paging Control Channel) – пейджинговый канал управления – предназначен для передачи пейджинговых сообщений к UE (МС) от eNodeB (БС).

 MCCH (Multicast Control Channel) – многопользовательский канал управления – необходим для передачи служебной информации одновременно к нескольким абонентским устройствам.

 DCCH (Dedicated Control Channel) – выделенный канал управления – служит для передачи служебной информации между конкретным абонентским устройством и сетью.

 CCCH (Common Control Channel) – общий канал управления – предназначен для обмена служебной информацией между UE (МС) и сетью в процедурах начального доступа UE (МС) в сеть до организации выделенного канала.

К трафиковым каналам относятся:

 DTCH (Dedicated Traffic Channel) – выделенный трафиковый канал – основной канал для передачи пользовательских данных между одним конкретным UE (МС) и сетью.

 MTCH (Multicast Traffic Channel) – многопользовательский трафиковый канал – служит для передачи широковещательной трафиковой информации. Хорошим примером использования этого канала может служить трансляция радио или ТВ-программ.

Транспортные каналы на радиоинтерфейсе в LTE

На радиоинтерфейсе в сети стандарта LTE применяется стек каналов для передачи данных между абонентским терминалом и сетью. Низший уровень в этом стеке образуют

физические каналы. По ним передаются транспортные, которые в свою очередь несут логические каналы.

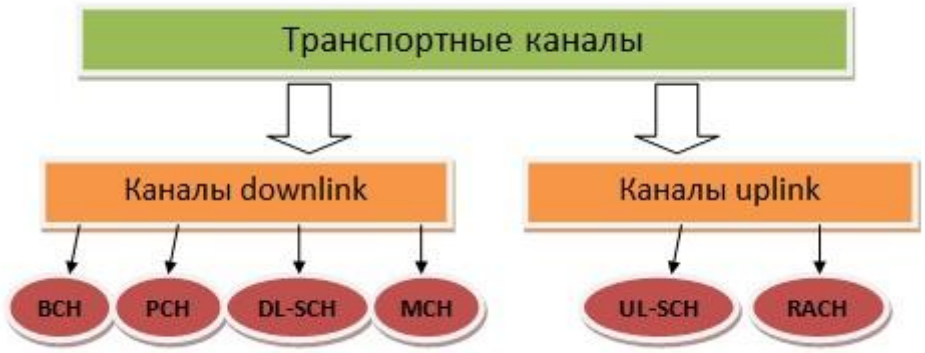


Рис. 3.102. Транспортные каналы LTE

Рассмотрим виды транспортных каналов на радиоинтерфйсе сети стандарта LTE. Все транспортные каналы можно классифицировать по направлению передачи: Uplink (от UE (МС) к eNodeB (БС)) и Downlink (от eNodeB (БС) к UE (МС)).

К транспортным каналам в Downlink относятся:

- BCH (Broadcast Channel) – широковещательный канал.
- PCH (Paging Channel) – канал для пейджинга.
- DL-SCH (Downlink Shared Channel) – общий канал для передачи данных вниз.
- MCH (Multicast Channel) – многопользовательский канал.

К транспортным каналам в Uplink относятся:

- RACH (Random Access Channel) – канал случайного доступа.
- UL-SCH (Downlink Shared Channel) – общий канал для передачи данных вверх.

Как было сказано выше, транспортные каналы передаются в логических каналах. На рисунке ниже представлена связь между логическими и транспортными каналами в LTE.

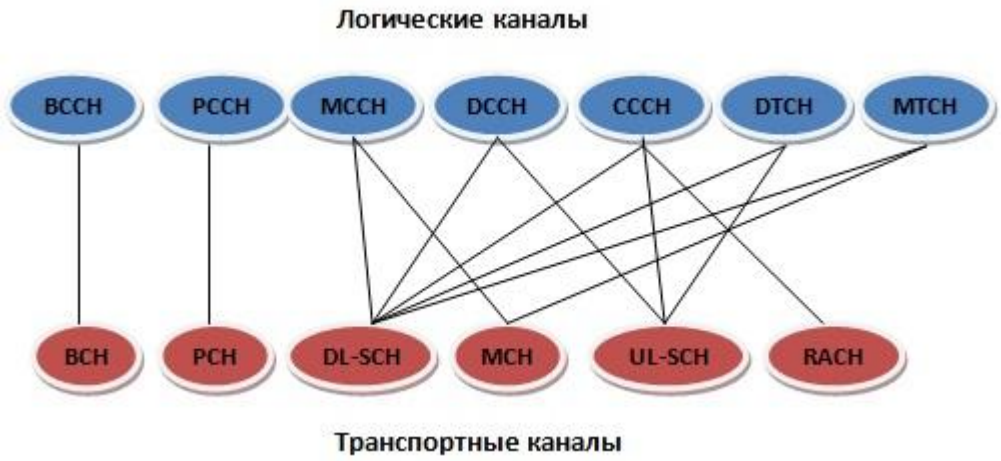


Рис. 3.103. Связь логических и транспортных каналов

Физические каналы на радиоинтерфейсе в LTE

Информация между UE (МС) и eNodeB (БС) передается не произвольным образом, а через четко организованную структуру каналов. Рассмотрим классификацию, виды и назначение физических каналов в сети LTE.

Рис. 3.104. Физические каналы LTE

Физические каналы можно классифицировать по направлению передачи информации: Downlink и Uplink.

К физическим каналам в Downlink относятся:

- PDSCH (Physical Downlink Shared Channel) - физический распределенный канал в направлении «вниз» - служит для высокоскоростной передачи мультимедийной информации.
- PDCCH (Physical Downlink Control Channel) – физический канал управления в направлении «вниз» - предназначен для передачи информации для управления конкретным UE (МС).
- CCPCH (Common Control Physical Channel) – общий физический канал управления – необходим для передачи общей для всех информации.

К физическим каналам в Uplink относятся:

- PRACH (Physical Random Access Channel) – физический канала произвольного доступа – служит для первичного доступа в сеть.
- PUCCH (Physical Uplink Control Channel) – физический канал управления в направлении «вверх» - необходим для передачи служебной информации от конкретной UE (МС) к eNodeB (БС).
- PUSCH (Physical Uplink Shared Channel) – физический распределенный канал в направлении «вверх» - предназначен для высокоскоростной передачи данных в Uplink.

Связь между транспортными и физическими каналами представлена на рисунке ниже.

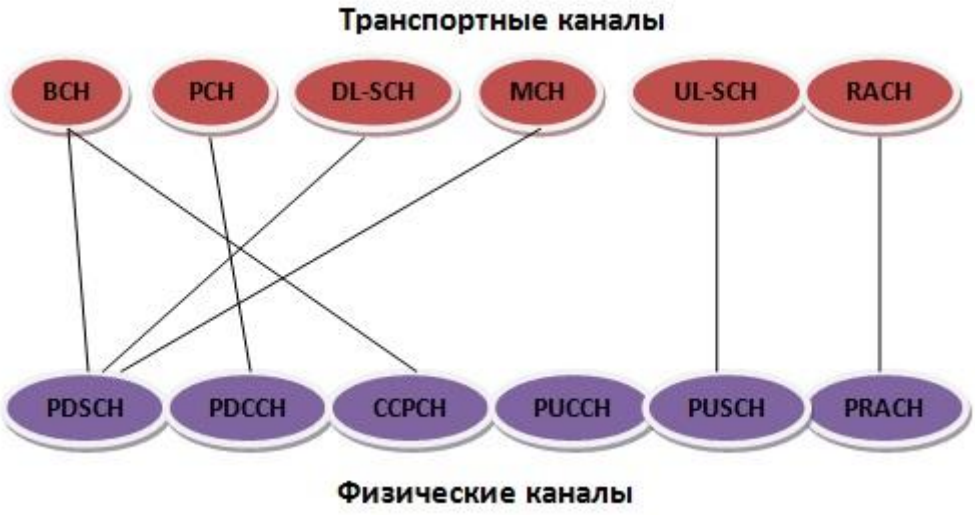


Рис. 3.105. Связь физических и транспортных каналов

Основные параметры LTE

Таблица 3.16. Основные параметры LTE

Название параметра	Параметр
Uplink (UL): восходящее соединение	SC-FDMA
Downlink (DL): нисходящее соединение	OFDMA
Ширина частотного диапазона, МГц	1,4; 3, 5; 10; 15; 20
Минимальный интервал между кадрами, мс	1
Шаг (частотный интервал) между поднесущими, кГц	15
Стандартная длина префикса CP, мкс	4,7
Увеличенная длина префикса CP, мкс	16,7
Схемы модуляции (Uplink)	BPSK, QPSK, 8PSK, 16QAM

Схемы модуляции (Downlink)	QPSK, 16QAM, 64QAM
Пространственное мультиплексирование	Один канал для Uplink-трафика на каждый абонентский терминал; До 4 каналов для Downlink-трафика на каждый абонентский терминал; MU-MIMO с поддержкой для восходящего (Uplink) и нисходящего (Downlink) соединений

Практическая реализация

Как было сказано выше, на практике будет реализован канал Downlink системы мобильной связи стандарта LTE. Структура данного канала представлена на рисунке 3.106 [25].

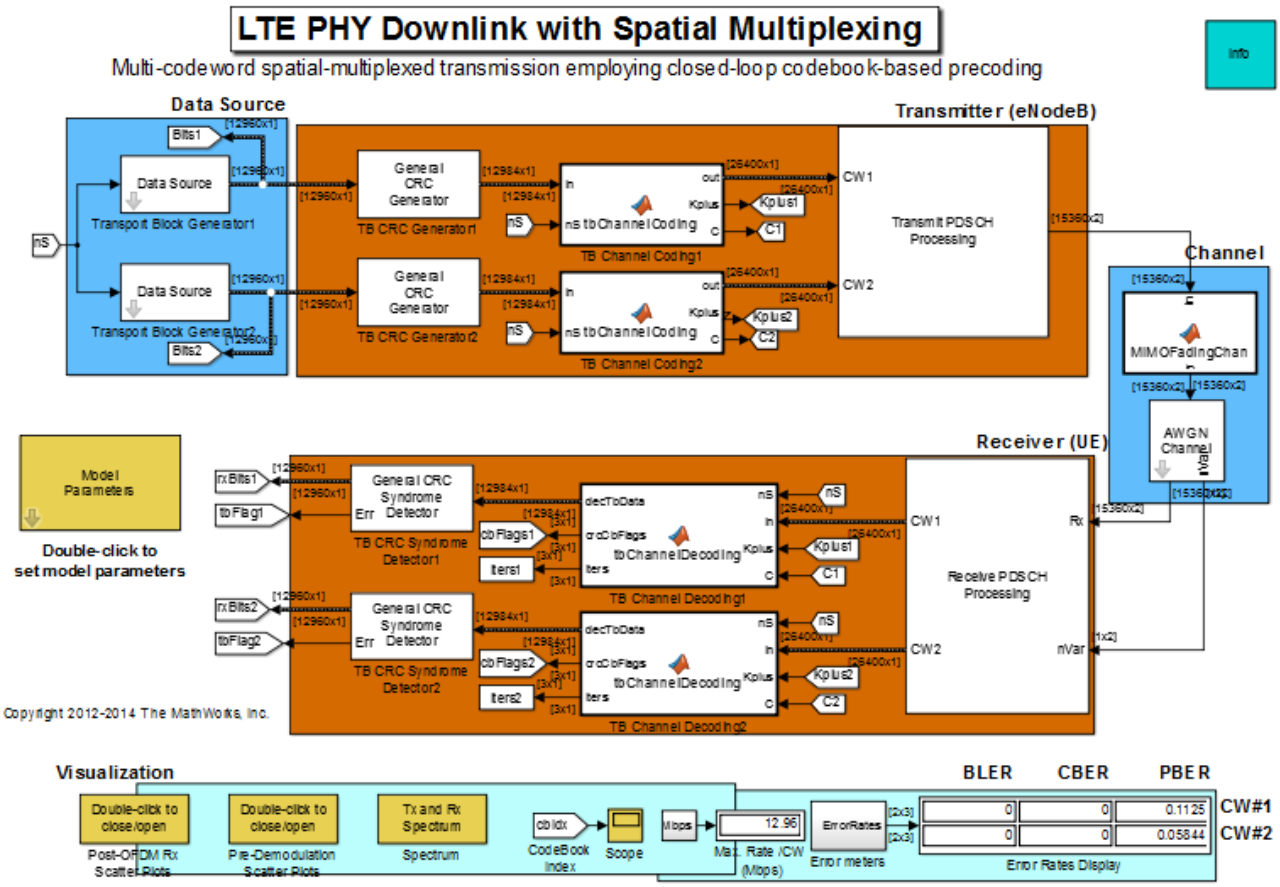


Рис. 3.106. Канал Downlink LTE Simulink MATLAB 2015b

Рассмотрим более подробно данный канал.

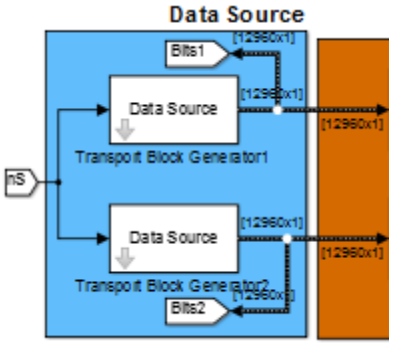


Рис. 3.107. Разделение исходного потока бит на параллельные потоки

- Кодирование помехоустойчивым кодом, в процессе которого значительно увеличивается число символов в отдельных потоках. В данной схеме используется код CRC.

Каждый отдельный параллельный поток кодируется данным кодом с заданным полиномом.

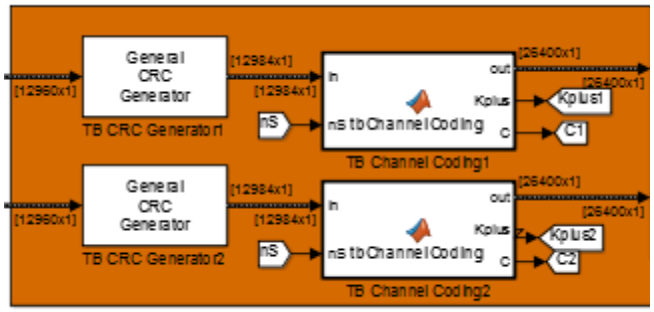


Рис. 3.108. Кодирование помехоустойчивым кодом

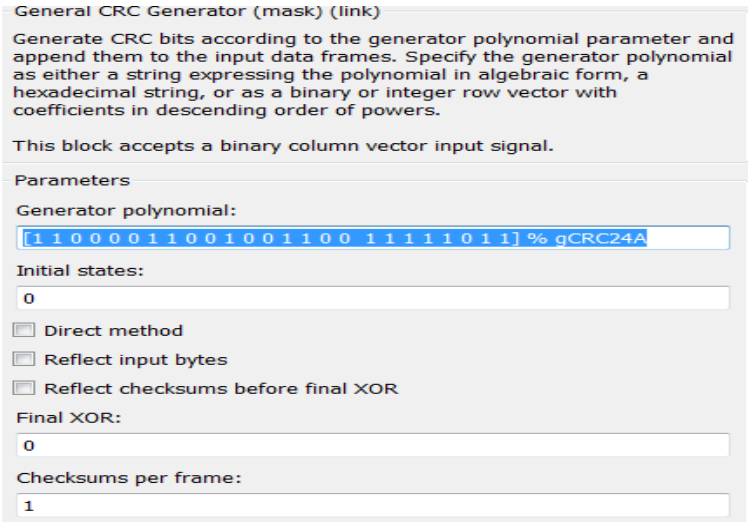


Рис. 3.109. Параметры CRC кодера

- Манипуляция выбранным в данный конкретный момент способом модуляции. В канале Downlink используются методы манипуляции: QPSK, 16QAM, 64QAM. Далее перемножение полученной последовательности каждого потока на свою поднесущую и БПФ (так называемая OFDM – модуляция). Где в результате получаем один сложный сигнал.

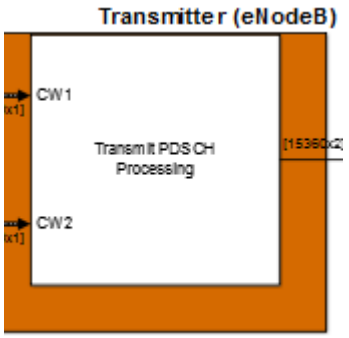


Рис. 3.110. Манипуляция выбранным в данный конкретный момент способом модуляции

Структура этого блока имеет следующий вид:

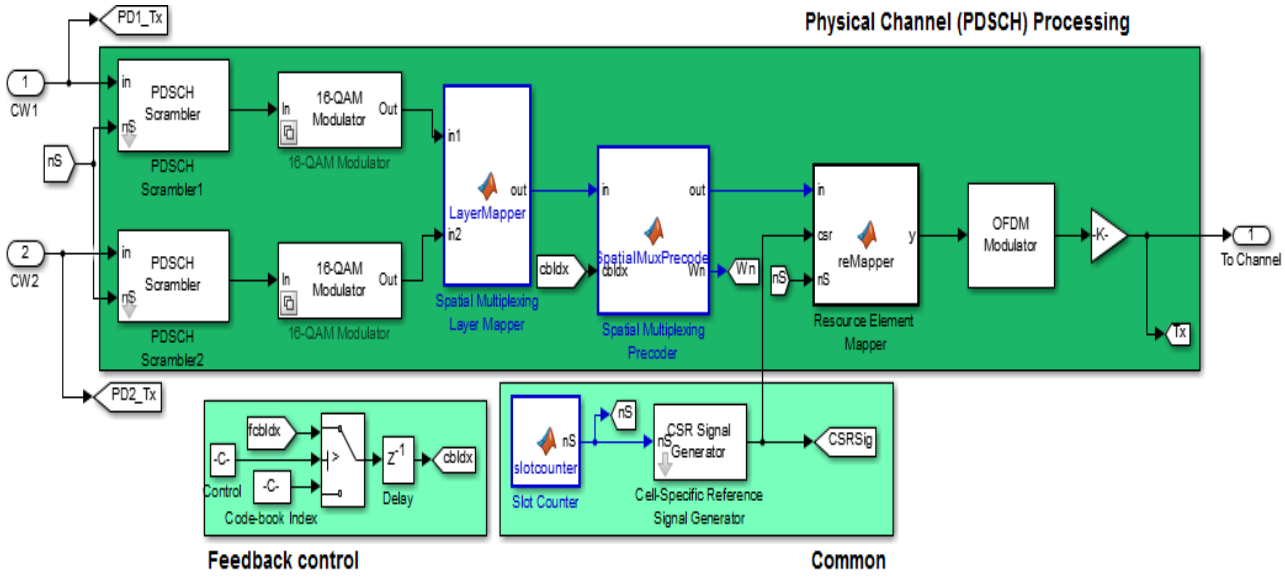


Рис. 3.111. Квадратурная манипуляция и получение OFDM символов

- Передача в эфир. Для этого используется технология MIMO 2x2 или 4x4 приемных/передающих антенн. Где один общий поток (сигнал) разделяется на 2 потока (2x2 антенна) или 4 потока (4x4 антенна).

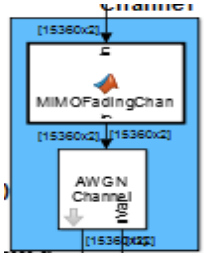


Рис. 3.114. Передача в эфир

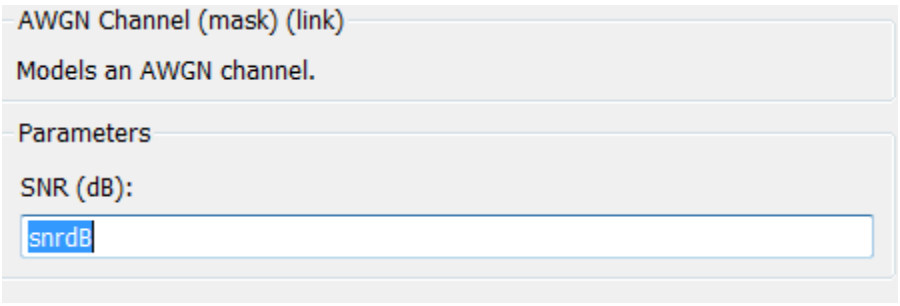


Рис. 3.111. Характеристики блока БГШ (AWGN)

Далее подпотоки MIMO объединяются в один поток, который приходит на мобильную станцию под воздействием помех.

Далее мобильная станция производит обратные преобразования, реализованные выше, а именно, получаем паралельные потоки. Потом производится обратное быстрое преобразование Фурье (ОБПФ). Затем производится демодуляция.

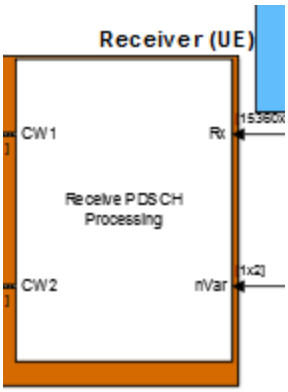


Рис. 3.113. Паралельные потоки-ОБПФ-демодуляция

Схема, входящая в данный блок:

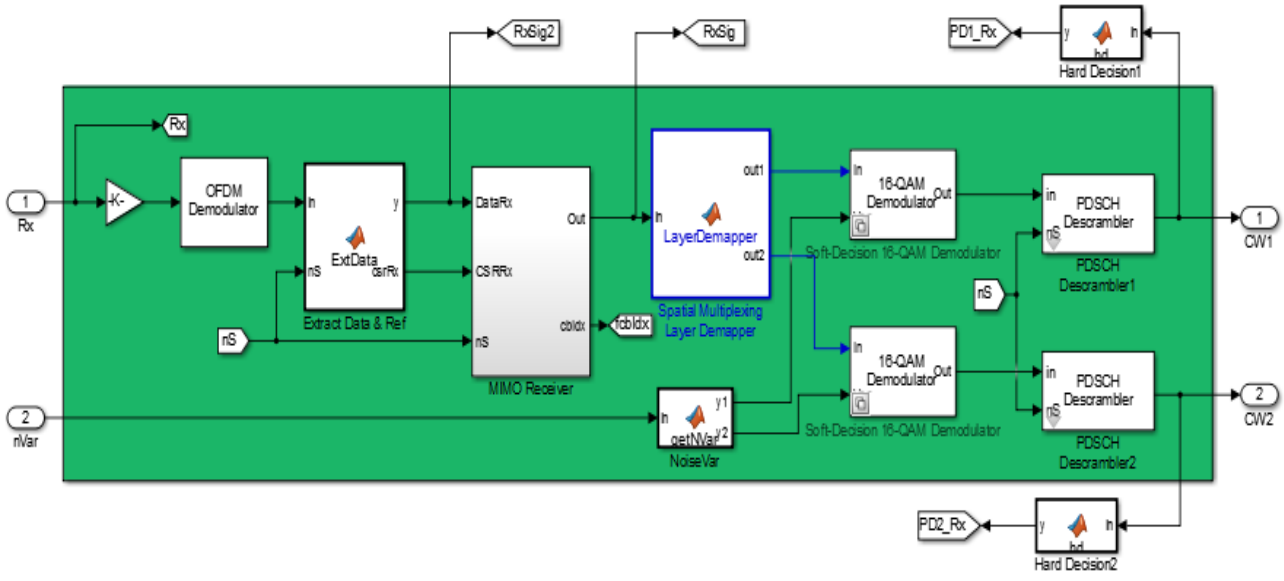


Рис. 3.114. Паралельные потоки-ОДПФ-демодуляция

Далее производится декодирование по соответствующему алгоритму CRC:

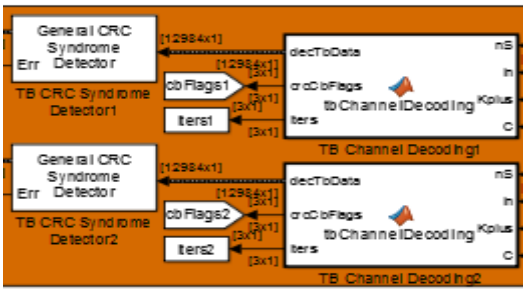


Рис. 3.115. Декодирование CRC

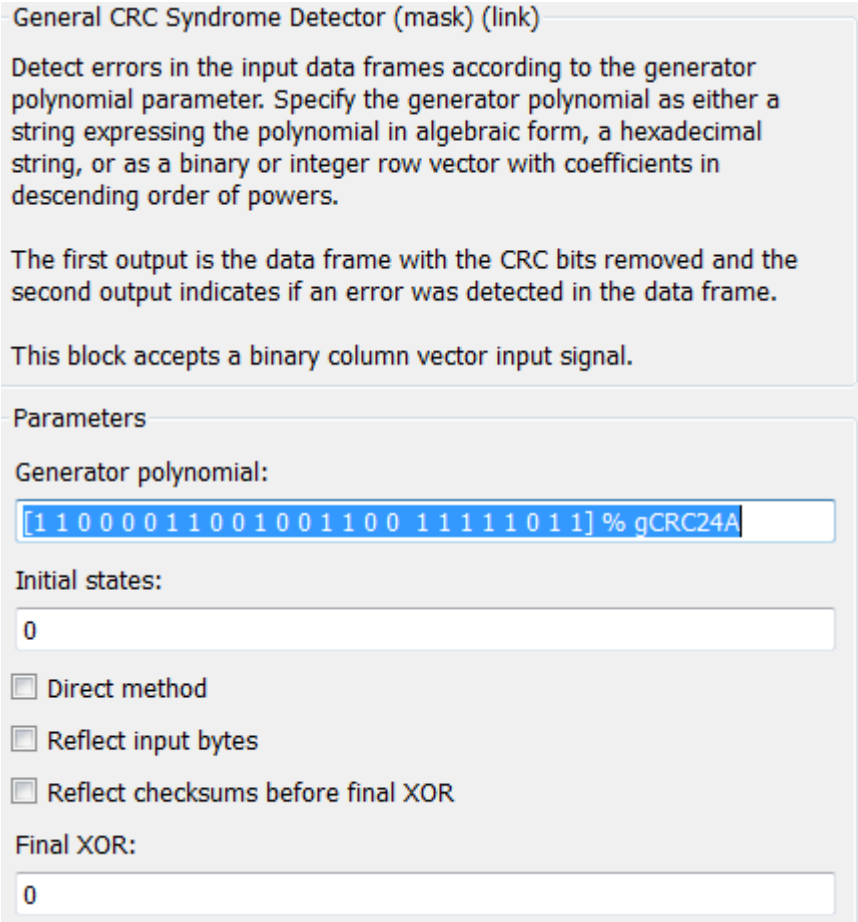


Рис. 3.116. Характеристики декодера CRC

После декодирования производится преобразование параллельных потоков в один исходный поток:

Рис. 3.117. Получение исходного потока

Данная схема позволяет формировать характеристики передачи данных по этому каналу, а именно это ширина спектра, количество антенн в MIMO, вид модуляции, отношение сигнал/шум:

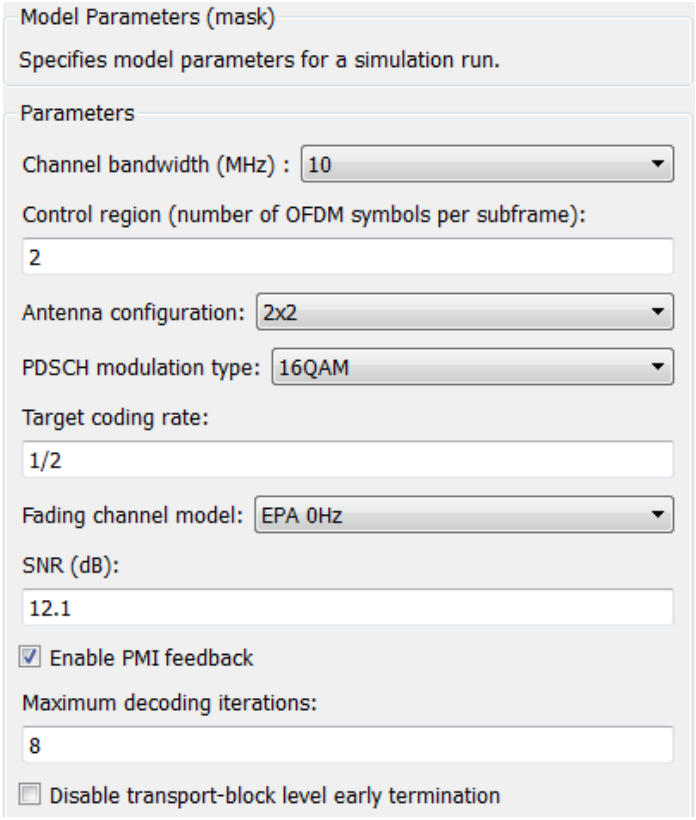


Рис. 3.118. Характеристики канала

В результате работы схемы можно получить некоторые зависимости:

1. Спектр передаваемого и принятого сигнала.

2. Диаграмму созвездий передаваемого и принятого сигнала (для каждой из антенн MIMO).

3. Итерации декодера в зависимости от времени и кодовых слов для каждого параллельного потока.

Также можно построить зависимость битовой вероятности ошибки при заданном отношении сигнал/шум каждого параллельного потока отдельно, меняя значения отношения сигнал/шум.

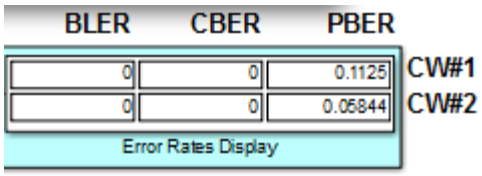


Рис. 3.119. Информация о битовой вероятности ошибки параллельных потоков

В качестве примера зададим следующие характеристики передачи данных:

- Ширина спектра - 10 МГц.
- Количество антенн MIMO – 4x4.
- Модуляция – QPSK.
- Отношение сигнал/шум – 1 дБ.

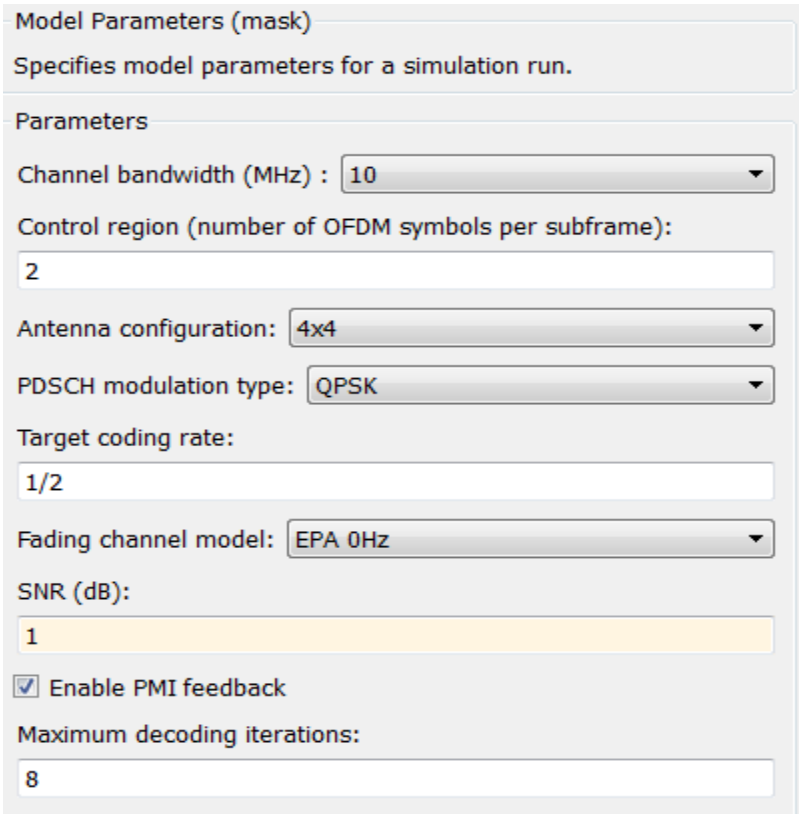


Рис. 3.120. Характеристики передачи данных

В результате получим следующие зависимости:

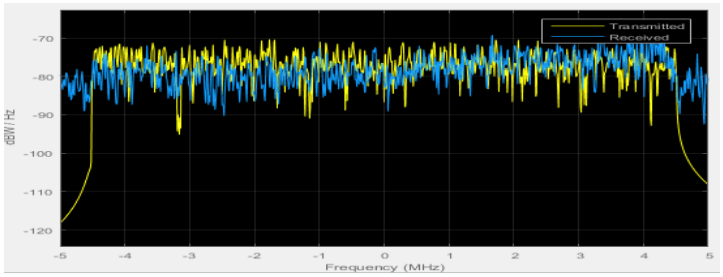


Рис. 3.121. Спектр входного (желтым) и выходного (синим) сигналов

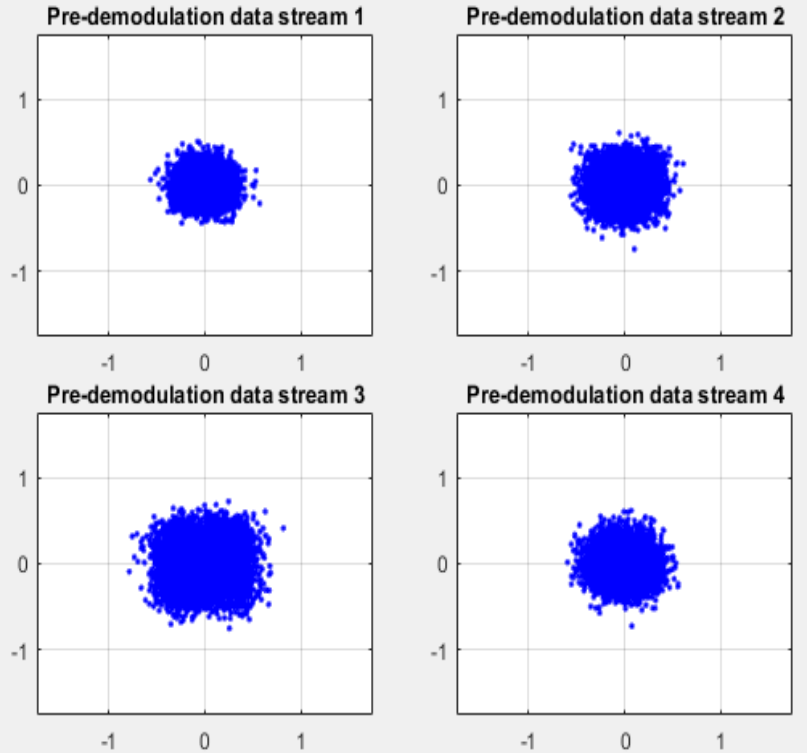


Рис. 3.122. Диаграмма созвездий переданного сигнала для каждой из антенн MIMO

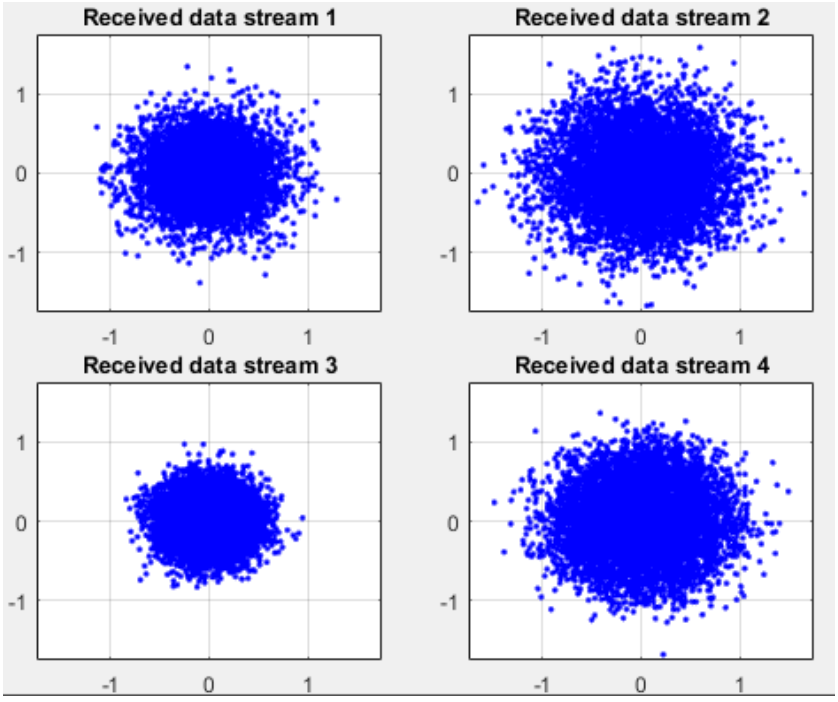


Рис. 3.123. Диаграмма созвездий принятого сигнала для каждой из антенн MIMO

На основании полученных значений, построим зависимость.

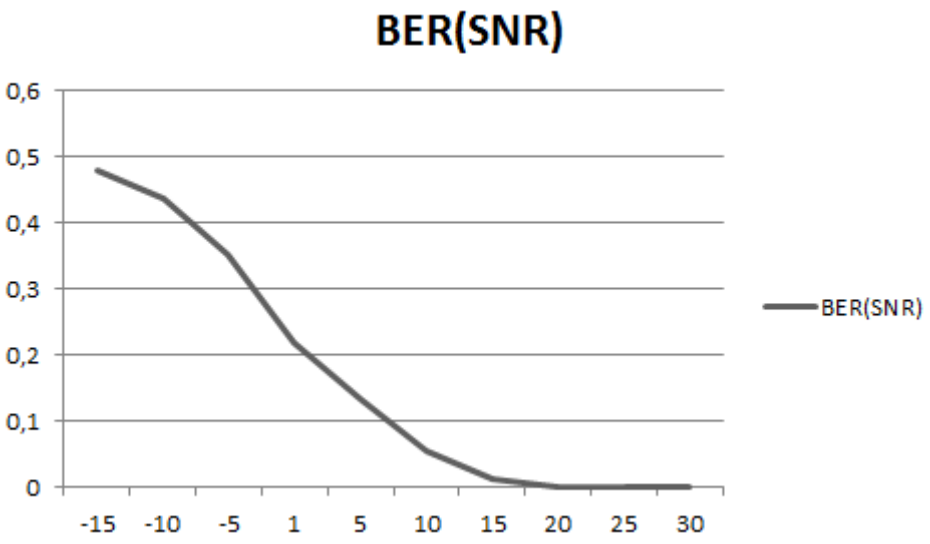


Рис. 3.124. Зависимость битовой вероятности ошибки от отношения сигнал/шум для первого потока

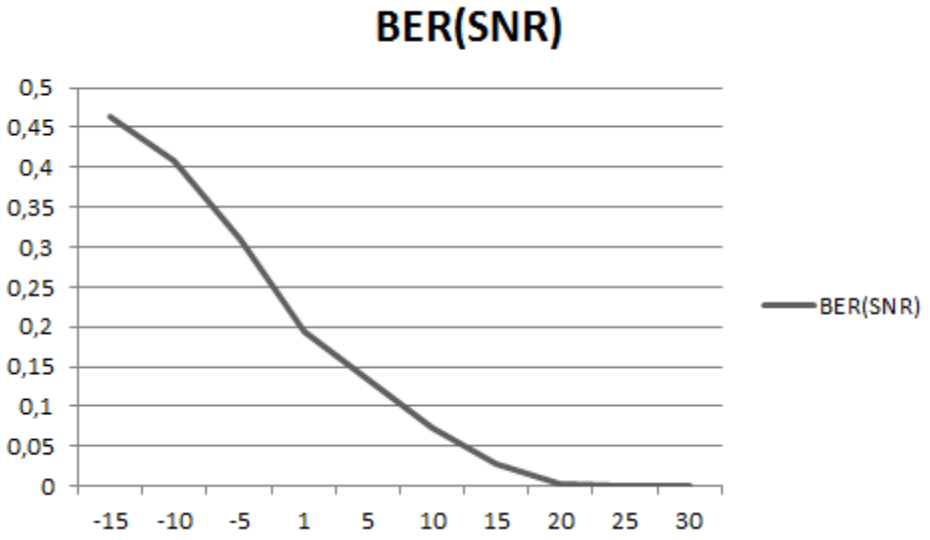


Рис. 3.125. Зависимость битовой вероятности ошибки от отношения сигнал/шум для второго потока

В качестве еще одного примера зададим следующие характеристики передачи данных:

- Ширина спектра - 10 МГц.
- Количество антенн MIMO – 2x2.
- Модуляция – QPSK.
- Отношение сигнал/шум – 1 дБ.

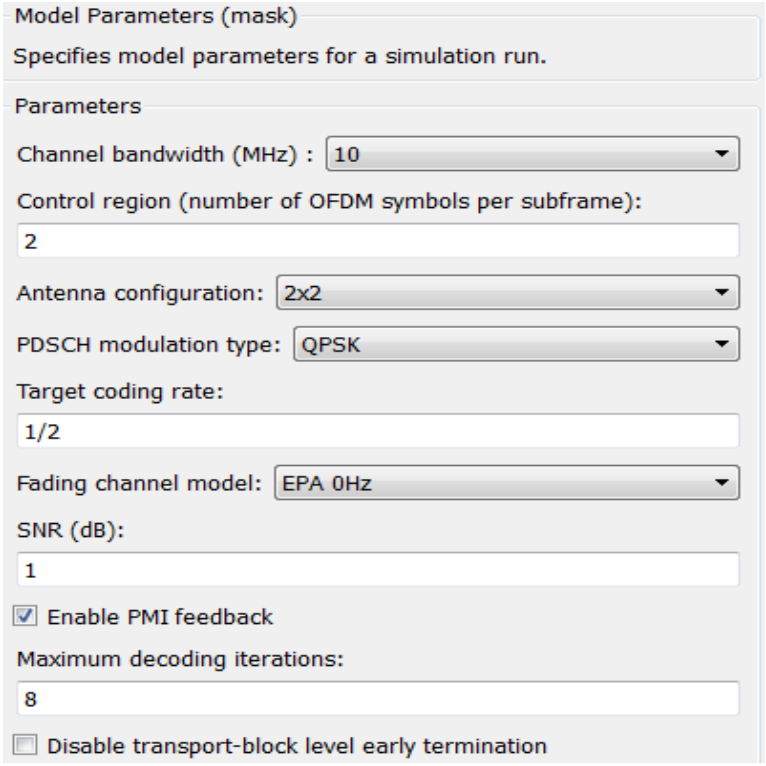


Рис. 3.126. Характеристики передачи данных

В результате получим следующие зависимости:

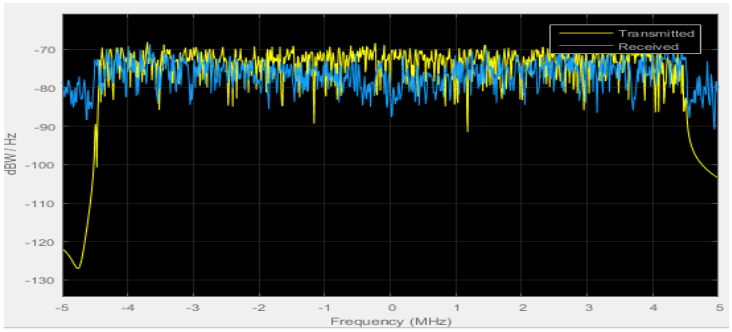


Рис. 3.127. Спектр входного (желтым) и выходного (синим) сигналов

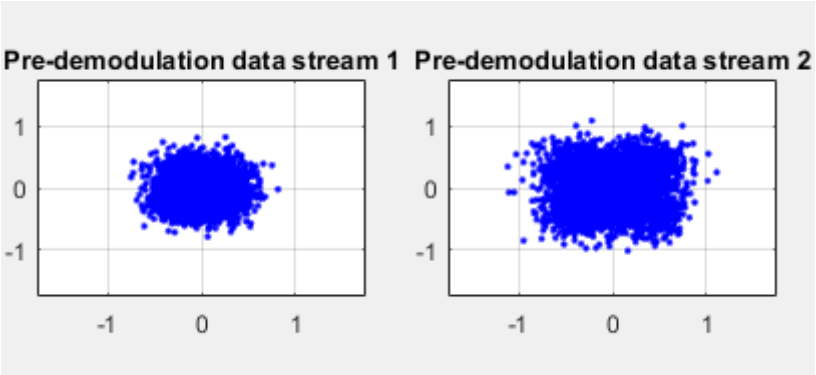


Рис. 3.128. Диаграмма созвездий переданного сигнала для каждой из антенн MIMO

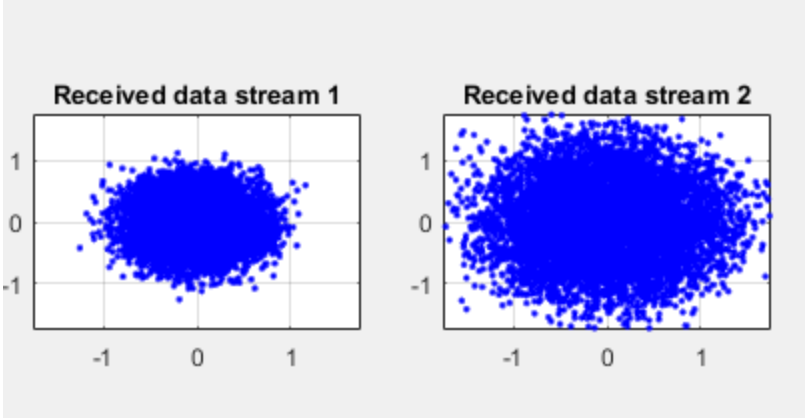


Рис. 3.129. Диаграмма созвездий принятого сигнала для каждой из антенн MIMO

Изменим отношение сигнал/шум – -15, -10, -5, 1, 5, 10, 15, 20, 25 и 30 дБ и построим зависимость битовой вероятности ошибки от отношения сигнал/шум для десяти точек для обоих параллельных потоков

На основании полученных значений, построим зависимость.

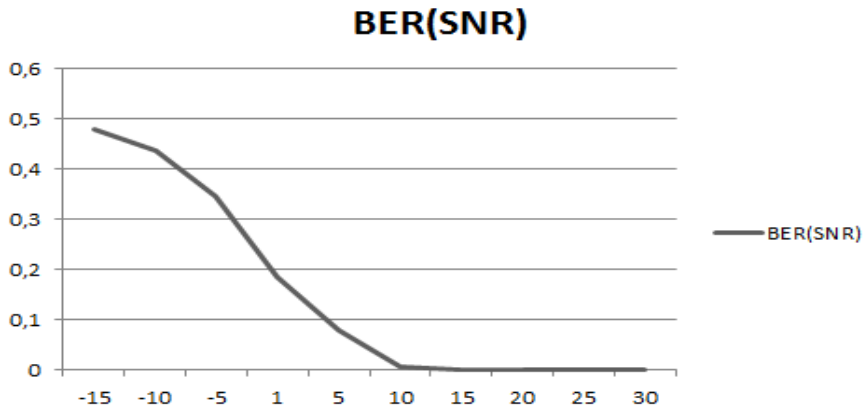


Рис. 3.130. Зависимость битовой вероятности ошибки от отношения сигнал/шум для первого потока

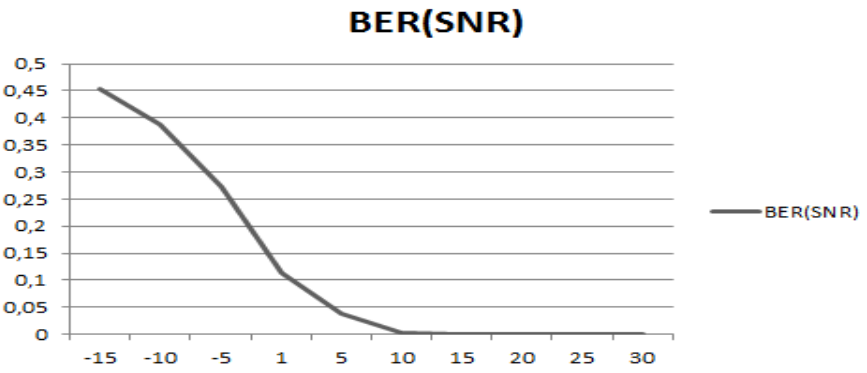


Рис. 3.131. Зависимость битовой вероятности ошибки от отношения сигнал/шум для второго потока

Методика и проведение исследования канала Downlink

Запустить Matlab 15 от имени администратора (обязательно).

В результате запуска на экране монитора появится следующее окно:

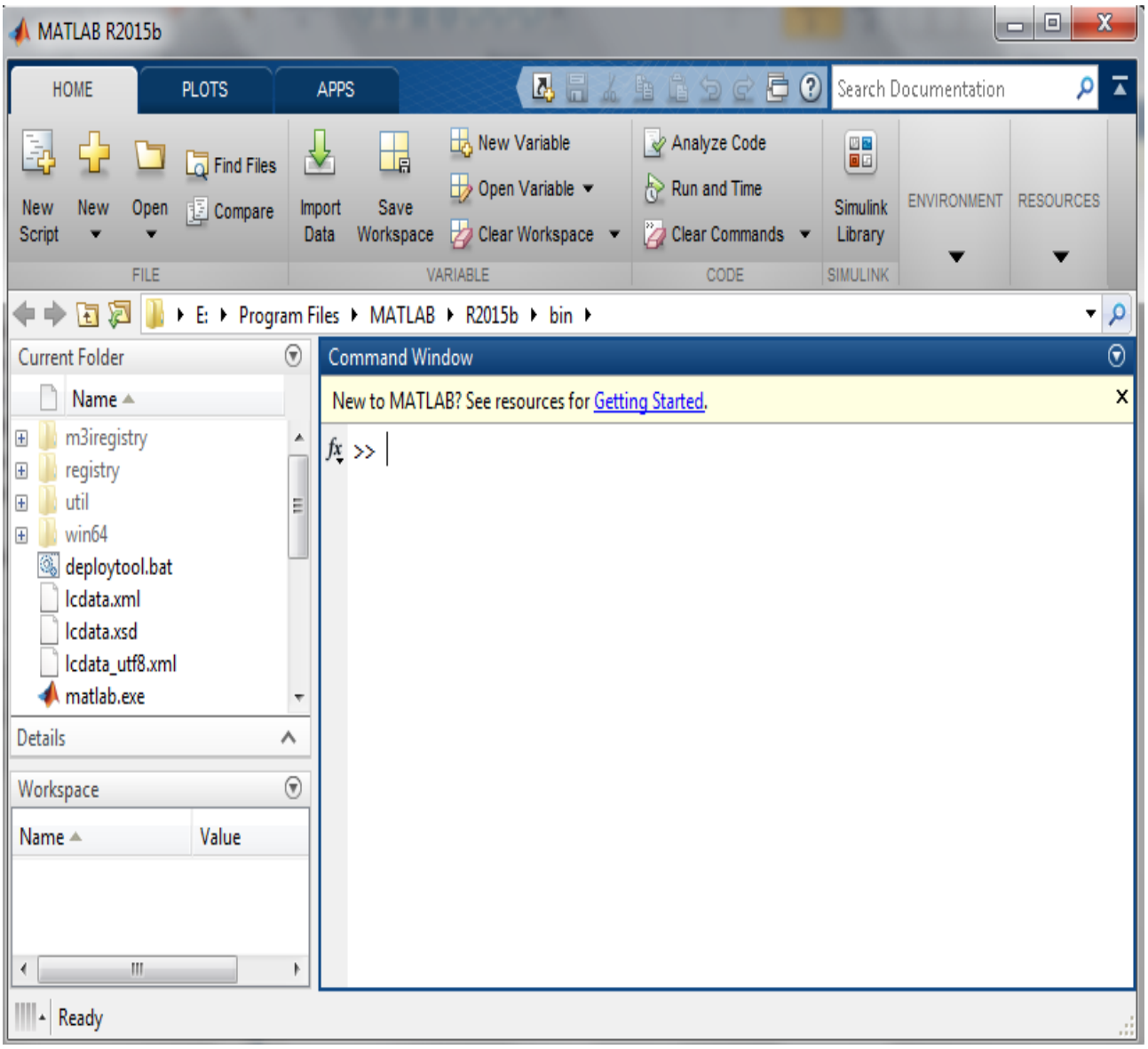


Рис. 3.132. Диалоговое окно Matlab 15

1. В командной строке программы прописать: cd ../ (при пропуске данного пункта могут возникнуть проблемы при компиляции).

2. В командной строке программы прописать LTEDownlinkExample, в результате откроется окно со схемой в программе, которое имеет следующий вид:

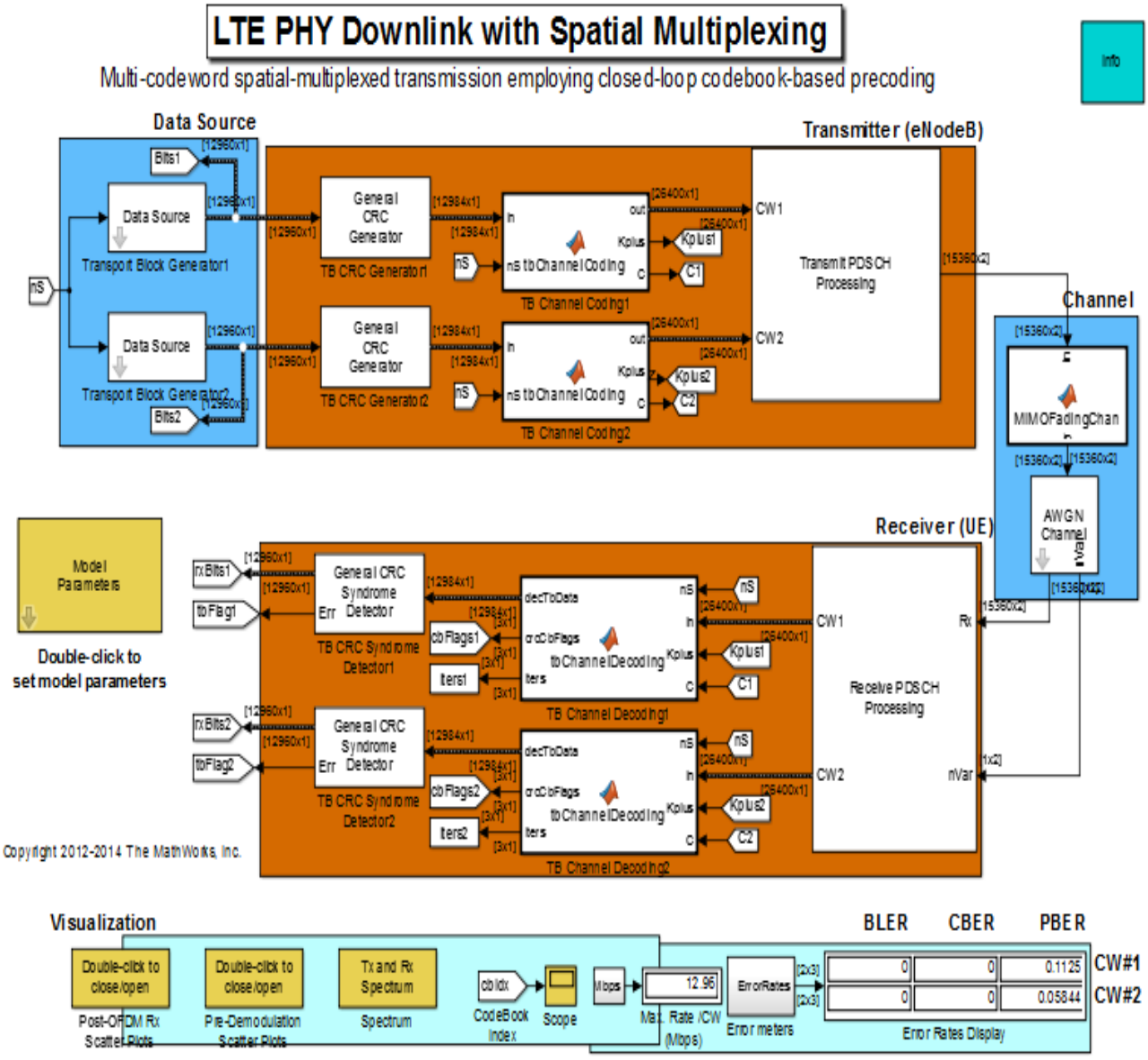


Рис. 3.133. Схема канала Downlink

3. Задать следующие характеристики передачи данных:

- Модуляция – QAM-16.
- Количество антенн MIMO 2x2.
- Ширина спектра – 10 МГц.

4. Изменять отношение сигнал/шум – -15, -10, -5, 1, 5, 10, 15, 20, 25, 30 дБ (SNR) и на каждом его значении фиксировать в отчете выходные зависимости, а именно спектр переданного и принятого сигналов, диаграммы созвездий на каждой из антенн MIMO для переданного и принятого сигналов, итерации декодера в зависимости от времени и кодовых слов первого потока и второго потока. Так же на каждом шаге фиксировать значение битовой вероятности ошибки (BER) обоих параллельных потоков. И после окончания исследования построить зависимости BER от SNR обоих параллельных потоков.

5. Содержание отчета

- Титульный лист.
- Цель работы.
- Теория канала Downlink.
- Исследуемая схема канала Downlink.
- Результаты работы по пунктам 6 и 7.
- Заключение.

В результате выполнения в разделе были выполнены следующие мероприятия:

1. Проведен теоритический анализ стандарта мобильной связи стандарта LTE. Проведен анализ сравнения данного стандарта с уже устаревающими стандартами на данный момент – UMTS (3G) и GSM (2G). Также было проведено аналитическое исследование физических каналов стандарта – Downlink (от БС к МС) и Uplink (от МС к БС), а также логические и транспортные каналы. Приведены обобщенные схемы формирования данных каналов.

2. Путем проведения компьютерной симуляции, была проверена достоверность теоритического исследования. В программе Matlab 15 были собрана схема канала Downlink.

3. С помощью компьютерной симуляции были получены различного рода зависимости при передаче информации по каналу. Самая важная из них это зависимость битовой вероятности ошибки от отношения сигнал/шум. В результате получились следующие значения:

Таблица 3.17. Зависимость BER от SNR при MIMO 4x4

сигнал/шум (дБ)	**1 поток (BER)**	**2 поток (BER)**
-15	0,4766	0,4537
-10	0,4347	0,3876
-5	0,3456	0,2729
1	0,1836	0,114
5	0,0774	0,039
10	0,0076	0,0027
15	0,000001	0,000002

20	**0**	**0**
25	**0**	**0**
30	**0**	**0**

Таблица 3.18. Зависимость BER от SNR при MIMO 2x2

сигнал/шум (дБ)	**1 поток (BER)**	**2 поток (BER)**
-15	0,4772	0,4645
-10	0,4354	0,4073
-5	0,3512	0,3096
1	0,2178	0,1933
5	0,1347	0,1345
10	0,056	0,074
15	0,0137	**0,0282**
20	0,0003	0,0037
25	**0**	0,000003
30	**0**	**0**

4. Анализируя полученные значения таблицы 3, можно сделать следующий вывод, что при увеличении отношения сигнал/шум, битовая вероятность ошибки стремится к нулю быстрее в MIMO 4x4, нежели в MIMO 2x2. Таким образом, использование большего числа приемо-передающих антенн, дает меньшие ошибки.

5. Была написана методика исследования канала Downlink.

6. Также я познакомился с различным программным обеспечением, для построения различного вида схем.

Подведя итог своего курсового проекта, можно сказать следующее, то, что я сделал, является основополагающим делом к дальнейшим, более трудным вещам. Курсовой проект был весьма увлекательным и полезным. С поставленными целями справился успешно.

4. ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ СИТЕМ ЦИФРОВОГО ТЕЛЕВИЗИОННОГО ВЕЩАНИЯ

4.1. Проектирование защищенной системы системы цифрового наземного телевизионного вещания DVB-T [17, 21]

Объектом исследования является система цифрового телевидения на базе стандарта DVB-T. Цель лабораторной работы – закрепленных знаний полученных при изучении дисциплины «Основы проектирования защищенных телекоммуникационных систем». Задача лабораторной работы – исследование основных характеристик системы цифрового наземного телевещания стандарта DVB-T.

В 1993 году группа ведущих европейских компаний-производителей вещательного оборудования образовала некоммерческую организацию по разработке стандартов цифрового телевизионного вещания, получившую название DVB Project.

Для каждой транспортной среды был разработан стандарт обработки и передачи транспортно потока, учитывающий ее специфику и в то же время максимально инфицированный со смежными стандартами. Для упрощения взаимного обмена программами выбраны такие параметры обработки, чтобы пропускная способность и число передаваемых ТВ программ во всех случаях оставались бы примерно одинаковыми. Документ для спутникового вещания получил сокращенное наименование DVB-S, для сетей кабельного телевидения - DVB-C, для наземного (эфирного) телевидения DVB-T.

Концепция стандарта DVB-T

Одним из первых решений данной организации было решение принять за основу всех разработок стандарт цифрового сжатия MPEG-2. Однако, данный стандарт не охватывает передачу цифрового сигнала по каналам связи и его необходимо дополнить документами, регламентирующими обработку сигнала перед подачей в канал.

Второе важное решение – использование общего MPEG-2 мультиплекса во всех средах распространения и максимальная унификация методов помехоустойчивого кодирования и модуляции. Во всех случаях используется код Рида-Соломона с единым размером блока, и в тех случаях где это необходимо, - сверточный код с единым набором относительных скоростей. Очень важна для широкого круга концепция «контейнера данных» - создание универсального цифрового канала, переносящего видео, аудио, данные пользователя в любых пропорциях и с высокими показателями качества обслуживания.

Передаваемая информация в системе DVB-T представляет собой пакеты транспортного потока MPEG-2. Для рассматриваемой системы содержание контейнера не имеет значение, она лишь приспосабливает данные транспортного мультиплексора MPEG-2 к свойствам и характеристикам канала передачи наземного телевизионного вешания,

стремясь наиболее эффективно донести их приемнику. Иными словами, стандарт DVB-T определяет только структуру передаваемого потока данных, систему канального кодирования и модуляции.

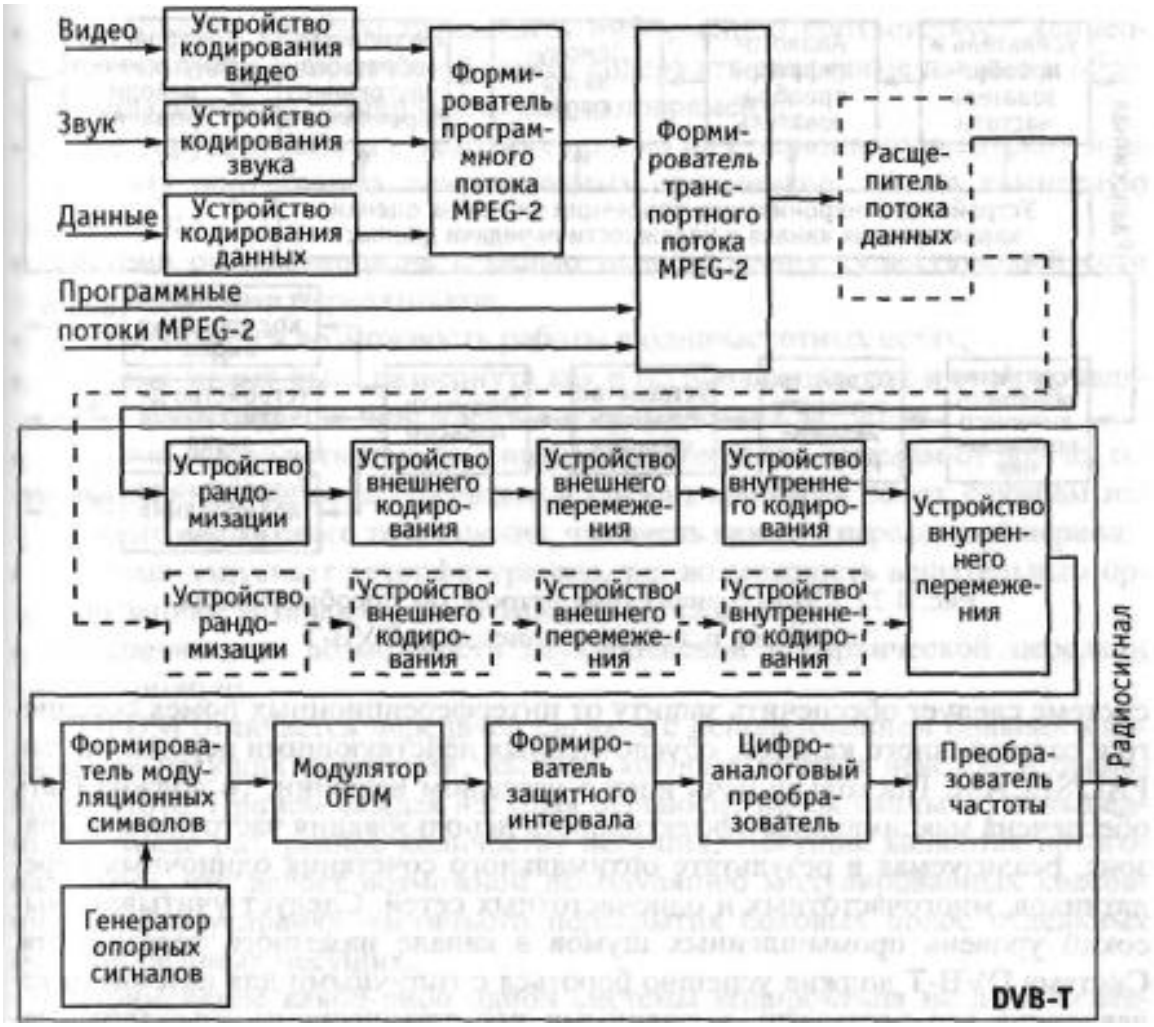


Рис. 4.1. Структурная схема передатчика системы DVB-T

На приемной стороне выполняются операции, обратные операциям производимым в приемнике.

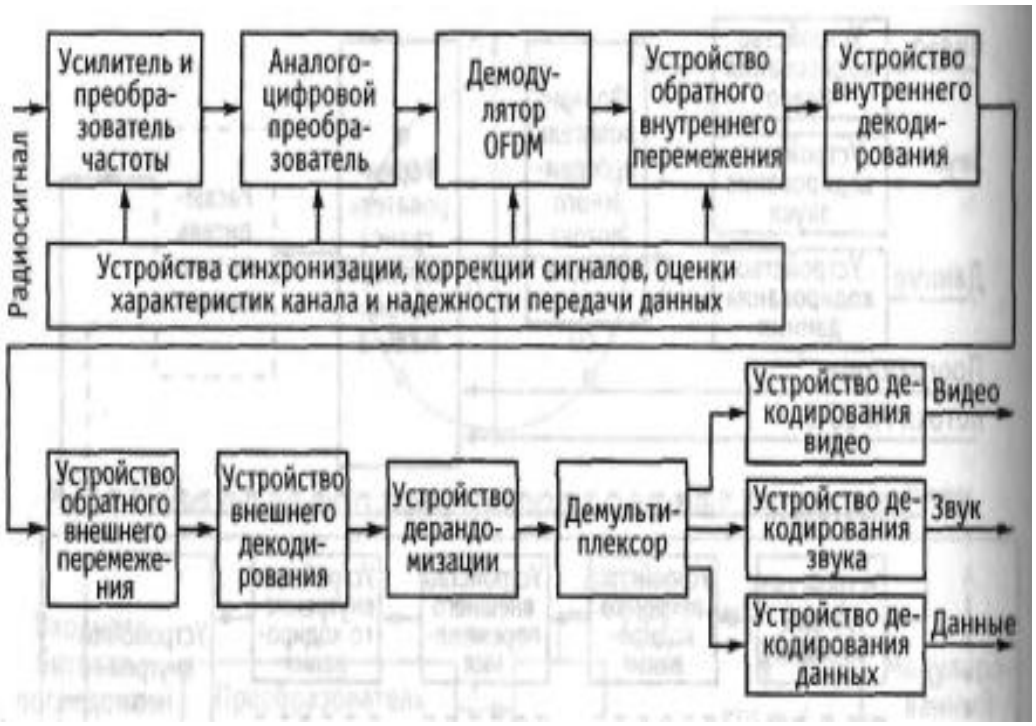


Рис. 4.2. Структурная схема приемника системы DVB-T

Обработка данных и сигналов в системе DVB-T

Адаптация транспортных пакетов MPEG-2 в системе DVB-T. Рандомизация

Адаптация транспортных пакетов MPEG-2 в исследуемой системе осуществляется путем включения в общий поток информационных 187 байт одного байта синхронизации.

Рис. 4.3. Адаптация транспортных пакетов в системе MPEG-2

Рандомизация данных является первой операцией, выполняемой в системе DVB-T. Ее цель – превратить цифровой сигнал в квазислучайный и тем самым решить две важные задачи. Первая – обеспечение возможности выделения из него тактовых импульсов (самосинхронизация). Вторая – приведение более равномерного энергетического спектра излучаемого радиосигнала. Рандомизация осуществляется путем сложения по модулю 2, то есть посредством логической операции «исключающее ИЛИ» цифрового потока данных и двоичной псевдослучайной последовательности.

Рис. 4.4. Структурная схема устройства рандомизации данных

Внешнее кодирование и перемежение

Как было отмечено выше, в системе внешнего кодирования для защиты всех 188 байт транспортного пакета (включая байт синхронизации) используется код Рида-Соломона (204, 188). В процессе кодирования к этим 188 байтам добавляется 16 проверочных байт. Стоит отметить, что при декодировании на приемной стороне это позволяет исправлять до восьми ошибочных байт в пределах каждого кодового слова длиной 204 байта.

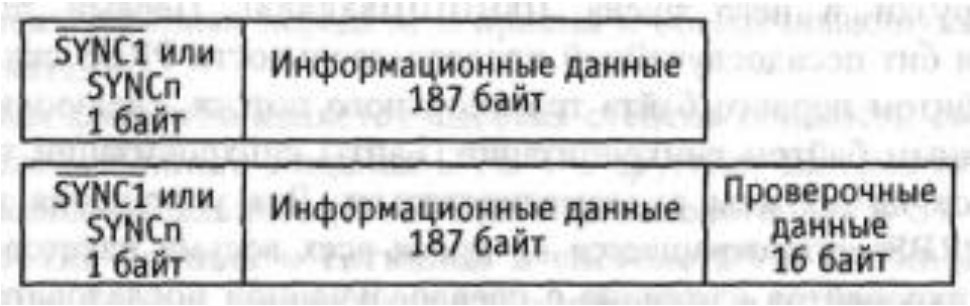


Рис. 4.5. Структурная схема устройства рандомизации данных

Внешние перемежение осуществляется путем изменения порядка следования байт в пакетах, защищенных от ошибок. В соответствии со схемой представленной на слайде перемежение выполняется путем последовательного циклического подключения источника и получателя данных к двенадцати ветвям, причем за одно подключение в ветвь направляется и снимается 1 байт данных. В одиннадцати ветвях включены регистры сдвига, содержащие разное количество ячеек и создающие увеличивающиеся от ветви к задержку. Первый же синхробайт поступает в 0 ветвь, которая не содержит задержки, что не создает проблем синхронизации.

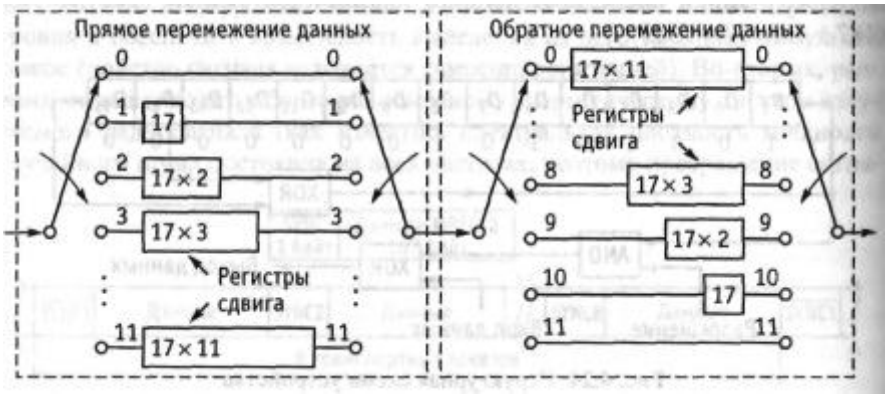


Рис. 4.6. Функциональная схема внутреннего перемежителя данных

Внутреннее кодирование

Функциональная и структурная схема кодера/декодера сверточного кода используемого в системе DVB-T может быть представлена в следующем виде:

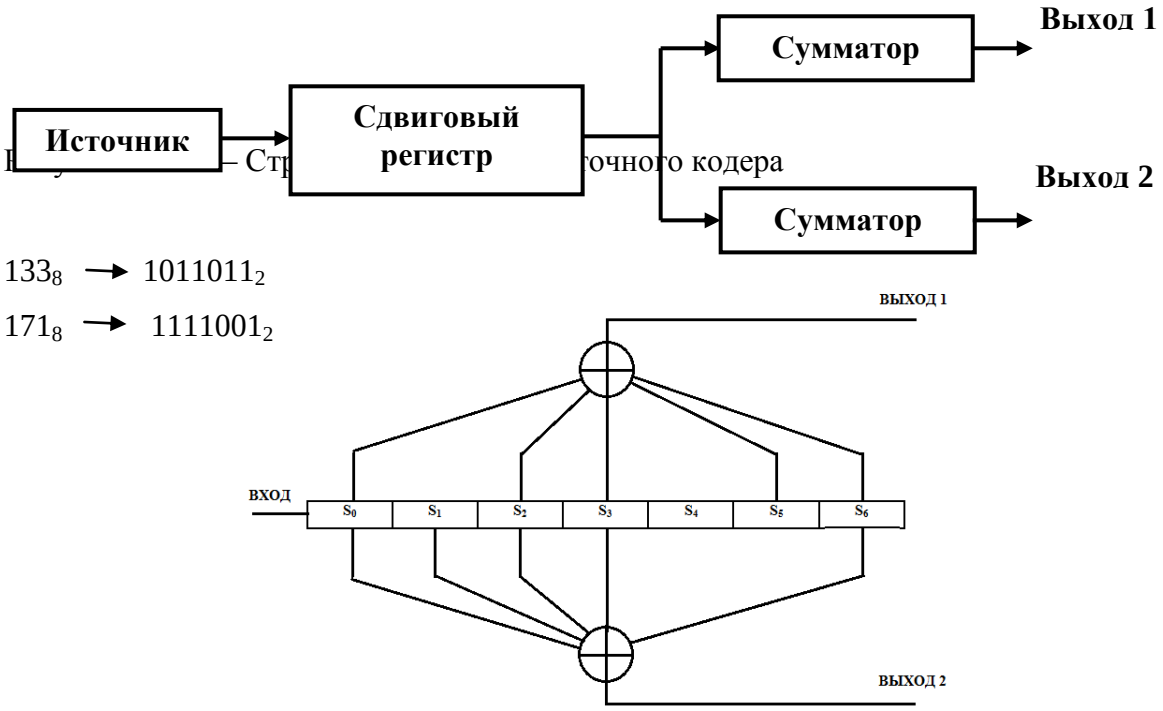


Рис. 4.7. Функциональная схема сверточного кодера 133,171

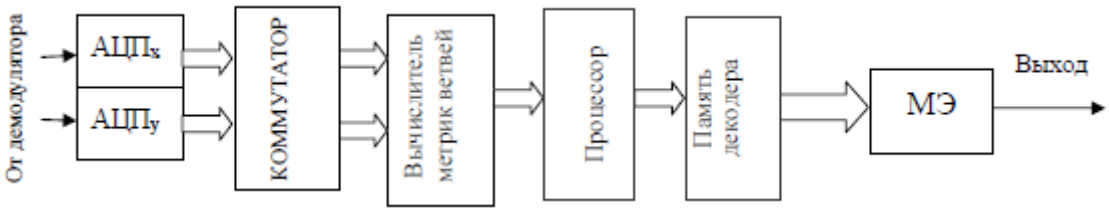


Рис. 4.8. Структурная схема декодера Витерби

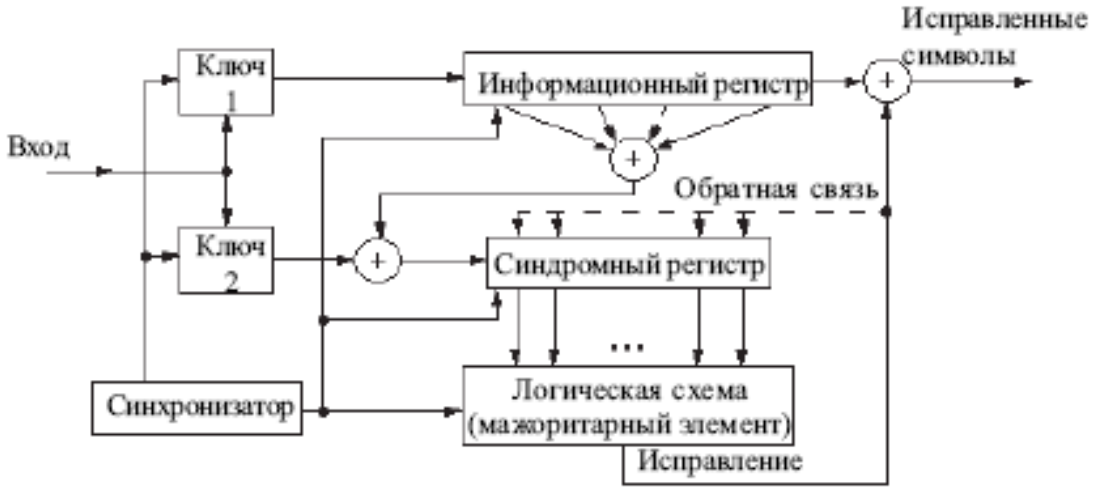


Рис. 4.9. Функциональная схема декодера Витерби

Внутреннее перемежение

Как показано на слайде внутреннее перемежение осуществляется в два этапа. На первом этапе цифровой поток с выхода сверточного кодера разделяется на m парциальных потоков. Каждый из потоков делится на блоки длиной 126 битов и поступает на отдельный блоковый перемежитель битов с поразрядным перемежением. Функция перемежения представлена на слайде.

Выходные потоки перемежителей группируются по одному биту с каждого выхода, образуя m-битовые кодовые слова, поступающие на вход символьного перемежителя.

$$H_0(w) = w;$$
$$H_1(w) = (w + 63) \bmod 126;$$
$$H_2(w) = (w + 105) \bmod 126;$$
$$H_3(w) = (w + 42) \bmod 126;$$
$$H_4(w) = (w + 21) \bmod 126;$$
$$H_5(w) = (w + 84) \bmod 126.$$

Рис. 4.10. Функция битового перемежения для QAM-64

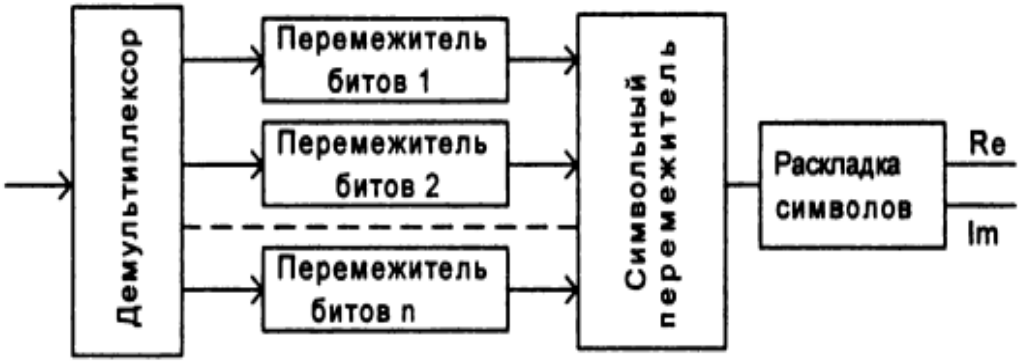


Рис. 4.11. Структурная схема внутреннего перемежителя системы DVB-T

Модуляция в системе DVB-T

В системе цифрового наземного телевизионного вещания используются следующие виды модуляции: QPSK, QAM-16 и QAM-64. Диаграммы созвездий проиллюстрированы на рисунке 4.12.

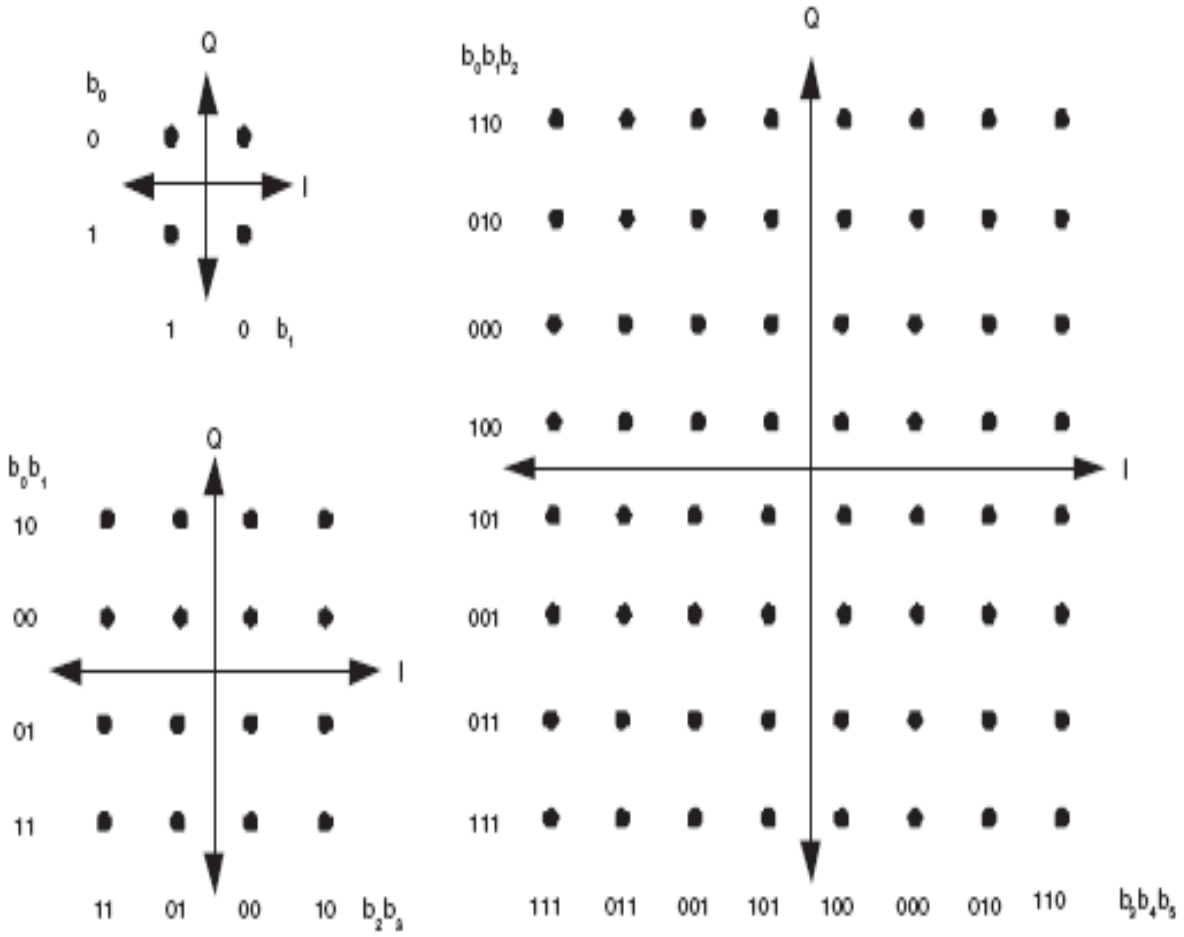


Рис. 4.13. Виды модуляции используемые в системе DVB-T

С внутреннего перемежителя биты поступают на модулятор QAM-64, затем происходит распределение по поднесущим с добавлением пилот-сигналов. К сформированному спектру применяется операция обратного быстрого преобразования Фурье (IFFT), добавляется циклический префикс. Далее полученный символ передается через канал с шумом и затем производятся обратные операции в приёмнике.

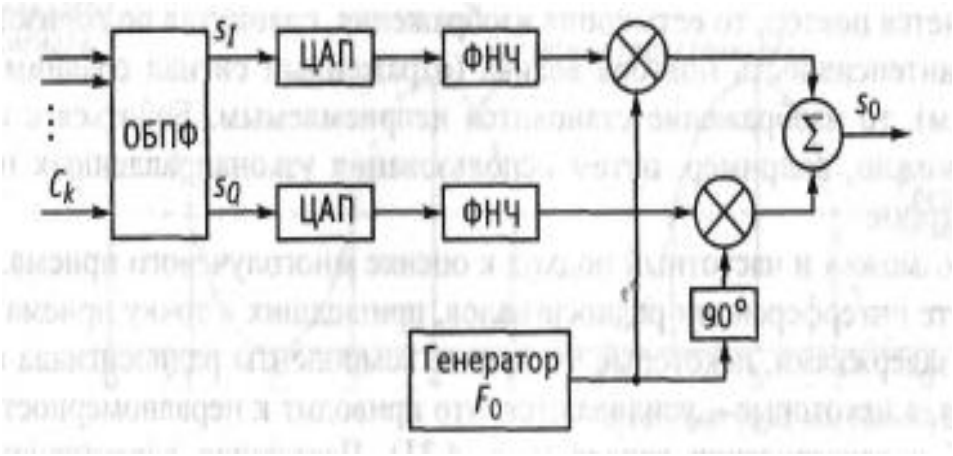


Рис. 4.14. Структурная схема формирователя OFDM-символа в системе DVB-T

Рис. 4.15. Структура OFDM-символа в системе DVB-T

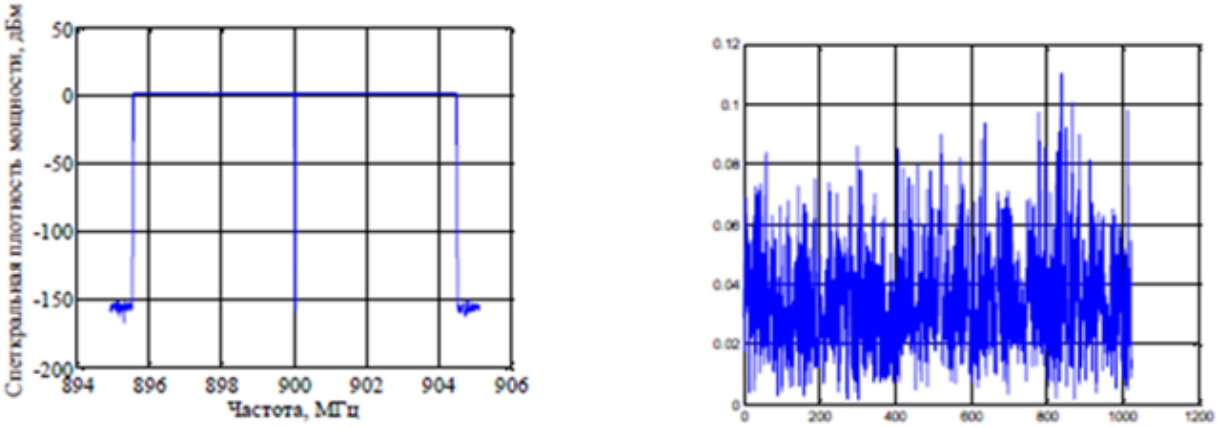


Рис. 4.16. Спектральное и временное представление OFDM-сигнала

Практическая часть [25]

В первую очередь была запущена модель системы DVB-T в программе Matlab следующим образом: Matlab R2015b – Simulink Library Browser – Open – dvbt.slx.

– Simulink

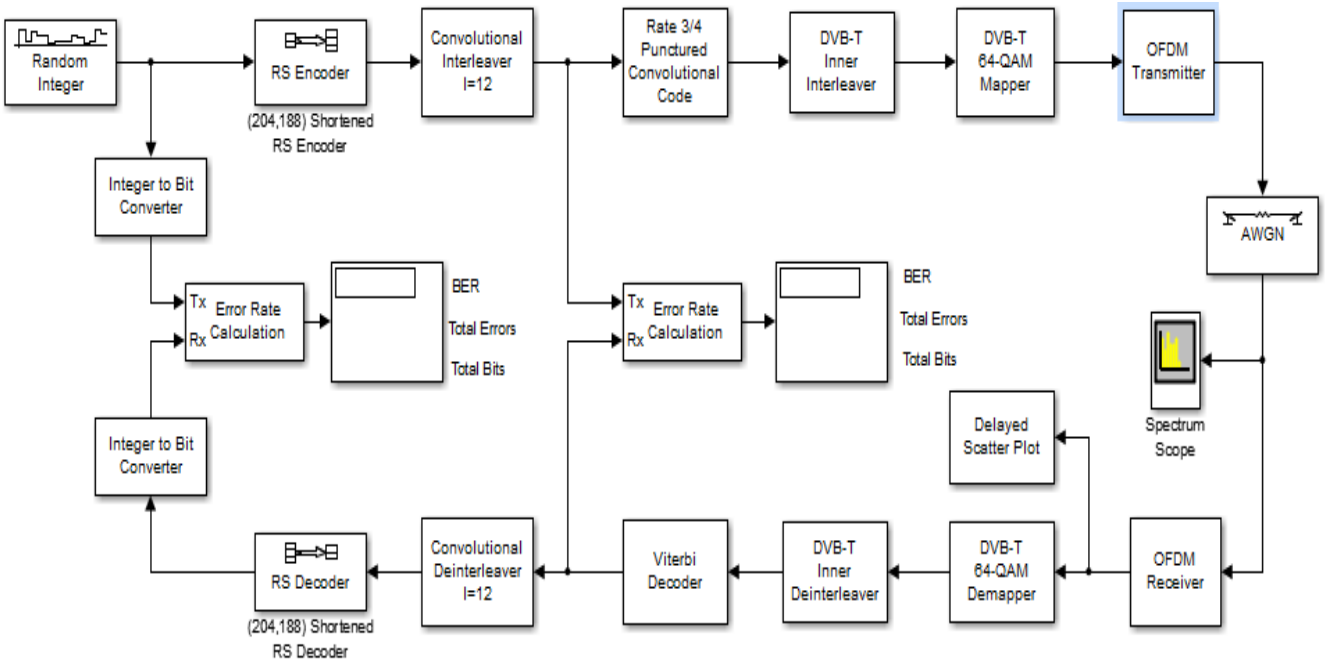


Рис. 4.17. Функциональная схема системы DVB-T реализованная в Matlab R2015b

Затем была исследована зависимость битовой вероятности ошибки (BER) от отношения сигнал/шум (SNR), путем изменения параметра SNR в блоке AWGN в диапазоне от 1 дБ до 25 дБ с шагом 4 дБ.

Результаты измерений представлены в таблице 4.1.

Таблица 4.1 – Зависимость BER от SNR для системы DVB-T

***SNR*, дБ**	1	5	9	13	17	21	25
BER	0.5	0.49	0.47	0.29	0.0016	$5x10^{-6}$	0

На основании данных представленных в таблице 5.1 был построен график зависимости битовой вероятности ошибки от отношения сигнал/шум.

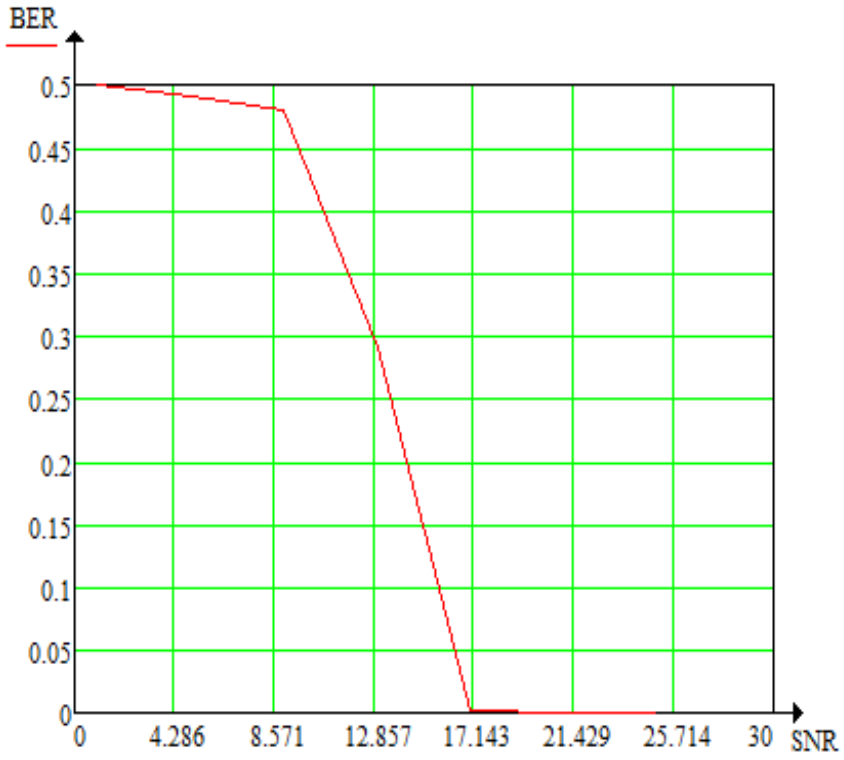


Рисунок 4.18. Зависимость BER от SNR для системы DVB-T при использовании 64-QAM

При исследовании зависимости битовой вероятности битовой ошибки от отношения сигнал/шум рассматриваемой системы телевизионного вещания были сняты изображения спектра передаваемого сигнала и диаграммы созвездий 64-QAM исследуемой системы при SNR равном 1 дБ, 13 дБ и 25 дБ.

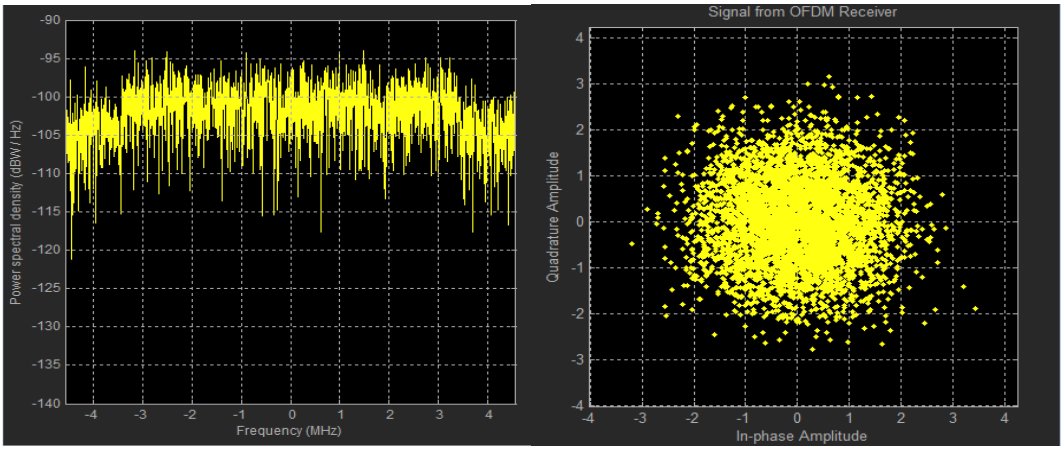


Рис. 4.19. Спектр OFDM-сигнала и диаграмма созвездий 64-QAM при SNR=1 дБ

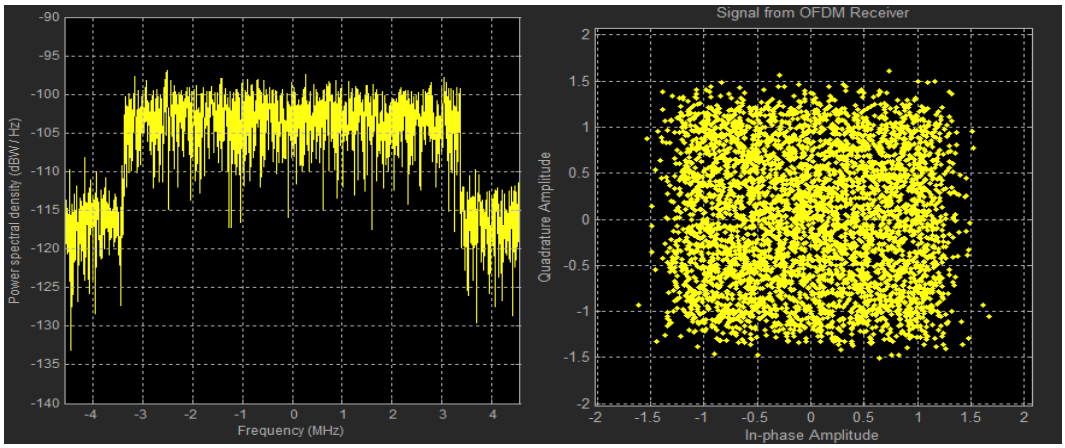


Рис. 4.20. Спектр OFDM-сигнала и диаграмма созвездий 64-QAM при SNR=13 дБ

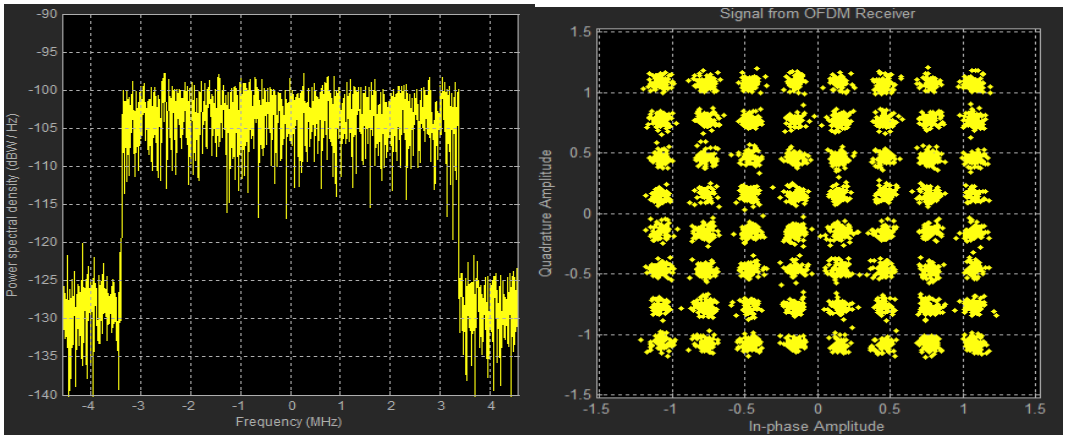


Рис. 4.21. Спектр OFDM-сигнала и диаграмма созвездий 64-QAM при SNR=25 дБ

В процессе выполнения данной работы были изучены основные теоретичиские аспекты системы цифрового наземного телевизионного стандарта DVB-T.

При выполнении практической части работы была построена зависимость битовой вероятности ошибки от отношения сигнал/шум, результат представлен в виде графика (рисунок 4.21). Полученная в ходе моделирования зависимость соответвсвует теоритическим данным.

Вместе с этим, были сняты изображения спектра OFDM-символа и диаграммы созвездий 64-QAM при прохождении сигнала в канале с аддитивным белым гауссовским шумом (АБГШ).

Полученные в результате моделирования данные позволяют сделать вывод о том, что безошибочная передача данных по каналу связи в системе DVB-T возможна при отношении сигнал/шум не менее 17 дБ.

4.2. Проектирование защищенной системы цифрового спутникового телевизионного вещания DVB-S и системы высокоскоростного цифрового спутникового ТВ-вещания DVB-S2 [17, 25]

Методы модуляции и канального кодирования DVB-S используются для первичного и вторичного распределения спутникового цифрового многопрограммного ТВ/ТВЧ в полосах системы стационарной спутниковой связи (FSS — Fixed Satellite Service) и системы спутникового вещания (BSS — Broadcast Satellite Service). Система предназначена для обеспечения сервиса «непосредственно-на-дом» (Direct To Home — DTH) с использованием потребительского интегрированного приемника-декодера (IRD — Integrated Receiver Decoder), а также для систем коллективного приема (SMATV — Satellite Master Antenna Television) и головных станций кабельного телевидения с возможностью повторной модуляции.

Таблица 4. 2. Максимальная скорость битового потока при ширине полосы телевизионного канала 8 МГц

Тип модуляции	Скорость кодирования	Рекомендуемая максимальная скорость, Мбит/с	Длина T2-кадра, OFDM-символов	Число кодовых слов в кадре
QPSK	1/2	7,4442731	60	50
	3/5	8,9457325		
	2/3	9,9541201		
	3/4	11,197922		
	4/5	12,948651		
	5/6	12,456553		
16-QAM	1/2	15,037432	60	101
	3/5	18,07038		
	2/3	20,107323		
	3/4	22,619802		
	4/5	24,136276		
	5/6	25,162236		
64-QAM	1/2	22,481705	60	151
	3/5	27,016112		
	2/3	30,061443		
	3/4	33,817724		
	4/5	36,084927		
	5/6	37,618789		
256-QAM	1/2	30,074863	60	202
	3/5	36,140759		
	2/3	40,214645		
	3/4	45,239604		
	4/5	48,272552		
	5/6	50,524472		

В системе применена модуляция QPSK и защита от ошибок на основе свер- точного кода и сокращенного кода Рида-Соломона. Система может быть использована в спутниковых ретрансляторах с различной шириной полосы.

На рис. 4.22 приведена функциональная структурная схема передающей части системы DVB-S. Система непосредственно совместима с телевизионными сигналами, закодированными по стандарту MPEG-2.

Техника помехоустойчивого кодирования, принятая в системе, разработана в целях достижения «квазибезошибочного» (QEF — Quasi-Error-Free) режима работы, при котором возможно возникновение менее одного случая неисправимой ошибки на час передачи, что соответствует уровню ошибки (BER — Bit Error Ratio) 10^{-10}-10^{-11} на входе демультиплексора MPEG-2.

При адаптации сигнала к спутниковому каналу связи осуществляются следующие операции:

- адаптация транспортного мультиплексирования с использованием статистического кодирования, аналогичного используемому в системе DVB-T ;
- внешнее кодирование с использованием кода Рида-Соломона RS(204,188,t = 8);
- сверточное перемежение;
- внутреннее кодирование с использованием сверточного кода с выкалыванием;
- система предусматривает сверточное кодирование со скоростями кода 1/2, 2/3, 3/4, 5/6 и 7/8;
- формирование сигнала в основной полосе частот;
- модуляция QPSK.

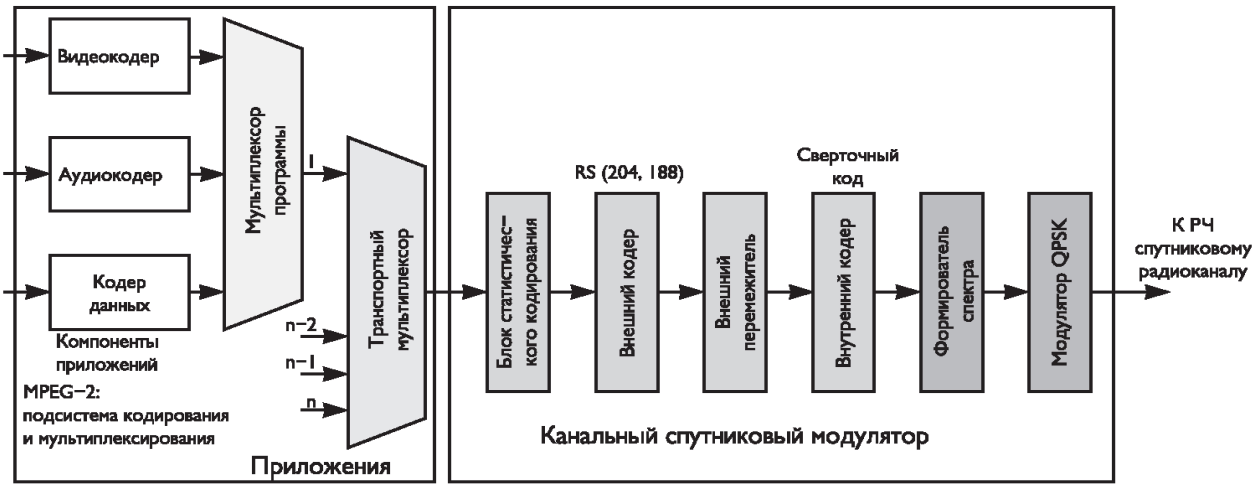


Рис. 4.22**.** Структурная схема передающей части системы DVB-S

DVB-S, принятый еще 1994 году, определяет структуру транспортных пакетов, канальное кодирование и схемы модуляции при передаче по спутниковым каналам сетей непосредственного вещания (DTH). Стандарт DVB-DSNG, появившийся на три года позже, выполняет те же задачи для профессиональных сетей, то есть для сетей передачи сигнала на пункты ретрансляции и спутниковых сетей сбора новостей. Второй стандарт отличается от первого, в основном тем, что рассчитан на более слабые передатчики, не вводящие спутниковый ретранслятор в режим насыщения и поэтому допускающие использование более высоких уровней модуляции – 8PSK и 16QAM.

Система высокоскоростного цифрового спутникового ТВ-вещания DVB-S2

DVB-S2 призван покрыть обе эти области, а также должен решить ряд задач, с которыми имеющиеся стандарты справляются плохо.

Схемы модуляции и способы помехозащитного кодирования

Новый стандарт предусматривает четыре возможных схемы модуляции (рис 4.23).

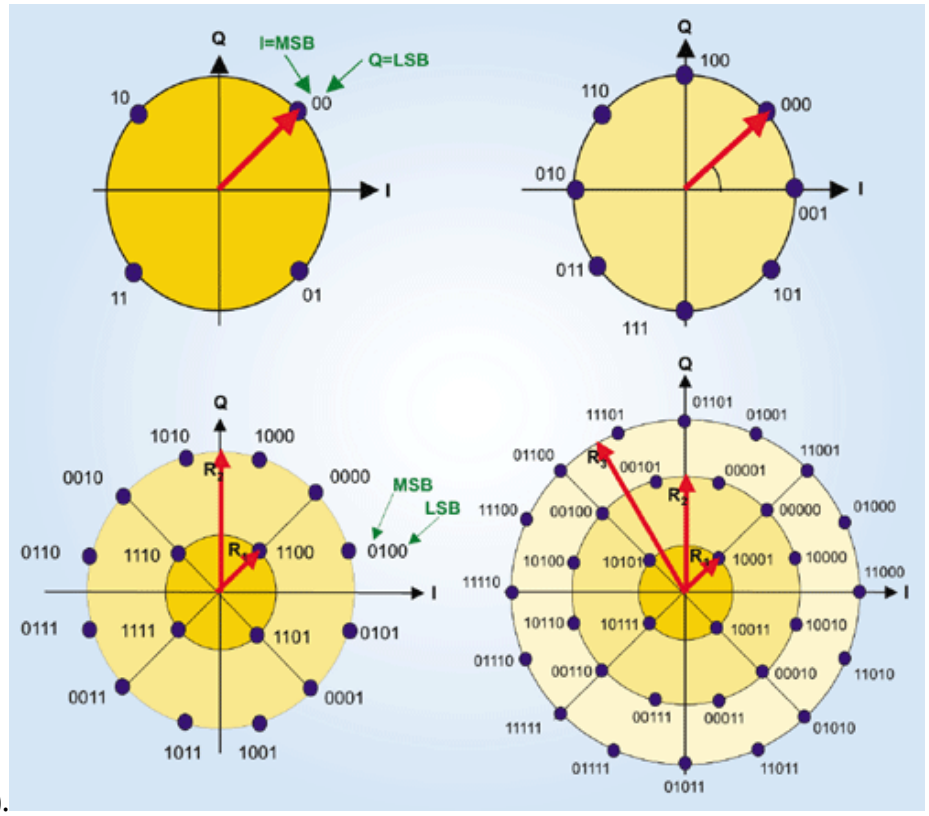


Рис. 4.23. Четыре схемы модуляции, применяемых в стандарте DVB-S2: QPSK, 8PSK, 16APSK, 32APSK

Первые две, QPSK и 8PSK, предназначены для использования в вещательных сетях. Передатчики транспондеров работают там в режиме, близкому к насыщению, что не позволяет модулировать несущую по амплитуде. Более скоростные схемы модуляции, 16 APSK и 32 APSK, ориентированы на профессиональные сети, где часто используются более слабые наземные передатчики, не вводящие бортовые ретрансляторы в нелинейный режим работы, а на приемной стороне устанавливаются профессиональные конвертеры (LNB), позволяющие с высокой точностью оценить фазу принимаемого сигнала. Эти схемы модуляции можно использовать и в системах вещания, но этом случае каналообразующее оборудование должно поддерживать сложные варианты предыскажений, а на приемной стороне должен быть обеспечен более высокий уровень отношения сигнал/шум.

Практическая часть индивидуального задания [25]

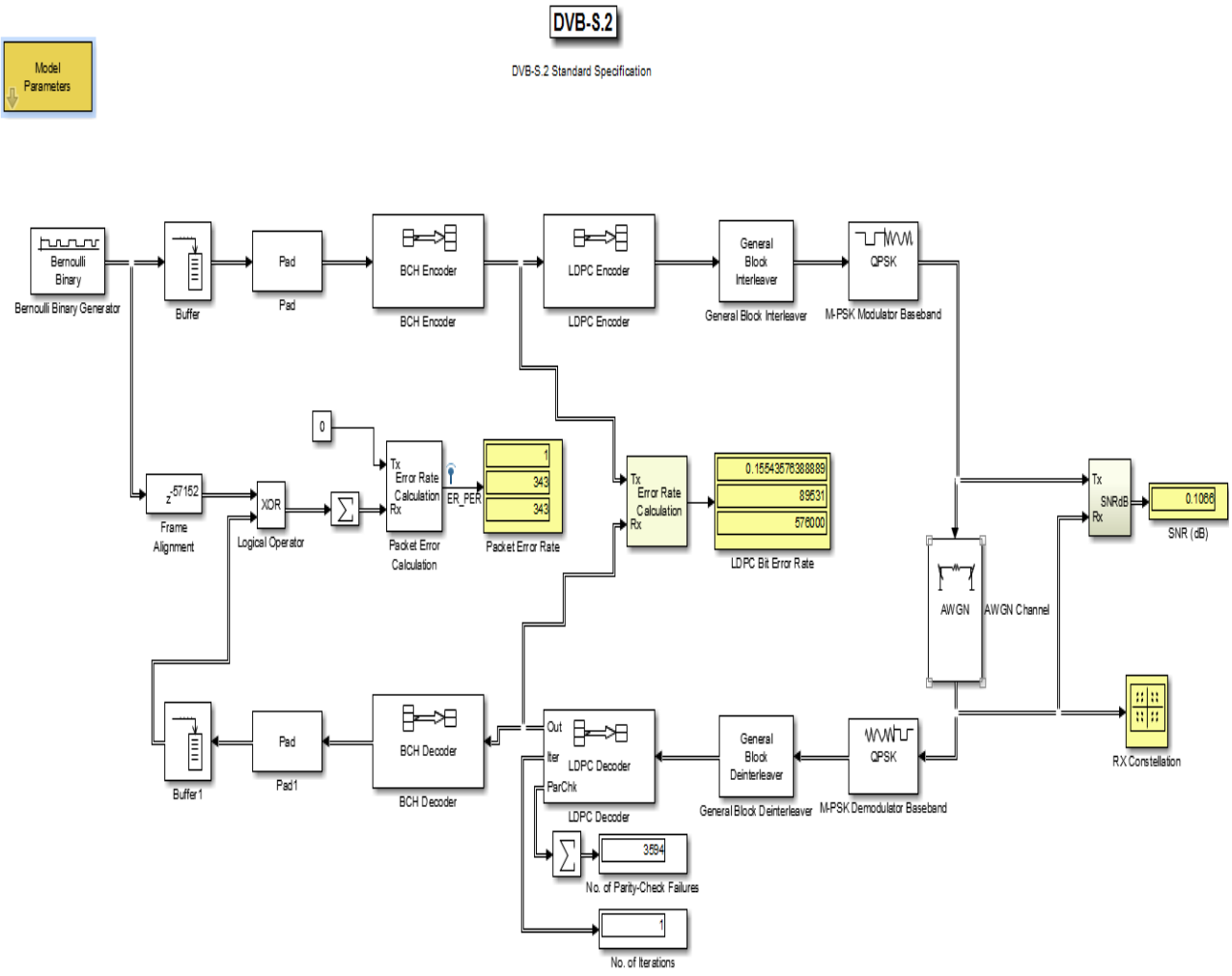


Рис. 4.24. Структура DVB-S2 в Simulink MATLAB 2015b

Структура модема и кодека DVB-S2 состоит из следующих модулей:

1. **Bernoulli sequence generator -** Первыйблокотвечает за генерациюсбалансированных, с точки зрения вероятностиинцидентов, случайной двоичнойпоследовательности. ПоследовательностьБернуллираспределениенулей и единицвероятностямири (p-1) соответственно. В этой модели, p =0,5в результатеравной вероятностьюпроисходитза0 и 1.Выходной сигнал этогокадрана основетого же размеракак пакетMPEG-TS, который содержит 188байта по8 бит, то есть 1504бит.

2. **BBFRAME buffering/unbuffering.** С выхода генератора пакеты буферизуется, создавая базовый диапазон кадра (BBFRAME). Размер этогокадразависит от скоростикодирования,чтобыBCHбыл равен размерам входного сигнала, на входе кодера.Информационные биты(DFL) может быть рассчитана по формуле:

DataField = K_{BCH}– 80

ГдеK_{BCH}является размервнешнеговходаFECкодерBCH, иразмер заголовка равен 80 BBFrame. СтруктураBBFRAMEпоказанона рисунке 4.24

3. BCH encoder/decoder - Одним из DVB-S2 достижений является прямое исправление ошибок, которые развернуты, чтобы уменьшить BER в передаче используется исправление ошибок BCH. Выход BBFrame буферизации блока на стороне отправителя, являются кадры бит, где BCH исправление ошибок с исправлением власти т будет применяться к ним. Для каждого из 11 скорости кодирования представлены в стандартных значений Kbch и нМПБ определяются в том числе Т-коррекции ошибок параметра. В таблицах 1 и 2 эти значения приведены для нормальных и коротких кадров, соответственно.

4. LDPCencoder/coder – Кодирование с проверкой четности. Отношение в скорости показывает, на сколько бит информации сколько приходиться бит с проверкой четности. Например ¼ имеет высокую степень проверки четности, и малую скорость, а 9/10 высокую скорость, но слабую проверку на четность. На стороне приемника, LDPC-декодер проверяет принятую последовательность до проверки четности

Ход работы

Вид модуляции Qpsk 1/4

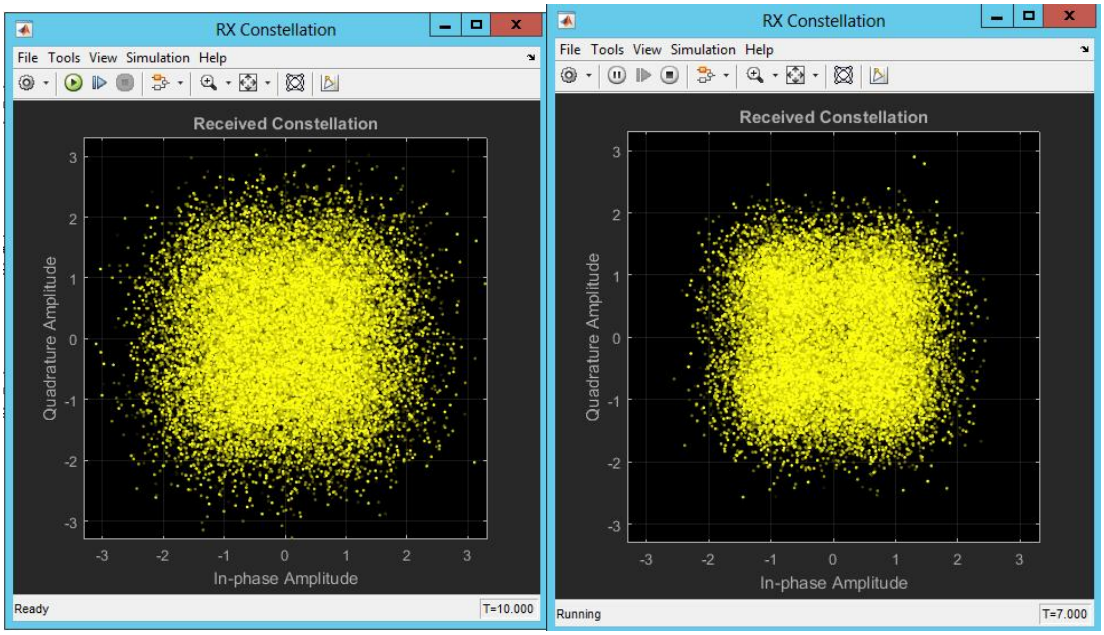


Рис. 4.25. Созвездие при Eb/N0 = 0.5 и Eb/N0 = 3.5

Вид модуляции Qpsk ¾

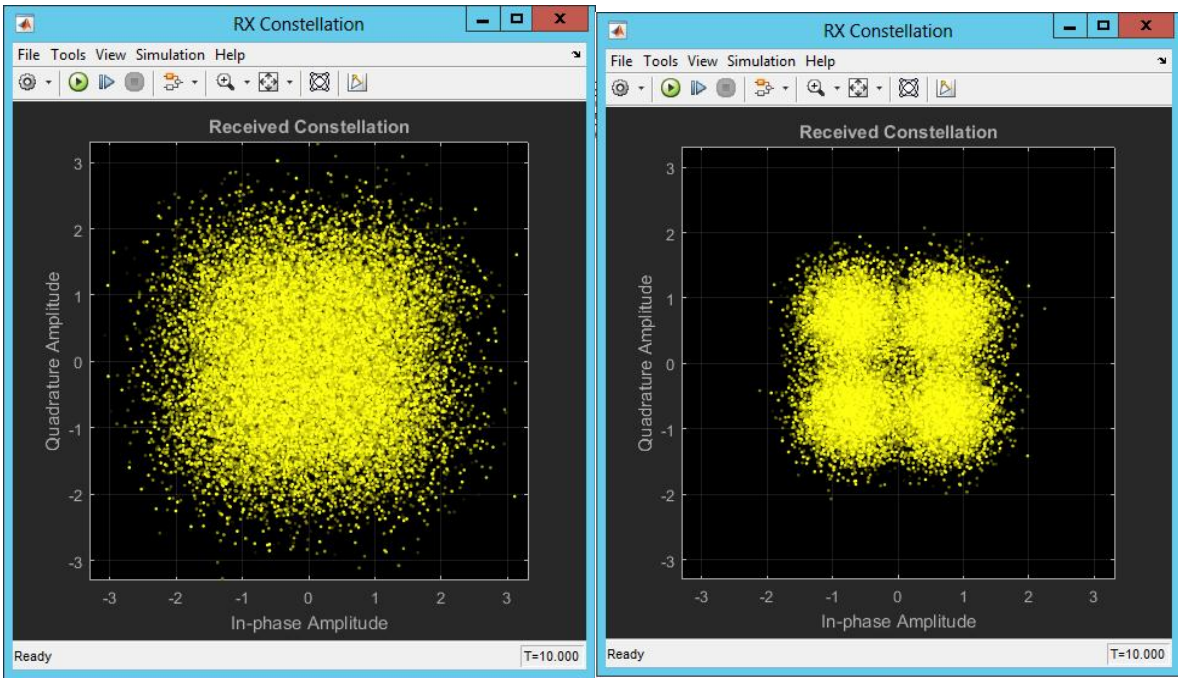


Рис. 4.26. Созвездие при Eb/N0 = 0,5 и Eb/N0 = 5

Вид модуляции - 8psk

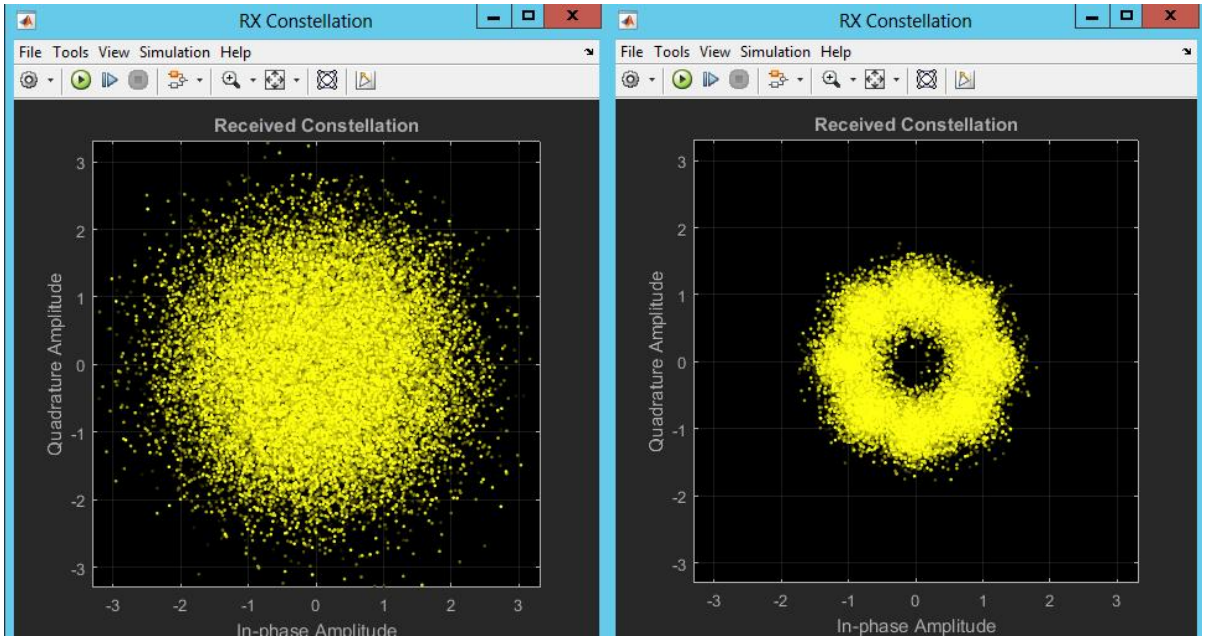


Рис. 4.27. Созвездие Eb/N0 = 0,5 и Eb/N0 = 12

Вид модуляции - 8psk9/10

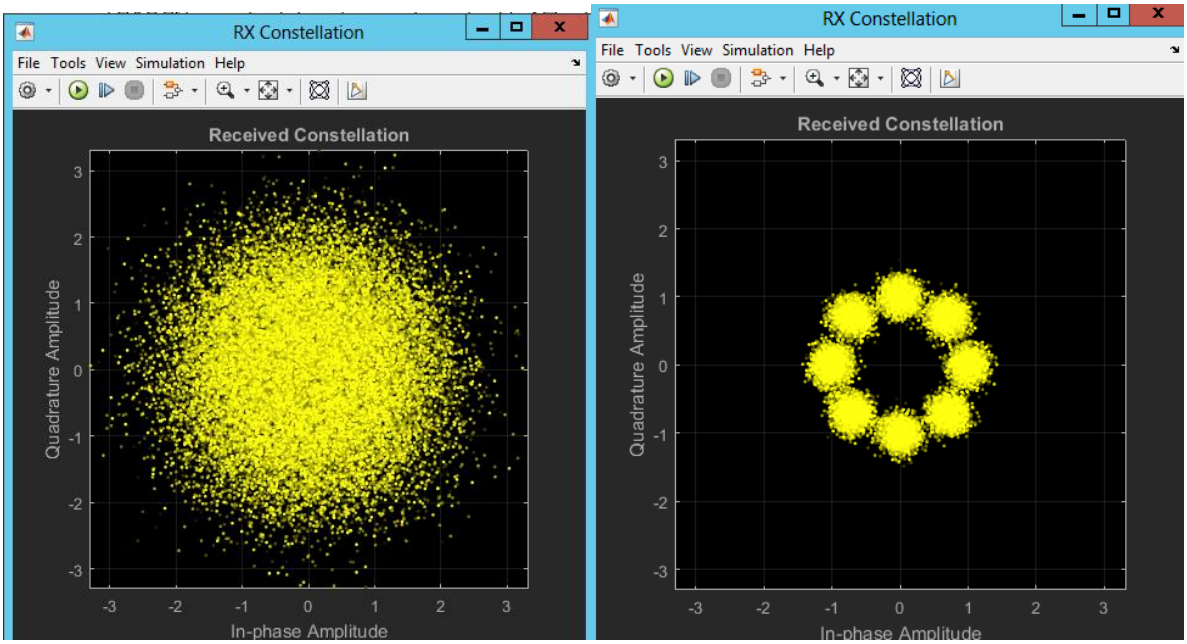


Рис. 4.28. Созвездие при Eb/N0 = 0.5 и Eb/N0 = 6

График зависимости Eb/N0 от BER

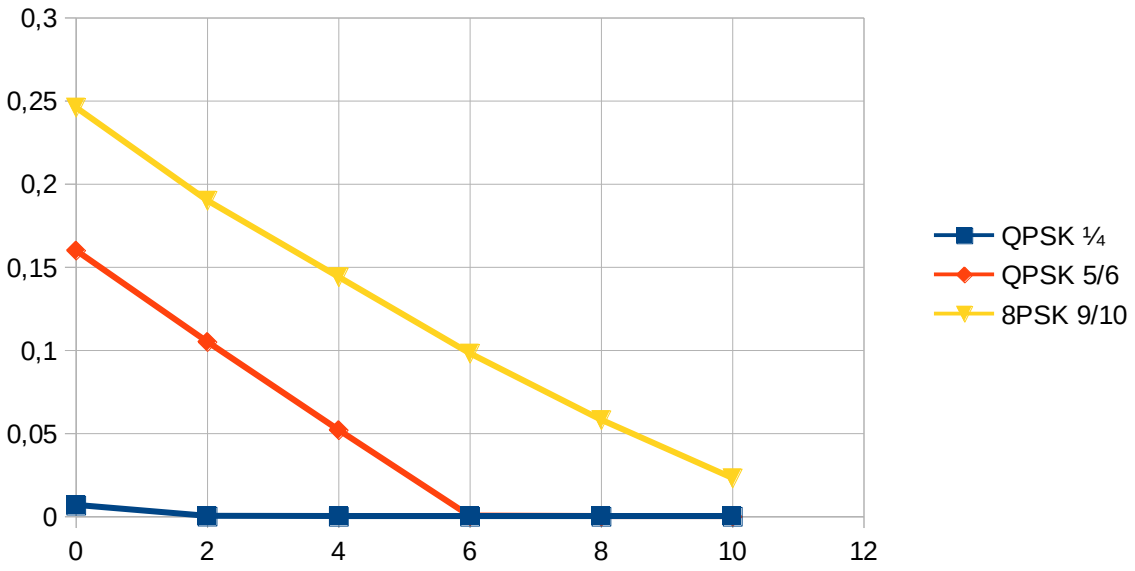


Рис. 4.29. График зависимости BER от Eb/N0

В ходе работы был изучен алгоритм стандарта DVB-S2, создан его рабочий макет, позволяющий увидеть получаемые созвездия, увидеть разность появляющихся ошибок при передаче на разных скоростях. Стандарт DVB-S2 являлся промежуточным звеном между DVB-S и DVB-C2, и не был реализован в полной мере, по сравнению с форматом DVB-S.

4.3. Проектирование защищенной системы цифрового кабельного телевизионного вещания DVB-C и системы высокоскоростного цифрового кабельного ТВ-вещания DVB-C2 [17, 25]

DVB-C – стандарт цифрового телевизионного вещания, который производится по кабелю. В основе стандартов DVB-C лежит стандарт кодирования движущихся изображений и звукового сопровождения MPEG-2.

Система цифрового кабельного телевизионного вещания DVB-C.

Система цифрового кабельного телевидения определяется как функциональный блок оборудования, выполняющий адаптацию ТВ-сигналов к характеристикам кабельного канала. Система DVB-C максимально гармонизирована со спутниковой системой DVB-S и может использовать источник местных ТВ-программ.

В связи с высокой помехозащищенностью кабельных каналов связи в системе

DVB-C не используется сверточное кодирование, но применяется многопозиционная QAM-модуляция — от 16-QAM до 256-QAM.

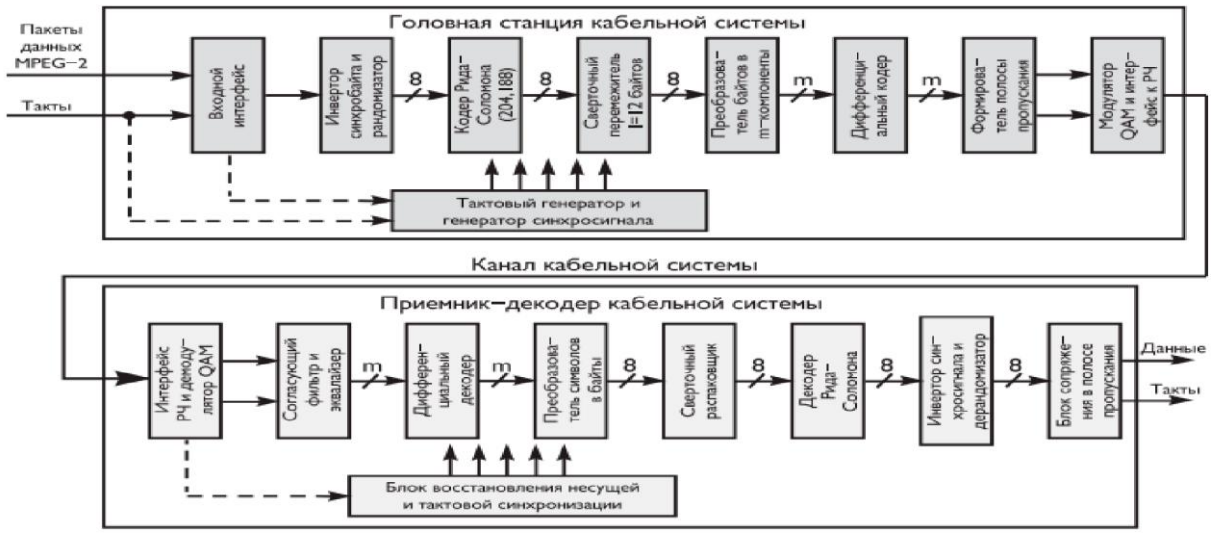


Рис. 4.30. Структурная схема системы цифрового кабельного телевидения DVB-C

В качестве входных сигналов на головной станции используются транспортные пакеты MPEG-2, поступающие через входной интерфейс на модуль, и рандомизирующий поток поступающих данных. Схема рандомизатора/дерандомизатора аналогична используемой в стандарте DVB-T.

Вслед за процессом рандомизации распределения энергии выполняется систематическое сокращенное кодирование Рида–Соломона каждого рандомизированного транспортного пакета MPEG-2, при t = 8, что обеспечивает возможность корректировки 8 ошибочных байтов в каждом транспортном пакете. Данный процесс добавляет 16 байтов четности к транспортному пакету MPEG-2 для получения кодового слова (204, 188).

Затем следует сверточный перемежитель состоящий из l = 12 звеньев, циклически присоединенных к входному потоку байтов с помощью коммутатора. Каждое звено представляет собой регистр FIFO размером M · j ячеек (M = 17 = N/l, N = 204 — длина защищенного от ошибок кадра, l = 12 — глубина перемежения, j — индекс звена). Ячейки FIFO содержат 1 байт, а работа коммутаторов входа и выхода синхронизирована. Притом неинвертированные и инвертированные синхронизирующие байты должны быть всегда адресованы в нулевое звено компоновщика, соответствующее нулевой задержке.

После сверточного перемежения производится точное перекодирование байтов в символы. Перекодирование должно быть основано на использовании границ байтов в системе модуляции. Длина символов m = log2 M, где M — число позиций Q A M – созвездия. Циклическая задача отображения для одного цикла определяется соотношением: 8k=n·m, (1) где k и n — числа преобразуемых байтов и последовательности двоичных символов, соответственно (см. табл. 4.5.).

Таблица 4.5 Коэффициенты преобразования байтов в последовательности символов.

Модуляция	m	n	k	$8k$
16-QAM	4	2	1	8
32-QAM	5	8	5	40
64-QAM	6	4	3	24
128-QAM	7	8	7	56
256-QAM	8	1	1	8

Для устранения потерь из-за скачков фазы несущей применяется дифференциальное кодирование двух старших битов (Ak и Bk) последовательности символов. Эти два старших бит каждого символа должны быть дифференциально закодированы для получения инвариантного относительно фазового сдвига на π/2 созвездия QAM. Дифференциальное кодирование двух старших битов (MSB) должно осуществляться согласно следующему Булеву выражению:

$$I_k = \overline{(A_k \oplus B_k)} \cdot (A_k \oplus I_{k-1}) \vee (A_k \oplus B_k) \cdot (A_k \oplus Q_{k-1});$$
$$Q_k = \overline{(A_k \oplus B_k)} \cdot (A_k \oplus Q_{k-1}) \vee (A_k \oplus B_k) \cdot (A_k \oplus I_{k-1}).$$

На рис. 5.197. приведен пример реализации преобразования байтов в символы.

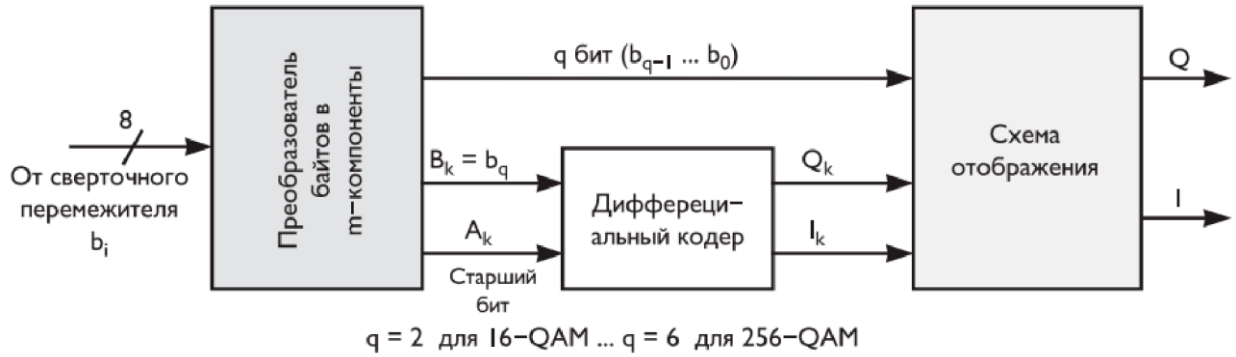


Рис. 4.31. Пример реализации преобразования байта в *m*-мерный вектор и дифференциального кодирования двух старших битов

Квадратурные сигналы I и Q с выхода схемы отображения перед модуляцией подвергаются фильтрации с помощью фильтра, характеристика которого соответствует соотношению при коэффициенте α = 0,15.

В табл. 2 приведены примеры расчетных значений символьной и информационной скоростей при разных кратностях модуляции в канале с полосой 8 МГц. Максимальная скорость достигает 38,1 Мбит/с, что соответствует пропускной

способности ствола спутникового ретранслятора с полосой 33 МГц в типовом режиме Fсимв = 27,5 Мсим/с, R = 3/4.

Таблица 4.6. Примеры расчетных значений символьной и информационной скоростей при использовании стандарта DVB-C.

Полезная информационная скорость (транспортный уровень MPEG-2), Мбит/с	Общая скорость, включая RS (204,188), Мбит/с	Кабельная символьная скорость, Мбод/с	Занимаемая полоса частот, МГц	Вид модуляции
38,1	41,34	6,89	7,92	64-QAM
31,9	34,61	6,92	7,96	32-QAM
25,3	27,34	6,84	7,86	16-QAM
18,9	20,52	3,42	3,93	64-QAM
16,0	17,40	3,48	4,00	32-QAM
12,8	13,92	3,48	4,00	16-QAM
9,6	10,44	1,74	2,00	64-QAM
8,0	8,70	1,74	2,00	32-QAM
6,4	6,96	1,74	2,00	16-QAM

Система высокоскоростного цифрового кабельного телевизионного вещания DVB-C2.

Стандарт кабельного цифрового телевизионного вещания DVB-C2 максимально унифицирован с новыми стандартами, обслуживающими спутниковую (DVB-S2) и эфирную (DVB-T2) транспортные среды.

На рис. 3 а–г приводится достаточно подробная структурная схема передающей части DVB-C2. Как в DVB-S2 и DVB-T2, в новом кабельном стандарте внутри одного физического канала предусмотрено выделение транспортных PLP физических каналов, которые могут обрабатывать и переносить обычный поток MPEG-2 TS или использоваться для передачи IP с применением GSE-протокола.

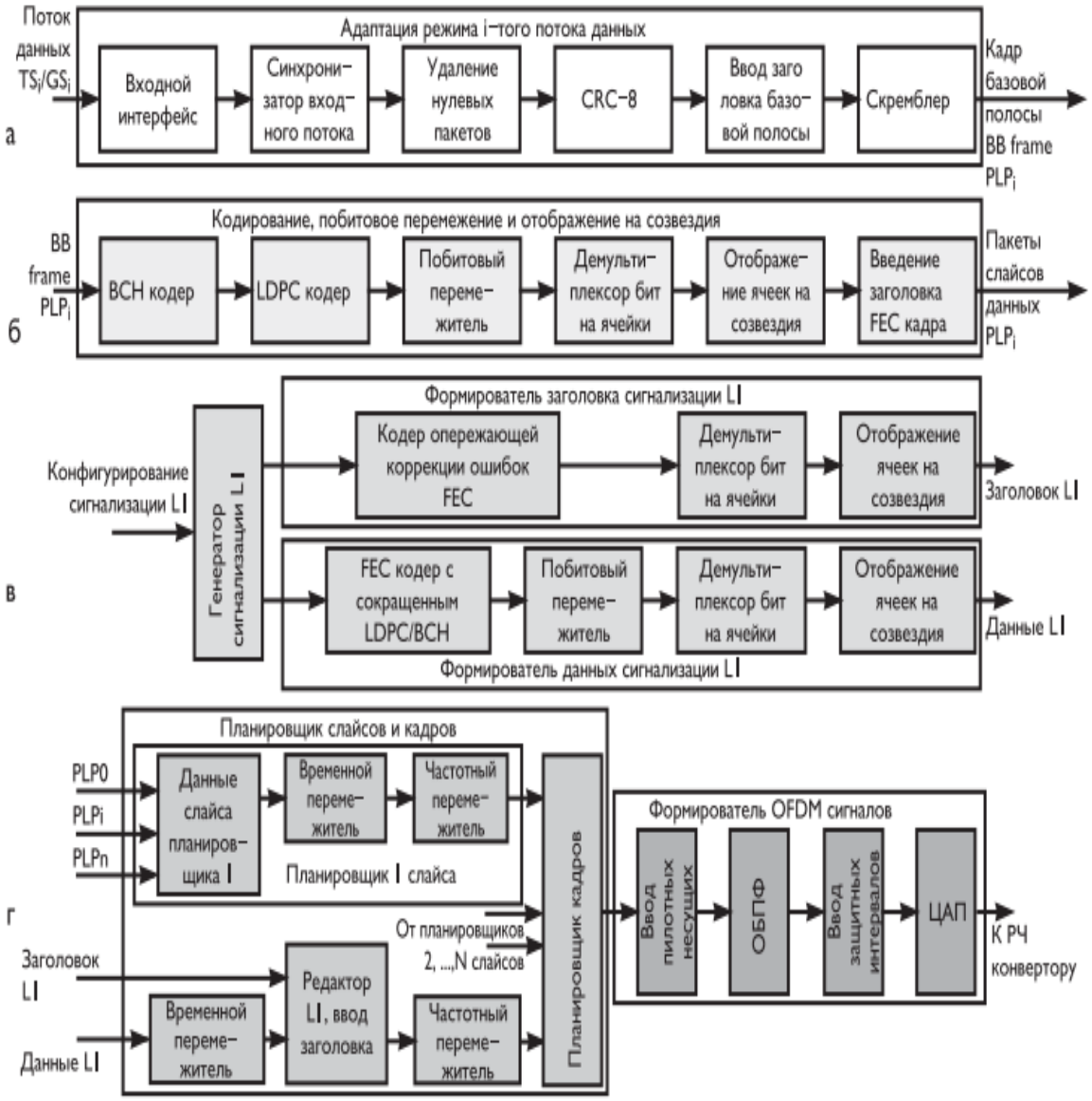


Рис. 4.32. Структурная схема передающей части системы DVB-C2

Вход системы DVB-C2 состоит из одного или из множества логических потоков данных. По одной магистрали физического уровня (PLP) передается один логический поток данных. Модули адаптации режима, по отдельности обрабатывающие содержимое каждой PLP, разбивают входной поток данных на поля данных, которые после адаптации потока должны сформировать кадры базовой полосы (BBFrame). Модуль адаптации режима включает в себя входной интерфейс, за которым следуют три опциональные подсистемы (синхронизатор входного потока, модуль удаления нулевых пакетов и кодер CRC-8), после которых он разбивает входной поток данных на поля данных и выполняет вставку заголовка базовой полосы (BBHeader) в начале каждого поля данных. Подсистема входного интерфейса обеспечивает преобразование входного сигнала во внутренний логически-битовый формат для каждой единичной магистрали физического уровня (PLP, рис.3а). Длина поля данных DFL на выходе интерфейса должна находиться в

пределах: 0 < DFL < (Kbch − 80),
где Kbch — количество битов в поле данных, защищенном кодами BCH и LDPC; 10-байтовый (80 битов) заголовок BBHeader присоединяется к началу поля данных и также защищен кодами LDPC и BCH.

Синхронизатор входного потока формирует поле, состоящее из 2 или 3 байтов (поле ISSY - Input Stream Synchronisation), в котором передается значение счетчика, тактируемого с тактовой частотой модулятора (1/T, где T = 7/64 мкс или T = 7/48 мкс для каналов с полосой пропускания 8 МГц или 6 МГц, соответственно), используемого приемником для восстановления точной синхронизации восстановленного выходного потока. Содержание поля ISSY зависит от формата входного потока и режимов обычной или повышенной эффективности, указанных в заголовке базовой полосы.

Установленные для передачи транспортных потоков требования предусматривают, чтобы скорости битовых потоков на выходе мультиплексора передатчиков и на входе демультиплексора приемников были постоянными на протяжении длительных периодов времени и сквозная задержка также была постоянной. Во входных транспортных потоках может присутствовать большая доля нулевых пакетов для адаптации сервисов с переменной скоростью битового потока в транспортных потоках с постоянной скоростью. В таком случае, во избежание излишних накладных расходов при передаче, нулевые пакеты TS должны быть удалены. Процесс выполняется таким образом, чтобы удаленные нулевые пакеты могли быть повторно вставлены в приемнике в точности на то же самое место, где они находились первоначально.

Кодирование CRC-8, как и в системах DVB-T2 и DVB-S2, применяется для детектирования ошибок на уровне пользовательского пакета, а 10-байтовый заголовок базовой полосы (BBHeader) фиксированного размера вводится перед полем данных для описания формата поля данных.

Перед поступлением на вход системы помехоустойчивого кодирования (см. рис.3б) цифровой поток базовой полосы скремблируется сдвиговым регистром с обратной связью. Порождающий полином последовательности PRBS — 1 + x^14 + x^15 — с инициируемой в начале каждого кадра BBFrame загрузкой в регистр кода 100101010000000.

Структура формата кадра с опережающей коррекцией ошибок BCH и LDPC для основного размера 64 800 битов и сокращенного размера 16 200 битов могут быть для LDPC кодов — 2/3, 3/4, 4/5, 5/6 и 9/1 и для LDPC кодов — 1/2, 2/3, 3/4, 4/5, 5/6 и 8/9, соответственно.

Сигнал с выхода кодера LDPC подвергается побитовому перемежению, которое состоит из перемежения проверочных битов, за ним следует перемежение со сдвигом начала

столбцов в соответствии с правилом системы DVB-C2 (информационные биты не перемежаются). Значения параметра Qldpc определены в табл. 4.7.

Таблица 4.7. Значения Qldpc для основных и сокращенных кадров.

Скорость кода	$N_{\text{ldpc}} = 64\,800$	$N_{\text{ldpc}} = 16\,200$
1/2	–	25
2/3	60	15
3/4	45	12
4/5	36	10
5/6	30	8
8/9	–	5
9/10	18	–

Конфигурация перемежения со сдвигом начала столбцов для каждого формата модуляции определена в табл. 4.8.

Таблица 4.8. Структура побитового перемежителя

Модуляция	Строки N_r		Столбцы N_c
	$N_{\text{ldpc}} = 64\,800$	$N_{\text{ldpc}} = 16\,200$	
16-QAM	8100	2025	8
64-QAM	5400	1350	12
256-QAM	4050	–	16
	–	2025	8
1024-QAM	3240	810	20
4096-QAM	5400	–	12
	–	675	24

.

При перемежении со сдвигом начала столбцов биты данных ui с перемежителя проверочных битов последовательно записываются в перемежитель со сдвигом начала столбцов по столбцам, и последовательно считываются по строкам (старший бит заголовка считывается первым). Запись стартовой позиции каждого столбца сдвигается на величину tc в соответствии с табл. 4.9.

Таблица 4.9

Модуляция		16-QAM		64-QAM		256-QAM		1024-QAM		4096-QAM	
N_{ldpc}		64 800	16 200	64 800	16 200	64 800	16 200	64 800	16 200	64 800	16 200
Столбцы N_c		8		12		16	8	20		12	24
Сдвиг t_c	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	2	0	1	0	0	0
	2	2	0	2	0	2	0	3	0	2	0
	3	4	1	2	2	2	1	4	2	2	0
	4	4	7	3	2	2	7	5	2	3	0
	5	5	20	4	2	3	20	6	2	4	0
	6	7	20	4	3	7	20	6	2	4	0
	7	7	21	5	3	15	21	9	2	5	1
	8	–	–	5	3	16	–	13	5	5	1
	9	–	–	7	6	20	–	14	5	7	1
	10	–	–	8	7	22	–	14	5	8	2
	11	–	–	9	7	22	–	16	5	9	2
	12	–	–	–	–	27	–	21	5	–	2
	13	–	–	–	–	27	–	21	7	–	3
	14	–	–	–	–	28	–	23	7	–	7
	15	–	–	–	–	32	–	25	7	–	9
	16	–	–	–	–	–	–	25	7	–	9
	17							26	8	–	9
	18							28	8	–	10
	19							30	10	–	10
	20										10
	21										10
	22										10
	23										11

Каждый кадр FECFRAME преобразовывается в кодированный и модулированный FEC блок с опережающей коррекцией ошибок. Для этого входные биты сначала демультиплексируются на параллельные модулирующие значения ячеек, и затем эти модулирующие значения отображаются на значения созвездия. Количество ячеек выходных данных и эффективное количество битов на ячейку ηmod заданы в табл. 4.10.

Таблица 4.10. Параметры побитового отображения на созвездия.

Длина блока LDPC-кода (N_{ldpc})	Режим модуляции	η_{mod}	Число выходных ячеек данных
64 800	4096-QAM	12	5400
	1024-QAM	10	6480
	256-QAM	8	8100
	64-QAM	6	10 800
	16-QAM	4	16 200
16 200	4096-QAM	12	1350
	1024-QAM	10	1620
	256-QAM	8	2025
	64-QAM	6	2700
	16-QAM	4	4050
	QPSK	2	8100

Битовый поток vdi, от побитового перемежителя демультиплексируется на Nsubstreams подпотоков (табл. 4.11).

Таблица 4.11. Количество подпотоков в демультиплексоре.

Модуляция	N_{ldpc}	Количество подпотоков $N_{substreams}$
QPSK	Любое	2
16-QAM	Любое	8
64-QAM	Любое	12
256-QAM	64 800	16
	16 200	8
1024-QAM	Любое	20
4096-QAM	64 800	12
	16 200	24

Демультиплексирование определяется как отображение подвергнутых побитовому перемежению входных битов, vdi, на выходные биты be,do на выходе демультиплексора di mod Nsubstreams — число входных битов; do = di div Nsubstreams — число битов в заданном потоке на выходе демультиплексора; e — количество демультиплексированных битовых потоков, (0 e < Nsubstreams), зависящее от di).

Каждое модулирующее значение ячеек, поступающее от демультиплексора, модулируется с использованием созвездий одного из типов: QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM или 4096-QAM. Созвездия и детализация применяемого к ним отображения реализуются в соответствии с кодом Грея.

Точки созвездий zq для каждого входного модулирующего значения ячеек [y0,q . . yη mod −1,q] нормализуются .в соответствии с табл. 4.12.

Таблица 4.12. Параметры демультиплексирования битов на подпотоки для всех кодовых скоростей (за исключением 2/3)

QPSK		
Вход	0	1
Выход	0	1

16-QAM								
Вход	0	1	2	3	4	5	6	7
Выход	7	1	4	2	5	3	6	0

64-QAM											
Вход	0	1	2	3	4	5	6	7	8	9	10	11
Выход	11	7	3	10	6	2	9	5	1	8	4	0

256-QAM ($N_{\text{ldpc}} = 64\,800$)															
Вход	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Выход	7	2	9	0	4	6	13	3	14	10	15	5	8	12	11	1

256-QAM ($N_{\text{ldpc}} = 16\,200$)								
Вход	0	1	2	3	4	5	6	7
Выход	7	3	1	5	2	6	4	0

1024-QAM ($N_{\text{ldpc}} = 64\,800$)																				
Вход	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Выход	8	16	7	19	4	15	3	12	0	11	10	9	13	2	14	5	17	6	18	1

1024-QAM ($N_{\text{ldpc}} = 16\,200$)																				
Вход	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Выход	8	3	7	10	19	4	9	5	17	6	14	11	2	18	16	15	0	1	13	12

4096-QAM ($N_{\text{ldpc}} = 64\,800$)												
Вход	0	1	2	3	4	5	6	7	8	9	10	11
Выход	8	0	6	1	4	5	2	3	7	10	11	9

4096-QAM ($N_{\text{ldpc}} = 64\,800$)																								
Вход	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Выход	8	0	6	1	4	5	2	3	7	10	11	9	6	17	13	20	1	3	9	2	7	8	12	0

Таблица 4.13. Нормирующие множители для ячеек данных.

Модуляция	Нормирующие множители
QPSK	$f_q = z_q/\sqrt{2}$
16-QAM	$f_q = z_q/\sqrt{10}$
64-QAM	$f_q = z_q/\sqrt{42}$
256-QAM	$f_q = z_q/\sqrt{170}$
1024-QAM	$f_q = z_q/\sqrt{682}$
4096-QAM	$f_q = z_q/\sqrt{2730}$

На рис. 5.197в приведена структура датчиков сигнала синхронизации кадров DVB - C2, содержащего два канал — формирователей заголовка и данных сигнализации L1 .

Кодирование заголовка сигнализации L1 осуществляется первоначально с помощью кодера Рида – Маллера (32, 16). При этом каждый бит 32-битового кодового слова Рида–Маллера разбивается на две ветви. Затем данные отображаются на созвездие QPSK для

устойчивого к ошибкам заголовка кадров FECFrame, или на созвездие 16-QAM для заголовка кадров FECFrame с повышенной эффективностью.

Данные сигнализации L1 подвергаются сокращенному LDPC/BCH – кодированию с последующим побитовым перемежением, демультиплексированием и 16-QAM модуляцией. На рис. 4.33г изображена структура планировщика слайсов, формирователя кадров и OFDM-сигналов системы DVB-C2.

Один или множество логических каналов PLP организуются в группу PLP, и одна или множество таких групп PLP образуют слайс данных. Система C2 может состоять из одного или множества слайсов данных. Предполагается, что приемник всегда должен иметь возможность принимать одну PLP-данных и связанную с ней общую PLP при ее наличии.

Для канала с шириной полосы 8 МГц максимальное число OFDM-несущих при передаче каждого слайса должно быть не более nKDCmax − KDCmin 3408 при fmax − fmin = 7,61 МГц и длительности символа TU = 448 мкс.

Данные слайса от каждого планировщика подвергаются временному и частотному перемежению. Временной перемежитель обычно содержит два банка памяти, в первый из которых осуществляется запись, а из второго производится считывание данных слайса, затем производится переключение режимов работы этих банков. Для реализации частотного перемежения производится изменение порядка считывания символов звездной диаграммы. Данные от планировщиков слайсов поступают на планировщик кадров, на который подаются также специальным образом обработанные данные синхронизации L1.

Структура кадра системы DVB-C2 поясняется рис. 4.33а.

Преамбула кадра включает LP символов (LP1), за ней следует LData символов данных. Преамбула несет информацию о символах блока синхронизации L1 (3408 поднесущих частот в полосе 7,71 МГц). Данные слайсов могут передаваться в произвольной полосе частот, не превышающей полосу частот передачи символов блока L1. Неиспользуемые частоты могут занимать часть всего кадра DVB-C2.

Данные сигнализации L1 циклически повторяются, что обеспечивает возможность восстановить полный L1 блок из частей двух блоков, как показано на рис. 5.199б. На входе формирователя OFDM-сигналов установлена схема ввода пилотных несущих, в состав которых входят пилотные несущие преамбулы, постоянные и рассеянные пилотные несущие в составе передаваемых символов данных, а также граничные пилотные несущие, несущие информацию о границах передачи символов данных.

Номера пилотных несущих преамбулы связаны соотношением: k mod DP = 0, (2) где DP = 6, т. е. эти пилотные несущие соответствуют значениям k = 0, 6, 12, . . . , 3402. Параметры пилотных несущих определены следующим образом:

$$\mathrm{Re}\left\{c^{P}_{m,l_P,k}\right\} = A_{PP} \cdot 2(1/2 - r_k), \quad \mathrm{Im}\left\{c^{P}_{m,l_P,k}\right\} = 0,$$

где AP P = 1, m — номер кадра, lP — номер символа преамбулы, k — индекс несущей, а rk определено только для значений k, кратных 6, и вычисляется по формуле:

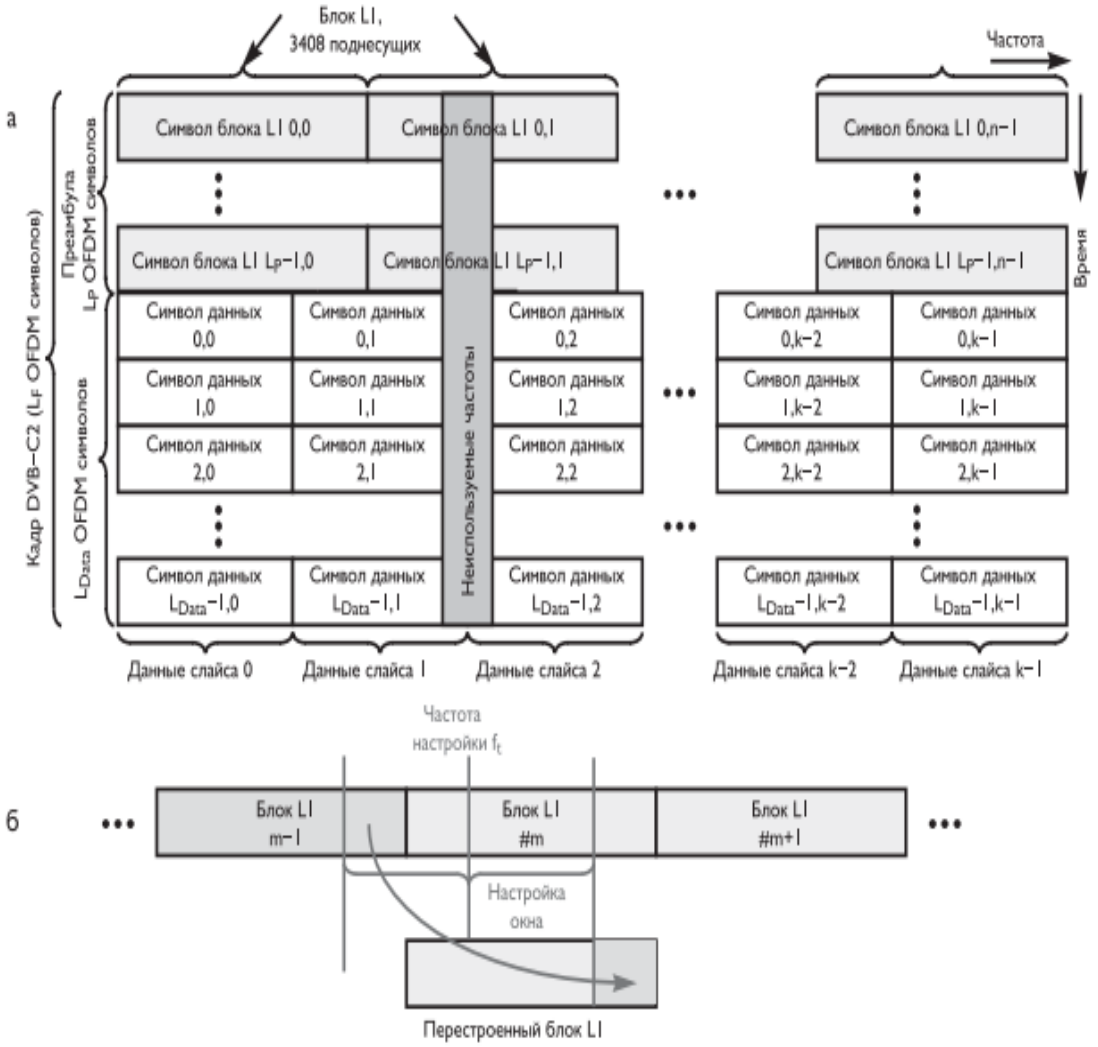


Рис. 4.33. Структура кадра системы DVB-C2.

$$r_k = \begin{cases} w^P_k, & k \bmod K_{L1} = 0; \\ r_{k-6} \oplus w^P_k, & \text{иначе}; \end{cases} \qquad w^P_k = w_k \oplus w'_i, i = (k \mod K_{L1})/D_P;$$

wi — PRBS регистра сдвига, определяемого соотношением x10 + x3 + 1, инициируемого последовательностью единиц, т. е. w0 , w1 , w2 , . . . = 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, . . . ; wk — PRBS регистра сдвига, определяемого соотношением x11 + x2 + 1, инициируемого последовательностью единиц, т. е. w0, w1, w2, . . . = 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, ... Номера локальных рассеянных пилотных несущих определяются следующим соотношением:

$$k \mod (D_X \cdot D_Y) = D_X \cdot (l \mod D_Y),$$

где k — индекс несущей, l — индекс символа данных, DX, DY определены в табл. 5.24.

Таблица 4.14. Коэффициенты, определяющие положение рассеянных пилотных несущих

Коэффициент защитного интервала	Выделение пилотных несущих (D_X)	Номер символов формирования рассеянных несущих (D_Y)
1/64	12	4
1/128	24	4

Кроме рассеяных пилотных несущих в каждый символ кадра, за исключением преамбулы, вводятся постоянные несущие. Индексы этих несущих локально в пределах блока из KL1= 3408 приведены в табл. 4.15.

Таблица 4.15. Индексы постоянных пилотных несущих.

96	216	306	390	450	486	780	804
924	1026	1224	1422	1554	1620	1680	1902
1956	2016	2142	2220	2310	2424	2466	2736
3048	3126	3156	3228	3294	3366		

В дополнение к рассеянным и постоянным пилотным несущим вводятся также граничные пилотные несущие, определяющие «края» в каждом символе. Такие пилотные несущие вводятся также на границах областей неиспользуемых частот. Некоторые OFDM-ячейки могут быть зарезервированы для подавления пиковых значений формируемого радиосигнала (PAPR). Резервируемые ячейки OFDM-сигнала S0 определяются соотношением: [k mod (8 · KL1)] − Dx (l mod DY) ∈ S0, 0 l LData, где k — абсолютный индекс несущей, LData — количество символов данных в кадре DVB-C2. Формируемый на выходе ОБПФ-сигнал может быть записан в следующем виде:

$$s(t) = Re\left\{\sum_{m=0}^{\infty}\left[\frac{1}{\sqrt{K_{\text{total}}}}\sum_{l=0}^{L_F-1}\sum_{k=K_{\min}}^{K_{\max}} c_{m,l,k}\cdot\psi_{m,l,k}(t)\right]\right\},$$

где

$$\psi_{m,l,k}(t) = \begin{cases} \exp\left[2\pi j\frac{k}{T_U}(t - T_G - lT_S - mT_F)\right] & \text{при } mT_F + lT_S \leqslant t \leqslant \\ & \leqslant mT_F + (l+1)T_S; \\ 0 & \text{иначе,} \end{cases}$$

k — номер поднесущей; l — номер символа OFDM от «0» до первого символа преамбулы кадра; m — номер кадра DVB-C2; Ktotal — количество используемых несущих, totalKmax − Kmin; LF — количество OFDM символов в кадре (исключая преамбулу); TU — длительность активной части символа; TG — длительность защитного интервала; TSTU +

TG — полная длительность символа; cm,l,k — комплексное значение k-й несущей в l-м OFDM-символе m-го кадра DVB-C2; TFLFTS — длительность кадра; Kmin и Kmax — индексы первой нижней и последней верхней активных несущих, соответственно.

Поскольку в системе DVB-C2 применены более эффективные методы помехоустойчивого кодирования по сравнению с системой DVB-C, возможно использование звездных диаграмм OFDM-сигналов более высокой размерности. Допустимые комбинации модуляций и параметров LDPC-кодирования приведены в табл. 5.26, в которой также указаны величины отношения сигнал/шум, требуемые для приема, квазисвободного от ошибок.

Таблица 4.16. Параметры OFDM-сигналов для каналов с полосой пропускания 6 МГц и 8 МГц.

Параметр	6 МГц 1/64	6 МГц 1/128	8 МГц 1/64	8 МГц 1/128
Количество OFDM-несущих в блоке сигнализации L1 — K_{L1}	3408	3408	3408	3408
Ширина полосы блока сигнализации L1	5,61 МГц	5,61 МГц	7,61 МГц	7,61 МГц
Дительность T_U в элементарных периодах T	$4096T$	$4096T$	$4096T$	$4096T$
Дительность T_U в мкс	597,3	597,3	448	448
Частотный интервал между несущими $1/T_U$ в Гц	1674	1674	2232	2232
Дительность T_G в элементарных периодах T	$64T$	$32T$	$64T$	$32T$
Дительность T_G в мкс	9,33	4,66	7	3,5

Таблица 4.17. Отношение сигнал/шум при различных параметрах системы DVB-C2.

Параметры LDPC кода	16-QAM	64-QAM	256-QAM	1024-QAM	4096-QAM
2/3	–	13,5 дБ	–	–	–
3/4	–	–	20,0 дБ	24,8 дБ	–
4/5	10,7 дБ	16,1 дБ	–	–	–
5/6	–	–	22,0 дБ	27,2 дБ	32,4 дБ
9/10	12,8 дБ	18,5 дБ	24,0 дБ	29,5 дБ	35,0 дБ

Для сравнения эффективностей использования систем кабельного цифрового телевизионного вещания DVB- C2 и DVB- C в табл.14 приведены допустимые скорости передачи информации при эквивалентной ширине канала 8 МГц.

Таблица 4.18. Максимальные скорости передачи информации в системах DVB-C и DVB-C2 при эквивалентной ширине канала 8 МГц.

Система		16-QAM	64-QAM	256-QAM	1024-QAM	4096-QAM
DVB-C		25 Мбит/с	38,4 Мбит/с	51,2 Мбит/с	–	–
DVB-C2	2/3	–	31,4 Мбит/с	–	–	–
	3/4	–	–	47,1 Мбит/с	58,9 Мбит/с	–
	4/5	25,1 Мбит/с	37,7 Мбит/с	–	–	–
	5/6	–	–	52,4 Мбит/с	65,4 Мбит/с	78,6 Мбит/с
	9/10	28,3 Мбит/с	41,4 Мбит/с	56,6 Мбит/с	70,7 Мбит/с	84,8 Мбит/с

В отличие от стандартов эфирного вещания, стандарт DVB-C2 может не подчиняться жесткой частотной сетке, поскольку кабельная сеть является закрытой экранированной средой и нет необходимости координировать использование ее спектра с эфирными присвоениями. Напротив, можно гибко адаптировать полосу канала под свои конкретные потребности, что позволяет расширить полосу передаваемого сигнала для размещения в нем большего количества услуг. Чтобы не усложнять и не удорожать абонентское оборудование, реализуется сегментированный прием таких каналов, аналогичный используемому в японской системе эфирного телевидения ISDB- T [8 .4 0]. Приемник со стандартной полосой пропускания извлекает из широкого пакета только необходимую часть спектра, не превышающую, например, 8 МГц.

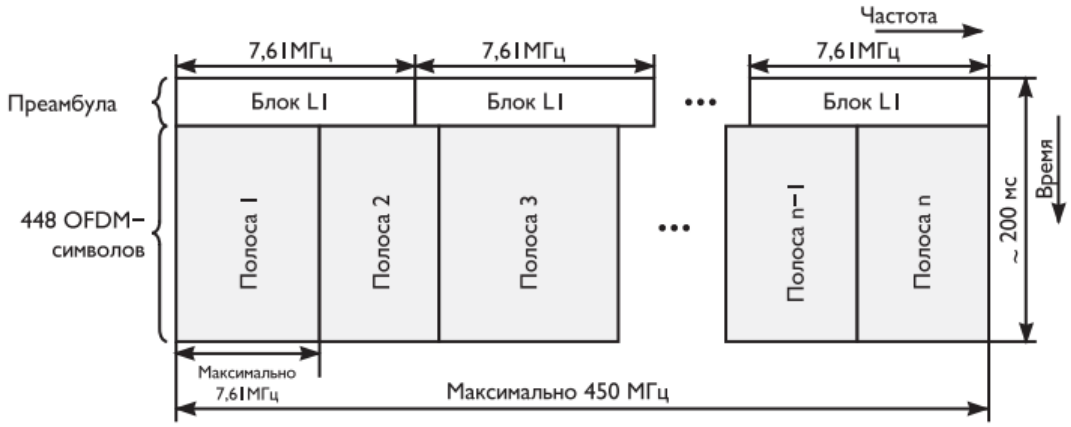


Рис. 4.34. Структура кадра DVB-C2 в частотно-временной области.

Структура кадра DVB- C2 показана на рис.5. Каждый кадр C2 начинается с преамбулы, состоящей из одного или более OFDM-символов и выполняющей две основные функции. С одной стороны, она обеспечивает надежную временную и частотную синхронизацию OFDM- сигнала и самой структуры. С другой стороны, преамбула содержит сигнализацию уровня L1, необходимую для декодирования потоков данных и содержащейся в них полезной информации. Преамбула состоит из циклически передаваемых блоков сигнализации L1, повторяющихся в каждой полосе 7,61 МГц широкого

канала. Фиксированное расположение блоков L1 и их повторение с шагом 7,61 МГц обеспечивают их прием при настройке тюнера на любые 8 МГц из занимаемого кадром диапазона.

Использование многопозиционной модуляции QAM (Quadrature Amplitude Modulation – квадратурная амплитудная модуляция), а также хорошего отношения S/N, который существенно снижает вероятность ошибок BER (Bit Error Rate – частота ошибочных бит) позволило внедрить цифровое телевидение в системы кабельного телевидения.

Практическая часть [25].

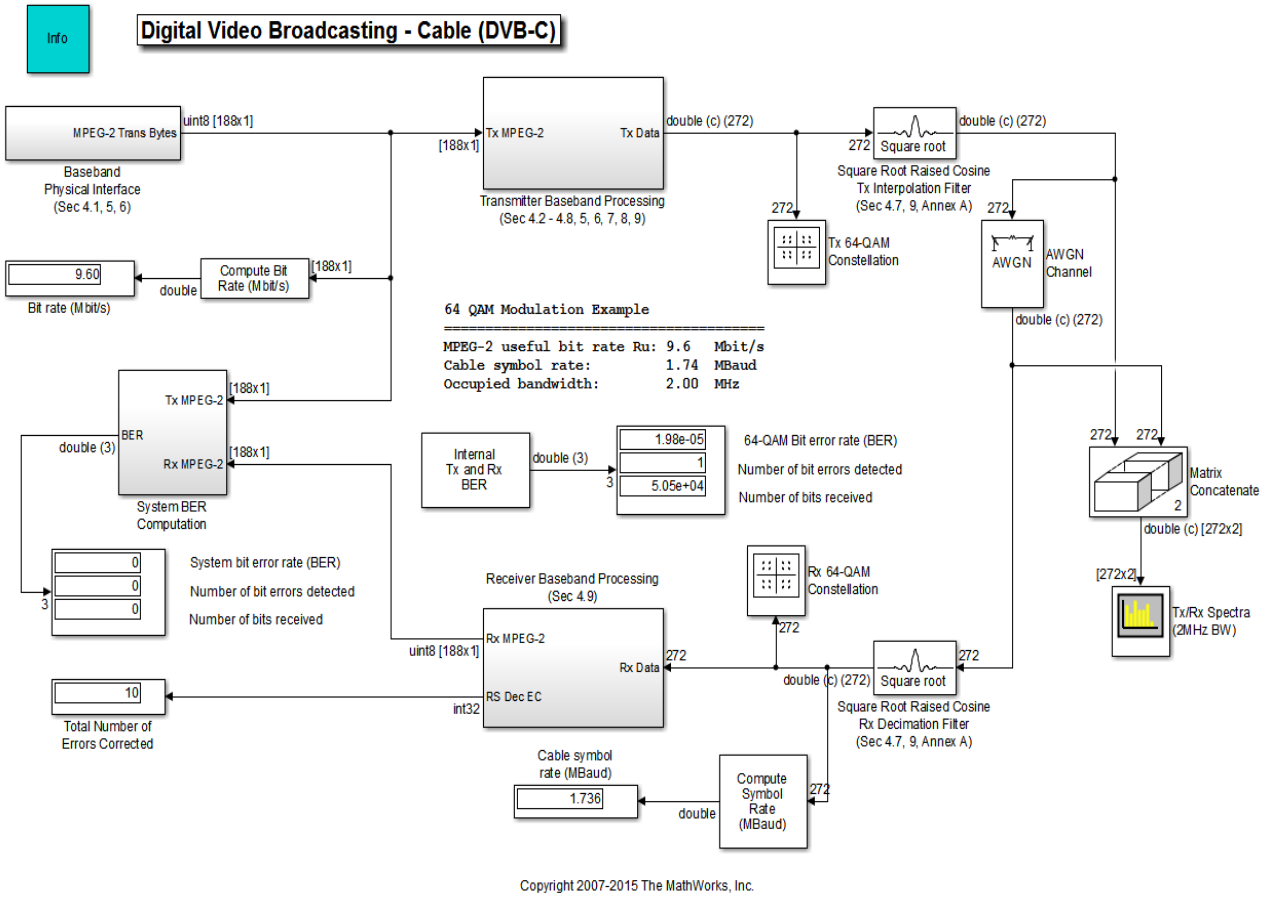


Рис. 4.35. Структурная схема системы цифрового кабельного телевидения DVB-C в Simulink MATLAB 2015

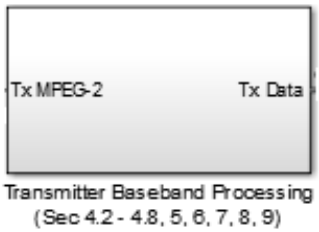


Рис. 4.36. Блок имитация потока данных MPEG- 2.

Внутри данного блока производится имитация потока данных MPEG- 2.

Представленный на рис. блок включает в себя:

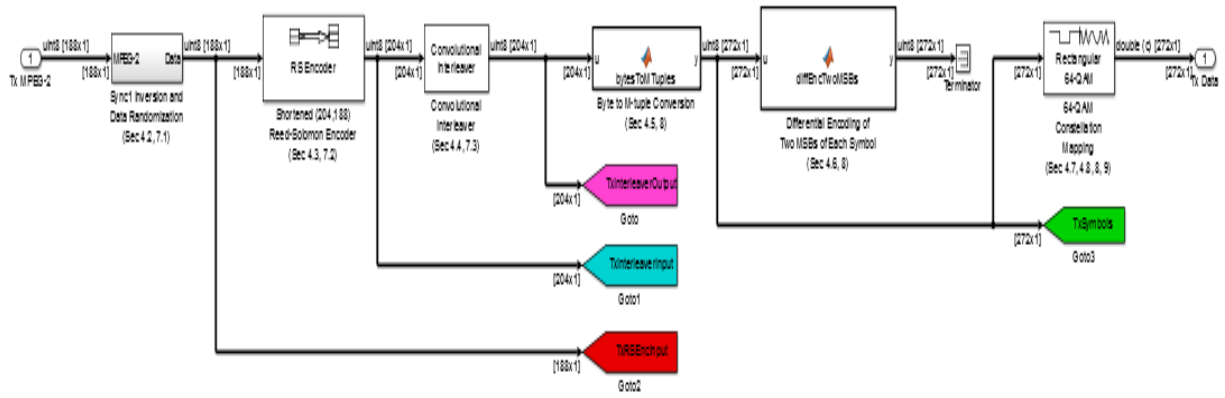


Рис. 4.37. Блок передатчика.

1. **Sync1 Inversion and Randomization**

Эта подсистема инвертирует байт, далее производится рандомизация с целью формирования спектра.

2. **Кодировщик Рида-Соломона (204, 188).**

Добавляет 16 паритетных байтов к MPEG-2.

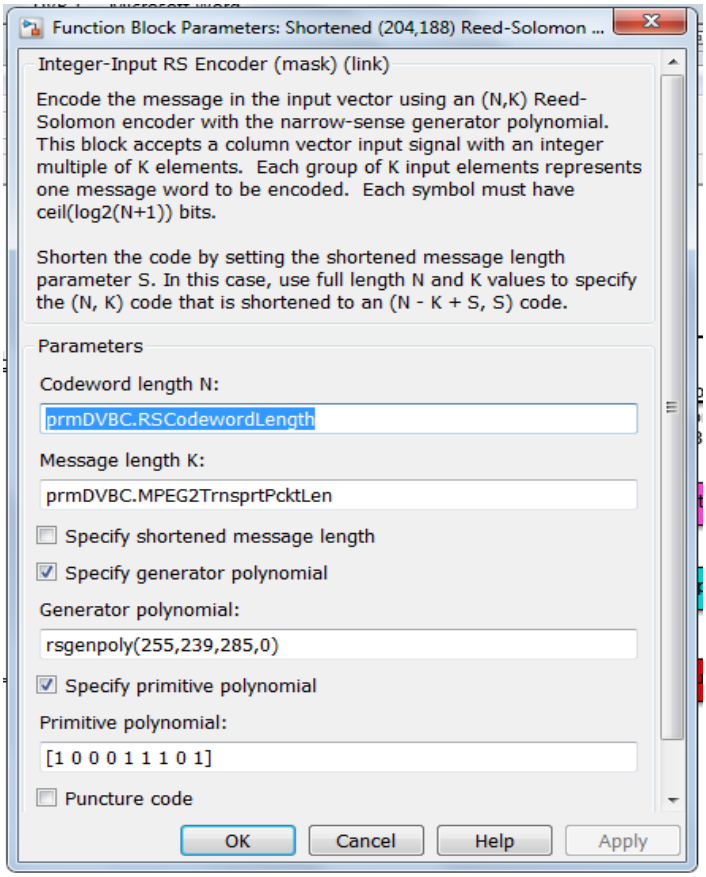


Рис. 4.38. Кодировщик Рида-Соломона (204, 188)

3. **Сверточный перемежитель.**

Процесс перемежения основан на подходе Форни.

4. **Байт (8 бит) с М- кортежами (6 -разрядная версия)**

Используется, чтобы преобразовать 8-битные байты данных в 6-битные.

5. Дифференциальное кодирование.

6. **Отображение 64-QAM созвездия.**

Отображает в основной полосе частот значения (I и Q) при передаче.

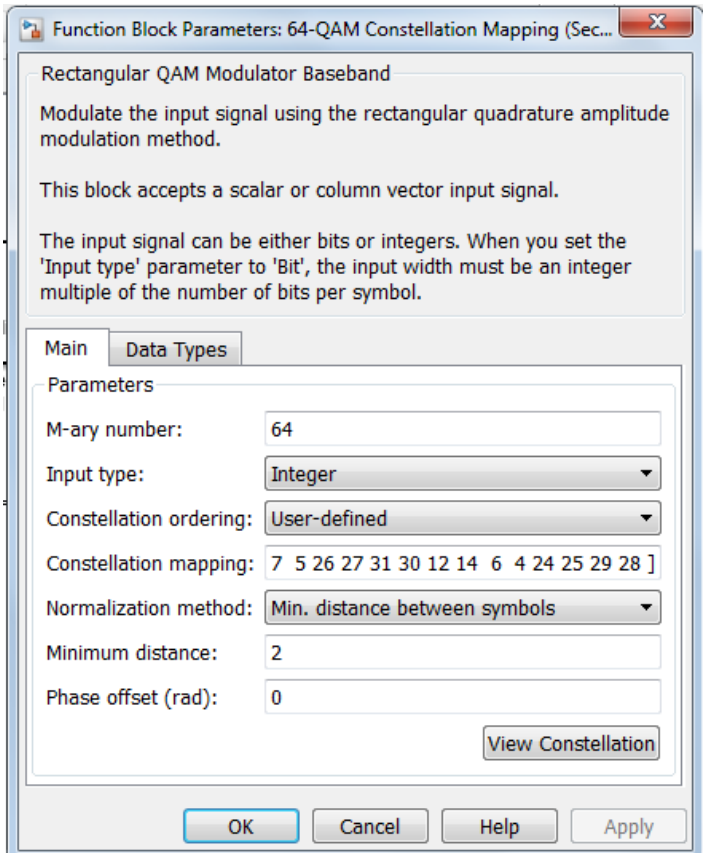
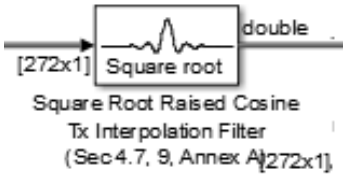
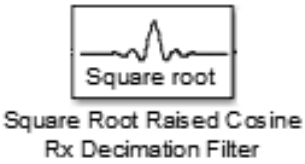


Рис. 4.39. Отображение 64-QAM созвездия.

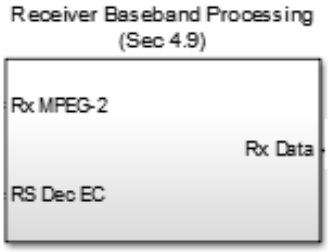


Этот блок выполняет низкочастотное формирование значений символов совокупности для передачи комплекса (I и Q).

Изменение белого гауссовского шума в пределах от 10^-4 до 10^-10,10^-11.



Прореживает (фильтрует) значения символа созвездия принимаемого комплекса (I и Q).



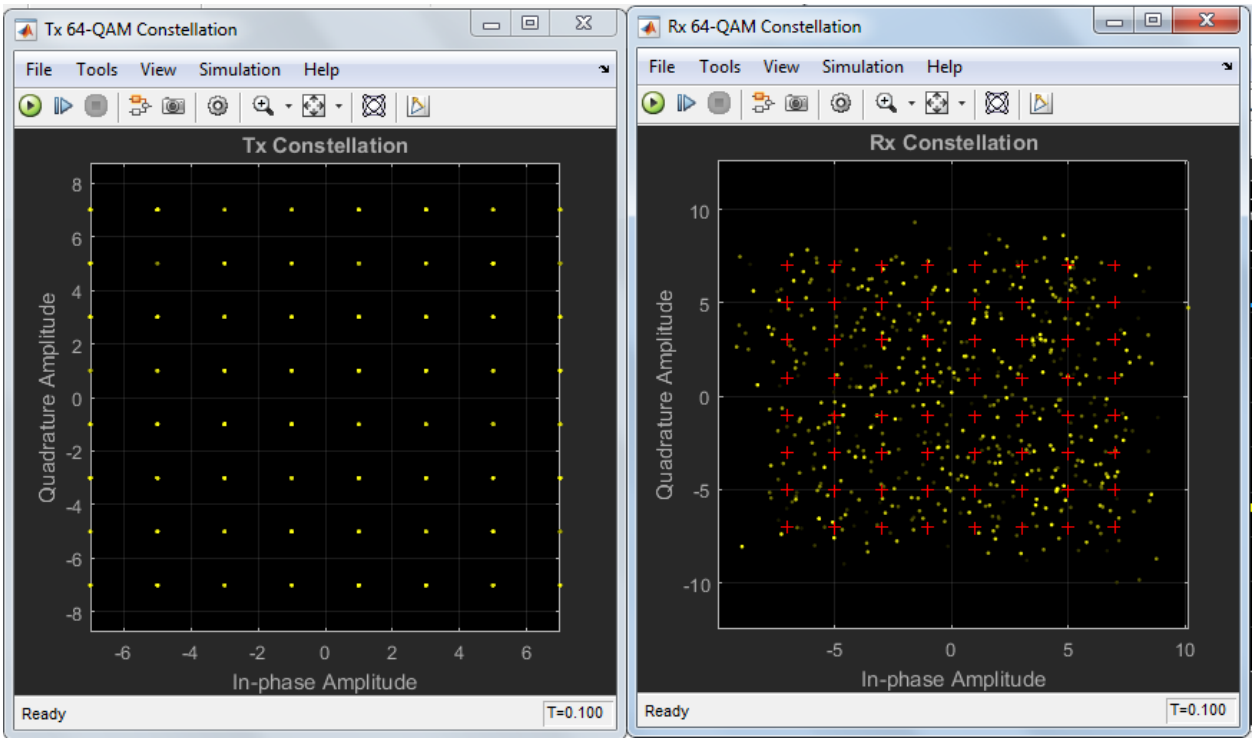


Рис. 4.40. Созвездия передатчика и приёмника при при Eb/No = 5 дБ.

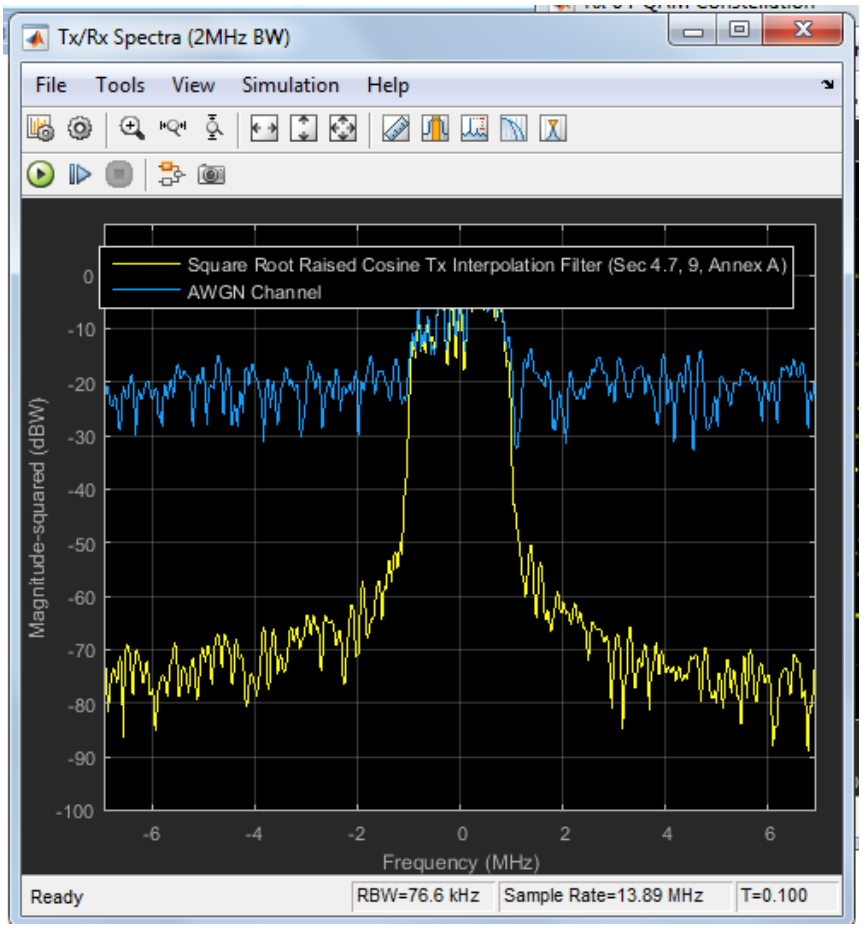


Рис. 4.41. Спектр передатчика и приёмника при при Eb/No = 5 дБ.

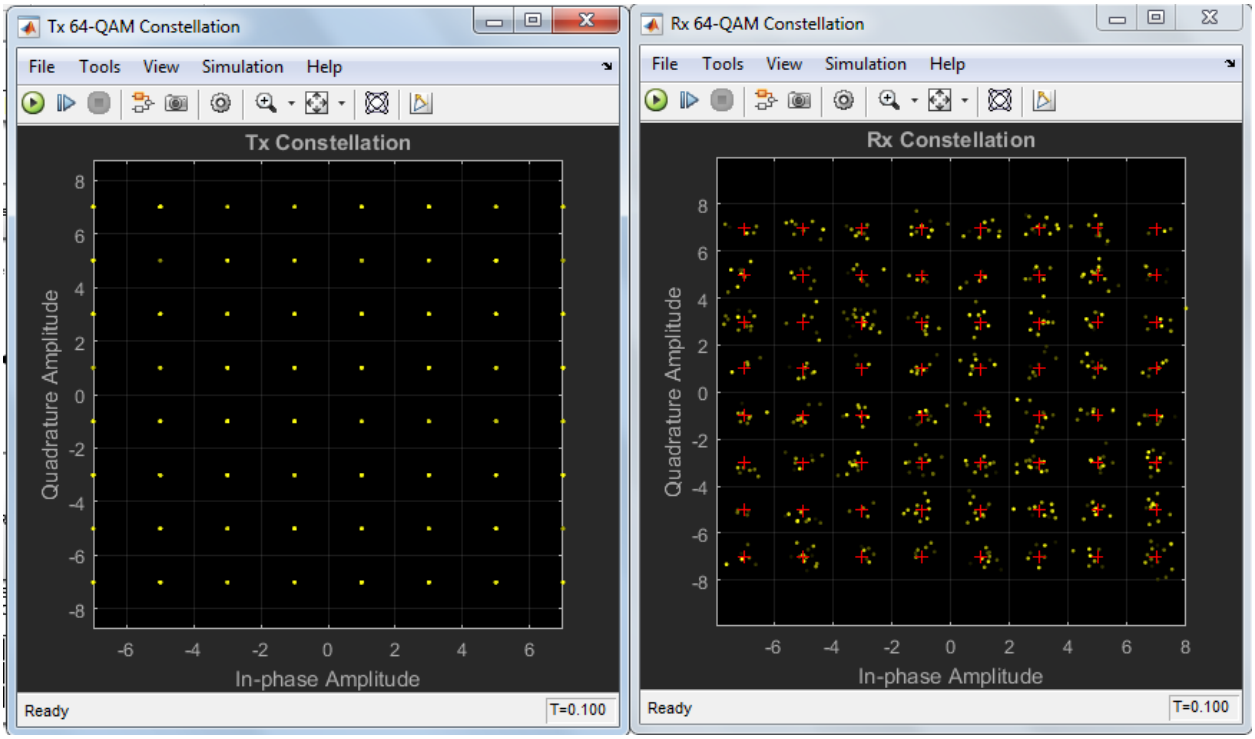


Рис. 4.42. Созвездия передатчика и приёмника при при Eb/No = 15 дБ.

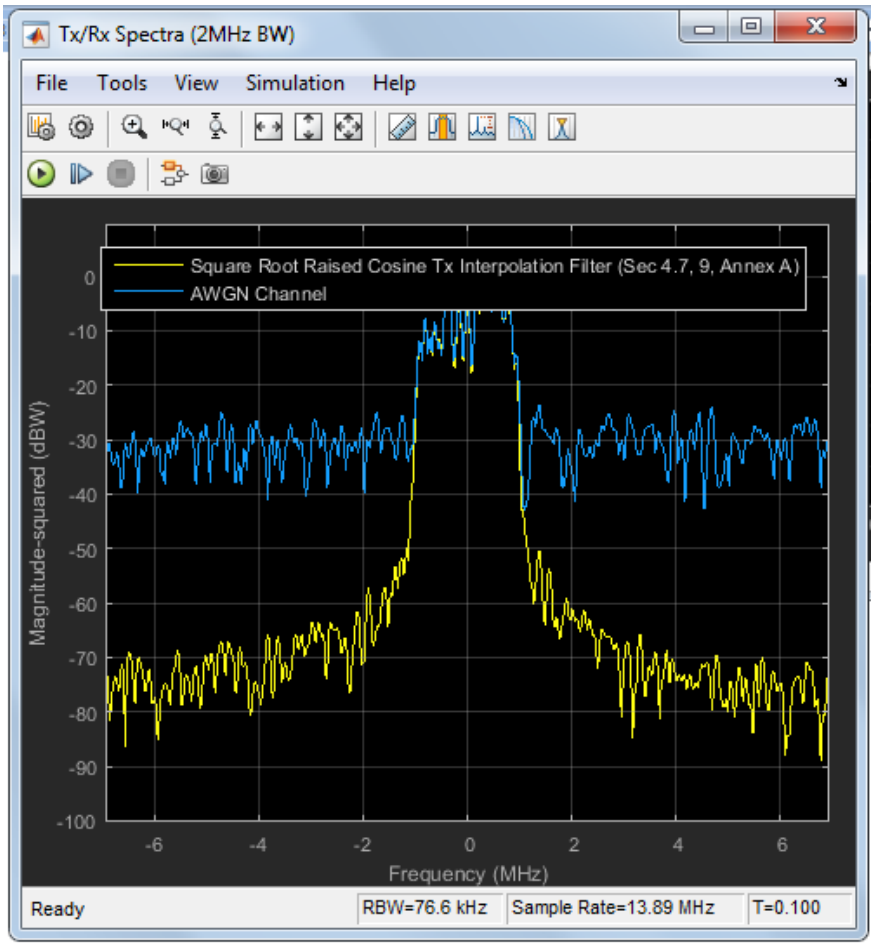


Рис. 4.43. Спектр передатчика и приёмника при при Eb/No = 15 дБ.

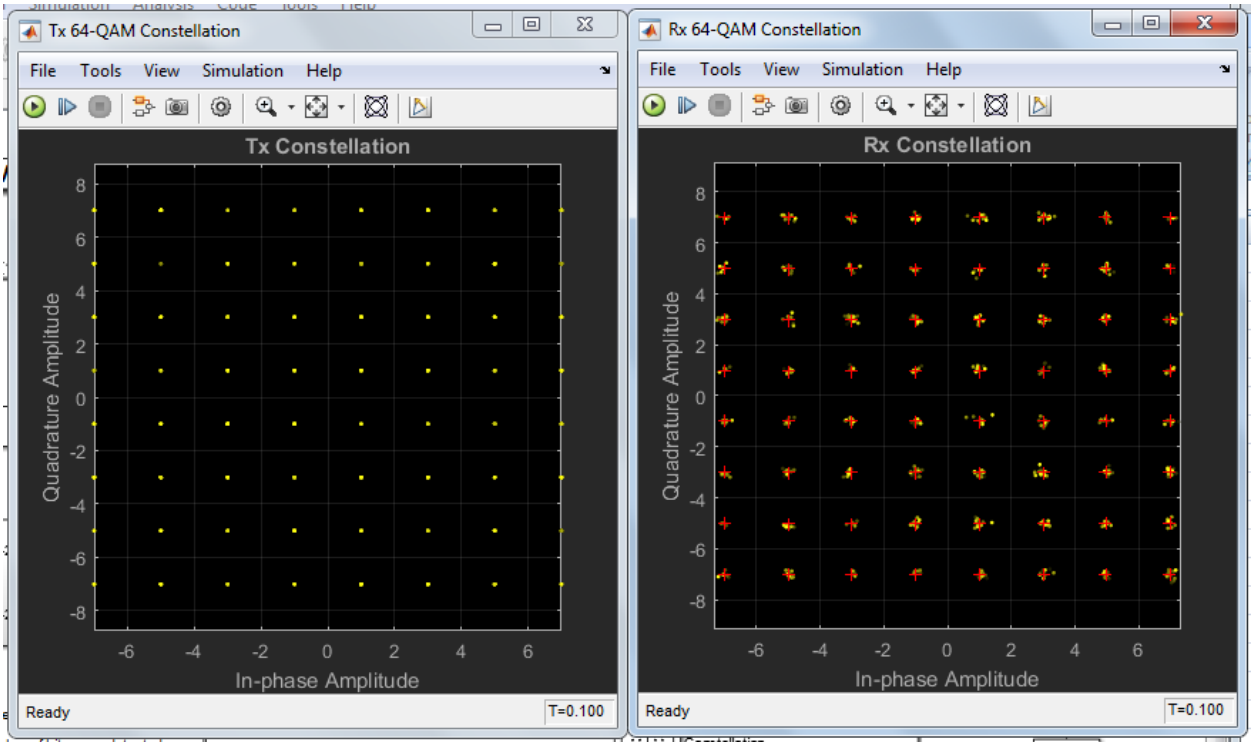


Рис. 4.44. Созвездия передатчика и приёмника при при Eb/No = 19 дБ.

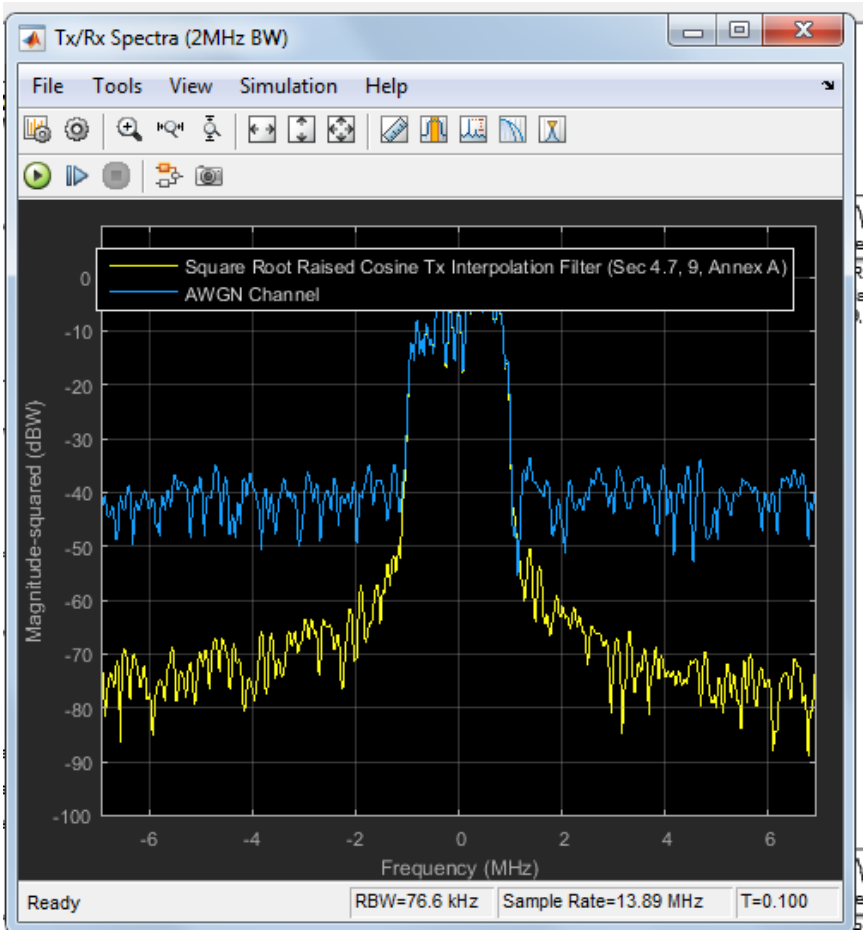


Рис. 4.45. Спектр передатчика и приёмника при при Eb/No = 19 дБ.

Таблица 4.19. График зависимость BER от Eb/No.

Eb/No, дБ	-10	-5	-2,5	-1	0	2	5	8	9	20
BER	0.4058	0.3359	0.2885	0.2563	0.03436	0.01264	0.001024	9.60 5E-6	0	0

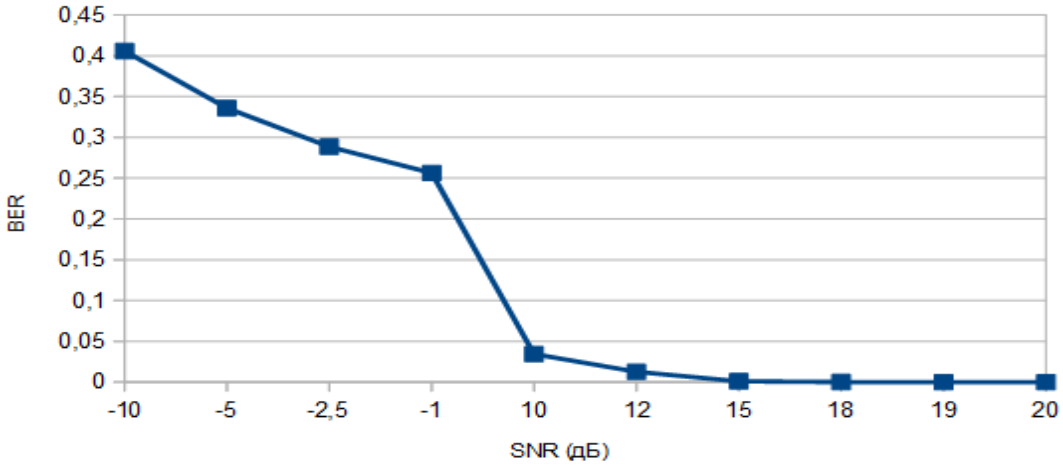


Рис. 4.46. Зависимость BER(SNR) для QAM-64.

На основе проведенного исследования можно сделать следующие выводы:

Использование многопозиционной модуляции QAM (Quadrature Amplitude Modulation – квадратурная амплитудная модуляция), а также хорошего отношения S/N, который существенно снижает вероятность ошибок BER (Bit Error Rate – частота ошибочных бит) позволило внедрить цифровое телевидение в системы кабельного телевидения.

4.4. Проектирование защищенной системы цифрового мобильного телевизионного вещания DVB-H и системы высокоскоростного цифрового мобильного ТВ-вещания DVB-H2 [17- 25]

DVB-H (*DigitalVideoBroadcasting – Handheld)* — европейский стандарт мобильного телевидения, один из семейства стандартов DVB. Стандарт DVB-H позволяет передавать цифровой видеосигнал на мобильные устройства, такие как КПК, мобильный телефон или портативный телевизор. Формально, этот стандарт был принят в ноябре 2004 года.

DVB-H является логическим продолжением стандарта DVB-T с поддержкой дополнительных возможностей, отвечающих требованиям для переносных мобильных устройств с автономным питанием.

Технологии мобильного вещания телевизионного вещания DVB-H

На сегодняшний день существует 8 форматов вещания, ориентированных на прием мобильными терминалами. Во-первых, это форматы DVB-T и DVB-H. Во-вторых, MediaFLO, закрытая система разработки компании Qualcomm. В-третьих, группа форматов, базирующихся на системе радиовещания DAB. К ней относятся MovioSystem, разработанная BritishTelecom, корейские форматы T-DMB и S-DMB, а также европейский профиль формата T-DMB. И, наконец, существует японский стандарт эфирного вещания ISDB-T, по своей

гибкости пригодный для любых видов эфирного вещания на любые терминалы.

Система DVB-H разработана на базе DVB-T, что обеспечивает их частичную совместимость. Она заключается в том, что трансляции DVB-H за исключением одного режима модуляции могут приниматься приемниками DVB-T, и в одном мультиплексированном потоке возможно совмещение трансляций DVB-H и DVB-T.

В то же время в DVB-H введен ряд добавлений на физическом уровне и заметно изменен канальный уровень.

DVB-T и DVB-H

Характеристики системы DVB-T неоднократно изложены в литературе1, поэтому напомним только его основные особенности. Главным отличием DVB-T от кабельной и спутниковой версий стандарта DVB является использование COFDM (CodedOrthogonalDivisionMultiplexing) модуляции. При таком способе модуляции применяется частотное мультиплексирование ортогональных несущих в сочетании с помехоустойчивым кодированием. Использование большого числа несущих позволяет удлинить время передачи каждого символа и выделить период защитного интервала для отстройки от помех многолучевого приема. В зависимости от количества ортогональных несущих в стандарте выделяется два режима 8К (8192 несущих) и 2К (2048 несущих). DVB-T предусматривает возможность использования трех видов модуляции — QPSK, 16 QAM и 64 QAM, четырех вариантов относительной длительности защитного интервала, а также пяти вариантов относительной скорости при наложении сверточного помехозащитного кодирования. Сочетания этих параметров позволяют гибко выбирать режим в зависимости от радиуса охвата соты, ландшафта и РЧ обстановки. Наличие защитного интервала дает возможность использовать DVB-T и для передачи на мобильные терминалы, в том числе движущиеся с большой скоростью. Но для передачи ТВ на мобильные телефоны и другие миниатюрные приемники эта система оказалась малопригодной. DVB-T оптимизирован для передачи стандартных ТВ потоков, в то время как карманные приемники имеют небольшие экраны, позволяющие воспроизвести картинку формата не более чем 1/4 CIF или 1/8 CIF. Кроме того, эти терминалы питаются от слабых аккумуляторных батарей, которые желательно эксплуатировать в максимально экономичном режиме. И, наконец, они имеют слабые приемные антенны и часто должны принимать сигнал в неблагоприятных условиях, в то время как размещение стационарных эфирных антенн может быть оптимизировано. С учетом всех этих обстоятельств для эфирной передачи на карманные мобильные терминалы был разработана специальная система DVB-H (DigitalVideoBroadcasting-Handheld), по возможности совместимая с DVB-T, но одновременно учитывающая перечисленные особенности приема. Рассмотрим компоненты DVB-H, относящиеся к физическому и

канальному уровням системы ISO/OSI.

Обобщенная архитектура системы DVB-H изображена на рисунке 1. Зеленым цветом помечены элементы, добавленные в DVB-H.

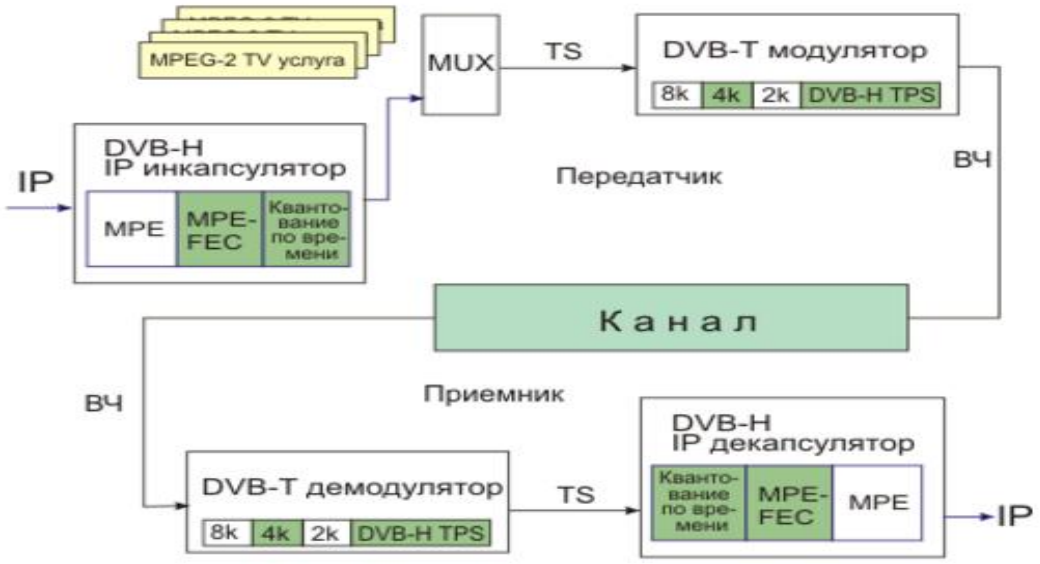


Рис. 4.47. Обобщенная архитектура системы DVB-H

Физический уровень

На физическом уровне система DVB-H максимально приближена к DVB-T. Поэтому укажем только дополнительные возможности, появившиеся в DVB-H.

Во-первых, к режимам модуляции 2K и 8K был добавлен еще один — 4K. Это дало дополнительную степень свободы в плане обмена максимальной скорости передвижения приемника на радиус охвата одной соты. Чем меньшее количество ортогональных несущих используется при COFDM модуляции, тем больший частотной интервал образуется между соседними несущими, и, соответственно, тем выше скорость движения терминала, при котором прием срывается из-за Доплеровского смещения частот. С другой стороны, чем меньше несущих, тем короче период, выделенный для передачи каждого COFDM символа и, с оответственно, короче защитный интервал. А сокращение защитного интервала снижает возможности отстройки от многолучевого приема, то есть уменьшает допустимый радиус соты. Для сетей DVB-T, рассчитанных в основном на стационарный прием, значительно более важным фактором является зона охвата. Что же касается сетей DVB-H, то там большую значимость приобретает возможность приема на скорости, а зона охвата в сильной мере ограничивается уровнем сигнала на входе тюнера.

Для возможности выбора компромиссного варианта был добавлен режим модуляции 4K, заполняющий нишу между 2K и 8K. Трансляции в режиме 4K могут приниматься только приемниками DVB-H.

Вторым дополнением на физическом уровне стала возможность более глубокого перемежения данных в режимах 4К и 2К. Канальное кодирование DVB-T предусматривает перемежение данных внутри одного COFDM символа. Оно в основном предназначено для компенсации селективных замираний, несущих при многолучевом приеме. В то же время мобильные терминалы с большей вероятностью могут оказаться в зоне действия широкополосных импульсных помех. И, как уже отмечалось, при приеме на скорости появляется доплеровское смещение частотного спектра, также приводящее к искажениям сигнала. Поэтому в стандартах мобильного вещания на базе COFDM (DAB, ISDB -T) для борьбы с последствиями длительных помех в цикл канального кодирования введено перемежение длинных серий данных, охватывающее десятки, а то и сотни OFDM символов.

Чем длиннее последовательность данных, участвующих в перемежении, тем эффективнее оказывается борьба с последствиями затуханий. Но для DVB-H такой путь невозможен. Во-первых, восстановление длинных последовательностей потребовало бы непрерывного приема, в то время как для целей энергосбережения в DVB-H реализован описанный ниже импульсный режим передачи. Во-вторых, для его осуществления необходимы большие объемы памяти, удорожающие приемник. И, наконец, это противоречит требованию совместимости с DVB-T. Поэтому было выбрано компромиссное решение. Для режима модуляции 8К, наиболее актуального для DVB-T, в DVB-H сохранено перемежение битов в рамках одного символа. А в режимах 4К и 2К, где каждый COFDM символ переносит меньшее количество информации, в качестве опции введена возможность временного перемежения, допускаемого объемами выделенной для этих целей памяти. Для 4К перемежение выполняется с глубиной в 2 COFDM символа, а для режима 2К — с глубиной в 4 COFDM символа. При активизации этой опции совместная передача трансляций DVB-H и DVB-T невозможна. Одновременно предусматривается опция дополнительной помехозащиты, реализованная на базе IP дейтаграмм и позволяющая в сильной мере компенсировать отсутствие глубокого перемежения. Принцип ее действия изложен позже.

Остальные механизмы внешнего и внутреннего канального кодирования, используемые в DVB-T, без изменения перенесены в DVB-H.Третье дополнение касается транспортной сигнализации (TPS — TransmissionParameterSignalling)2, в которую добавлены два бита, индицирующие наличие в потоке услуг, передаваемых в формате DVB-H, а также наличие дополнительной кодозащиты, реализуемой на базе IP дейтаграмм.Четвертым дополнением стала возможность использования полосы 5 МГц при условии, что эта она выделяется не в вещательном диапазоне. Она добавлена к полосам 6, 7 и 8 МГц,

допускаемых к использованию в DVB-T. Ее планируется применять при развертывании сетей DVB-H в США в L-диапазоне (1,670-1,675 ГГц).

Таблица 4.20. Параметры режимов 2K, 4K, 8K

Параметр	2K	4K	8K
Число активных несущих	1705	3409	6817
Число информационных несущих	1512	3024	6048
Длительность периода T, мс	0,109	0,109	0,109
Полезная символьная часть T_u, мс	224	448	896
Разнос между несущими $1/T_u$, Гц	4464	2232	1116
Разнос между несущими K_{min}и K_{max}, МГц	7,61	7,61	7,61

Канальный уровень

Одно из основных отличий DVB-H от DVB-T заключается в том, что в новой системе вся информация должна передаваться в форме IP дейтаграмм, инкапсулируемых в транспортные пакеты MPEG-2 TS с использованием метода многопротокольной инкапсуляции (MPE MultiProtocolEncapsulation). Это один из четырех методов инкапсуляции пакетов данных в транспортные пакеты MPEG-2 TS, определенных DVB, единственно пригодный для передачи потоковых услуг. Схема инкапсуляции показана на рисунке 5.213.

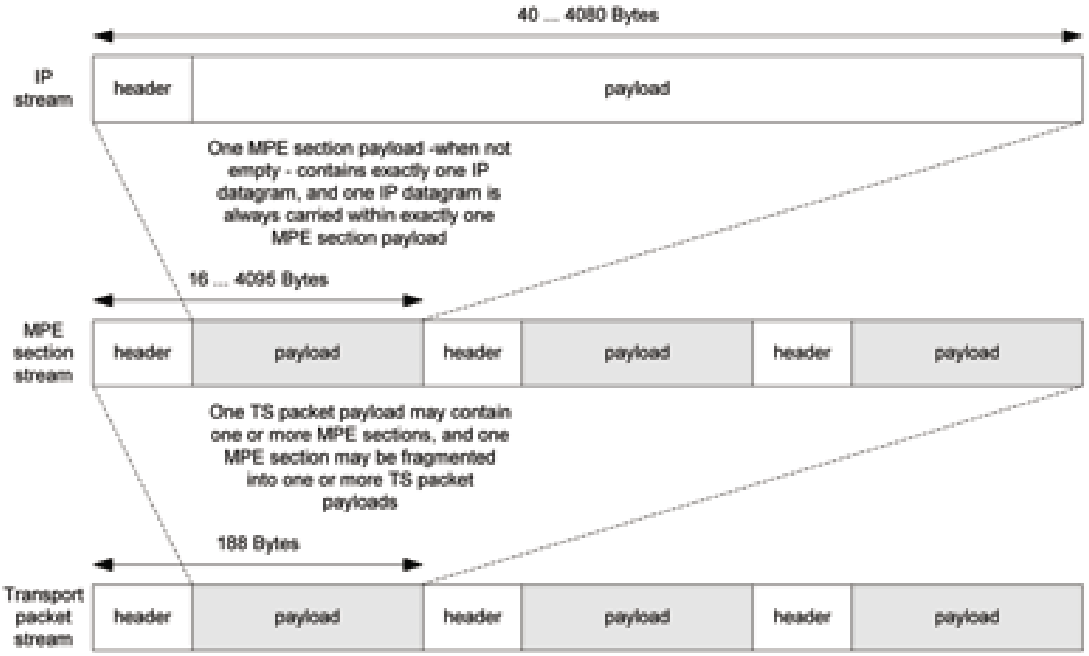


Рис. 4.48. Формат IP дейтаграммы

IP пакеты инкапсулируется в MPE секции, а те, в свою очередь, — в транспортные пакеты MPEG-2 TS, переносящие элементарные потоки. Каждый IP пакет занимает одну MPE секцию, длина который практически не коррелирована с емкостью пакетов MPEG2-TS. В одном пакете может передаваться множество MPE секций, и, наоборот, одна секция может занимать несколько транспортных пакетов.

Данные, относящиеся к одной услуге, инкапсулируется в транспортные пакеты MPEG-2 с постоянным идентификационным номером PID. Использование такого стека обусловлено тремя причинами.

Во-первых, в системах DVB-H предполагается передавать ТВ потоки, компрессированные не в MPEG-2, а в более эффективных форматах, в первую очередь, в H.264 /AVC3, для которых процесс инкапсуляции компрессированных аудио и видео в транспортные пакеты MPEG-2 TS жестко не специфицирован и обычно реализуется как раз через IP/MPE инкапсуляцию. Более того, DVB-H потенциально рассматривается как составная часть гибридной системы доставки мультимедийных услуг (IPDC).

В связи с этим понятие элементарного потока в DVB-H определяется иначе, чем в стандарте MPEG-2. В DVB-H это просто поток, передаваемый в пакетах с одним PID-ом. Снята жесткая корреляция элементарного потока с данными определенного типа. В одном элементарном потоке могут передаваться все данные, относящиеся к определенной ТВ программе или даже к нескольким программам. В последнем случае потоки разных ТВ программ будут передаваться в дейтаграммах с разным мультикастовым IP адресом и заключаться в MPE секции с разными MAC адресами. Аналогичным образом могут передаваться и не телевизионные услуги.

MPE-FEC

В DVB-H канальное кодирование накладывается на всю последовательность IP дейтаграмм, передаваемых в одном слоте, то есть на максимально возможный объем данных. Это кодирование введено в качестве опции и выполняется кодом Рида-Соломона. Принцип кодирования показан на рисунке 4.49.

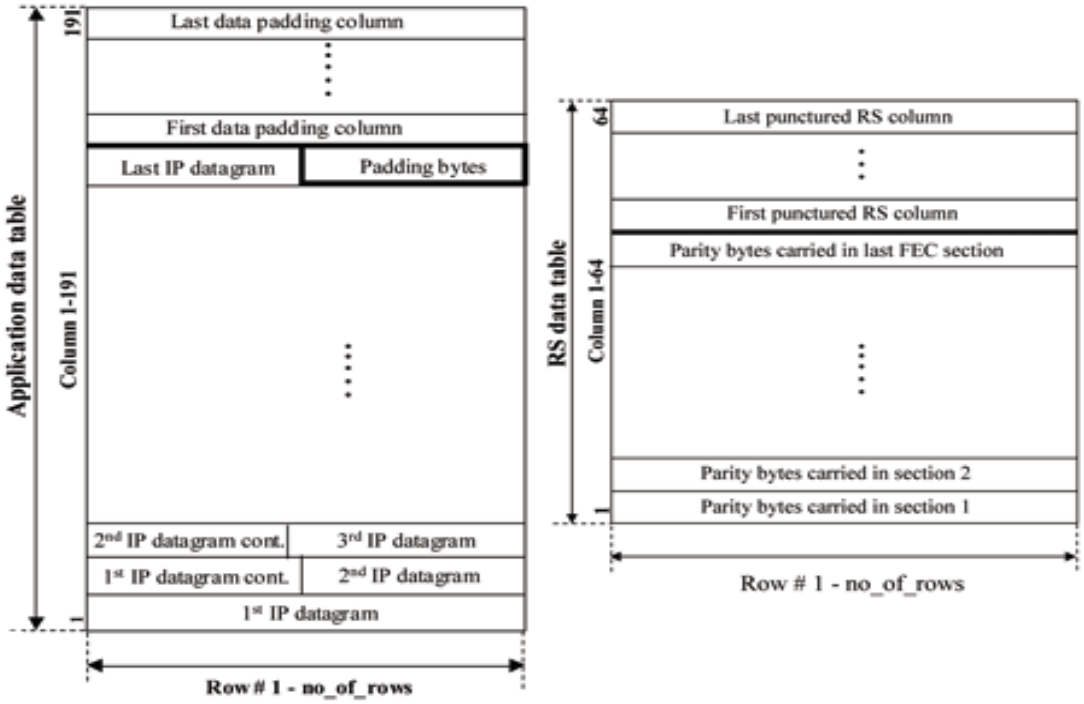


Рис. 4.49. Кодирование пакетов кодом Рида-Соломона

IP дейтаграммы помещаются в таблицу ApplicationDataTable, в которой последовательно заполняются столбцы начиная с левого верхнего угла. Высота столбцов может составлять от 1 до 1024 байт в зависимости длины дейтограмм, а их количество всегда одинаково — 191. Если в таблице остается пустое место, то оно заполняется холостыми байтами. Затем каждый ряд таблицы кодируется кодом Рида–Соломона (255, 191), в результате чего формируется 64 контрольных байта, заносимых в соответствующий ряд FEC таблицы. Затем обе таблицы инкапсулируются в пакеты MPEG-2 TS и транслируются в одном слоте. Вначале — информационная часть, а затем – контрольная. Причем байты контрольной таблицы при инкапсуляции считываются не рядами, как формируются, а колонками. Так создается виртуальное перемежение контрольных байт, требующее минимальных ресурсов приемника для восстановления их последовательности. Этот метод помехозащитного кодирования получил название MPE-FEC. MPE-FEC декодирование рекомендуется проводить на базе модели канала со стиранием4. Такое декодирование используется в каналах с пакетной передачей и включает два этапа.

На первом этапе с помощью циклического (CRC-x) кода выявляются искаженные пакеты и локализуются пораженные части потока. На втором этапе выполнятся восстановление пораженных пакетов, что при предварительной локализации искажений происходит более эффективно. CRC-x кодирование — стандартный способ помехозащиты пакетов информации. В частности, каждая MPE секция защищается кодом CRC-32. При использовании MPE-FEC незащищенными остаются служебные таблицы. Но с учетом того, что их содержание в большинстве случае довольно статично, то после несколько циклов

передачи ресиверу удается получить нужную информацию даже в сложных условиях. Посылка, защищенная MPE-FEC, может быть принята и ресиверами DVB-T. Но они будут игнорировать контрольные байты и не смогут воспользоваться защитой MPE-FEC.

Таким образом, особенности канального уровня формата DVB-H не препятствуют приему трансляций ресиверами DVB-T. Они просто будут принимать их неоптимальным образом. различными будут и условия приема трансляций DVB-T и DVB-H. Экспериментальные измерения показали, что для достижения передатчиками DVB-H и DVB-T одинаковой зоны охвата мощность первого должна быть на 20 дБ больше. В то же время требуемый для устойчивого приема уровень несущая/шум в DVB-H в среднем на 30% ниже, а максимально возможная скорость движения приемника – на 40% выше. В таблицах 5.16 и 5.17 представлены расчетные значения цифровых потоков для разных форматов модуляции и длительностей используемых интервалов.

Таблица 4.21. MPE-FEC кодированием в 3/4

Модуляция	Скорость кодирования	Защитный интервал			
		¼	1/8	1/16	1/32
QPSK	1/2	3,74	4,15	4,39	4,52
	2/3	4,98	5,53	5,86	6,03
	3/4	5,6	6,22	6,59	6,79
	5/6	6,22	6,92	7,32	7,54
	7/8	6,53	7,26	7,69	7,92
16QAM	1/2	7,46	8,3	8,78	9,05
	2/3	9,95	11,06	11,71	12,07
	3/4	11,2	12,44	13,17	13,58
	5/6	12,44	13,82	14,64	15,08
	7/8	13,07	14,51	15,37	15,83
64QAM	1/2	11,2	12,44	13,17	13,58
	2/3	14,93	16,59	17,57	18,1
	3/4	16,79	18,66	19,76	20,36
	5/6	18,66	20,74	21,95	22,62
	7/8	19,6	21,77	23,06	23,75

Таблица 4.22. Длительность интервалов MPE-FEC кодированием в 3/4

Параметр	Режим											
	2k	*4k*	*8k*	*2k*	*4k*	*8k*	*2k*	*4k*	*8k*	*2k*	*4k*	*8k*
Полезная символьная часть T_U	2048 T 224 мкс											
Защитный интервал Δ/T_U	1/4			1/8			1/16			1/32		
Длительность защитного интервала Tg	512 T 56 ms	1024 T 112 ms	2048 T 224 ms	256 T 28 ms	512 T 56 ms	1024 T 112 ms	128 T 14 ms	256 T 28 ms	512 T 56 ms	64 T 7 ms	128 T 14 ms	256 T 28 ms
Полная символьная продол-жительность $T_S=\Delta+T_U$	2560 T 280 ms	5120 T 560 ms	10240 T 1120 ms	2304 T 252 ms	4608 T 504 ms	9216 T 1008 ms	2176 T 238 ms	4352 T 476 ms	8704 T 952 ms	2112 T 231 ms	4224 T 462 ms	8448 T 924 ms

В стандарте DVB-T в качестве базовой используется OFDM модуляция, благодаря которой и достигаются уникальные свойства в части возможности построения одночастотных сетей (SFN – SingleFrequencyNetwork), возможности обеспечения низкого требуемого отношения несущая/шум (C/N), высокой защиты от переотраженных объектов и низкой чувствительности к эффекту Доплера (при приеме в движении). Помимо основных видов модуляции (QPSK, 16 QAM и 64 QAM) в стандарте DVB-T используется также и иерархическая модуляция, позволяющая в потоке с высоким приоритетом передавать меньшее число программ и даже с более худшим качеством, но со значительным увеличением зоны покрытия, представляя тем самым вести прием на мобильные устройства.

DVB-H2

DVB-H2 (NewGenerationHandheld) - на основе стандарта DVB-T2, DVB-NGH открывает путь для улучшения возможностей приема сигнала на мобильные и портативные устройства.

Они включают в себя MIMO (MultipleInputMultipleOutput, мультивход и мультивыход), частотно-временное разнесение (TFS) с одним тюнером, повернутые созвездия, улучшена и расширена проверка на четность с низкой плотностью, более эффективное чередование по времени и ультра-надежный уровень сжатия Layer-1. Спецификация DVB-NGH также включает гибридные профили, где наземные и спутниковые методы передачи данных могут быть объединены.

DVB-NGH охватывает последние модуляции и технологии кодирования и может рассматриваться как наиболее сложный радиоинтерфейс наземного вещания. Кроме того, он также предлагает дополнительную гибкость в эксплуатации, например, различные виды защиты для аудио- и видеопотоков в одном сервисе.

Разработка структурной схемы программного комплекса [25]

Система DVB-H была реализована в программной среде Matlab 2015a. Для того, чтобы запустить систему необходимо вести команду: open_system('commdvbt_alt');

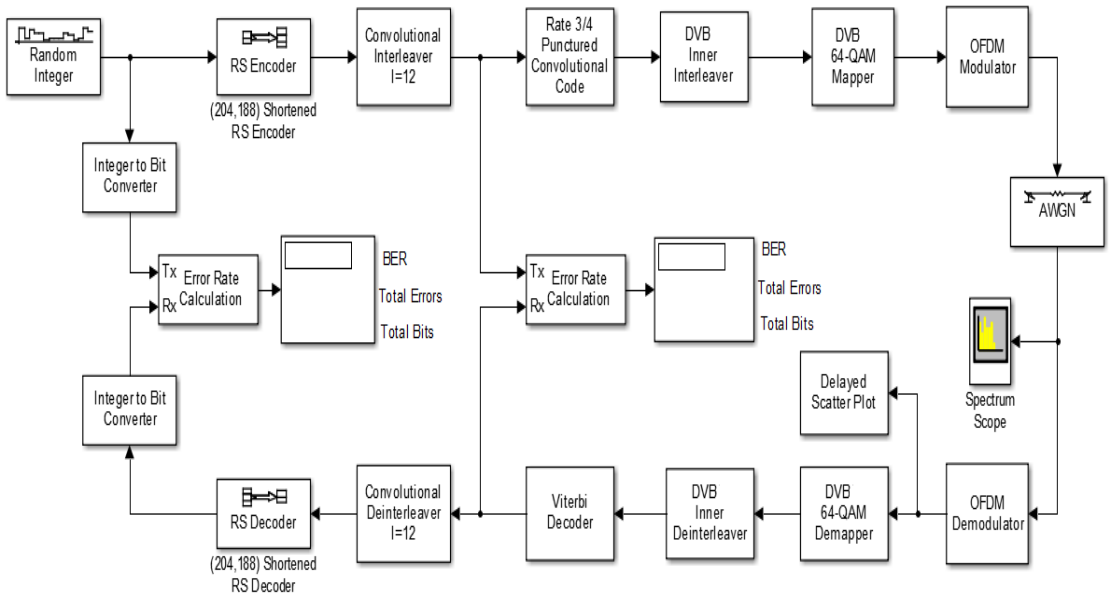


Рис. 4.50. Структурная схема DVB-H в режиме 2k Mode

Передающая часть структурной схемы системы состоит из следующих блоков:

RandomInteger–Генератор псевдослучайное последовательности.

RSEncoder – Код Рида-Соломона (255,191).

ConvolutionalInterleaver – Сверточныйперемежитель.

PuncturedConvolutionalCode – Сверточный кодер, с порождающими полиномами G1=171 и G2=133.

DVBInnerInterleaver – Внутренний перемежитель, состоящий из бит перемежителя и символьного перемежителя. В битовом перемежителеданныедемультиплексируются на v подпотоков, где v = 2, 4 и 6 дляQPSK, 16 -QAM и 64 - QAM, соответственно.

DVBM-QAMMapper – Все данные поднесущих объединяются в одном символе OFDM, которые модулируются с использованием QPSK, 16-QAM, 64-QAM.

OFDMModulator – Каждый символ состоит из 6817 и 1705 несущих для 8k и 2k режимовсоответственно. Длительность символа состоит из двух частей: полезная часть и защитный интервал (1/4, 1/8, 1/16, 1/32).

AWGN – Канал с шумами.

Практическая часть

Запустить модель системы DVB-H в программе Matlab следующим образом: Matlab R2015 – Simulink Model – Open – dvbh.slx [25].

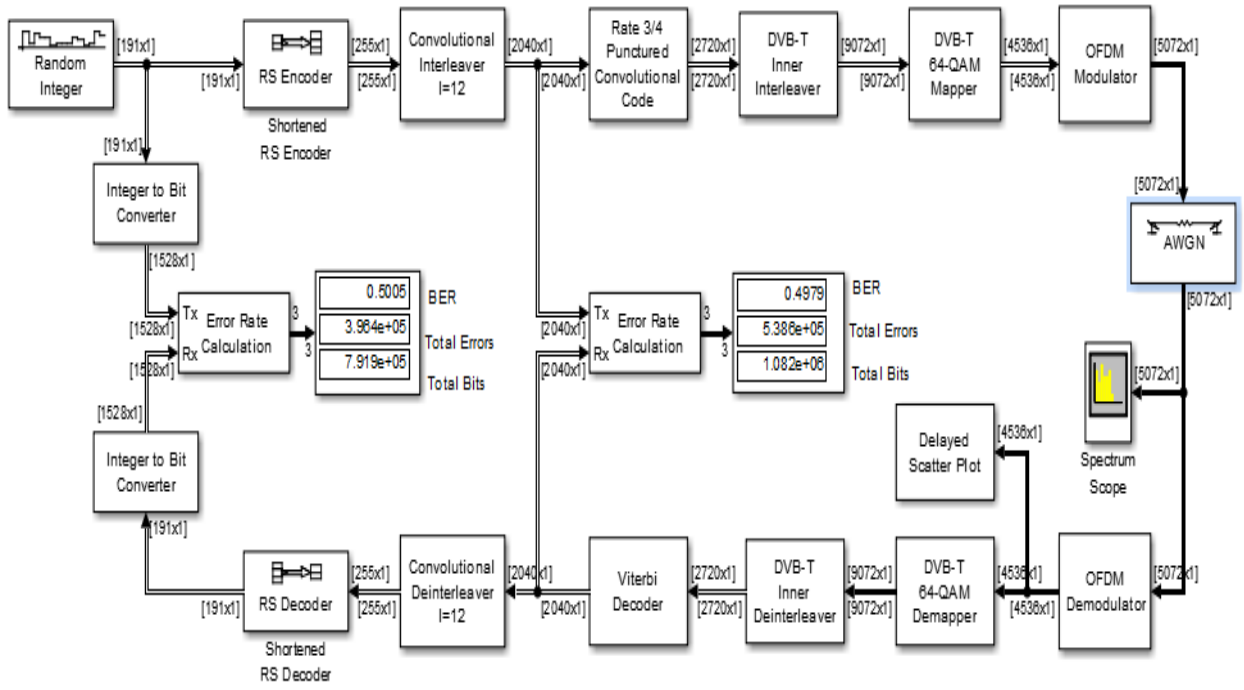


Рис. 4.51. Функциональная схема системы DVB-H реализованная в Matlab R2015b – Simulink

Выставить необходимые параметры для следующих блоков: Random-Integer Generator, RS Encoder-Decoder, Параметры DVB Inner Deinterleaver (Buffer3), OFDM modulator-demodulator (для QPSK длина FFT: 5072, для 16-QAM длина FFT: 2804).

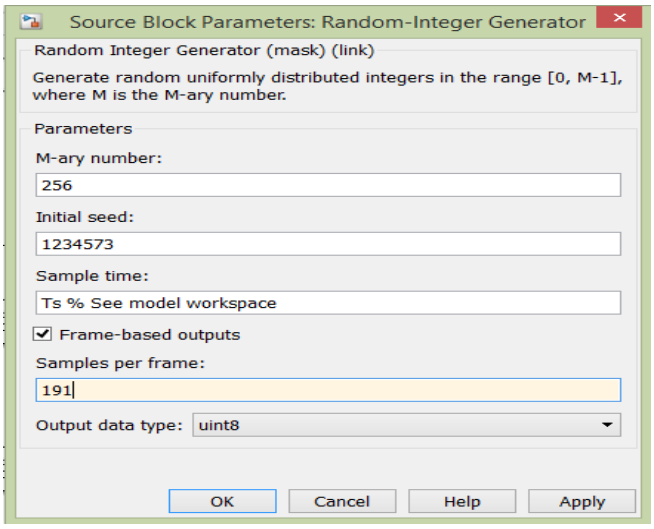


Рис. 4.52. Параметры Random-Integer Generator

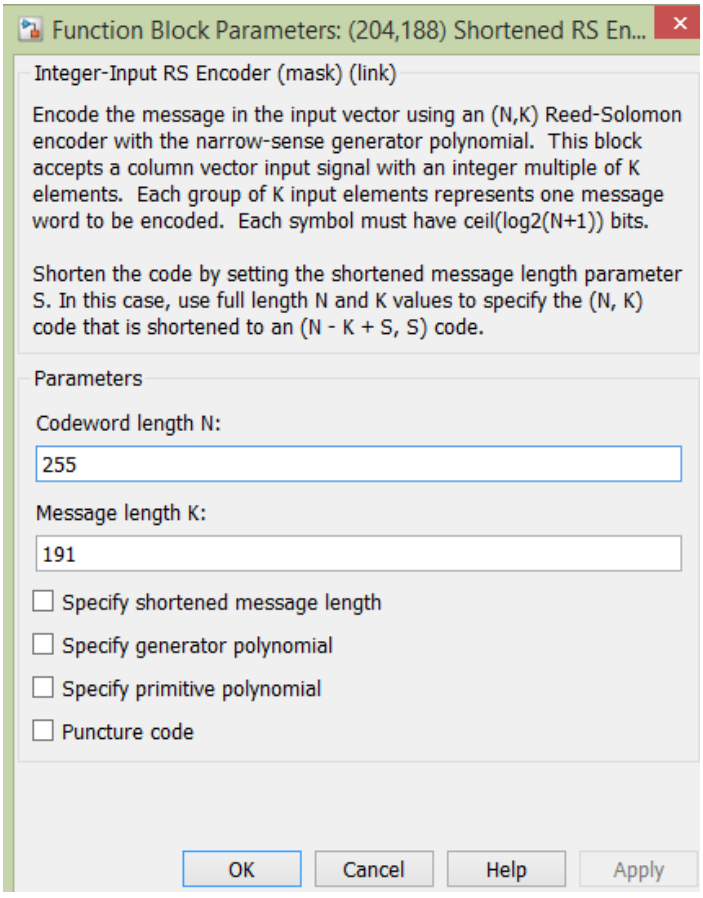


Рис. 4.53. Параметры RS Encoder-Decoder

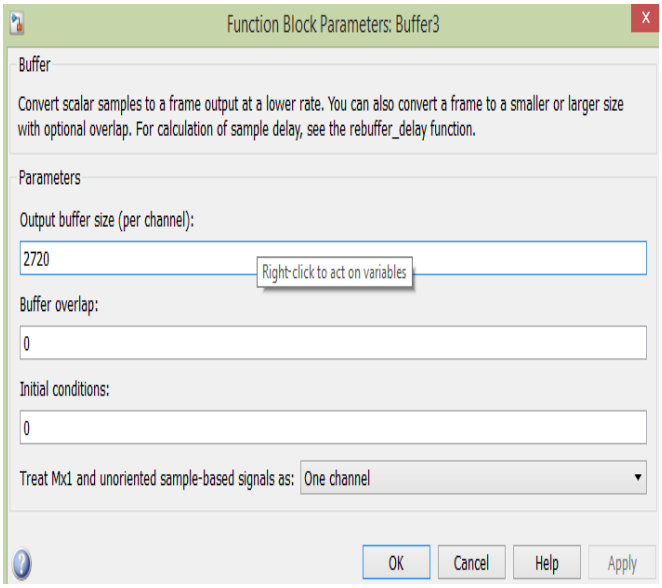


Рис. 4.54. Параметры DVB Inner Deinterleaver (Buffer3)

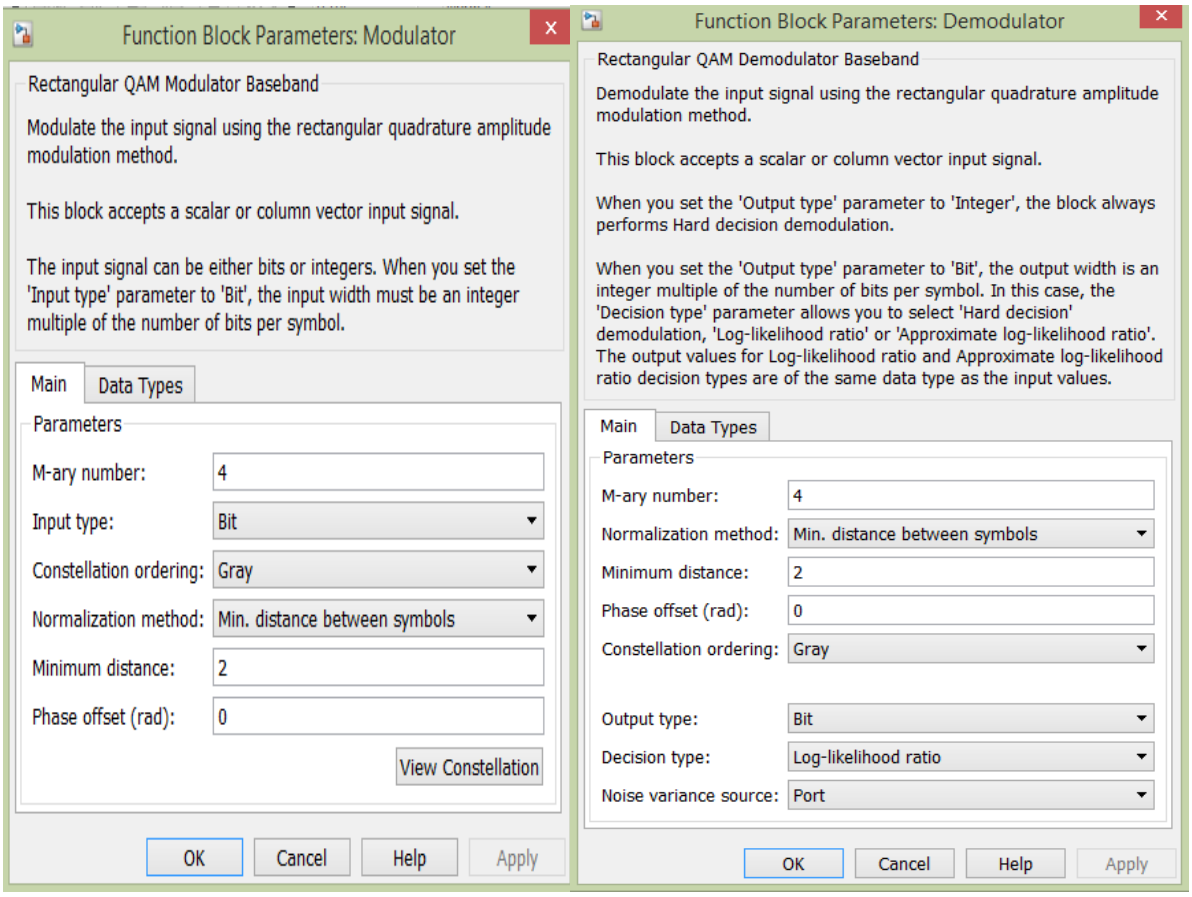


Рис. 4.55. Параметры QPSK модулятора

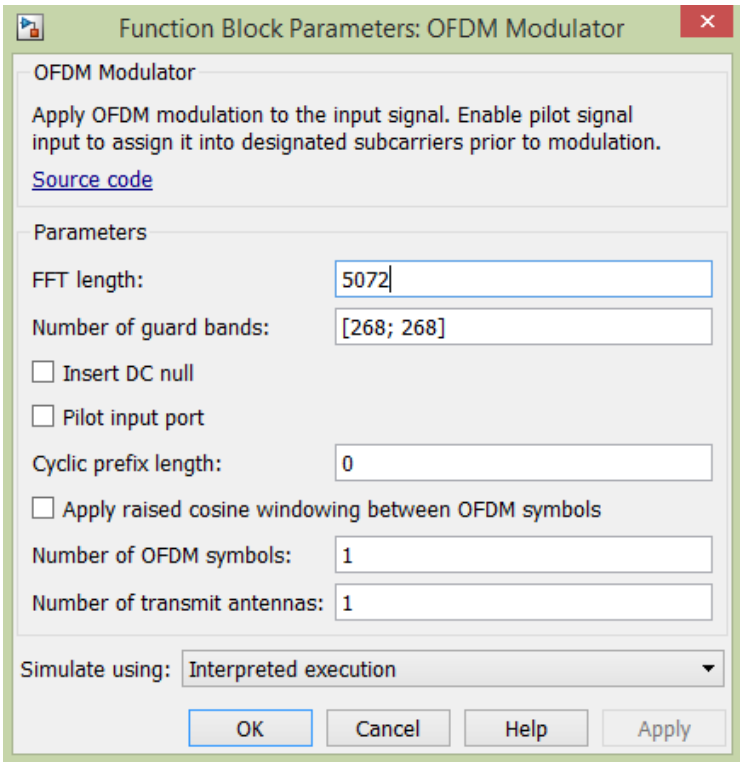
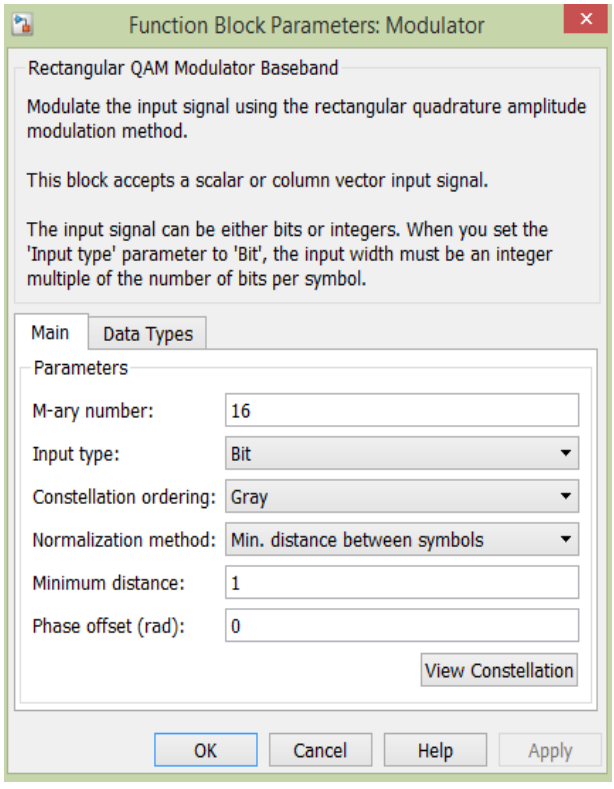


Рис. 4.56. Параметры OFDM modulator-demodulator



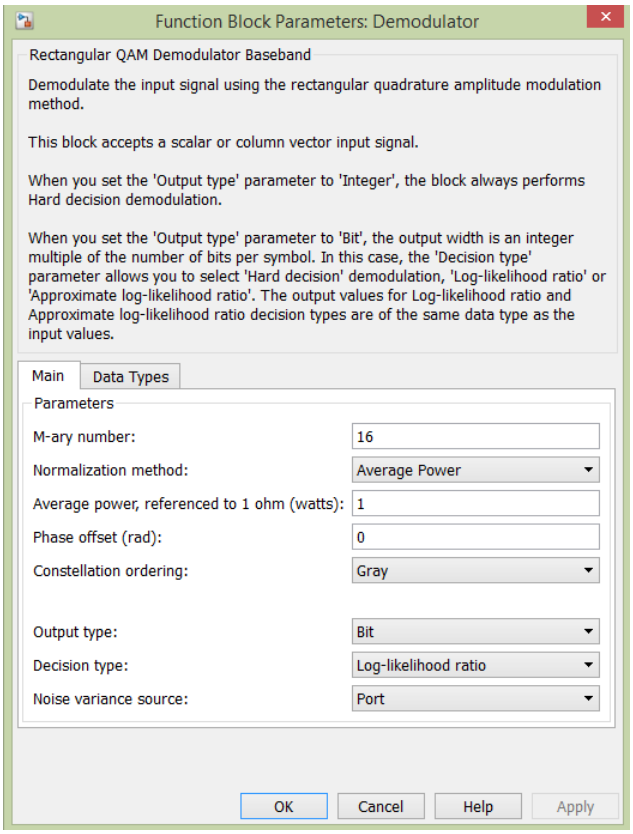


Рис. 4.57. Прарметры 16-QAM модулятора

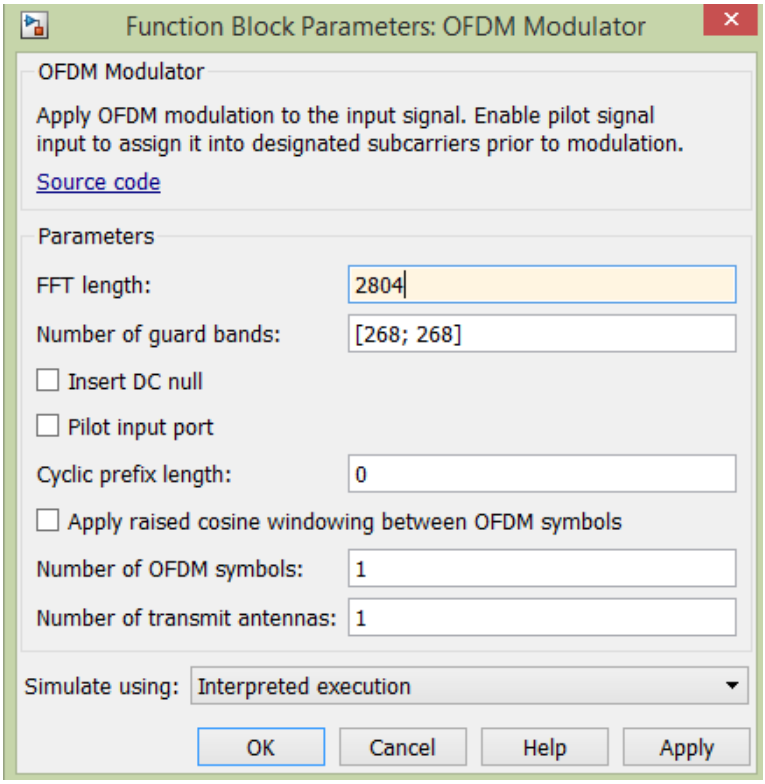


Рис. 4.58. Параметры OFDM modulator-demodulator

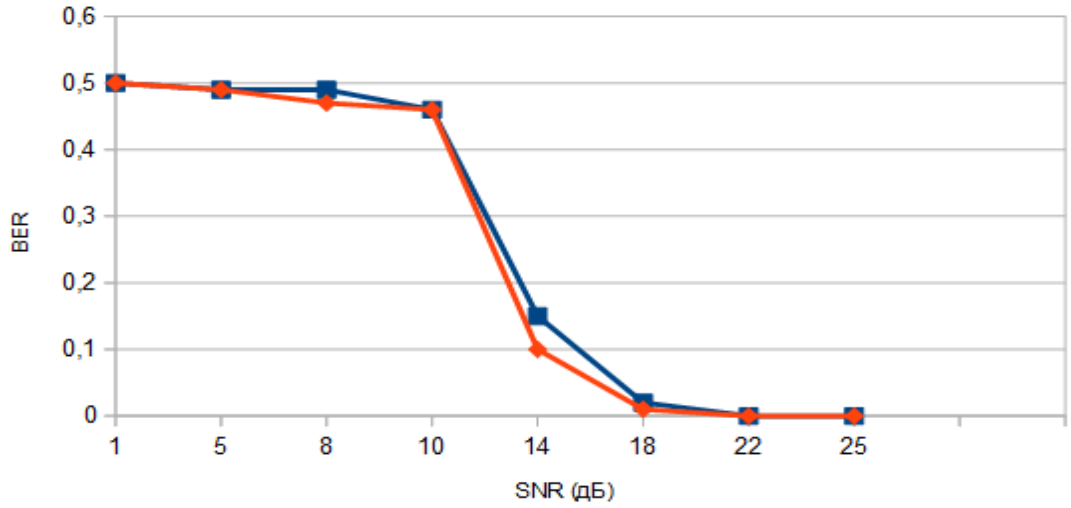


Рис. 4.59. Зависимость BER от SNR для системы DVB-H при использовании QPSK (синий) и 16-QAM (красный).

При исследовании зависимости битовой вероятности битовой ошибки от отношения сигнал/шум рассматриваемой системы мобильного вещания были сняты изображения спектра передаваемого сигнала и диаграммы созвездий QPSK и 16-QAM исследуемой системы при SNR равном 1 дБ, 18 дБ.

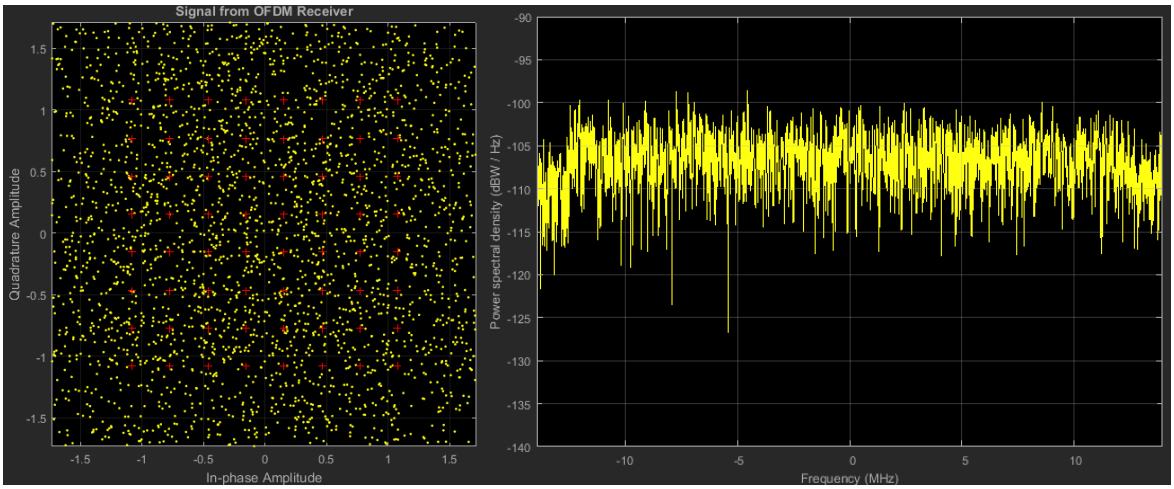


Рис. 4.60. Спектр OFDM-сигнала и диаграмма созвездий QPSK при SNR=1 дБ

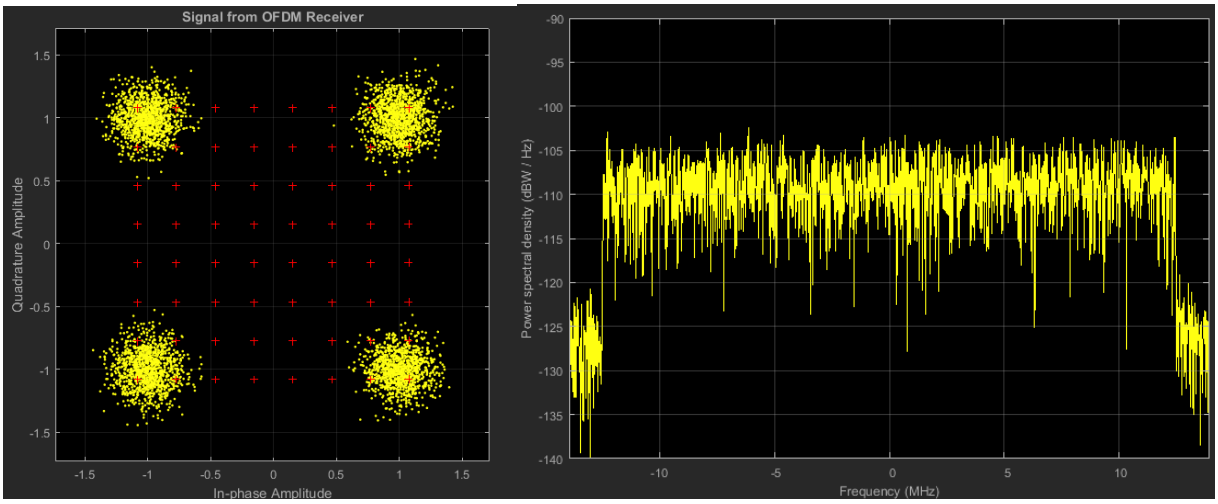


Рис. 4.61. Спектр OFDM-сигнала и диаграмма созвездий QPSK при SNR=18Б

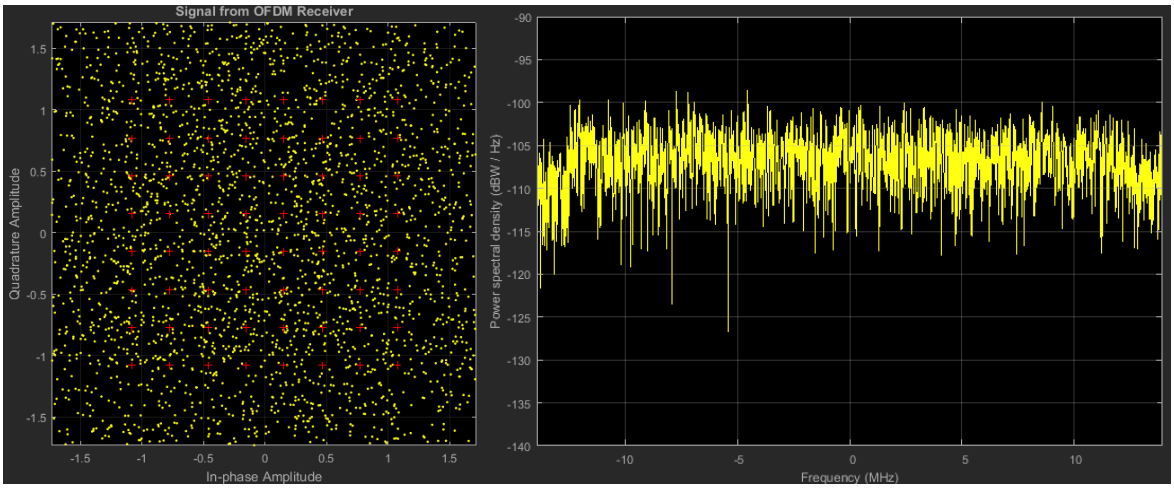


Рис. 4.62. Спектр OFDM-сигнала и диаграмма созвездий 16-QAM при SNR=1 дБ

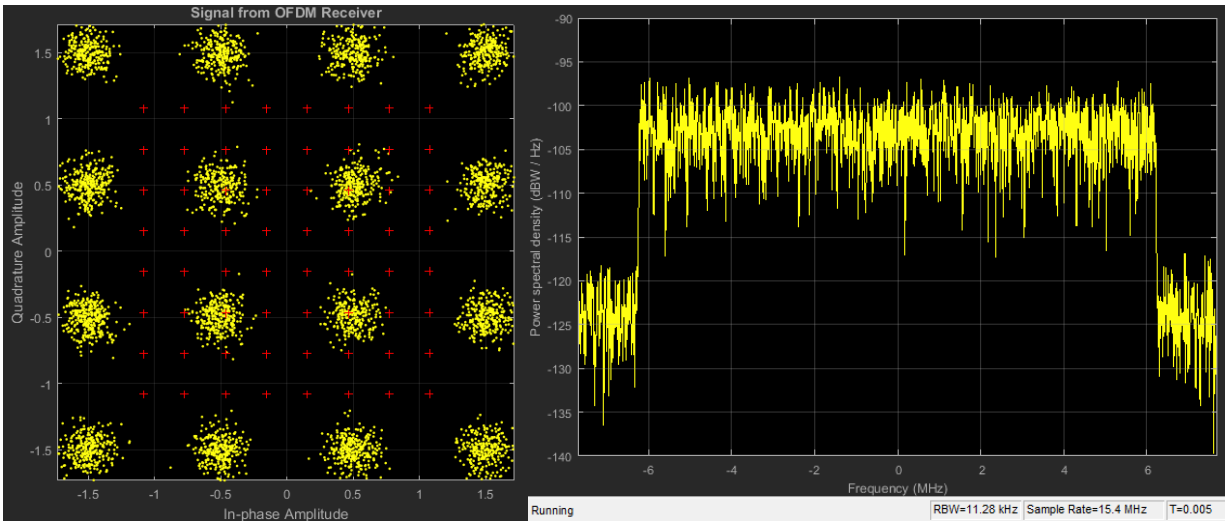


Рис. 4.63. Спектр OFDM-сигнала и диаграмма созвездий 16-QAM при SNR=18Б

В процессе выполнения данной лабораторной работы были изучены основные теоретичиские аспекты системы цифрового мобильного телевизионного стандарта DVB-H

При выполнении практической части работы была построена зависимость битовой вероятности ошибки от отношения сигнал/шум для QPSK и 16-QAM модуляции. Результат представлен в виде графика (рисунок 4.63).

Были сняты изображения спектра OFDM-символа и диаграммы созвездий QPSK и 16-QAM при прохождении сигнала в канале с аддитивным белым гауссовским шумом.

Полученные в результате моделирования данные позволяют сделать вывод о том, что безошибочная передача данных по каналу связи в системе DVB-T возможна при отношении сигнал/шум не менее 18 дБ.

DVB-H является обновлением для основного стандарта, которое решает проблемы мобильного приема. Главное нововведение - timeslicing. Передатчик циклически выдает в эфир пакеты, принадлежащие всем транслируемым каналам по очереди. Передача осуществляется короткими импульсами с использованием максимальной пропускной способности канала. Приемник включается только в определенные моменты, когда необходимо загрузить очередную порцию видеопотока. Это позволило в 10 раз увеличить продолжительность автономной работы портативных телевизоров. Дело в том, что для приема DVB-T применяются довольно сложные чипы, производятся интенсивные математические вычисления. И когда система работает постоянно, без перерыва, то автономность лучших образцов мобильных устройств достигает 20-40 минут. В свою очередь техника, основанная на DVB-H, способна функционировать до 10 часов от одного заряда батареи.

Другая особенность стандарта - высокая помехоустойчивость за счет введения механизма коррекции ошибок. В обычном DVB-T используется разнесенный прием на несколько антенн, что позволяет системе выбирать наименее поврежденный сигнал. В портативном устройстве такое решение реализовать труднее.

Третья важная особенность - DVB-H основывается на IP-протоколе, а это значительно упрощает и удешевляет построение вспомогательной инфраструктуры. Возможным становится использование готовых, недорогих программных решений.

ЗАКЛЮЧЕНИЕ

В учебном пособии рассмотрены основы проектирования защищенных телекоммуникационных систем. Проектирование защищеннах инфокоммуникационны систем: 1. Проектирование защищенной IP-АТС на базе программного обеспечения ASTERISK; 2. Проектирование системы обеспечения защищенного маршрутизируемого взаимодействия при использовании программного обеспечения VIPNET OFFICE; 3. Проектирование защищенной многоточечной видеоконференц связи на базе WEB-технологии. Впервые представлено проектирование защищенных систем на базе MATLAB 2015b Simulink модемов и кодеков современных телекоммуникационных систем стандарта CDMA, системы мобильной связи стандарта IEEE 802.11 (WiFi), мобильной связи стандарта IEEE 802.15.4 ZigBee, системы мобильной связи стандарта IEEE 802.15.1 (Bluetooth), системы мобильной связи стандарта IEEE 802.16 (WiMAX), системы мобильной связи стандарта IEEE 802. 20 LTE, системы цифрового наземного телевизионного вещания DVB-T, системы цифрового спутникового телевизионного вещания DVB-S и системы высокоскоростного цифрового спутникового ТВ-вещания DVB-S2, системы цифрового кабельного телевизионного вещания DVB-C и системы высокоскоростного цифрового кабельного ТВ-вещания DVB-C2, системы цифрового мобильного телевизионного вещания DVB-H и системы высокоскоростного цифрового мобильного ТВ-вещания DVB-H2.

Получены основные характеристики ТКС в зависимости от параметров систем, характеристик сигналов и влияния шумов и многолучевости (для CDMA). Представлены созвездия для модуляторов, спектры сигналов на входе и выходе канов связи, а также Зависимости вероятности битовой ошибки от отношения сигнал/шум и многолучевости.

Материалы учебного пособия могут быть использованы как для учебных целелей, так и как справочный материал при проектировании ТКС - представлен курс лекций и компьютерный практикум для каждой из проектируемых защищенных систем.

В приложении даны задания на самостоятельную работу: 1. Оптимизация методов помехоустойчивого кодирования я телекоммуникационных систем; 2. Криптоанализ классических шифров; 3. Криптоанализ шифротекстов, полученных методом гаммирования; 4. Криптоанализ алгоритма RSA.

К учебному пособию прикладывается CD-диск с программным обеспечением для всех комплексов, включенных в пособие, а также пакетами MATLAB 2015b и NI LabVIEW со всем установочным ПО. Программные комплексы позволят читателю самостоятельно провести моделирование для ТКС со своими характеристиками.

ЛИТЕРАТУРА

1. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей. Учебное пособие для вузов / Е.Б. Алексеев, В.Н. Гордиенко, В.В. Крухмалев и др.; Под редакцией В.Н. Гордиенко и М.С. Тверецкого. - М.: Горячая линия - Телеком, 2008. - 392 с.

2. Росляков А.В., Самсонов М.Ю., Шибаева И.В. IP-телефония. – М.: Эко-Трендз, 2003.-250с.

3. Жданов А. Г., Смирнов Д. А., Шипилов М. М. Передача речи по сетям с коммутацией пакетов (IP-телефония). - СПб, 2001. – 148с.

4. Гольдштейн Б. С., Пинчук А. В., Суховицкий А. Л. IP-телефония. - М.: Радио и связь, 2001.-336с.

5. Гольдштейн Б.С., Зарубин А.А., Саморезов В.В., Протокол SIP, Справочник., - СП.: БХВ, 2005.-456с.,

6. IPTop. Протокол инициирования сеансов связи - SIP. [Электронный ресурс]/ – Режим доступа: http://www.iptop.net/sip/. Дата обращения: 1.04.2014.

7. Официальный сайт компании ОАО «ИнфоТеКС». ViPNetOFFICE. [Электронный ресурс] / – Режим доступа: http://infotecs.ru/products/catalog.php?SECTION_ID=&ELEMENT_ID=411

8. ОАО "Инфотекс", Москва, Россия. Межсетевой экран / ViPNet Office Firewall / Руководство администратора.

9. http://web-in-learning.blogspot.ru/2012/02/openmeetings.html (дата запроса 31.10.2015)

10. http://old.stel.ru/videoconference/tech_vc/podrobno/vks-management.php (дата запроса 31.10.2015)

11. http://wiki.first-leon.ru/index.php/OpenMeetings (дата запроса 31.10.2015)

12.https://ru.wikipedia.org/wiki/видеоконференция (дата запроса 31.10.2015)

13. Современные методы и средства управления в сетях видеоконференцсвязи / М.В. Виноградов – 2013. стр. 7

14. Банкет В.Л. Помехоустойчивое кодирование в телекоммуникационных системах: учебн. пособие. - Одесса: ОНАС им А.С. Попова, 2011. - 104 с.

15. Банкет В.Л. Сигнально-кодовые конструкции в телекоммуникационных системах. - Одесса: Фешкс, 2009. - 180 с.

16. Мелихов С.В. Аналоговое и цифровое радиовещание: Учебное пособие. Издание второе, исправленное. - Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2012. – 233 с.

17. Модуляция, кодирование и моделирование в телекоммуникационных системах: Учебное пособие / Голиков А. М. – 2016. 516 с. Режим доступа: https://edu.tusur.ru/training/publications/6088.

18. Скляр Б. Цифровая связь. — М.: Издательский дом Вильямс. 2003 — 1104с

19. Феер К.: Беспроводная цифровая связь. М.: Радио и связь, 2000. - 520 с.

20. Крейнделин В.Б., Колесников А.В. Оценивание параметров канала в системах связи с ортогональным частотным мультиплексированием. Учебное пособие / МТУСИ.-М., 2010. -29 с.

21. Дворкович В.П., Дворкович А.В. Цифровые видеоинформационные системы (теория и практика) Москва: техносфера, 2012. – 1008 с.

22. Майков, Д.Ю. Оценка сдвига частоты для процедуры Initial Ranging в системе «мобильный WiMax» / Д.Ю. Майков, А.Я. Демидов, Н.А. Каратаева, Е.П. Ворошилин // Доклады ТУСУРа. – 2011. – №2 (24). – 59-63 с.

23. Серов А. В. Эфирное цифровое телевидение DVB-T/H. - БХВ-Петербург, 2010 – 465 с.

24 . Стандарт DVB-H. Система мобильного ТВ вещания. [Электронный ресурс] – Режим доступа: http://www.konturm.ru/tech.php?id=dvbh

25.http://www.mathworks.com/examples/simulink-communications/mw/comm_product-LTEDownlinkExample-lte-phy-downlink-with-spatial-multiplexing

26. Алгоритм RSA : метод. указания к выполнению лабораторных работ для студентов спец. 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем» очной формы обучения / сост.: О. Н. Жданов, И. А. Лубкин ; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2007. – 38 с.

ПРИЛОЖЕНИЕ 1.
ЗАДАНИЯ НА САМОСТОЯТЕЛЬНУЮ РАБОТУ

П1.1. Оптимизация методов помехоустойчивого кодирования для телекоммуникационных систем

Помехоустойчивое кодирование является эффективным способом оптимизации ТКС. На практике инженеру проектровщику ТКС приходится решать задачи оптимизации на основе численных расчетов и соответствующего сравнения методов помехоустойчивого кодирования и выбора конкретных методов и соответствующим им кодов. Решение именно такой задачи положено в основу СР [1].

Исходные данные заданы в таблице вариантов П1.2:

1. Цифровая информация передается двоичным кодом. Виды передаваемой цифровой информации:

ДК - данные компьютерного обмела;

ЦТЛФ - цифровая телефония;

ЦТВ - сообщения цифрового ТВ;

ЦЗВ - сообщения цифрового звукового вещания.

2. Канал святи - канал с постоянными параметрами и аддитивным белым гауссовым шумом.
3. Отношение с/ш на входе демодулятора $h_б = E_б / N_0$.
4. Методы модуляции: ФМ-2, ФМ-4.
5. Прием - когерентный.
6. Производительность источника $R_{ист}(бит/с)$.
7. Полоса пропускания канала $F_K(кГц)$.
8. Вероятность ошибки бита в сообщениях, отдаваемых получателю, не более *p.*
9. Допустимая сложность декодера СК (показатель сложности решетки кода) - не более *W.*

Необходимо:

1. Выбрать и обосновать выбор корректирующего кода для проектируемой ТКС, обеспечивающего требуемую вероятность ошибки бита p в сообщениях, отдаваемых получателю, при условии выполнения следующих ***ограничений:***

   1.1. *Полоса частот* кодированного сигнала не должна превышать полосу пропускания канала F_K.

1.2. При использовании сверточных кодов *показатель сложности* решетки кода должен быть не более величины *W*.

2. Разработать и дать подробное описание *структурной и функциональных схем кодера и декодера* выбранного кода и обосновать их параметры.
3. Проанализировать показатели энергетической и частотной эффективности телекоммуникационной системы и сравнить их с предельными значениями эффективности.

4. Сделать *заключение* по выполненной работе.

Содержание пояснительной записки работы:

1. Задание и исходные данные.
2. Описание структурной схемы проектируемой телекоммуникационной системы с указанием мест включения кодера помехоустойчивого кода, модулятора, демодулятора и декодера с подробными пояснениями выполняемых ими функций.
3. Классификация корретирующих кодов по структуре. Сравнительный анализ преимуществ и недостатков помехоустойчивых блоковых и сверточных кодов. Обоснование применения в проекте сверточных кодов.
4. Классификация и сравнительный анализ алгоритмов декодирования сверточных кодов. Обоснование выбора алгоритма Витерби для декодирования СК.
5. Расчет ширины спектра цифрового сигнала с заданным видом модуляции.
6. Расчет ширины спектра кодированного цифрового сигнала с заданным видом модуляции в зависимости от скорости кода.
7. Определение допустимой скорости кода $R^*_{КОД}$ из условия *непревышения* полосой частот кодированного сигнала полосы пропускания канала (ограничение 1.1).
8. Определение перечня кодов со скоростями, превышающими допустимую скорость $R^*_{КОД}$, которые могут быть использованы для решения поставленной задачи.
9. Выбор СК из этого перечня, обеспечивающего заданную вероятность ошибки бита (условие 1) и удовлетворяющего требованию ограничения по сложности декодера (ограничение 1.2).
10. Проверочный расчет зависимости вероятности ошибки на выходе декодера выбранного СК.
11. Разработка и описание структурных и функциональных схем кодера и декодера выбранного СК.
12. Заключение с подведением итогов выполненной работы.
13. Список использованных источников.

Методические указания к выполнению КР

Расчет ширины спектра сигнала ФМ-2 (ФМ-4) следует производить по рекомендациям материалов главы 1. Применение корректирующих кодов со скоростью $R^*_{КОД}$ приводит к расширению спектра кодированного сигнала в $(K_F = 1/R_{КОД})$ раз. С другой стороны, корректирующая способность кода возрастает с уменьшением скорости кода (т.е. с увеличением избыточности). Поэтому *задача оптимизации* параметров корректирующего кода состоит в выборе кода со скоростью, при которой ширина спектра кодированного сигнала *не превышает заданную полосу пропускания канала.* Если требуемая полоса пропускания канала для передачи ФМ сигнала с информационной скоростью $R_{ИСТ}$ равна $F_{(ФМ)}$, а скорость кода выбрана равной $R_{КОД}$, то полоса пропускания канала, необходимая для передачи кодированного ФМ сигнала, будет равна

$$F_{К(ФМ-СК)} = \frac{F_{(ФМ)}}{R_{КОД}}.$$

Тогда из условия непревышения этой полосой частот сигнала полосы пропускания канала ($F_{К(ФМ-СК)} < F_К$) получаем простое *условие для выбора скорости кода*

$$R^*_{КОД} > R_{КОД} = \frac{F_{(ФМ)}}{F_К}. \qquad (П1.1)$$

Сказанное иллюстрируется рисунком 5.1. Ширина спектра кодированного ФМ сигнала пропорциональна коэффициенту расширения полосы. По мере снижения скорости кода (возрастания K_F) полоса расширяется и достигает значения полосы пропускания канала. На этом же рисунке показана зависимость АЭВК от K_F (что равноценно скорости кода). Пересечение кривой полосы с граничным заданным значением $F^*_К$ определяет допустимое значение коэффициента расширения полосы пропускания канала $K_p = 1/R_{КОД}$ и, соответственно, скорость кода $R^*_{КОД}$. Первым этапом выбора корректирующего кода.является выбор класса кодов (класс блоковых либо непрерывных (сверточных) кодов). Используя материалы разделов 8 и 11, рекомендуется *аргументированно обосновать выбор класса сверточных кодов* для применения в своей работе. Среди алгоритмов декодирования СК по широте практического применения *лидирующее место* занимает алгоритм Витерби. Рекомендуется в работе применить именно алгоритм Витерби. В разделе проекта с обоснованием применения этого алгоритма следует привести сведения о сложности реализации алгоритма. Среди кодов, отобранных по критерию скорости в соответствии с

формулой (5.1), могут оказаться коды с различной длиной кодового ограничения (и, соответственно, с различной сложностью декодера). Помехоустойчивость декодирования СК характеризуется величиной ЭВК. В таблицах кодов не приводятся значения ЭВК при определенном уровне вероятности ошибки декодирования. В то же время, величина асимптотического энергетического выигрыша (АЭВК) является верхней оценкой ЭВК. Поэтому при отборе кодов рекомендуется использовать величины АЭВК, значения которых имеются в таблицах приложения А. Среди отобранных кодов-кандидатов следует применить код, *обеспечивающий максимальный АЭВК и удовлетворяющий требованиям по скорости и слоэ/сно- сти декодера.* Окончательные данные о вероятности ошибки на выходе декодера следует получить на основе расчетов зависимости вероятности ошибки декодирования от отношения сигнал/шум для выбранного кода. В случае невыполнения требований задания рекомендуется *применить код с большей величиной АЭВК.*

Пример расчетов и процедуры оптимизации кода

Исходные данные:

1. Вид передаваемой цифровой информации - ЦТЛФ.

3. Отношение с/ш $h_б$ = 4 дБ.
4. Метод модуляции: ФМ-4.
5. Прием-когерентный.
6. Производительность источника $R_{ИСТ}$ = 64 кбит/с
7. Ширина полосы частот канала F_K = 100 кГц.

8. Допустимая вероятность ошибки бита $p = 10^{-5}$.

9. Допустимая сложность решетки кода W = 150.

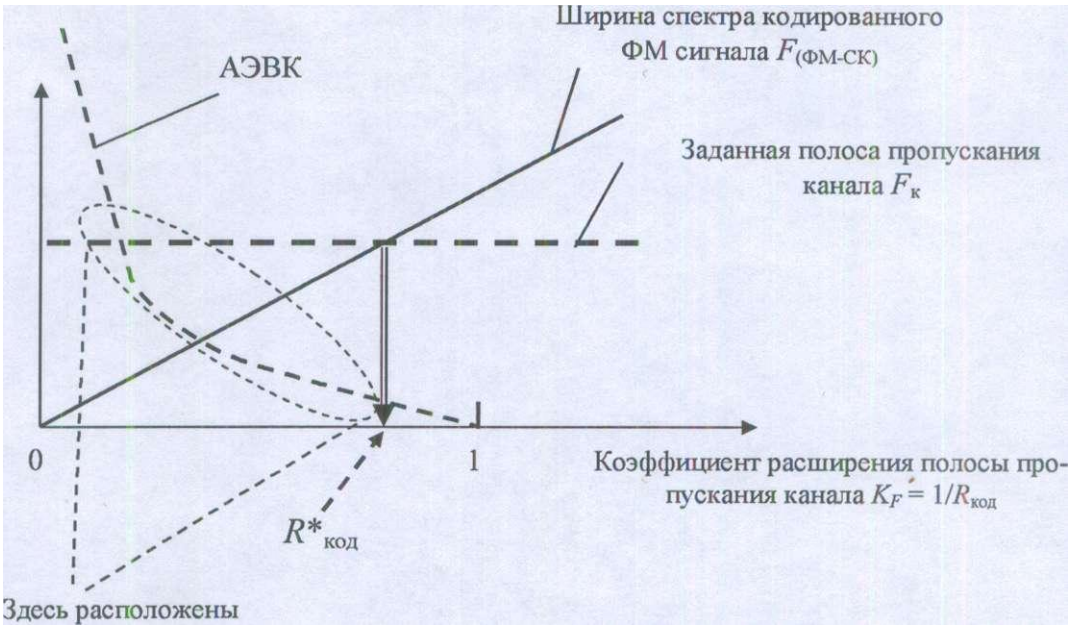


Рис. П1.1. К процедуре оптимизации кода

1. Расчет полосы пропускания канала связи, необходимой для передачи цифровой информации с заданной скоростью методом ФМ-4, производим по формуле $F_{(ФМ-4)} = [R_{ИСТ}(1-\alpha)]/2,$ где α - коэффициент ската спектра. Задаваясь значением $\alpha =$ 0,4, получаем $F_{(ФМ-4)} = [R_{ИСТ}(1-\alpha)]/2$ = [64(1 + 0,4)]/2 = 44,8 кГц.
2. В соответствии с формулой (5.1) определяем предельное значение скорости С К

$$R^*_{КОД} > \frac{F_{ФМ-СК}}{F_К} = \frac{44{,}8}{100} = 0{,}448.$$

3. По таблицам СК отбираем коды, удовлетворяющие требованию по скорости. Данные об этих кодах сведены в таб. П1.1.

Таблица П1.1. Характеристики СК для выбора кода

Скорость кода $R_{КОД}$	Порождающие многочлены	ДКО v	Сложность решетки W	АЭВК дБ
1/4	463,535,733,745	8	512	8,29
1/3	557,663,711	8	512	7,78
1/2	53,75	5	64	6,02
1/2	61,73	5	64	6,02
1/2	71,73	5	64	6,02
1/2	133,171	6	128	6,99
1/2	247,371	7	256	6,99

Из таблицы видно, что для выполнения поставленной задачи могут быть использованы СК со скоростями $R_{КОД} = 1/2,$ которые обеспечивают достаточно большой АЭВК. На аснове данных таблицы выбираем для проекта код с порождающими многочленами (133, 171), который при скорости $R_{КОД} = 0{,}5$ обеспечивает АЭВК = 6,99 дБ. Данные расчета вероятности ошибки приведены в главе 1.

Видно, что применение выбраного кода обеспечивает выполнение задания: при отношении сигнал/шум $h_б^2 = 4$ дБ вероятность ошибки декодирования менее $3 \cdot 10^{-5}$ Сравнение с кривыми помехоустойчивости некодированной ФМ (рис. 11.1) показывает, что при вероятности ошибки $p = 10^{-5}$ этот код обеспечивает ЭВК 5,3 дБ.

Таблица П1.2. Исходные данные для выполнения СР

Номер варианта для выполнения СР должен соответствовать номеру фамилии студента в журнале академической группы							
Номер варианта	Вид перед, информ.	Отношение С/Ш на входе $h_б^2$, *дБ*	Метод модул.	Производит. источника $R_{ИСТ}$, кбит/с	Полоса пропуск, канала $F_К$, кГц	Вер. ошибки бита p	Сложи. декодера W
1	ДК	4,0	ФМ-4	64	80	10^{-6}	150
2	ЦТЛФ	5,0	ФМ-4	16	25	10^{-4}	160
3	ЦЗВ	6,0	ФМ-2	256	800	10^{-5}	170
4	ДК	6,5	ФМ-2	64	200	10^{-6}	180
5	ЦТЛФ	4,0	ФМ-4	16	25	10^{-4}	250
6	ЦЗВ	7,0	ФМ-4	128	200	10^{-5}	350
7	НТВ	5,0	ФМ-2	2400	7000	10^{-8}	560
8	ДК	6,0	ФМ-4	32	50	10^{-6}	200

9	ЦТЛФ	5,0	ФМ-2	24	70	10^{-4}	300
10	ЦЗВ	4,5	ФМ-4	256	400	10^{-5}	250
11	ЦТВ	5,5	ФМ-2	3000	1200	10^{-8}	550
12	ДК	4,0	ФМ-4	48	70	10^{-6}	150
13	ЦТЛФ	5,0	ФМ-4	32	50	10^{-4}	250
14	ЦЗВ	7,0	ФМ-2	256	800	10^{-5}	300
15	ЦТВ	4,0	ФМ-4	4500	1300	10^{-9}	550
16	ДК	7,0	ФМ-4	56	90	10^{-6}	150
17	ЦТЛФ	5,0	ФМ-2	24	70	10^{-4}	160
18	ЦЗВ	4,5	ФМ-4	256	400	10^{-5}	200
19	ЦТВ	5,5	ФМ-4	5000	1400	10^{-9}	550
20	ДК	6,0	ФМ-2	64	200	10^{-6}	150
21	ЦТЛФ	7,5	ФМ-4	256	400	10^{-4}	250
23	ЦЗВ	6,5	ФМ-4	16	50	10^{-5}	150
24	ДК	6,0	ФМ-4	64	150	10^{-6}	150
25	ЦГЛФ	4,5	ФМ-2	16	25	10^{-6}	200
26	ЦТВ	5,0	ФМ-2	6000	16000	10^{-9}	550
27	ЦЗВ	6,0	ФМ-4	384	600	10^{-5}	250
28	ДК	4,5	ФМ-4	64	100	10^{-6}	150
29	ЦГЛФ	5,0	ФМ-2	16	50	10^{-4}	250
30	ЦТВ	5,5	ФМ-2	5500	32000	10^{-9}	560
31	ЦГЛФ	4,5	ФМ-4	64	200	10^{-5}	150
32	ДК	5,0	ФМ-4	64	300	10^{-5}	250

Примеры расчетов для разных вариантов

Вариант №7

Таблица П1.3. Параметры проектируемой ТКС

Номер варианта для выполнения индивидуальной работы должен соответствовать номеру фамилии студента в журнале академической группы							
Номер варианта	Вид перед. Информации	Отношение С/Ш $h_б^2$, дБ	Метод модуляции	Произв. источника $R_{ист}$, кбит/с	Пропускная способность канала $F_к$, кГц	Вер. Ошибки бита	Сложн. декодера
7	ЦТВ	5.0	ФМ-2	2400	7000	10^{-8}	560

Структурная схема проектируемой телекоммуникационной системы

В общем виде обобщенная структурная схема проектируемой ТКС может быть сформирована в виде, представленном на рисунке П1.1.

В передатчике кодер вносит в информационное сообщение избыточность в виде проверочных символов. Закодированные символы поступают на модулятор, который преобразует их в аналоговый сигнал.

В приемнике демодулятор преобразует принятый сигнал в последовательность чисел, представляющих оценку переданных данных – метрики. Метрики поступают в декодер, который исправляет возникающие при передаче ошибки, используя внесенную кодером избыточность [24].

Классификация корректирующих кодов

Обнаружение ошибок в технике связи — действие, направленное на контроль целостности данных при записи/воспроизведении информации или при её передаче по линиям связи. Исправление ошибок (коррекция ошибок) — процедура восстановления информации после чтения её из устройства хранения или канала связи.

Для обнаружения ошибок используют коды обнаружения ошибок, для исправления — корректирующие коды(коды, исправляющие ошибки, коды с коррекцией ошибок, помехоустойчивые коды).

В общем виде классификация корректирующих кодов может быть представлена в следующем виде:

1. Блочные коды:
   - 1.1 Линейные коды общего вида;
   - 1.1.2 Коды Хемминга;
   - 1.2 Линейные циклические коды:
     - 1.2.1 Коды CRC;
     - 1.2.2 Коды БЧХ;
     - 1.2.3 Коды коррекции ошибок Рида — Соломона;
2. Сверточные коды;
3. Каскадные коды.

Стоит отметить, что блочные коды, как правило, хорошо справляются с редкими, но большими пачками ошибок, их эффективность при частых, но небольших ошибках (например, в канале с АБГШ), менее высока.

Вместе с этим, сверточные коды эффективно работают в канале с белым шумом, но плохо справляются с пакетами ошибок. Более того, если декодер ошибается, на его выходе всегда возникает пакет ошибок.

Так как в начальных условиях поставленной задачи не были сформулированы требования к методам кодирования, выбор остановился на сверточных кодах. Однако, при

проектировании телекоммуникационных систем необходимо четко формировать критерии оптимальности разрабатываемой системы.

Классификация методов декодирования сверточных кодов

Классификация методов декодирования сверточных кодов имеет следующий вид:

1. Алгебраические методы декодирования;
2. Вероятностные методы декодирования:
   - 2.1 Алгоритм последовательного декодирования;
   - 2.2 Алгоритм Витерби.

Алгоритм Витерби характеризуется постоянством вычислительной работы, однако сложность декодера Витерби растет, как при переборных алгоритмов, по экспоненциальному закону от длины кодового ограничения сверточного кода.

Так как в данной работе в целях оптимизации проектируемой системы будут использоваться короткие сверточные коды, сложность декодера будет мала, что позволяет использовать алгоритм декодирования Витерби.

Расчет и оптимазация параметров телекоммуникацонной системы

Расчет ширины спектра цифрового сигнала с заданным видом модуляции:

$$F_{ФМ-2} = \frac{R_{ист} \cdot (1+\alpha)}{2} = \frac{2400 \cdot 10^3 \cdot (1+0.4)}{2} = 1.68 МГц .$$

Расчет ширины спектра кодированного цифрового сигнала с заданным видом модуляции в зависимости от скорости кода:

$$R_{код*} = \frac{F_{ФМ-2}}{F_к} = \frac{1680 \cdot 10^3}{7000 \cdot 10^3} = 0.24 .$$

Следовательно скорость кода должна быть не менее 0.24. Полученный результат позволяет сформировать список подходящих сверточных кодов в виде представленном в таблице П1.4.

Татлица П1.4. Перечень подходящих сверточных кодов

Скорость кода $R_{код}$	Порождающие многочлены	ДКО ν	Сложность решетки W	АЭВК, дБ
1/4	463,535,733,745	8	512	8,29
1/3	557,663,711	8	512	7,78
1/2	53,75	5	64	6,02
1/2	61,73	5	64	6,02
1/2	71,73	6	64	6,02
1/2	133,171	6	128	6,99
1/2	247,371	7	256	6,99

В силу того, критерием оптимальности проектируемой ГКС является простота используемого кодера/декодера, был выбран код /133,171/ с длиной кодового ограничения 7, который при скорости кода 0.5 обеспечивает АЭВК = 6.99 дБ.

Изложенное позволяет рассчитать ширину спектра кодированного цифрового сигнала:

$$F_{ФМ-2+СК} = \frac{F_{ФМ-2}}{R_{код}} = \frac{1680 \cdot 10^3}{0.5} = 3.36 МГц$$

Рисунок 6.2 позволяет сделать вывод о том, что применение выбранного кода обеспечивает выполнение поставленной задачи, так как при отношении С/Ш = 5 дБ вероятность ошибки декодирования меньше 10^{-5}.

Сравнение с кривыми помехоустойчивости некодированной ФМ показывает, что при вероятности ошибки 10^{-8} этот код обеспечивает значение ЭВК более 10 дБ.

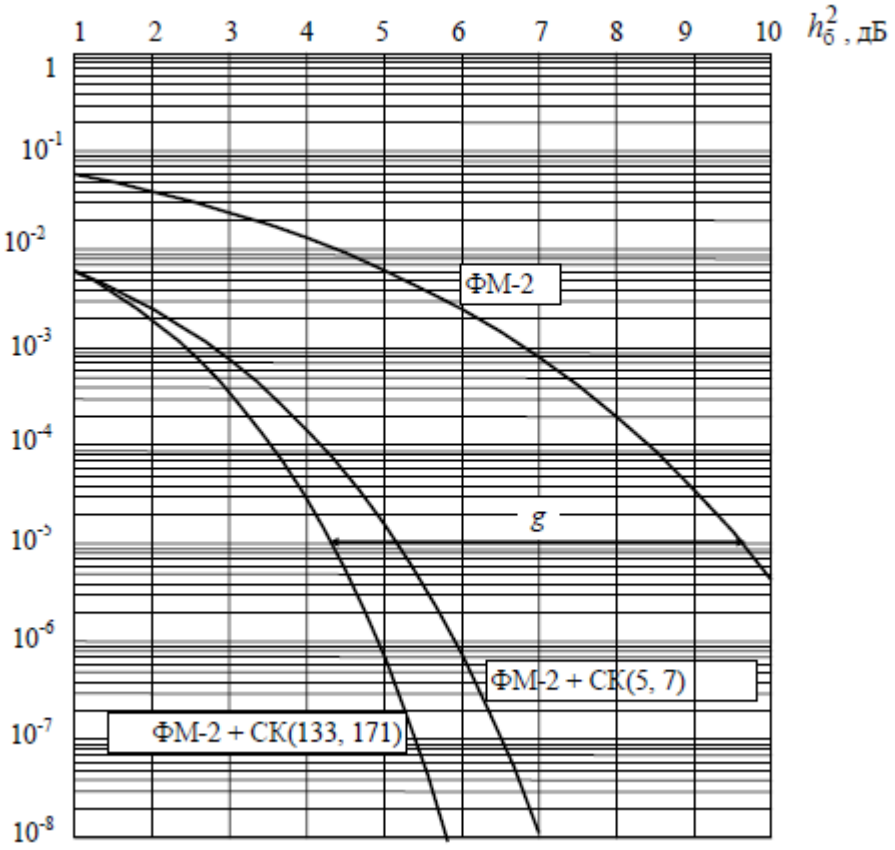


Рис. П1.2. Помехоустойчивость декодирования сверточных кодов

Проверочный расчет вероятности ошибки на выходе декодера:

$$Q = 0.65 \cdot \exp(-0.44 \cdot (z + 0.75)^2) = 0.65 \cdot$$
$$\cdot \exp(-0.44 \cdot (5.01 + 0.75)^2) = 2.972 \cdot 10^{-7}$$

$$p_o = w_{df} \cdot Q \cdot (\sqrt{2 \cdot d_f \cdot R_{код} \cdot h_б}) = 36 \cdot 2.972 \cdot 10^{-7} \cdot (\sqrt{2 \cdot 10 \cdot 0.5 \cdot 5}) = 7.565 \cdot 10^{-5}$$

Расчет показал, что реальное значение вероятности ошибки кодера меньше теоретического значения, следовательно, условия задачи были выполнены.

Разработка кодера и декодера сверточного кода 133,171

В предыдущем разделе был описан выбор сверточного кодера /133,171/. Функциональная и структура схема кодера/декодера может быть представлена в следующем виде:

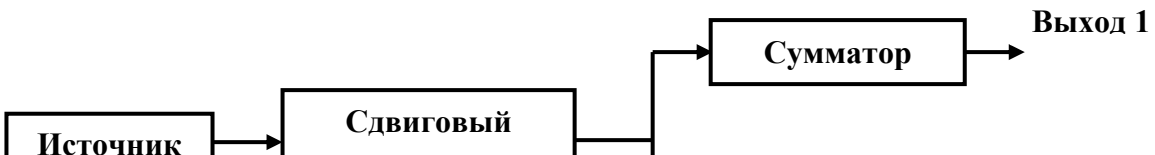


Рис. П1.3. Структурная схема сверточного кодера

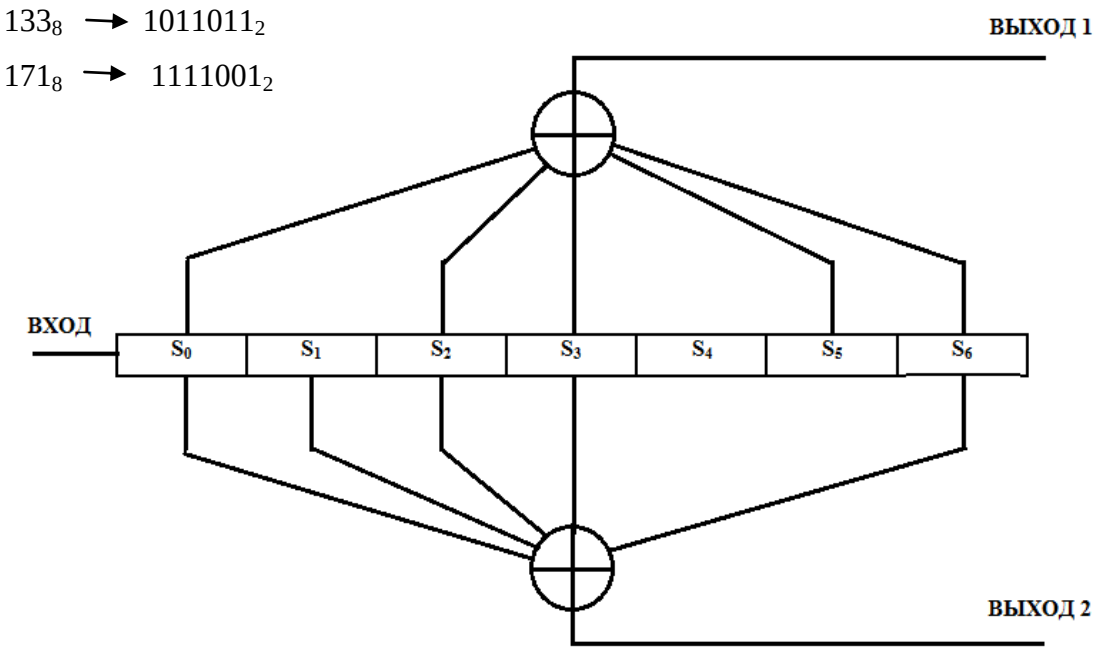


Рис. П1.4. Функциональная схема сверточного кодера 133,171

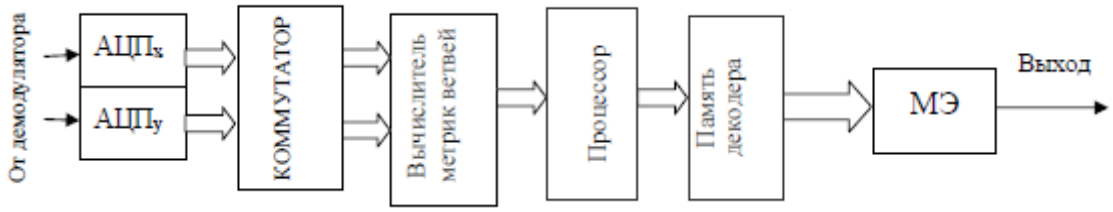


Рис. П1.5. Структурная схема декодера Витерби

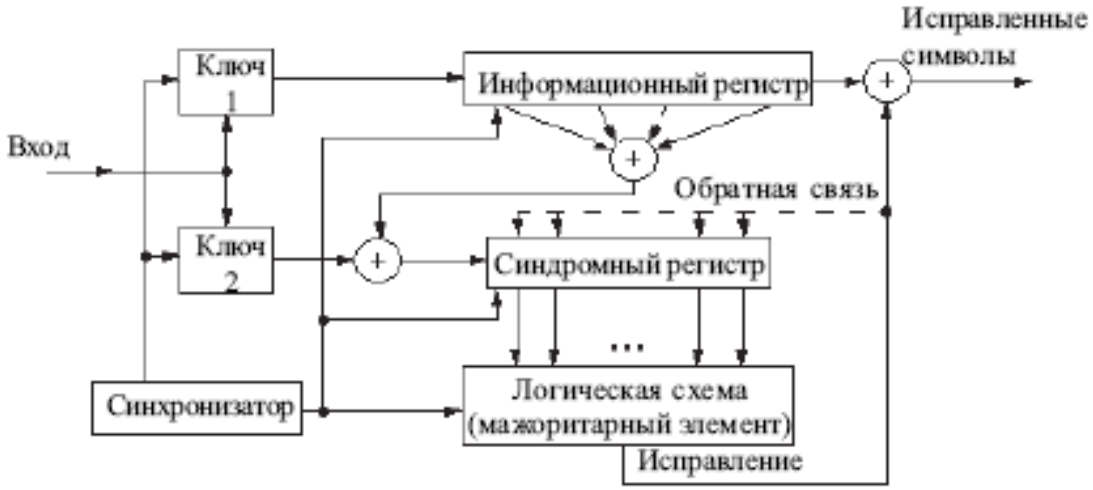


Рис. П1.6. Функциональная схема декодера Витерби

В результате выполнения данной индивидуальной работы было сделано следующее:

1. Спроектирована телекоммуникационная система с использованием сверточного кодера;

2. Рассчитаны и оптимизированы параметры сверточного кода используемого в ТКС в целях повышения ее эффективности и помехоустойчивости;

3. Предложены структурные и функциональные схемы кодера и кодера, используемых в разработанной ТКС.

Варианты № 16, 3, 8

Для решения поставленной задачи предложены общие параметры проектируемой ТКС, которые представленные в таблице П1.5.

Таблица П1.5. Параметры проектируемой ТКС

Номер варианта	Вид перед. инф-ии	Отношение С/Ш $h_б^2$, дБ	Метод модуляции	Произв. источника $R_{ист}$, кбит/с	Пропускная способность канала $F_к$, кГц	Вер. ошибки бита p	Сложн. декодера W
16	ДК	7,0	ФМ-4	56	90	10^{-6}	150
3	ЦЗВ	6,0	ФМ-2	256	800	10^{-5}	170
8	ДК	6,0	ФМ-4	32	50	10^{-6}	200

Структурная схема проектируемой телекоммуникационной системы

Структурная схема проектируемой телекоммуникационной системы представлена на рисунке П1.2.

Источник сообщения генерирует бинарную последовательность с определенной скоростью $R_{ист}$. Курсивом отмечены блоки, которые кодируют и декодируют информацию с применением помехоустойчивых кодов (вводится избыточность при кодировании, например код Хемминга, БЧХ, сверточный код). Что касается источника, то он кодируется и декодируется с помощью таких алгоритмов как, Хаффмана, Шеннона-Фано или Лемпела-Зива. В данных алгоритмах не вводится избыточность. Помимо кодирования система связи содержит в себе квадратурную модуляцию/демодуляцию. Где на выходе модулятора мы получаем сначала комплексные числа (квадратурные и синфазные составляющие), которые в свою очередь садятся на несущие, сдвинутые на 90 градусов и в конечном итоге суммируются. Демодуляция представляет собой обратный процесс. Варианты работы содержит в себе модуляцию ФМ-2 или BPSK, которая имеет только два синфазных значения постоянной амплитуды и фазы 0 и 180 градусов и ФМ-4 или QPSK, которая имеет четыре значения постоянной амплитуды и фазы. И, конечно же, любая система передачи не обходится без воздействия на нее шумов, в канале беспроводной сети (канал связи).

4 Классификация корректирующих кодов

Обнаружение ошибок в технике связи — действие, направленное на контроль целостности данных при записи/воспроизведении информации или при её передаче по линиям связи. Исправление ошибок (коррекция ошибок) — процедура восстановления информации после чтения её из устройства хранения или канала связи.

Для обнаружения ошибок используют коды обнаружения ошибок, для исправления — корректирующие коды(коды, исправляющие ошибки, коды с коррекцией ошибок, помехоустойчивые коды).

Преимущества и недостатки блоковых кодов:

Блоковые коды, как правило, хорошо справляются с редкими, но большими пачками ошибок, их эффективность при частых, но небольших ошибках (например, в канале с АБГШ), менее высока.

Преимущества и недостатки свёрточных кодов:

Свёрточные коды эффективно работают в канале с белым шумом, но плохо справляются с пакетами ошибок. Более того, если декодер ошибается, на его выходе всегда возникает пакет ошибок. Выбор в индивидуальной работе сверточных кодов обосновывается тем, что свёрточное кодирование - очень простая операция. Кодирование свёрточным кодом производится с помощью регистра сдвига, отводы от которого суммируются по модулю два. Таких сумм может быть две (чаще всего) или больше.

Классификация корректирующих кодов по структуре представлена на рисунке в.

Классификация методов декодирования сверточных кодов

Классификация методов декодирования сверточных кодов имеет следующий вид:

3. Алгебраические методы декодирования;
4. Вероятностные методы декодирования:
   - 4.1 Алгоритм последовательного декодирования;
   - 4.2 Алгоритм Витерби.

Задача декодирования сверточного кода заключается в выборе пути (в этом и состоит отличие декодирования сверточных кодов) вдоль решетки наиболее похожего на принятую последовательность. Каждый путь вдоль решетчатой диаграммы складывается из ветвей соединяющих узлы. Каждой ветви решетки соответствует кодовое слово из двух бит. Каждую ветвь на каждом периоде можно пометить расстоянием Хемминга между полученным кодовым словом и кодовым словом, соответствующим ветви. Складывая расстояния Хемминга ветвей, составляющих путь, получим метрику соответствующего пути. Данная метрика будет характеризовать степень подобия каждого пути принятой последовательности. Чем меньше метрика, тем более похожи путь и принятая последовательность. Таким образом, результатом декодирования будет информационная последовательность, соответствующая пути с минимальной метрикой. Если в одно и тоже состояние входят два пути выбирается тот, который имеет лучшую метрику. Такой путь называется выжившим. Отбор выживших путей проводится для каждого состояния. Это не иначе как алгоритм декодирования Витерби и он наиболее эффективный.

Расчет ширины спектра цифрового сигнала с заданным видом модуляции

Вариант	Расчеты
16	$F_{ФМ4} = \frac{R_{ист}*(1+\alpha)}{2} = \frac{56*(1+0,4)}{2} = 39,2$ кГц
3	$F_{ФМ4} = \frac{R_{ист}*(1+\alpha)}{2} = \frac{256*(1+0,4)}{2} = 179,2$ кГц
8	$F_{ФМ4} = \frac{R_{ист}*(1+\alpha)}{2} = \frac{32*(1+0,4)}{2} = 22,4$ кГц

Определение допустимой скорости кода из условия непревышения полосой частот кодированного сигнала полосы пропускания канала

Вариант	Расчеты
16	$R_{код*} = \frac{F_{ФМ4}}{F_K} = 0.436$
3	$R_{код*} = \frac{F_{ФМ4}}{F_K} = 0.224$

8	$R_{\text{код}*} = \frac{F_{\text{ФМ4}}}{F_K} = 0{,}448$

Определение кода

Полученный результат позволяет сформировать список подходящих сверточных кодов в виде, представленном в таблице П1.6.

Таблица П1.6. Характеристики СК для выбора кода

Скорость кода $R_{\text{код}}$	Порождающие многочлены	ДКО ν	Сложность решетки W	АЭВК, дБ
1/4	463,535,733,745	8	512	8,29
1/3	557,663,711	8	512	7,78
1/2	53,75	5	64	6,02
1/2	61,73	5	64	6,02
1/2	71,73	5	64	6,02
1/2	133,171	6	128	6,99
1/2	247,371	7	256	6,99

Вариант	Условия
16	СК со скоростями 1/2 и сложностью решетки W не более 150
3	Все СК со сложностью решетки W не более 170
8	СК со скоростями ½ и сложностью решетки W не более 200

Произведен выбор СК из перечня, обеспечивающего заданную вероятность ошибки бита и удовлетворяющего требованию ограничения по сложности декодера.

Вариант	Выбранный СК
16	Код с порождающими многочленами (133, 171), который при скорости 1/2 обеспечивает АЭВК = 6,99 дБ
3	Код с порождающими многочленами (133, 171), который при скорости 1/2 обеспечивает АЭВК = 6,99 дБ
8	Код с порождающими многочленами (133, 171), который при скорости 1/2 обеспечивает АЭВК = 6,99 дБ

Расчет ширины спектра кодированного цифрового сигнала с заданным видом модуляции в зависимости от скорости кода

Вариант	Расчеты
16	$F_{ФМ4+СК} = \frac{F_{FM4}}{R_{код}} = \frac{39{,}2}{0{,}5} = 78{,}4$ кГц
3	$F_{FM2+СК} = \frac{F_{FM2}}{R_{код}} = \frac{179{,}2}{0{,}5} = 358{,}4$ кГц

8	$F_{ФМ4+СК} = \frac{F_{FM4}}{R_{код}} = \frac{22,4}{0,5} = 44,8$ кГц

Рисунок П1.7 позволяет сделать вывод о том, что применение выбранного кода обеспечивает выполнение поставленной задачи, так как

Вариант	Отношение С/Ш $h_б^2$, дБ	Вероятность ошибки декодирования меньше
16	7,0	10^{-6}
3	6,0	10^{-5}
8	6,0	10^{-6}

Сравнение с кривыми помехоустойчивости некодированной ФМ показывает, что

Вариант	Вероятность ошибки	АЭВК, дБ
16	10^{-6}	более 10
3	10^{-5}	9,4
8	10^{-6}	более 10

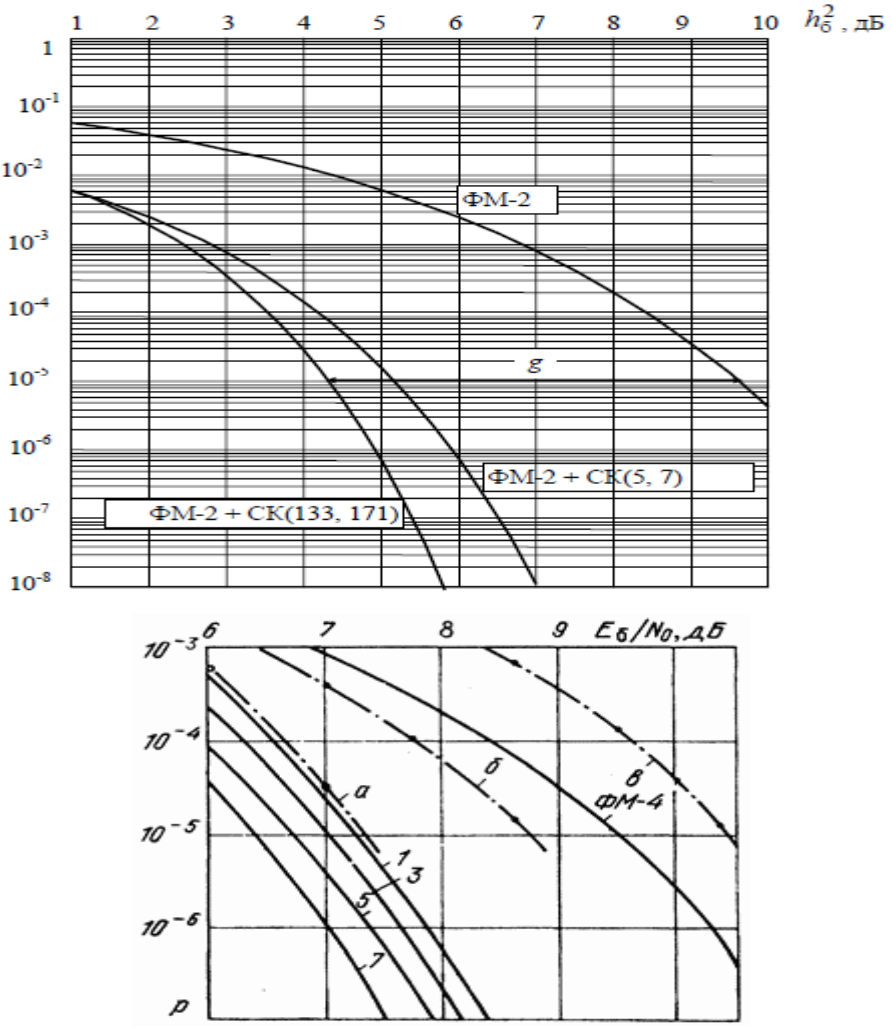


Рис. П1.7. Помехоустойчивость декодирования сверточных кодов

Проверочный расчет зависимости вероятности ошибки на выходе декодера

В результате получим (примерно для заданной вероятности ошибки бита):

Вариант	Расчеты
16	$Q = \frac{1}{x * \sqrt{2\pi}} * \exp\left(-\frac{x^2}{2}\right) = \frac{1}{5{,}01 * \sqrt{2\pi}} * \exp\left(-\frac{5{,}01^2}{2}\right) = 4{,}45 * 10^{-5}$ $p_d = w_{df} \cdot Q \cdot \sqrt{2 \cdot d_f \cdot R_{kod} \cdot h_b} = 36 \cdot 4.45 \cdot 10^{-5} \cdot \sqrt{2 \cdot 10 \cdot 0.5 \cdot 7} = 4.2 \cdot 10^{-3}$
3	$Q = \frac{1}{x * \sqrt{2\pi}} * \exp\left(-\frac{x^2}{2}\right) = \frac{1}{4 * \sqrt{2\pi}} * \exp\left(-\frac{4^2}{2}\right) = 3{,}3 * 10^{-5}$ $p_d = w_{df} \cdot Q \cdot \sqrt{2 \cdot d_f \cdot R_{kod} \cdot h_b} = 36 \cdot 3.3 \cdot 10^{-5} \cdot \sqrt{2 \cdot 10 \cdot 0.5 \cdot 6} = 9.2 \cdot 10^{-3}$
8	$Q = \frac{1}{x * \sqrt{2\pi}} * \exp\left(-\frac{x^2}{2}\right) = \frac{1}{5{,}01 * \sqrt{2\pi}} * \exp\left(-\frac{5{,}01^2}{2}\right) = 4{,}45 * 10^{-5}$ $p_d = w_{df} \cdot Q \cdot \sqrt{2 \cdot d_f \cdot R_{kod} \cdot h_b} = 36 \cdot 4.45 \cdot 10^{-5} \cdot \sqrt{2 \cdot 10 \cdot 0.5 \cdot 6} = 4.2 \cdot 10^{-3}$

Расчет показал, что реальное значение вероятности ошибки кодера меньше теоретического значения, следовательно, условия задачи были выполнены.

Разработка кодера и декодера СК 133, 171

В предыдущем разделе был описан выбор сверточного кодера (133,171).

$133_8 = 1011011_2; 171_8 = 1111001_2$

Функциональная и структура схема кодера/декодера может быть представлена в следующем виде:

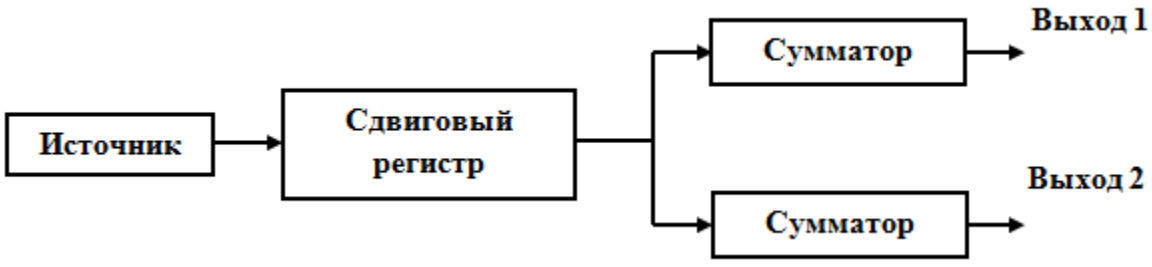


Рис. П1.8. Структурная схема сверточного кодера

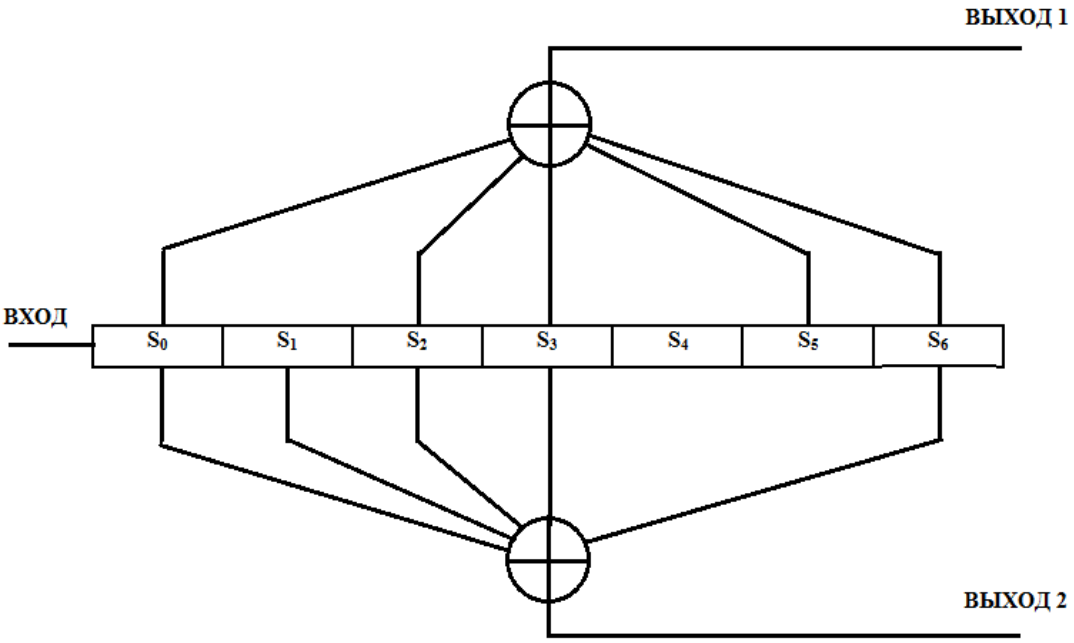


Рис. П1.9. Функциональная схема сверточного кодера 133,171

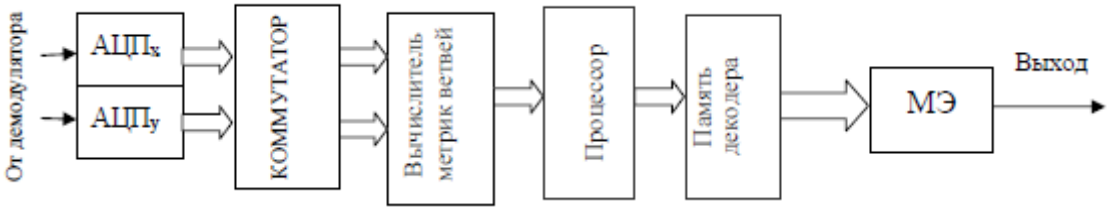


Рис. П1.10. Структурная схема декодера Витерби

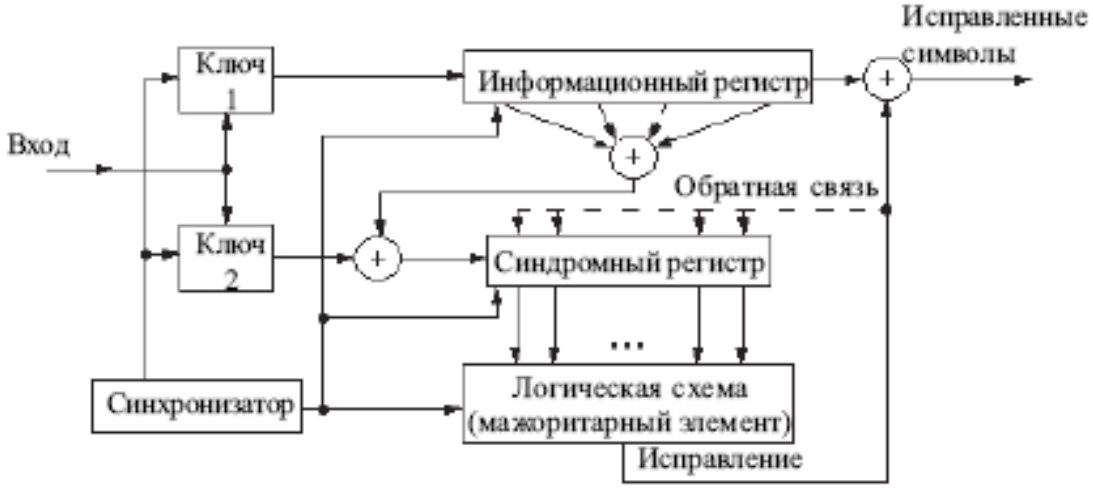


Рис. 5.11. Функциональная схема декодера Витерби

кодера со скоростью 1/2.

В результате выполнения данного индивидуального задания было выполнено следующее:

- Спроектирована телекоммуникационная система с использованием сверточного кодера;
- Рассчитаны и оптимизированы параметры сверточного кода используемого в ТКС в целях повышения ее эффективности и помехоустойчивости при различных начальных заданных условиях (ширина спектра, скорость кода, битовая вероятность ошибки в зависимости от заданного значения отношения сигнал/шум);
- Предложены структурные и функциональные схемы кодера и кодера, используемых в разработанной ТКС.

ПРИЛОЖЕНИЕ 2.
ЗАДАНИЯ НА САМОСТОЯТЕЛЬНУЮ РАБОТУ

П2.1. Задания на криптоанализ классических шифров[27]

Шифр столбцовой перестановки

При решении заданий на криптоанализ шифров перестановки необходимо восстановить начальный порядок следования букв текста. Для этого используется анализ совместимости символов, в чем может помочь таблица сочетаемости.

Таблица П2.1. Сочетаемость букв русского языка

Г	С	Слева		Справа	Г	С
3	97	л, д, к, т, в, р, н	**А**	л, н, с, т, р, в, к, м	12	88
80	20	я, е, у, и, а, о	**Б**	о, ы, е, а, р, у	81	19
68	32	я, т, а, е, и, о	**В**	о, а, и, ы, с, н, л, р	60	40
78	22	р, у, а, и, е, о	**Г**	о, а, р, л, и, в	69	31
72	28	р, я, у, а, и, е, о	**Д**	е, а, и, о, н, у, р, в	68	32
19	81	м, и, л, д, т, р, н	**Е**	н, т, р, с, л, в, м, и	12	88
83	17	р, е, и, а, у, о	**Ж**	е, и, д, а, н	71	29
89	11	о, е, а, и	**З**	а, н, в, о, м, д	51	49
27	73	р, т, м, и,	**И**	с, н, в, и, е,	25	75

		о, л, н		м, к, з		
55	45	ь, в, е, о, а, и, с	**К**	о, а, и, р, у, т, л, е	73	27
77	23	г, в, ы, и, е, о, а	**Л**	и, е, о, а, ь, я, ю, у	75	25
80	20	я, ы, а, и, е, о	**М**	и, е, о, у, а, н, п, ы	73	27
55	45	д, ь, н, о, а, и, е	**Н**	о, а, и, е, ы, н, у	80	20
11	89	р, п, к, в, т, н	**О**	в, с, т, р, и, д, н, м	15	85
65	35	в, с, у, а, и, е, о	**П**	о, р, е, а, у, и, л	68	32
55	45	и, к, т, а, п, о, е	**Р**	а, е, о, и, у, я ,ы, н	80	20
69	31	с, т, в, а, е, и, о	**С**	т, к, о, я, е, ь, с, н	32	68
57	43	ч, у, и, а, е, о, с	**Т**	о, а, е, и, ь, в, р, с	63	37
15	85	п, т, к, д, н, м, р	**У**	т, п, с, д, н, ю, ж	16	84
70	30	н, а, е, о, и	**Ф**	и, е, о, а, е, о, а	81	19
90	10	у, е, о, а, ы, и	**Х**	о, и, с, н, в, п, р	43	57
69	31	е, ю, н, а, и	**Ц**	и, е, а, ы	93	7
82	18	е, а, у, и, о	**Ч**	е, и, т, н	66	34
67	33	ь, у, ы, е, о, а, и, в	**Ш**	е, и, н, а, о, л	68	32
84	16	е, б, а, я, ю	**Щ**	е, и, а	97	3
0	100	м, р, т, с, б, в, н	**Ы**	л, х, е, м, и, в, с, н	56	44

0	100	н, с, т, л	**Ь**	н, к, в, п, с, е, о, и	24	76
14	86	с, ы, м, л, д, т, р, н	**Э**	н, т, р, с, к	0	100
58	42	ь, о, а, и, л, у	**Ю**	д, т, щ, ц, н, п	11	89
43	57	о, н, р, л, а, и, с	**Я**	в, с, т, п, д, к, м, л	16	84

Таблица П2.2. Сочетаемость букв английского языка

Г	С	Слева		Справа	Г	С
19	81	l,c,d,m,n,s,w,t,r,e,h	**A**	n,t,s,r,l,d,c,m	6	94
55	45	y,b,n,t,u,d,o,s,a,e	**B**	e,l,u,o,a,y,b,r	70	30
61	39	u,o,s,n,a,i,l,e	**C**	h,o,e,a,i,t,r,l,k	59	41
52	48	r,i,l,a,n,e	**D**	e,i,t,a,o,u	54	46
8	92	c,b,e,m,v,d,s,l,n,t,r,h	**E**	r,d,s,n,a,t,m,e,c,o	21	79
69	31	s,n,f,d,a,i,e,o	**F**	t,o,e,i,a,r,f,u	52	48
36	64	o,d,u,r,i,e,a,n	**G**	e.h.o.r.a.t.f.w.i.s	42	58
7	93	g,e,w,s,c,t	**H**	e,a,i,o	90	10
13	87	f,m,w,e,n,l,d,s,r,h,t	**I**	n,t,s,o,c,r,e,m,a,l	17	83
28	72	y,w,t,s,n,e,c,b,a,c	**J**	u,o,a,e,m,w	88	12
53	47	y,u,i,n,a,r,o,c	**K**	e,i,n,a,t,s	68	32
52	48	m,p,t,i,b,u,o,e,l,a	**L**	e,i,y,o,a,d,u	65	35
69	31	s,d,m,r,i,a,o,e	**M**	e,a,o,i,p,m	71	29
89	11	u,e,o,a,i	**N**	d,t,g,e,a,s,o,i,c	32	68
21	79	o,d,l,p,h,n,e,c,f,s,i,r,t	**O**	n,f,r,u,t,m,l,s,w,o	18	82
47	53	r,l,t,n,i,p,m,a,o,u,e,s	**P**	o,e,a,r,l,u,p,t,i,s	59	41
20	80	o,n,l,e,d,r,s	**Q**	u	100	0
70	30	p,i,u,t,a,o,e	**R**	e,o,a,t,i,s,y	61	39
48	52	d,t,o,u,r,n,s,i,a,e	**S**	t,e,o,i,s,a,h,p,u	41	59
43	57	u,o,d,t,f,e,i,n,s.a	**T**	h,i,o,e,a,t,r	38	62
35	65	p,f,t,l,b,d,s,o	**И**	n,s,t,r,l,p,b,c	8	92
88	12	r,u,o,a,i,e	**V**	e,i,o,a	99	1

48	52	g,d,y,n,s,t,o,e	**W**	a,h,i,e,o,n	80	20
95	5	u,n,i,e	**X**	p,t,i,a,u,c,k,o	38	62
24	76	b,n,a,t,e,r,l	**Y**	a,o,s,t,w,h,i,e,d,m	38	62
88	12	o,n,a,i	**Z**	e,i,w	86	14

При анализе сочетаемости букв друг с другом следует иметь в виду зависимость появления букв в открытом тексте от значительного числа предшествующих букв. Для анализа этих закономерностей используют понятие условной вероятности.

Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А.А.Марковым (1856 — 1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная-гласная (*г,г*), гласная-согласная (*г,с*), согласная-гласная (*с,г*), согласная-согласная (*с,с*) в русском тексте длиной в 10^5 знаков. Результаты подсчета отражены в следующей таблице:

Таблица П2.12. Чередование гласных и согласных

	Г	С	Всего
Г	6588	38310	44898
С	38296	16806	55102

Пример решения:

Дан шифр-текст: СВПООЗЛУЙЬСТЬ_ЕДПСОКОКАЙЗО

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5x5. Известно, что шифрование производилось по столбцам, следовательно, расшифрование следует проводить, меняя порядок столбцов.

С	В	П	О	О
З	Л	У	Й	Ь
С	Т	Ь	_	Е
Д	П	С	О	К
К	А	Й	З	О

Необходимо произвести анализ совместимости символов (Таблица сочетаемости букв русского и английского алфавита, а также таблицы частот биграмм представлена выше). В

первом и третьем столбце сочетание СП является крайне маловероятным для русского языка, следовательно, такая последовательность столбцов быть не может. Рассмотрим другие запрещенные и маловероятные сочетания букв: ВП (2,3 столбцы), ПС (3,1 столбцы), ПВ (3,2 столбцы). Перебрав их все, получаем наиболее вероятные сочетания биграмм по столбцам:

В	О	С	П	О
Л	Ь	З	У	Й
Т	Е	С	Ь	_
П	О	Д	С	К
А	З	К	О	Й

Получаем осмысленный текст: ВОСПОЛЬЗУЙТЕСЬ_ПОДСКАЗКОЙ

Задание: Расшифровать фразу, зашифрованную столбцовой перестановкой.

1. ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО
2. ДСЛИЕЗТЕА_Ь_ЛЬЮВМИ_ _АОЧХК
3. НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ
4. ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ
5. СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ
6. _ОНКА_БНЫЕЦВЛЕ_К_ТГОАНЕИР
7. НЗМАЕЕАА_Г_НОТВОССОТЬЯАЛС
8. РППОЕААДТВЛ_ЕБЬЛНЫЕ_ПА_ВР
9. ОПЗДЕП_ИХРДОТ_И_ВРИТЧ_САА
10. ВКЫОСИРЙУ_ОЬВНЕ_СОАПНИОТС
11. ПКТИРАОЛНАОИЧ_З_ЕСЬНЕЛНЖО
12. ИПКСОЕ_ТСМНАЧИ_ОЕН_ГДЕЛА_
13. АМВИННЬТЛЕАНЕ_ЙОВ_ОПХАРТО
14. АРЫКЗЫ_КЙТНЛ_ААЫ_ОЛБКЫТРТ
15. _ПАРИИВИАРЗ_БРА_ИСТЬЛТОЕК
16. П_ЛНАЭУВКАА_ЦИИВР_ОКЧЕДРО
17. ЖВНОАН_АТЗОЬСН_ЫО_ФВИИКИЗ
18. ОТВГОСЕЬЬТАДВ_С_ЬЗАТТЕЫАЧ
19. ЯАМРИТ_ДЖЕХ_СВЕД_ТСУВЕТНО
20. УЬБДТ_ОЕГТВ_ОЫКЭА_ВКАИУЦИ
21. ЛТБЕЧЛЖЫЕ_ _ОАПТЖРДУ_ЛМНОА
22. ИТПРКРФАГО_АВЯИА_ЯНЖУАКАН

23. ПКЕЕРРПО_ЙУСТ_ИТПСУТЛЯЕИН
24. ИЬЖЗНСД_ТДН_ЕТ_НУВЕУРЫГОЫ
25. ЕОУРВА_НЬРИАДИЦЕПИ_РНШВЫЕ

Шифр двойной перестановки

Пример решения:

Дан шифр-текст: ЫОЕЧТТОУ_СНСОРЧТРНАИДЬН_Е

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. известно, что шифрование производилось сначала по столбцам, а затем по строкам, следовательно, расшифрование следует проводить тем же способом.

Ы	О	Е	Ч	Т
Т	О	У	_	С
Н	С	О	Р	Ч
Т	Р	Н	А	И
Д	Ь	Н	_	Е

Производим анализ совместимости символов. Если в примере столбцовой перестановки можно было легко подобрать нужную комбинацию путем перебора, то здесь лучше воспользоваться таблицей частот букв русского языка (см. приложение). Для оптимизации скорости выполнения задания можно проверить все комбинации букв только в первой строке. Получаем ОЕ-15, ОЧ-12, ЕТ-33, ТЕ-31, ЧО-х, ЕО-7, ЧЫ-х, ОЫ-х, ТЫ-11, ТЧ-1, ЧЕ-23 (где х-запрещенная комбинация).

Из полученных результатов можно предположить следующую комбинацию замены столбцов **2 4 3 5 1:**

О	Ч	Е	Т	Ы
О	_	У	С	Т
С	Р	О	Ч	Н
Р	А	Н	И	Т
Ь	_	Н	Е	Д

Теперь необходимо переставить строки в нужном порядке. **3 2 4 5 1:**

С	Р	О	Ч	Н
О	_	У	С	Т
Р	А	Н	И	Т
Ь	_	Н	Е	Д
О	Ч	Е	Т	Ы

Получаем осмысленный текст: СРОЧНО_УСТРАНИТЬ_НЕДОЧЕТЫ

Задание: Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки)

1. СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН
2. МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ
3. АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_
4. ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН
5. ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО
6. АРАВНРСВЕЕОАВ_ЗАНЯА_КМРЕИ
7. А_ЛТАВЙООЛСО_ТВ_ШЕЕНЕСТ_Ь
8. ФИ_ЗИММУЫНУУБК_Е_ДЬШЫИВЧУ
9. ВР_ЕСДЕИ_ТПХРОИ_ЗБУАДНУА_
10. ЦТААЙПЕЕ_ТБГУРРСВЬЕ_ОРЗВВ
11. АВАРНСЧАА_НЕДВЕДЕРПЕОЙ_ИС
12. ДОПК_СОПАЛЕЧНЛ_ГИНЙОИЖЕ_Т
13. ЛУАЗИЯНСА_ДТДЕАИ_ШРФЕОНГ_
14. С_ОЯНВ_СЬСЛААВРЧЕАРТОГДЕС
15. ЗШАФИПРАЛОЕНЖ_ОЬН_ДАРВОНА
16. КЭЕ_ТДУМБ_ЬСЗЕДНЕЗМАОР_ТУ
17. _ЕАЛЯРАНВЯАЧДА_ЕРПЕСАНВ_Ч
18. _И_ЕНТРЗИ_ОКЕВНОДЛЕША_ИМП
19. РОБДОЕВПС_МСХЬА_ _ИВПСНИОТ
20. ЕСДНОГТЕАНН_НЕОВМР_ЕУНПТЕ
21. _ЙЕСТОВО_НИИНЛАЕТИЖДСОПВ_
22. НДИАЕОЫЛППНЕ_ _НВЕАНГТ_ИЗЛА
23. П_БИРДЛЬНЕВ_ОП_ОПЗДЕВЫГЕА
24. МДООИТЕЬ_СМТ_НАДТЕСУБЕХНО
25. АИНАЛЖНОЛЕШФ_ЗИ_УАРОЬСНЕ_

Шифр простой замены

Криптоанализ шифра простой замены основан на использовании статистических закономерностей языка. Так, например, известно, что в русском языке частоты букв распределены следующим образом:

Таблица 1.13. Частоты букв русского языка
(в 32-буквенном алфавите со знаком пробела)

- 0,175	О 0,090	Е,Ё 0,072	А 0,062
И 0,062	Т 0,053	Н 0,053	С 0,045
Р 0,040	В 0,038	Л 0,035	К 0,028
М 0,026	Д 0,025	П 0,023	У 0,021
Я 0,018	Ы 0,016	З 0,016	Ь,Ъ 0,014
Б 0,014	Г 0,013	Ч 0,012	Й 0,010
Х 0,009	Ж 0,007	Ю 0,006	Ш 0,006
Ц 0,004	Щ 0,003	Э 0,003	Ф 0,002

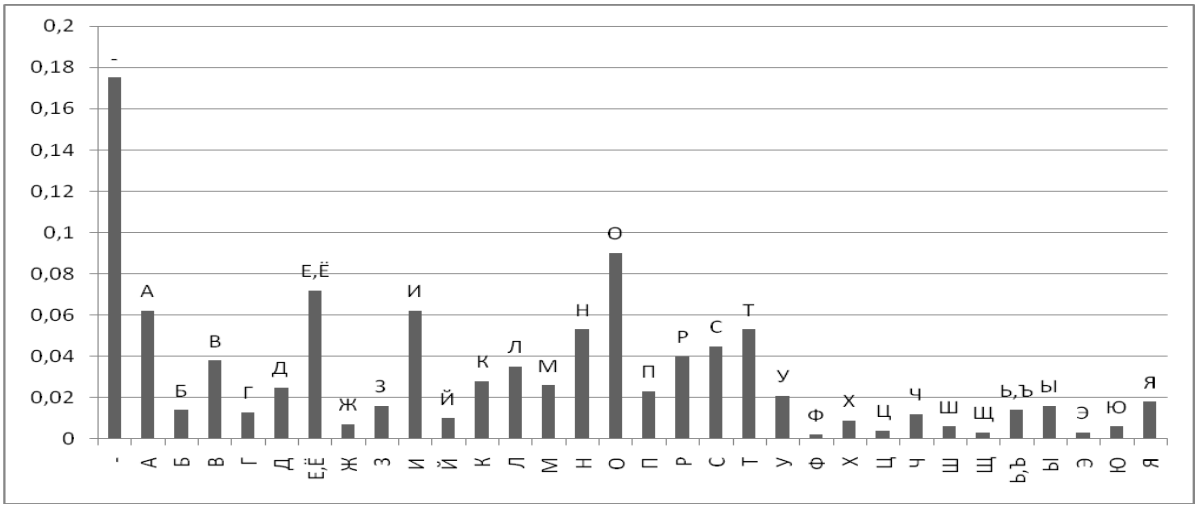


Рис. 1.28. Диаграмма частот букв русского языка

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы k-грамм при k>2, однако для учебных целей вполне достаточно ограничиться биграммами. Неравновероятность k -грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы:

	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П
А	2	12	35	8	14	7	6	15	7	7	19	27	19	45	3	11
Б	5					9	1		6			6		2	21	
В	35	1	5	3	3	32		2	17		7	10	3	9	58	6
Г	7				3	3			5		1	5		1	50	
Д	25		3	1	1	29	1	1	13		1	5	1	13	22	3
Е	2	9	18	11	27	7	5	10	6	15	13	35	24	63	7	16
Ж	5	1			6	12			5					6		
З	35	1	7	1	5	3			4		2	1	2	9	9	1
И	4	6	22	5	10	21	2	23	19	11	19	21	20	32	8	13
И	1	1	4	1	3		1	2	4		5	1	2	7	9	7
К	24	1	4	1		4	1	1	26		1	4	1	2	66	2
Л	25	1	1	1	1	33	2	1	36		1	2	1	8	30	2
М	18	2	4	1	1	21	1	2	23		3	1	3	7	19	5
Н	54	1	2	3	3	34			58		3		1	24	67	2
О	1	28	84	32	47	15	7	18	12	29	19	41	38	30	9	18
П	7					15			4			9		1	46	

СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО,

СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА

Полезной является информация о сочетаемости букв, то есть о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм.

Имеется в виду таблица, в которой слева и справа от каждой буквы расположены наиболее предпочтительные "соседи" (в порядке убывания частоты соответствующих биграмм). В таких таблицах обычно указывается также доля гласных и согласных букв (в процентах), предшествующих (или следующих за) данной букве.

Пример криптоанализа шифра замены

Известно, что зашифровано стихотворение Р. Киплинга в переводе С.Я. Маршака. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены. Таблица частот букв русского языка приведена выше.

29 15 10 17 29 22 25 31 15 33 35 41 43 45 35 57 45 25 17 59 15 10 25 41 25 69, 59 78 29 82 25 78 25 17 15 10 88 90 78 25 62 25 22 10 57 73 79 35 67 78 90 88 29 45 35 29, 54 57 90 31 90 73 22 88 15 88 29 15 17 69 41 25 15, 70 17 90 57 43 59 15 78 15 62 22 25 17 57 25 69 88 15 82 17 25 88 29 45 35…

Подсчитаем частоты шифрообразований:

Обозначение	9	5	0	7	2	5	1	3	5	1	3	45	7
Количество		0				2						4	

Обозначение	9	9	8	2	8	0	2	3	9	7	4	70
Количество												1

Из таблица частот букв русского языка видно, что чаще всего встречается буква О, на втором месте Е. В нашем шифр-тексте чаще всего встречается обозначение 25 (12 раз), на втором месте идет обозначение 15 (10 раз), остальные обозначения им существенно уступают. Поэтому можем выдвинуть гипотезу: 25=О, 15=Е. Однако, текст у нас не очень большой, поэтому закономерности русского языка проявляются в нем не обязательно в строгом соответствии с таблицей частот букв русского языка. Поэтому возможен и вариант: 25=Е, 15=О. Но тогда последнее слово в третьей строке имеет окончание ЕО, что возможно, но все же более вероятный вариант ОЕ. Итак, будем работать с текстом, считая, что 25=О, 15=Е.

Теперь нам поможет знак препинания: «29, …». Крайне маловероятно, чтобы запятая стояла после согласной. Итак, 29 – гласная, причем вероятнее всего 29=И или 29=А, т.к. гласные Я, Ю, Э, У встречаются в осмысленных текстах на русском языке намного реже, чем И и А, что не противоречит таблице частот шифр-текста.

В последней строке: 88 15, но 15=Е, следовательно, 88 – согласная, причем наиболее вероятные значения – это Н и Т. Итак, 25=О, 15=Е, 29=А $\binom{А}{И}$, 88=$\binom{Н}{Т}$. Теперь третье слово в третьей строке имеет 4 варианта:

- 29=И, 88=Н: 22 Н Е Н И Е
- 29=И, 88=Т: 22 Т Е Т И Е
- 29=А, 88=Н: 22 Н Е Н А Е
- 29=А, 88=Т: 22 Т Е Т А Е

Из рассмотренных вариантов лишь один является осмысленным, и он позволяет найти значение 22. Имеем: 22=М и третье слово в третье строке М Н Е Н И Е.

Теперь рассмотрим второе слово в первой строке. Е 10 17 И, причем 10 и 17 – согласные, и это не М и не Н. Наиболее вероятное слово Е С Л И, т.е. 10=С, 17=Л. Конечно, если мы, продолжая работать с текстом, вдруг получим «нечитаемое» слово, то придется вернуться к этому этапу и рассмотреть другие варианты. Однако, это маловероятно, поскольку вряд ли в стихотворении были слова наподобие Е Р Т И, Е В Л И и т.п.

Далее, первое слово второй строки: 59 78 И, причем 59 и 78 – согласные, и это не С, не Л, не М и не Н. Так что это слово П Р И, т.е. 59=П, 78=Р. Тогда шестое слово первой строки 45 О Л П Е, что дает значение 45=Т и тогда при 57=В получаем фрагмент «…В Т О Л П Е…». Также второе слово последней строки П Е Р Е 62 дает нам значение 62=Д.

Далее рассмотрим начало второй строки: «П Р И 82 О Р О Л Е С Н 90 Р О Д О М …». Из него следует, что 82=К и 90=А.

Зная, что 82=К, посмотрим на самое последнее слово К Л О Н И Т 35, откуда станет ясно, что 35=Ь.

Перед последней атакой выпишем текст, заменяя известные обозначения буквами.

И Е С Л И М О 31 Е 33 Ь 41 43 Т Ь В Т О Л П Е С О 41 О 69,
П Р И К О Р О Л Е С Н А Р О Д О М С В 73 79 Ь 67 Р А Н И Т Ь
И, 54 В А 31 А 73 М Н Е Н И Е Л 69 41 О Е,
70 Л А В 43 П Е Р Е Д М О Л В О 69 Н Е К Л О Н И Т Ь…

Из последней строки: 69=Ю, тогда слова Л Ю 41 О Е и С О 41 О Ю определяют 41: 41=Б. Теперь из четвертого слова первой строки Б 43 Т Ь получаем, что 43=Ы. А первое слово из последней строки 70 Л А В Ы – это Г Л А В Ы. Слово в первой строке М О 31 Е 33 Ь

угадывается из контекста: М О Ж Е Ш Ь, т.е. 31=Ж, 33=Ш. Теперь второе слово в третьей строке запишется как 54 В А Ж А 73, откуда, с учетом контекста: 54=У, 73=Я. После этого окончание второй строки имеет вид «… С В Я 79 Ь 67 Р А Н И Т Ь». Легко определяются буквы 79=З, 67=Х.

Ответ: И Е С Л И М О Ж Е Ш Ь Б Ы Т Ь В Т О Л П Е С О Б О Ю,
П Р И К О Р О Л Е С Н А Р О Д О М С В Я З Ь Х Р А Н И Т Ь
И, У В А Ж А Я М Н Е Н И Е Л Ю Б О Е,
Г Л А В Ы П Е Р Е Д М О Л В О Ю Н Е К Л О Н И Т Ь…

Задания: Расшифровать текст. Каждой букве алфавита соответствует двузначное число.

1.

58 62 32 39 99 31 29 58 72 62 99 58 13 54 15 56 31 63 39 72 84 15 13 56 77 15 82 56 56 56 58 54 29 77 56 – 39 99 56 31 56 7732 12 15 54 31 48 7663 15 52 13 39 72 39 5416 72 39 32 72 62 58 58 15,37 62 7752 39 13 39 72 39 32 3931 62 54 39 77 84 39 21 31 3916 72 62 99 58 13 15 54 56 13 4616 39 58 13 95 16 15 13 62 12 46 31 39 6272 15 77 54 56 13 56 6284 31 39 32 56 7658 63 62 7233 62 12 39 54 62 33 62 58 52 39 9199 62 29 13 62 12 46 31 39 58 13 56.56 31 63 39 72 84 15 82 56 39 31 31 48 6213 62 76 31 39 12 39 32 56 5616 72 39 33 31 3954 39 53 12 565437 56 77 31 62 58,39 37 72 15 77 39 54 15 31 56 62,16 72 39 56 77 54 39 99 58 13 54 39,39 13 52 72 48 5433 62 12 39 54 62 52 9531 62 37 48 54 15 12 48 6254 39 77 84 39 21 31 39 58 13 5616 3958 52 39 72 39 58 13 5616 39 12 95 33 62 31 56 295639 37 72 15 37 39 13 52 6256 31 63 39 72 84 15 82 56 56,1513 15 52 21 6216 3915 54 13 39 84 15 13 56 77 15 82 56 5616 72 39 56 77 54 39 99 58 13 54 62 31 31 48 76,95 16 72 15 54 12 62 31 33 62 58 52 56 765656 31 48 76 16 72 39 82 62 58 58 39 54.

2.

3925 20 34 82 6366 46 35 20 25 828639 51 74 35 51 66 20 4437 25 27 51 35 44 20 90 37 51 25 25 51 6391 20 11 37 46 4825 20 37 61 51 14 82 8266 82 35 29 82 91 25 5174 51 24 78 51 24 59 46 86 51 44 74 20 25 37 37,37 44 82 31 11 37 82 51 46 25 51 34 82 25 37 828637 25 27 51 35 44 20 90 37 51 25 25 48 4446 82 78 25 51 14 51 18 37 59 44,51 74 82 35 20 90 37 59 446690 82 25 25 48 44 3761 10 44 20 18 20 44 37,8661 20 25 86 51 39 66 86 51 44 1066 82 86 46 51 35 10 3766 51 46 51 39 51 6366 39 59 91 37.56 46 51 86 20 66 20 82 46 66 5924 35 10 18 37 7851 35 18 20 25 37 91 20 90 37 63,4651,66 51 18 14 20 66 25 5135 82 91 10 14 29 46 20 46 20 4435 20 91 14 37 56 25 48 7837 66 66 14 82 24 51 39 20 25 37 63, 35 10 86 51 39 51 24 37 46 82 14 3744 25 51 18

37 7837 9125 37 7891 25 20 31 4651 61 51 66 25 51 39 25 48 7839 37 24 20 78 10 18 35 51 91,25 5125 82 10 24 82 14 59 31 4624 51 14 42 25 51 18 5139 25 37 44 20 25 37 5924 20 25 25 48 4439 51 74 35 5166 20 44,66 56 37 46 20 59,56 46 5151 61 82 66 74 82 56 82 25 37 8237 25 27 51 35 44 20 90 37 51 25 25 51 6361 82 91 51 74 20 66 25 51 66 46 3725 8237 44 82 82 4666 44 48 66 14 20,82 66 14 3751 46 66 10 46 66 46 39 10 82 4639 37 24 37 44 20 5910 18 35 51 91 20.

3.

74 29 23 27 17 99 71 254932 29 34 27 63 32 25 17 99 60 62 25 34 95 29 53 59 82 27 71 29 77 99 34 27 91 17 99 71 49 99 27 15 60 32 25 50 27 17 62 27 95 27 50 25 91 32 59 77 95 29 50 25 99 59,25 99 74 29 53 25 59 17 99 25 91 23 49 71 25 17 99 604925 34 32 25 71 95 27 82 27 32 32 2529 50 17 25 15 77 99 32 59 7762 95 25 53 95 29 23 32 25 17 99 60 34 15 35 17 27 99 27 71 25 12 2599 95 29 45 49 74 29. 62 95 27 63 34 2771 17 27 12 25,50 27 17 62 27 95 27 50 25 91 32 29 3595 29 50 25 99 29 17 29 82 49 8362 2517 27 50 2762 95 25 34 59 74 99 25 7150 27 53 25 62 29 17 32 25 17 99 4917 71 35 53 29 32 2917 32 29 15 49 23 49 27 8232 29 34 27 63 32 2595 29 50 25 99 29 77 10 27 12 2525 50 25 95 59 34 25 71 29 32 49 3549 95 27 53 27 95 71 49 95 25 71 29 32 49 27 8274 95 49 99 49 23 32 89 837425 99 74 29 53 5950 15 25 74 25 7162 49 99 29 32 49 354953 29 62 25 82 49 32 29 77 10 49 8359 17 99 95 25 91 17 99 71.34 15 3562 25 17 15 27 34 32 49 8325 62 99 49 82 29 15 60 32 2562 95 49 82 27 32 27 32 49 2734 49 17 74 25 71 89 8382 29 17 17 49 71 25 7112 25 95 35 23 27 9153 29 82 27 32 89.74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 95 29 50 25 99 8934 25 17 99 49 12 29 27 99 17 3525 62 99 49 82 49 53 29 67 49 27 9162 95 25 12 95 29 82 82 32 25 12 2525 50 27 17 62 27 23 27 32 49 35.

4.

48 2318 40 94 35 62 53 94 25 53 15 3591 35 40 35, 52 23 5253 40 3594 35 40 2394 23 91 52 94 49 24 23 84 8994 23 64 55 53 15 18 53 91, 24 53 88 23 62 12 25 7694 2364 35 24 49, 35 9449 88 5348 94 23 24,41 91 3591 23 5231 49 15 53 91. 47 91 3541 49 62 84 91 62 3535 91 41 23 84 91 2531 29 24 3564 35 27 35 88 5394 2391 35,52 35 91 35 55 35 5335 9425 84 64 29 91 23 24,52 35 40 15 2348 23 62 53 55 94 49 2448 2349 40 35 242541 49 91 8994 5394 23 24 53 91 53 24 94 2315 53 62 49 12 52 49,12 53 15 12 49 6053 18 4994 23 62 84 91 55 53 41 49.53 40 3594 35 40 23,62 29 48 62 23 6284 62 35 25 1815 62 25 88 53 94 25 53 18 52 35 24 53 31 23 94 25 53 62 35 48 15 49 27 23,64 35 24 49 41 25 24 23 35 91 55 23 88 53 94 94 29 7684 25 40 94 23 243564 55 53 64 38 91 84 91 62 25 2594 2364 49 91 25 2564 35 41 91 256291 4988 5384 53 52 49 94 15 4949 15 23 55 25 24 23 84 8935 31 3541 91 35 – 91 35.52 23 52 35 76-91 3564 55 53 15 18 53 918440 24 49 27 25 1884 91 49 52 35 1835 91 24 53 91 53 246291 53 18 94 35 91 49.

5.

79 6131 96 28 35 85 5226 30 24 21 52 85 59 49 79 30 88 7949 30 52 79 59 85 26 30 24 21 59 85 42 79 88 61 28 35 86 5096 28 52 30 50,24 30 96 74 21 59 9059 30 96 30 24 85 61 8626 96 85 88 79 96 79 24 61 79 1128 52 79 78 31 85, - 21 50 30 96 85 31 21 61 59 31 85 1126 79 24 96 79 59 35 79 31 5996 30 31 52 21 50 61 79 1131 21 96 35 85 61 31 85,2126 79 78 30 50 2867 868561 30 35:35 79 24 2467 79 28 24 30 61,35 96 85 61 21 24 69 21 35 9052 30 35,61 79 96 50 21 52 90 61 86 1196 79 59 35,42 24 79 96 79 49 86 1149 30 59,49 79 52 79 59 8669 49 30 35 2159 26 30 52 79 1126 46 30 61 85 69 86,88 79 52 28 67 86 3088 52 21 42 21,96 79 49 61 86 3067 30 52 86 3042 28 67 86,42 21 88 79 96 30 52 79 3052 85 69 79,61 3085 59 26 79 96 78 30 61 61 79 3024 21 74 3061 21 50 30 31 79 5061 2149 79 42 96 21 59 35 61 86 30 26 96 86 29 85 31 85..

6.

56 27 54 54 27 56 51 32 82 16 63 49 27 63 11 30 73 35 23 54 89 70 27 63 27 493270 35 16 97 82 16 67 73 27 51 30 56 32 6370 29 63 27 49 32 73 29 5473 2748 29 13 29 82 56 82 27 9554 27 35 27 18 51 29,97 56 2770 29 63 305151 35 15 63 89 48 16.16 63 15 11 51 3082 2949 65 27 54 32 63 304929 61 2763 32 48 30-27 56 51 35 15 56 30 233227 11 70 27 35 27 18 32 56 29 63 89 82 30 23,27 82 3051 30 5111 1573 35 29 54 70 27 49 65 32 38 30 63 3073 35 32 23 56 82 16 6770 49 56 35 29 97 16.82 27 49 51 27 1351 29 54 3027 8227 73 16 49 56 32 6370 29 63 27 49 32 73 29 54 82 15 9516 73 27 353270 15 56 30 38 32 6332 92-73 27 5411 30 61 30 18 82 32 51 3049 63 27 18 29 82 82 16 67 61 30 92 29 56 16.27 8249 16 82 16 6361 30 92 29 56 1673 27 5413 15 24 51 163270 92 27 24 29 6373 2749 56 16 73 29 82 89 51 30 13.

7.

3428 68 91 1383 10 65 27 6849 10 26 65 27 68 75 26 39 785375 83 53 18 26 36 62 91.26 10 74 53 1349 10 83 10 65 5353 36 68 72 28 1028 13 18 86 10 27 53 75 3983 6857 26 18 10 91535736 53 6528 68 91 10,83 68 75 27 1334 13 24 13 18 53 36 74 5336 10 74 10 36 57 36 13,83 68 74 1091 10 91 1036 1368 26 74 18 62 34 10 27 1036 10 75 26 13 86 3968 74 36 10.83 18 10 34 28 10,26 57 2650 62 27 6883 68 65 57 86 13.26 57 2649 10 83 10 65 5334 19 13 27 53 75 395334 75 1375 68 50 68 1583 18 68 83 53 26 10 27 53.49 10 83 10 65 5310 27 74 68 72 68 27 44,83 68 28 72 68 18 13 34 80 13 72 6891 10 75 27 10,83 68 26 10,75 26 10 18 68 1568 28 13 86 28 625313 96 1327 13 74 10 18 75 26 34-91 13 36 26 68 27 1053,74 10 86 13 26 75 44,34 10 27 13 18 39 44 36 74 53.3483 18 53 65 68 86 13 15 26 13 91 36 68 26 53 96 10,5318 44 28 68 9123 26 68 2628 78 75 75 10 36 28 13 18-34 26 44 36 57 2772 68 27 68 34 573434 68 18 68 26,23 26 10 74 53 1572 18 53 47 – 75 26 13 18 34 44 26 36 53 74,86 28 57 96 53 15,74 68 72 28 1018 10 36 13 36 68 1386 53 34 68 26 36 68 1353 75 83 57 75 26 53 2628 57 65.

8.

45 34 26 34 9777 34 47 49 67 14 22 49 6747 34 49 39 77 6953 89 26 1097 10 49 10 77 45 53 31 10 14 10 47 22.17 90 56 14 34 77 67 49,49 67 75 49 1053 14 5349 26 90 47 10,77 3439 47 56 34 3156 26 67 52 34 13 10 84 22 5377 34 47 49 67 14 22 49 67 28 34 84 26 67 31,67 49 10 97 90 31 10 14 53 47 223128 70 89 49 53 9314 10 56 10 9356 47 10,5345 34 84 90 26 34 93 69 58 37 28 67 31 10 7047 84 10 14 22 77 10 7053 89 14 10,31 90 47 39 77 39 31 75 53 47 22,47 14 67 31 77 6713 10 14 67,53 9734 89 6728 67 26 69 90,31 56 26 90 47 49 53 31 10 14 1013 34 26 84 31 3453 97 26 70 69 77 39 5869 67 97 39 28 67 26 24 53 70,53 14 5356 26 67 49 10 53 77 10.97 10 84 34 2839 52 53 84 67 89 6797 31 34 26 22 49 1052 26 67 47 10 14 533156 34 45 2269 14 7047 13 53 89 10 77 53 7028 39 47 67 26 10,5353 89 26 1077 10 45 53 77 10 14 10 47 2247 77 67 31 10.

9.

81 49 86 49 1273 92 5081 50 15 5062 47 4915 56 50 51 7673 33 94 7615 94 65 81 47 76.94 76 47 49 81 47 76,15 7662 47 76 2628 16 5162 76 2628 76 51 70 58 76 2673 86 65 84 76 94,47 7615 94 65 81 47 7615 56 50 51 76.24 16 51 7062 76 49 2694 76 86 76 28 94 3362 49 47 1765 84 4915 76 92 15 49 6247 4924 86 49 51 70 96 50 51 50.56 76 31 73 5047 49 62 47 76 31 7624 76 73 65 62 50 513386 49 58 33 5115 56 50 567 065 62 47 16 62.47 65,47 50 73 7684 4943 76 56 7081 56 76-56 7673 49 51 50 56 70…1724 76 58 49 519294 76 51 51 49 73 84.76 94 50 12 50 92 58 33 15 709294 50 28 33 47 49 56 496586 49 94 56 76 86 50,1773 49 86 84 50 51 15 1765 92 49 86 49 47 47 76.86 49 94 56 76 86 76 6228 16 51 5062 76 51 76 73 50 1784 49 47 96 33 47 5028 50 51 70 12 50 94 76 92 15 94 76 31 7692 76 12 86 50 15 56 50.94 76 31 73 501792 76 58 49 51,76 47 5081 56 76-56 7615 76 15 86 49 73 76 56 76 81 49 47 47 7624 33 15 50 51 50,62 76 84 49 5647 76 92 16 2665 94 50 12.

10.

2043 40 13 15 91 31 5475 31 91 12.88 56,88 40 29 1571 3113 15 91 1249 91 15 – 91 1529 31 54 40 91 12…1715 61 69 31 44,2075 15 36 31 546275 25 15 29 84 65 31 25 56.90 4415 62 40 43 40 54 65 2088 31 17 58 65 15 62 90 2690,75 15-17 90 29 90 44 15 44 56,88 31 29 40 54 31 62 90 2649 31 54 15 17 31 621791 31 44 88 58 1315 49 62 40 13901725 15 43 15 17 15 4436 40 25 34 90 62 3188 4036 31 31.15 8862 56 25 90 5449 91 15-91 1515 49 31 88 1275 25 15 91 90 17 88 1575 40 13 88 56 69 31 31.29 40 71 3117 15 88 20 84 69 31 31.56 17 90 29 31 1744 31 88 20,75 25 15 29 84 65 31 2588 31 65 62 15 54 12 62 1544 90 88 56 9175 15 44 56 49 40 54 65 20,17 65 91 40 17 54 20 2015 91 17 90 65 36 56 8449 31 54 84 65 91 1288 4044 31 65 91 15,88 1517 65

3171 3117 43 20 5465 31 61 201725 56 62 90,43 40 91 56 36 90 5465 90 52 40 25 31 91 569043 40 52 15 17 15 25 90 54.

11.

65 27,67 40 58 34 11 4727 4227 45 82 34 11 14 4914 89 95 47.65 14 90 36 89 3434 67 36 90 36 45 67 11 36 65 65 34 89 34,11 17 82 34 67 1924 3495 40 45 17 34 45 82 36 24 65 14 7025 36 82 34 90 36 73.70 34 67 4945 67 95 40 65 40,17 34 45 95 36 24 1458 34 67 34 95 34 7334 65 1445 36 73 90 40 4517 95 36 59 47 11 40 82 14,24 40 11 65 341465 40 24 36 42 65 3417 34 24 25 49 67 4040 25 36 95 14 58 34 45 40 25 14,69 67 3411 45 3642 3645 27 11 36 95 36 65 65 40 4924 36 95 42 40 11 40,90 82 36 6534 34 65,4558 34 36 7345 34 11 36 67 45 58 14 7345 34 31 6317 34 24 24 36 95 42 14 11 40 36 6765 34 95 25 40 82 19 65 47 3624 14 17 82 34 25 40 67 14 90 36 45 58 14 3634 67 65 34 32 36 65 14 49,17 34 65 36 25 65 34 89 2765 40 82 40 42 14 11 40 36 6767 34 95 89 34 11 82 31,17 95 14 45 47 82 40 36 6765 4089 40 45 67 95 34 82 1459 40 82 36 67 65 47 3667 95 27 17 17 471434 59 25 36 65 14 11 40 36 67 45 4917 95 34 18 45 34 31 63 65 47 25 1424 36 82 36 89 40 56 14 49 25 14.4017 34 67 34 25 2763 24 36 45 1965 14 58 40 5865 3617 34 82 40 89 40 36 67 45 4965 36 82 36 89 40 82 19 65 3417 95 36 59 47 11 40 67 1945 34 11 36 67 45 58 14 2559 34 36 11 47 2517 82 34 11 56 40 25,“25 34 95 45 58 14 2524 19 49 11 34 82 40 25”.36 42 36 82 1490 67 34-45 58 40 65 24 40 8295 40 63 89 34 95 14 67 45 4917 3417 34 82 65 34 73…

12.

14 701465 3659 47 82 34,4058 40 5842 36.17 95 34 45 67 34-65 40 17 95 34 45 67 3432 36 45 67 36 95 3425 27 42 14 58 34 11,65 4011 14 24-45 67 40 65 24 40 95 67 65 47 3636 11 95 34 17 36 34 14 24 47,4563 40 17 40 24 65 34 89 36 95 25 40 65 45 58 14 25 1440 11 67 34 25 40 67 40 25 14,14 67 40 82 19 49 65 45 58 14 25 1440 58 11 40 82 40 65 89 40 25 14,32 11 36 24 45 58 14 25 1459 40 63 27 58 40 25 14,59 36 82 19 89 14 73 45 58 14 25 1425 14 65 40 25 14,18 95 40 65 56 27 63 45 58 14 25 1445 14 89 40 95 36 67 40 25 141432 11 36 73 56 40 95 45 58 14 25 1490 40 45 40 25 14.17 95 36 24 25 36 67 4745 65 40 95 49 42 36 65 14 49,11 63 49 67 47 3617 3434 67 24 36 82 19 65 34 45 67 14,25 34 42 65 3459 36 6334 45 34 59 47 7070 82 34 17 34 6717 95 14 34 59 95 36 45 67 141195 40 63 65 47 7058 34 65 56 40 7036 11 95 34 17 4758 40 5882 36 89 40 82 19 65 34,67 40 581465 4090 36 95 65 34 2595 47 65 58 36-58 40 58,45 34 59 45 67 11 36 65 65 34,1417 95 34 14 63 34 32 82 3467 95 27 24 40 25 1465 36 11 36 24 34 25 47 7025 40 63 27 95 27“14 65 67 36 65 24 40 65 67 34 11”.

13.

60 46 5746 52,28 15 57 3912 32 60 32 3246 5752 55 30 12 61 11 55 57 32 12 41,37 46 60 37 32 9152 32 11 55 12 32 75 4646 5730 32 20 15 75 46 25 99 20 52 32 52 52 4667 55 25 55 12 12 32 12 39 52 19 63“52 99 57 32 36”75 46 12 61 28 75 99(18 32 37 57 3952 99 57 32 3667 46 60 32 25 63 159991 32 57 25 46 60 46 3660 19 37 46 57 19“37 67 99 25 55 12 3930 25 15 52 46 ”67 4620 32 91 12 32).57 5537 55 91 55 4167 57 99 28 75 55.75 25 55 37 55 60 32 74,37 57 46 99 5767 25 99 20 52 55 57 39,99 20 41 45 52 19 36,11 12 99 52 52 46 75 25 19 12 19 36,37 15 67 32 25 55 29 25 46 11 99 52 55 91 99 28 32 37 75 99 36,60 19 37 46 57 52 19 36.“11 48 99 – 29 25 – 11 60 32 52 55 11 74 55 57 39”,52 46 60 32 36 18 99 3637 55 91 46 12 32 5729 12 32 75 57 25 46 52 52 46 3625 55 20 60 32 11 75 99,46 37 52 55 45 32 52 52 19 3655 67 67 55 25 55 57 15 25 46 36,78 46 25 11 4699 91 32 52 15 32 91 46 36“57 32 63 52 99 75 46 3611 60 55 11 74 55 57 3967 32 25 60 46 78 4660 32 75 55”(63 46 57 4111 4675 46 52 74 5511 60 55 11 74 55 57 46 78 4637 57 46 12 32 57 99 41,37 46 78 12 55 37 52 4663 25 46 52 46 12 46 78 99 99,46 37 57 55 12 46 37 3932 45 3267 41 57 52 55 11 74 55 57 393712 99 18 52 99 9112 32 57)…

14.

15 48 3252 326067 32 25 60 19 3625 55 2091 55 20 15 25 1567 25 99 63 46 11 99 12 466078 46 12 46 60 15,28 57 4628 99 52,46 57 60 32 28 55 60 18 99 3620 5530 32 20 46 67 55 37 52 46 37 57 3930 55 20 19,30 19 12 75 12 55 37 37 99 28 32 37 75 99 9137 15 63 46 67 15 57 28 99 75 46 91. 60 37 60 46 3260 25 32 91 4146 52 67 46 25 55 30 46 57 55 12 52 55 37 46 60 32 37 57 39,46 30 46 25 15 11 46 60 55 60 37 15 63 46 67 15 57 52 19 3267 46 11 37 57 15 67 197530 55 20 3232 91 75 46 37 57 52 19 91 9911 55 57 28 99 75 55 91 99,37 99 78 52 55 12 39 52 19 91 9925 55 75 32 57 55 91 99,67 25 9991 55 12 32 36 18 32 9167 25 99 75 46 37 52 46 60 32 52 99 997557 46 52 61 37 32 52 39 75 46 3652 99 57 9960 20 12 32 57 55 60 18 99 91 996052 32 30 32 37 5537 4637 60 99 37 57 46 91,25 55 37 37 19 67 55 4160 46 25 46 63 5525 55 20 52 46 74 60 32 57 52 19 6346 37 12 32 67 99 57 32 12 39 52 19 6399 37 75 25-9911 55 48 3267 46 12 46 37 55 91 9967 25 46 57 99 60 46 67 32 63 46 57 52 19 6391 99 52.28 57 46 75 55 37 55 32 57 37 4167 46 11 37 57 15 67 46 6060 46 11 52 19 63,28 99 5230 19 1252 3257 55 7525 32 57 99 60. 46 11 52 9957 46 12 39 75 4637 57 46 12 30 193775 46 12 61 28 75 46 369967 25 32 37 12 46 60 15 57 19 32“37 67 99 25 55 12 39 75 99”-75 46 57 46 25 19 3252 32 20 60 55 52 19 3278 46 37 57 99,6046 57 12 99 28 99 3246 5720 11 32 18 52 99 6367 55 25 57 99 20 55 52,15 91 32 12 9967 25 32 46 11 46 12 32 60 55 57 3930 19 37 57 25 469930 32 2091 55 12 32 36 18 32 78 4660 25 32 11 5511 12 4137 46 30 37 57 60 32 52 52 46 78 4646 25 78 55 52 99 20 91 55.9960 37 32.

15.

45 74 5431 10 26 38 23 74,86 74 5425 89 26 38 16 74 7475 1645 56 90 25 86 90 75 90 10 2616 74 23 56 86 75 45 16 75 7495 10 13 31 95 10 51 74 16 89 74,36 75 95 75 5936 74 95 74 91 75 31

89 90 23 74 749036 95 89 26 89 90 8313 26 75 25 86 89-75 86 86 75 47 75,45 86 7575 16 8945 74 86 90 74 95 7525 56 86 75 33,75 29 95 10 86 89 90 23 89 25 389013 95 74 16 89 748925 26 56 91,86 75 95 45 10 26 899045 10 19 75 29 74,33 10 3331 89 33 89 7475 29 74 13 38 42 16 8389 1329 95 10 13 89 26 89 89,75 86 86 75 47 75,45 86 7536 75 31 90 74 95 16 56 26 25 4286 56 36 75 4633 10 46 54 10 16,2575 31 89 16 10 33 75 90 83 5456 25 74 95 31 89 74 5416 10 36 10 31 10 90 23 89 468916 1026 74 25 16 56 5925 90 89 16 38 59,8916 1075 86 26 89 45 16 75 47 7536 10 95 16 422531 95 56 47 75 47 7533 75 16 86 89 16 74 16 86 10.109021 86 7590 95 74 54 4286 74,16 1029 10 13 74,51 89 26 899025 90 75 7456 31 75 90 75 26 38 25 86 90 89 74,25 36 10 26 8916 1045 89 25 86 74 16 38 33 89 9136 95 75 25 86 83 16 33 10 919033 75 16 31 89 17 89 75 16 89 95 75 90 10 16 16 75 4636 95 75 91 26 10 31 74,36 95 89 16 89 54 10 26 8931 56 23,51 95 10 26 8916 1013 10 90 86 95 10 3367 95 56 33 86 83,31 51 74 548929 89 67 23 86 74 33 25 839086 95 8936 10 26 38 17 1086 75 26 19 89 16 75 46-8975 33 16 1086 10 3356 59 86 16 7525 90 74 86 89 26 89 25 38,8954 56 13 83 33 1089 47 95 10 26 10,8967 56 86 29 75 26 36 75 86 74 26 74 90 89 13 75 95 56…

16 89 45 74 47 75 9021 86 75 4 613 26 75 25 86 8916 7429 83 26 7536 26 75 91 75 47 75,16 10 75 29 75 95 75 86-86 10 33 75 4616 10 25 86 95 75 4633 10 3395 10 138936 95 89 31 10 74 8629 75 74 90 75 47 7533 56 95 10 51 10…

1036 75 86 75 5436 95 89 23 74 2633 75 16 74 178936 75 25 86 75 95 75 16 16 89 5454 83 25 26 42 548929 74 13 31 74 26 38 59.54 75 95 25 33 75 46 13 54 74 4616 10 33 75 16 74 17-86 7536 75 31 10 2613 16 10 33,33 75 86 75 95 75 47 7575 16 8951 31 10 26 8945 74 86 90 74 95 7525 56 86 75 33,8921 86 7529 83 26 7525 26 75 90 16 7554 74 31 16 83 4695 74 9029 75 74 90 75 4686 95 56 29 83,21 86 7575 13 16 10 45 10 26 75,45 86 7516 10 45 10 26 10 25 3895 10 29 75 86 83,8916 89 45 74 47 7556 51 7416 7489 13 54 74 16 89 86 38,16 7475 25 86 10 16 75 90 89 86 38,16 7436 74 95 74 89 47 95 10 86 38…

16.

15 22 67 30 93 4922 94 65 94 44 49,4939 51 22 75 49 411115 22 4911 53 51 75 51 78 94,44 4927 51 22 67 44 86 51,26 49 39 51 75“78 45 94 – 62 75 – 78 11 51 44 49 78 91 49 22 72 14”,9411 67 26 93 5 144 51 90 6793 51 44 94 11 6753 75 67 41 49 45 94 11 49 93 15 3035 49 15 67 11 67 14,44 5145 78 49 11 65 94 1444 94 86 49 86 94 4115 20 75 53 75 94 26 67 11,44 5153 67 78 67 26 75 51 11 49 11 65 94 14,35 22 6751 90 6715 39 51 75 22 5853 75 51 27 72 11 49 51 2215 67 11 15 51 3944 51 53 67 78 49 93 51 86 881167 27 75 49 26 5127 51 15 53 93 67 22 44 67 90 6735 51 75 44 67 90 6753 75 94 26 75 49 86 49,44 5126 44 49 20 18 51 90 6745 49 93 67 15 22 94.

67 35 51 75 51 78 44 67 1445 51 15 2286 67 39 49 44 78 94 75 49-9439 49 26 88 751511 94 86 94 44 90 67 399415 22 75 49 65 94 93 67 1453 51 75 51 27 51 45 86 49 39 9478 11 94 44 88 93

94 15 5811 53 51 75 51 78.26 78 51 15 5841 11 49 22 49 93 6753 75 67 45 51 86 22 67 75 67 11,36 67 44 49 75 51 149486 75 67 44 65 22 51 14 44 67 111590 94 75 93 30 44 78 49 39 9493 49 39 53,44 6744 51 75 51 49 93 58 44 67 1426 49 78 49 35 51 1427 72 93 6727 7267 15 11 51 22 94 22 5811 15 2027 49 26 88.67 15 22 49 11 49 93 67 15 5844 51 39 49 93 6753 67 93 67 159453 30 22 51 4422 51 39 44 67 22 72,86 67 22 67 75 88 20 44 51 26 11 49 44 72 5190 67 15 22 9494 15 53 67 93 58 26 67 11 49 93 9439 49 15 22 51 75 15 86 94.11 15 5127 93 94 45 518615 49 39 67 93 51 22 88,27 93 94 45 51,27 93 94 45 51,67 4411 72 75 49 15 22 49 51 2244 4990 93 49 26 49 41,44 49 11 94 15 49 51 2244 49 7890 67 93 67 11 67 14,88 45 5153 75 51 86 75 49 15 44 6715 93 72 65 44 67,86 49 8635 49 15 67 11 67 1467 2215 86 88 86 9444 88 78 94 2253 67 7844 67 1544 51 26 44 49 86 67 39 88 2039 51 93 67 78 94 20,53 67 15 93 51 78 44 20 201115 11 67 51 1445 94 26 44 94…

22 94 41 67 44 58 86 6718 51 93 86 44 88 9327 51 15 65 88 39 44 72 1453 94 15 22 67 93 51 22-9439 51 93 67 78 94 3067 27 67 75 11 49 93 49 15 58,35 49 15 67 11 67 1453 67 78 93 67 39 94 93 15 301186 67 93 51 44 86 49 41,44 6788 53 49 15 22 5844 5188 15 53 51 93,9415 11 67 2049 11 22 67 39 49 22 94 35 51 15 86 88 2011 94 44 22 67 11 86 8844 5111 72 75 67 44 94 93.78 11 5122 51 44 94,27 51 15 65 88 39 44 6711 72 44 72 75 44 88 1194 26 -53 67 7836 20 26 51 93 30 45 49,53 67 78 41 11 49 22 94 93 9451 90 679488 11 67 93 67 86 93 94 44 4978 75 88 90 88 2015 22 67 75 67 44 88,1122 51 39 44 67 22 88.

17.

56 67 9218 58 39 99 27 87 67 5625 56 80 67 10 17 92 39 6225 5627 24 95 56 3195 46 27 73 56 3117 58 39 58 67 95 589256 95 40 24 40 17 92 39 626939 40 17 56 67 58-56 18 99 92 46 67 56 87,69 5669 39 3680 17 92 67 2739 40 87 56 17 58 73 40.25 56 39 73 56 10 17 92,56 43 92 80 40 10,95 56 23 80 4023 17 40 24 4025 46 92 69 14 95 67 27 739573 58 87 67 56 73 58.69 39 5869 56 95 46 27 2325 46 92 67 10 17 5638 58 73 95 92 5856 38 58 46 73 40 67 92 10.25 46 92 18 56 46 56 699225 27 17 62 73 56 6924 80 58 39 6218 14 17 5625 46 58 69 58 17 92 95 56 5887 67 56 43 58 39 73 69 56,23 17 40 24 4046 40 24 18 58 23 40 17 92 39 62.56 80 67 40 95 5618 17 40 23 56 80 40 46 1073 58 8743 58 80 69 27 8767 58 80 58 17 10 8773 46 58 67 92 46 56 69 56 9567 4087 40 95 58 73 58 9273 14 39 10 38 58 95 46 40 73 67 56 25 56 69 73 56 46 58 67 67 14 8767 40 39 73 40 69 17 58 67 92 10 8792 67 39 73 46 27 95 73 56 46 4056 67 9239 56 69 58 46 99 58 67 67 5673 56 38 67 5624 67 40 17 92,24 4038 58 8725 46 92 99 17 92.25 56 67 10 73 92 1067 5892 87 58 17 92,80 17 1038 58 23 5695 56 67 95 46 58 73 67 5625 46 58 80 67 40 24 67 40 38 58 67 1469 39 5871 73 9299 73 27 95 92-67 5656 7367 92 8271 73 56 23 56 9267 5873 46 58 18 56 69 40 17 56 39 62.

67 5825 46 56 99 17 569287 92 67 27 73 14,95 40 9556 6727 69 92 80 58 1751 58 17 6292 8267 58 17 58 23 95 56 23 569271 95 24 56 73 92 38 58 39 95 56 23 5625 27 73 58 99 58 39 73 69

92 10-73 46 9225 27 17 62 73 4025 5625 46 40 69 56 87 2718 56 46 73 27,27 39 14 25 40 67 67 14 5838 58 46 73 56 69 56 3127 31 87 56 3173 27 87 18 17 58 46 56 69,17 40 87 25 56 38 58 95,25 58 46 58 95 17 36 38 40 73 58 17 58 319295 67 56 25 56 95.73 46 9269 14 25 27 95 17 14 8271 95 46 40 67 406969 92 80 5869 58 46 73 92 95 40 17 62 67 14 8225 46 10 87 56 27 23 56 17 62 67 92 95 56 69-56 67 9239 40 87 14 58,67 92 95 40 95 56 3156 99 92 18 95 92…

18 56 80 46 56 39 73 9246 40 80 92,56 6725 56 69 73 56 46 92 1725 46 5639 58 18 1025 56 17 36 18 92 69 99 27 36 39 1051 92 73 40 73 27:“38 73 5656 80 92 6738 58 17 56 69 58 9525 56 39 73 46 56 92 17,80 46 27 23 56 3124 40 69 39 58 23 80 4046 40 24 17 56 87 40 73 6239 87 56 43 58 73”.92,25 56 82 17 56 25 40 6925 5625 17 58 38 27 39 73 46 40 99 92 17 276924 67 40 9573 56 23 56,38 73 5667 40 25 40 46 67 92 9580 56 17 43 58 6718 80 92 73 58 17 62 67 5639 73 56 10 73 6267 4099 27 82 58 46 58,80 56 39 73 40 1795 92 67 43 40 1792 2425 46 92 99 92 73 14 8267 40 8095 56 17 58 67 56 8767 56 43 58 67.

18.

67 58 26 19 88 2332 37 15 23 90 63 7146 63 26-63 2658 2463 23 3732 956763 15 32 88 58 26-6726 58 6741 16 24 90 63 52 30 2449 63 2688 26 37 23 38 23 16 6758 2390 26 41 90 63 68 24 58 58 26 7685 15 67 76 24 15 24.19 26 15 23 38 88 2663 15 32 88 58 24 2490 88 24 16 23 63 7163 23 37,46 63 26 41 5437 15 23 95 676758 2438 23 76 24 63 67 16 6768 26 68 90 24,67 58 23 46 2437 63 26 – 63 2658 24 19 16 32 85 54 4426 46 24 58 7141 54 90 63 15 2690 88 24 16 23 24 6390 26 26 63 68 24 63 90 63 68 32 11 30 67 2468 54 68 26 88 546724 30 24,46 24 19 2688 26 41 15 26 19 26,85 15 67 76 24 63 90 5237 16 24 68 24 63 23 63 71,68 15 23 95 67 58 2367 88 24 26 16 26 19 67 46 24 90 37 23 52,85 32 90 63 7188 23 95 243258 24 19 266758 2441 32 88 24 6388 26 37 23 38 23 63 24 16 71 90 63 68,58 263746 24 76 3258 23 7616 67 83 58 52 5237 16 24 68 24 63 23?63 26-63 26…49 63 26 6356 67 58 23 1685 26 38 68 26 16 52 1626 88 58 67 7676 23 73 26 7615 24 83 67 63 7158 24 90 37 26 16 71 37 2638 23 88 23 46.58 2441 54 16 2658 67 37 23 37 26 4437 15 23 95 67,90 26 68 24 15 83 24 58 58 26 4473 68 23 63 37 67 76 6763 15 24 58 67 15 26 68 23 58 58 54 76 6715 24 41 52 63 23 76 67-85 15 26 90 63 26-58 23 85 15 26 90 63 2626 37 15 24 90 63 58 54 2485 23 15 63 67 38 23 58 54,88 23 68 58 54 76-88 23 68 58 2619 15 26 38 67 68 83 67 2488 26 41 15 23 63 71 90 5268 90 2495 2488 2626 85 16 26 63 2367 76 85 24 15 67 23 16 67 38 76 23,90 67 15 24 46 7188 23 58 58 26 4441 23 38 54,90 68 26 1132 19 15 26 38 326837 26 58 29 2437 26 58 29 26 6868 54 85 26 16 58 67 16 67.58 23 19 15 52 58 32 16 6758 26 46 58 26 4485 26 15 26 44,85 26 15 24 38 23 16 6737 26 16 11 46 37 32,85 15 26 58 67 37 16 6758 2341 23 38 3285 26 8885 26 37 15 26 68 26 7676 15 23 37 23,38 23 16 26 95 67 16 679085 26 16 88 11 95 67 58 5476 67 58,85 26 90 63 15 24 16 52 16 6767 3819 15 23 58 23 63 26 76 24 63 26 6867,90 85 15 23 68 24 88 16 67 68 2615 24 83 67 68,46 63 2688 26 90 63 23 63 26 46 58 2658 23 85 23 37 26 90

63 67 16 67,38 16 26 15 23 88 58 2685 26 16 11 41 26 68 23 16 67 90 7188 24 16 26 7615 32 3790 68 26 67 736732 41 15 23 16 67 90 7168 26 90 68 26 52 90 6741 24 3876 23 16 24 44 83 24 19 2688 16 5290 24 41 5232 15 26 58 23.

19.

3492 45 25 90 30 25 7116 62 37 7155 7189 18 96 6255 85 22 71 11 6262 24 62 89 71 55 55 6285 55 16 71 92 71 24 55 62 11 62-90 30 49 30 24 55 18 7124 16 85 92 30 55 18 7152 37 85 55 24 18,49 30 92 62 22 25 3022 85 24 16 18 7392 58 89 30 67 71 25,90 58 89 55 30 2086 71 16 25 302416 45 89 85 25 62 1449 30 24 16 18-89 92 62 52 20 11 7168 16 6249 62 96 62 37 71 55 62,25 62 96 8562 5530 34 24 16 92 30 96 85 71 4692 62 52 62 14,49 30 92 3089 30 55 62 2525 62 55 24 71 92 34 62 34,49 62 22 30 16 18 9439 96 30 25 62 552462 89 71 90 90 30 92 30 37 85 34 30 45 86 85 14 8534 62 52 5816 30 89 96 71 16 25 30 14 85,24 16 30 92 18 9425 62 14 49 30 24,62 89 67 30 92 49 30 55 55 18 9439 62 55 30 92 85 258549 92 62 22 30 2052 92 71 89 71 52 71 55 19,85 90 62 89 96 85 22 30 34 67 30 203452 37 62 55 7124 16 19 45 -25 30 25 -71 11 62-16 30 1452 62 24 16 30 16 62 22 55 6262 49 18 16 55 62 11 6249 58 16 71 67 71 24 16 34 71 55 55 85 25 30,14 30 16 92 62 24 302455 71 14 30 96 18 1424 16 30 37 71 14,3462 52 85 5549 92 71 25 92 30 24 55 18 9452 71 55 1992 71 67 85 34 67 71 11 6249 62 85 24 25 30 16 1924 22 30 24 16 19 2055 3089 71 92 71 11 58.49 92 71 52 71 96 19 55 6224 25 92 62 14 55 18 7149 62 37 85 16 25 85,55 7124 49 62 24 62 89 55 18 7149 92 85 34 96 71 22 1934 55 85 14 30 55 85 7124 71 92 19 71 90 55 18 7311 92 30 89 85 16 71 96 71 94.

85 14 71 96 62 24 198562 92 58 37 85 71,3025 30 2537 71.49 92 85 96 85 22 55 18 7392 30 90 14 71 92 62 3462 73 62 16 55 85 22 85 9455 62 37,34 16 62 92 62 94,25 30 92 14 30 55 55 18 9467 34 71 94 46 30 92 24 25 85 9449 71 92 62 22 85 55 55 85 252452 34 58 14 2052 71 24 20 16 25 30 14 8549 92 85 22 85 55 52 30 96 62 34,3016 30 25 37 7149 62 16 71 92 16 18 9449 85 24 16 62 96 71 16-25 62 96 19 1689 62 96 71 7122 71 1452 34 30 52 46 30 16 85 96 71 16 55 71 11 6234 62 90 92 30 24 16 30,55 6258 73 62 37 71 55 55 18 948524 14 30 90 30 55 55 18 94-85 14 71 55 55 6216 30 25 62 7162 92 58 37 85 7114 62 37 55 6289 71 9062 24 62 89 18 7349 92 62 89 96 71 1449 92 85 62 89 92 71 24 16853449 62 92 16 62 34 18 7316 92 58 86 62 89 30 73.34 24 7149 92 62 52 58 14 30 55 62.90 52 71 67 55 85 7149 62 96 85 46 30 852489 62 96 19 67 85 1449 62 52 62 90 92 71 55 85 71 1462 16 55 62 24 20 16 24 202524 58 89 10 71 25 16 30 142430 34 16 62 14 30 16 85 22 71 24 25 85 1462 92 58 37 85 71 1455 3049 96 71 22 71,90 30 16 6255 7162 24 62 89 6255 30 34 62 92 62 22 71 55 55 18 9425 30 92 30 89 85 5585 96 8549 92 62 24 16 71 55 19 25 85 9449 85 24 16 62 96 71 163425 30 92 14 30 55 713490 52 71 67 55 85 7314 71 24 16 30 7324 22 85 16 30 45 16 24 2055 71 49 92 71 14 71 55 55 18 1430 16 92 85 89 58 16 62 1458 34 30 37 30 45 86 71 11 6224 71 89 2025 30 89 30 96 19 71 92 62,49 85 24 19 14 71 55 55 62 11 6292 30 90

92 71 67 71 55 85 2055 7116 92 71 89 58 45 1685,3462 89 86 71 14,49 62 52 62 90 92 71 55 85 9455 71 34 18 90 18 34 30 45 16,49 62 25 302485 7349 62 14 62 86 19 4555 7124 62 16 34 62 92 20 1622 71 11 62-16 62 55 71 90 30 25 62 55 55 62 11 62.

20.

16 7453 74 47 47 8531 85 66 74 29 58 55 7416 96 74 66 85 55 11 66 5896 11 12 91 74 74 50 96 11 12 91 85 49 53 58 8547 11 33 74 26 74 31 2329 47 85 2645 29 85 55 74 29,96 11 12 33 85 96 74 29,33 11 96 74 285829 74 12 96 11 47 55 11-66 85 68 28 74 29 35 53 28 5847 35 16 85 96 47 74 29 96 85 33 85 91 91 23 85,47 29 85 96 28 11 21 18 58 8591 74 29 85 91 61 28 58 3366 11 28 74 33,66 85 68 28 74 29 35 53 28 5829 96 85 33 85 9188 35 55 6166 5891 8529 55 74 96 74 4933 58 96 74 29 74 49,47 55 11 96 85 91 61 28 58 8511 29 55 74 50 35 47 23,68 96 74 33 11 31 91 23 8568 96 35 12 74 29 58 28 58-55 96 11 28 58,91 85 29 85 47 55 6174 55 28 35 31 1129 12 43 29 53 11 43 47 435891 85 29 85 31 74 33 7428 35 31 1147 16 85 53 58 29 53 11 4316 74 79 11 96 91 11 4333 11 53 58 91 11…31 74 29 74 66 61 91 7447 28 74 96 7474 9174 55 33 85 55 58 66,88 55 7447 96 85 31 5829 47 85 68 7438 55 74 68 7496 11 12 91 74 74 50 96 11 12 58 4391 8516 74 16 11 31 11 85 55 47 4391 5829 74 85 91 91 23 26,91 5816 74 66 58 45 85 49 47 28 58 2633 11 53 58 91,29 74 74 50 18 852974 28 96 85 47 55 91 74 47 55 43 26,91 11 47 28 74 66 61 28 7433 74 79 91 7447 35 31 58 55 6116 7455 74 33 35,88 55 7474 9129 58 31 85 664729 85 96 26 74 55 35 96 23,91 8591 11 50 66 21 31 11 85 55 47 4391 5833 11 66 85 49 53 58 2616 96 58 12 91 11 28 74 2988 96 85 12 29 23 88 11 49 18 58 91 23,28 11 28-55 74:33 74 50 58 66 61 91 23 2616 11 55 96 35 66 85 49,16 74 47 55 74 2991 1174 50 74 88 58 91 85,16 96 74 29 85 96 28 5831 74 28 35 33 85 91 55 74 29,12 11 47 55 11 29,50 66 74 28 16 74 47 55 74 29…91 58 88 85 68 7416 74 31 74 50 91 74 68 74.47 58 8545 85 91 91 74 8591 11 50 66 21 31 85 91 58 8591 8591 1153 35 55 28 3516 96 58 50 11 29 66 43 66 7474 16 55 58 33 58 12 33 11.

74 9116 74 47 33 74 55 96 85 6666 85 29 85 85-55 11 3374 5516 11 91 11 33 85 96 58 28 11 91 23 74 55 26 74 31 58 66 1111 47 62 11 66 61 55 58 96 74 29 11 91 91 11 4331 74 96 74 68 11,91 852916 96 58 33 85 9635 79 85,31 11 66 85 28 7491 8555 11 28 11 4374 79 58 29 66 85 91 91 11 43.5835 55 23 28 11 66 11 47 6174 91 1116 96 43 33 85 26 74 91 61 28 742955 74 55 47 11 33 23 4968 74 96 74 31 74 28,68 31 8558 2653 85 47 55 85 96 28 1131 74 66 79 91 1150 23 66 1129 23 49 55 58 91 1133 85 47 55 91 74 68 7491 85 66 85 68 11 66 11.

21.

40 77 40,29 75 5875 28 75!15 61 75 23 40 52 672929 54 52 1115 75 65 58 5415 84 40 29 54 61 67 28 75 77 7558 84 11 18 77 75 61 67 28 54 35 40,77 52 1115 75 37 11 84 11 52 54 28 11,28 4028 11 29 49 37 75 35 75 13,35 29 40 52 84 40 58 28 75 1335 54 84 15 54 65 28 75 1315 75 37

58 40 13 11 28 58 1129 75 90 29 49 72 40 11 58 37 8015 18 72 35 4029 84 11 13 11 2815 11 84 29 75 4113 54 84 75 29 75 41,5415 75 5211 1137 58 29 75 61 75 1337 61 75 82 11 28 4015 54 84 40 13 54 52 35 4054 9029 75 29 37 1118 8237 58 40 84 54 28 28 49 4680 52 11 84,35 40 35 54 13 5415 40 61 54 61 5461 11 5890 4037 58 7552 7515 75 80 29 61 11 28 54 8028 4035 75 28 29 11 41 11 84 1158 40 35 54 4629 75 5858 84 11 46 52 20 41 13 75 29 75 35-37 20 84 84 11 40 61 54 37 58 54 65 11 37 35 75 1137 75 65 11 58 40 28 54 11,11 37 61 5429 52 18 13 40 58 67 37 80,28 7513 11 37 58 28 49 46,28 40 52 7515 75 61 40 77 40 58 67,29 15 75 61 28 1118 37 58 84 40 54 29 40 11 58.54 33 7528 40 77 61 80 52 28 7515 75 35 40 90 49 29 40 11 5852 75 33 61 11 37 58 67,15 84 75 80 29 61 11 28 28 18 2054 4652 11 84 82 40 29 75 412915 11 84 29 18 2013 54 84 75 29 18 20:28 1835 40 3582 11,75 28 4075 58 15 84 40 29 54 61 4028 4011 29 84 75 15 11 41 37 35 54 4192 84 75 28 5826 11 61 49 4137 58 84 11 61 35 75 29 49 4133 40 58 40 61 67 75 285458 75 84 82 11 37 58 29 11 28 28 7515 75 84 29 40 61 4075 58 28 75 72 11 28 54 803777 11 84 13 40 28 37 35 75 4154 13 15 11 84 54 11 41,4029 52 75 33 40 29 75 3575 52 182972 11 37 58 28 40 52 26 40 58 75 1333 11 84 11 77 75 29 49 1133 40 58 40 84 11 5475 52 28 75 77 7554 9029 75 11 28 28 49 4615 75 84 58 75 2926 11 61 49 4652 29 4065 40 37 4015 40 61 54 61 5415 7558 75 4158 75 65 35 111877 75 84 54 90 75 28 58 40,77 52 1135 40 35 75 13 18 -58 7533 52 54 58 11 61 67 28 75 13 1829 75 80 35 1115 75 65 18 52 54 61 37 8077 11 84 13 40 28 37 35 54 4135 84 11 41 37 11 84…75 33 19 11 35 58 54 29 28 75 37 58 5484 40 52 5437 58 75 54 5818 58 75 65 28 54 58 67,65 58 7529 7529 58 75 84 18 2013 54 84 75 29 18 2090 52 11 72 28 54 41,15 18 37 58 675428 11 29 11 61 54 35 54 4129 75 11 28 28 75-13 75 84 37 35 75 4192 61 75 5829 13 11 37 58 113737 75 20 90 28 54 35 40 13 5415 40 58 84 18 61 54 84 75 29 40 6115 84 54 61 11 77 40 20 23 54 1129 75 52 495415 40 84 1884 40 9029 84 75 52 1133 4952 40 82 1137 58 84 11 61 80 6115 7528 40 37 58 75 80 23 54 13,4028 1115 84 54 29 54 52 11 29 72 54 13 37 8015 75 52 29 75 52 28 49 1361 75 52 35 40 1335 84 54 77 37-13 40 84 54 28 11.

22.

56 9631 57 87 3756 7584 77 87 24 96 73 68 75,56 7550 37 16 42 68 77,7720 73 3737 49 56 77 39 77 87 37,39 73 3712 84 9616 91 64 56 91 87 37.75 56 84 73 16 91 68 94 75 7531 57 87 7544 16 37 84 73 577556 96 49 77 73 96 14 87 75 12 57:96 84 87 7556 7744 37 28 37 68 37 56 56 75 68 9656 96 7356 7550 37 16 42 68 77,56 7584 77 87 24 96 73 68 75,96 84 87 7573 77 2673 37 87 41 68 3784 77 87 24 96 73 68 7731 96 4950 37 16 42 68 7775 87 7550 37 16 42 37 6831 96 4984 77 87 24 96 73 68 75-56 9673 3739 73 3756 9612 64 37 28 75 73 41,56 3728 77 35 9656 9644 16 75 31 87 75 35 77 73 41 84 61.12 84 9644 16 96 35 56 75 9616 77 84 68 87 77 28 5787 96 73 61 736839 96 16 73 91,1235 75 49 56 4184 87 96 28 91 96 7356 96 26 96 28 87 96 56 56 3744 16 96 73 12 37 16 61 73 4149 77 44 77 84 56 37 1412 77 16 75 77 56 73.56 91 35 56 3768 77 6826 37 35

56 3731 57 84 73 16 96 9637 73 84 82 28 7784 26 77 73 57 12 77 73 41 84 61,91 31 75 16 77 73 41 84 616839 96 16 73 37 12 37 1426 77 73 96 16 7575 4950 37 16 37 28 68 77,12 84 73 91 44 77 96 731284 75 87 9149 77 44 77 84 56 37 1412 77 16 75 77 56 7337 73 64 37 28 77…

12 96 84 4137 68 16 91 35 77 82 22 75 1426 75 1612 56 96 49 77 44 56 3784 73 77 8756 9644 16 37 84 73 3739 91 35 75 26-12 16 77 35 28 96 31 56 57 26.44 37 28 37 49 16 96 12 77 73 4184 87 96 28 37 12 77 87 3712 84 96 647512 84 61.44 41 82 22 75 6444 75 12 3784 37 87 28 77 73 75 68 37 12-1273 37 26,39 73 3737 56 7556 9684 37 87 28 77 73 75 68 7512 37 12 84 96,7750 16 91 44 44 7749 77 64 12 77 73 7775 4912 37 96 56 56 37 1468 37 56 73 16 16 77 49 12 96 28 68 75,44 16 96 84 73 77 16 96 87 37 50 3750 37 84 73 75 56 75 39 56 37 50 3764 26 57 16 61-1273 37 26,39 73 3737 5612 37 12 84 9656 9644 37 16 73 41 9675 87 7512 87 77 28 96 87 96 94,75 87 7573 377528 16 91 50 37 961237 28 56 37 2687 75 94 96,7744 37 87 68 37 12 56 75 6849 28 96 42 56 96 1473 77 14 56 37 1444 37 87 75 94 75 75.12 84 9612 37 49 26 37 35 56 37,68 37 50 28 7791 84 87 37 12 87 96 56 56 37 50 3784 75 50 56 77 87 7756 96 7356 7791 84 87 37 12 87 96 56 56 37 2626 96 84 73 96.

23.

22 10 75 6247 1074 10 24 88 47 39 35 66 15 75 58 10 47 64 53 5385 66 35 10 69 62 28 10 24 5366 49 53 47 47 10 49 64 10 58 3928 22 88 17 10 79 47 88 1547 66 22 53.4447 10 85 17 10 28 53 24 75 443551 66 75 58 53 47 53 64 88.35 10 3572 62 28 10 24 6647 8817 10 69,4466 80 37 80 10 2469 49 88 75 3937 74 53 17 66 58 28 66 17 88 47 53 885385 66 35 66 15,22 37 28 75 58 28 10,35 66 58 66 17 62 8853 75 85 62 58 62 28 10 88 79 39,66 35 10 69 10 28 79 53 75 392849 10 28 47 6669 47 10 35 66 74 62 4274 88 75 58 10 42.79 53 17 66 35 53 8828 66 17 66 58 1072 62 24 5317 10 75 85 10 42 47 37 58 62,37 75 10 49 39 72 1037 58 66 47 37 24 102875 37 74 88 17 35 10 42.4428 66 79 88 242842 66 24 24,51 49 8858 37 74 10 47 47 62 8869 88 17 35 10 24 1069 62 72 35 6666 58 17 10 31 10 24 5364 28 88 58 625349 88 58 10 24 5353 47 58 88 17 39 88 17 10.37 49 53 28 53 58 88 24 39 47 66,47 6642 66 69 44 53 4747 8837 69 47 10 2474 88 47 44.66 4785 17 66 58 44 47 37 2417 88 51 53 75 58 17 10 64 53 66 47 47 37 9735 47 53 51 37.4428 69 44 2417 37 22 35 37,66 72 7 41 03 54 73 7 2485 88 17 662872 17 66 47 69 66 28 37 9722 88 17 47 53 24 39 47 53 64 3753,75 35 24 66 47 53 28 79 53 75 3947 10 49 17 10 75 35 17 62 58 62 74 5375 58 17 10 47 53 64 10 74 53,75 58 66 24 35 47 37 24 75 447585 88 17 28 66 1553 6974 47 66 31 88 75 58 28 1047 88 66 31 53 49 10 47 47 66 75 58 88 15,35 66 58 66 17 62 8885 66 49 75 58 88 17 88 51 10 24 5374 88 47 4425 58 66 1547 66 22 39 97.74 66 8853 74 44,42 66 17 42 8824 37 53 7572 66 17 42 88 75,72 62 24 6647 10 22 88 17 58 10 47 662835 47 53 51 88,5322 88 17 47 53 24 1088 80 8847 8837 75 85 88 24 5328 62 75 66 42 47 37 58 39.

24.

6152 16 36 26 14 5416 45 24 29 4595 1129 36 95 86 36 16 29 451452 49 75 36 4797 36 93 95 61 54 26 6197 3626 86 45 97 49 95 41 29 11 47.93 49 30 61 86 95 11 93 56 11 86 83 8995 36 47 49 1695 11 37 36 93 14 54 26 6195 1130 86 36 16 36 4721 86 11 33 49,2636 29 95 11 47 1495 1130 95 45 86 16 49 95 95 14 8993 30 36 16 14 29,33 11 54 29 14 891471 11 52 16 36 19 49 95 95 83 89,36 52 95 49 26 49 95 95 83 8952 11 54 98 26 86 16 11 93 36 89;75 93 49,29 11 2997 36 47 95 14 54 36 26 4147 95 49,26 86 36 61 54 1197 54 61 33 95 11 6126 29 11 47 49 89 29 11.21 86 3652 83 54 1126 11 47 11 6152 36 54 41 19 11 6129 36 47 95 11 86 1130 75 36 26 86 14 95 14 56 49.6186 36 54 29 95 45 5493 30 49 16 41,36 95 1197 36 93 93 11 54 11 26 41.97 36 93 97 36 86 36 54 29 36 4775 36 16 49 54 1154 98 26 86 16 11.3049 4952 49 71 33 11 54 36 26 86 95 36 4726 30 49 86 496145 71 95 11 5426 49 52 61.95 1145 71 29 36 8933 49 54 49 71 95 36 8929 16 36 30 11 86 1454 49 33 11 5461,97 36 26 86 11 16 49 30 19 14 891436 52 16 98 71 75 19 14 89,1416 11 71 75 54 61 93 83 30 11 5454 49 97 95 14 95 4595 1197 36 86 36 54 29 49.6145 26 54 83 19 11 5475 36 54 36 26.95 4926 36 30 26 49 4747 36 89-52 49 7136 52 49 16 86 36 95 36 30,95 49 97 16 14 61 86 95 83 89,97 36 37 36 33 14 8995 1147 11 75 95 14 86 36 78 36 95 95 45 9871 11 97 14 26 41.

-45 93 14 30 14 86 49 54 41 95 36,-26 29 11 71 11 5436 95,-95 11 2693 30 36 491447 8336 93 95 36.30 97 16 36 24 49 47,30 3626 95 4995 14 24 86 3695 4926 97 36 26 36 52 95 3630 83 71 30 11 86 4145 93 14 30 54 49 95 14 49.6116 36 52 29 3626 97 16 36 26 14 54:

-71 95 11 24 14 86,30 26 4921 86 3626 36 95?

-97 16 14 24 49 4797 36 26 54 49 93 95 14 8926 36 95.-33 49 26 86 36 4736 9597 36 29 11 71 11 5495 1197 45 26 86 36 89 97 45 71 83 16 49 29,

26 86 36 61 30 19 14 8995 1147 16 11 47 36 16 95 36 8929 16 83 19 29 4995 36 24 95 36 75 3626 86 36 54 14 29 11.-86 49 52 49 97 16 14 93 49 86 26 61,95 11 30 49 16 95 36 49,45 30 14 93 49 86 4147 95 36 33 49 26 86 30 3626 95 36 30,97 16 49 33 93 4924 49 4793 36 52 49 16 49 19 41 26 6193 3621 86 36 8995 36 24 14.29 11 29 36 4926 49 75 36 93 95 6124 14 26 54 3697 3686 30 36 49 47 4529 11 54 49 95 93 11 16 98?

25.

48 84 13 3394 13 48 42 33 46 82,84 13 82 4894 82 46 84 33 4213 88 82 84 16 46 1625 8250 17 481342 61 37 78 50 511682 42 13 82 84 16 46 1650 48 17 341376 82 25 82 1672 82 46 48 69 17 82 28 82,28 84 4851 75 4875 84 33 46 1646 33 84 33 17,75 33 37 82 13 17 341638 48 37 17 16 46 33.82 1713 58 94 25 33 69 58 13 33 4676 82 75 48 46 33 17 16 34,163476 82 25 33 69 58 13 33 4648 50 5113 94 48,38 42 8217 1648 94 42 781350 16 37 48.1376 37 16 28 82 37 64 17 4817 48 17 33 13 16 94 42 17 82 28 8272 58 46 8294 82 72 37 33 17 8213 94 48,38 42 8284 82 13 48 46 82

94 78 76 82 13 16 84 33 42 7851 75 4851 94 82 76 64 16 501638 42 8269 37 34 4217 58 17 4869 84 37 33 13 94 42 13 51 61 21 16 48:28 82 37 82 84 33,75 33 37 25 16 481688 82 46 82 84 17 58 4894 42 37 33 17 58,94 82 25 37 82 13 16 21 33,94 25 37 58 42 58 481369 48 50 17 58 8828 46 51 72 16 17 33 88,72 82 37 82 69 84 34 21 16 4850 82 37 3425 82 37 33 72 46 16,82 37 51 84 16 3413 82 91 17 58,16 17 94 42 37 51 50 48 17 42 5813 37 33 38 48 13 33 17 16 341650 51 69 58 25 16,76 46 48 17 16 42 48 46 78 17 58 8875 48 17 21 16 17,17 48 76 82 84 13 16 75 17 58 4869 13 48 69 84 581676 46 33 17 48 42 58,25 37 33 94 25 16,25 82 42 82 37 58 50 1676 82 46 78 69 51 61 42 94 3417 48 13 48 37 17 58 48,25 82 28 84 3376 16 64 51 4294 13 82 1650 48 37 69 25 16 48

25 33 37 42 16 17 58,37 33 94 42 48 17 16 341650 16 17 48 37 334 65 894 8213 94 48 50 1616 8894 82 25 37 82 13 48 17 17 58 50 1669 33 50 48 38 33 42 48 46 78 17 58 50 1694 13 82 91 94 42 13 33 50 16,94 48 37 48 72 37 34 17 58 8833 17 28 48 46 82 13,38 48 9188 46 48 72-88 13 33 46 331676 37 48 13 82 69 17 48 94 48 17 16 4828 82 94 76 82 84 33,37 33 69 84 33 38 5117 33 28 37 33 841364 25 82 46 33 88,19 16 28 51 37 5876 42 16 981698 33 37 48 91,88 37 33 17 34 21 16 48 94 341394 33 50 82 5094 48 37 84 98 4876 16 37 33 50 16 84,42 48 17 7872 58 25 33,17 3325 82 42 82 37 82 5076 82 25 82 16 42 94 3469 48 50 46 34,1637 58 72 58,17 3325 82 42 82 37 82 9194 42 82 16 42

72 58 25,76 51 94 42 58 17 1613 94 48 50 16 46 82 94 42 16 13 82 28 8272 82 28 33.82 1751 13 16 84 48 4613 48 21 1617 48 82 76 16 94 51 48 50 58 48,42 33 25 16 48,25 33 2551 46 16 98 58,82 94 13 48 21 48 17 17 58 4828 33 69 82 13 58 50 1637 82 75 25 33 50 16,1625 16 42 33,25 82 42 82 37 58 9151 50 16 37 33 48 4276 37 1669 13 51 25 33 8838 48 46 82 13 48 38 48 94 25 82 28 8228 82 46 82 94 33.

Пример решения самостоятельной работы

15 вариант

Скользящая перестановка

Текст для расшифровки: _ПАРИИВИАРЗ_БРА_ИСТЬЛТОЕК

Текст содержит 25 символов, т.е. записываем его в таблицу 5*5.

_	П	А	Р	И
И	В	И	А	Р
З	_	Б	***Р***	***А***
_	И	С	***Т***	***Ь***
Л	Т	О	***Е***	***К***

Расшифровку следует проводить меня порядок столбцов.

Воспользуемся таблицей сочетаемости букв. 4 и 5 столбцы идут друг за другом, т.к. биграммы РА, ТЬ и ЕК наиболее распространенные. 2 и 4 столбец идут друг за другом, т.к. биграммы ИТ и ТЕ тоже распространены. По выше перечисленным признакам не трудно догадаться, что столбцы будут располагаться в следующем порядке: 2,4,5,3,1. И зашифрованной фразой будет: ***При_аварии_разбить_стекло*.**

В данном случае дешифровать текст можно было обычным методом перебора, не обращаясь к таблице сочетаемости букв.

Шифр двойной перестановки

Текст для расшифровки: ЗШАФИПРАЛОЕНЖ_ОЬН_ДАРВОНА.

Текст содержит 25 символов, т.е. записываем его в таблицу 5*5.

З	Ш	А	Ф	И
П	Р	А	Л	О
Е	Н	Ж	_	О
Ь	Н	_	Д	А
Р	В	О	Н	А

Расшифровку следует проводить меня порядок столбцов и строк.

Глядя на зашифрованный текст по первым пяти символам можно сразу предположить, что столбцы меняются следующим образом: 1,3,2,5,4.

З	А	Ш	И	Ф
П	А	Р	О	Л
Е	Ж	Н	О	_
Ь	_	Н	А	Д
Р	О	В	А	Н

Глядя на вторую таблицу можно, также, без труда определить порядок строк: 2,4,3,1,5.

Расшифрованный текст: Пароль_надежно_зашифрован.

Шифр простой замены

Расшифрованный текст:

ЧЕМ ДАЛЬШЕ, ТЕМ СИЛЬНЕЕ ОН ЧУВСТВОВАЛ НЕШУТОЧНОЕ РАЗДРАЖЕНИЕ, ПОРОЮ ПЕРЕХОДИВШЕЕ В ПРИЛИВЫ ЗЛОСТИ-ОТТОГО, ЧТО ОНИ ЧЕТВЕРО СУТОК, ОБРАТИВШИСЬ В ЗРЕНИЕ И СЛУХ, ТОРЧАЛИ В ЧАЩОБЕ, КАК ДИКИЕ ОБЕЗЬЯНЫ ИЗ БРАЗИЛИИ, ОТТОГО, ЧТО ПОДВЕРНУЛСЯ ТУПОЙ КАЙМАН, С ОДИНАКОВЫМ УСЕРДИЕМ НАПАДАВШИЙ И НА ЛЕСНУЮ СВИНЬЮ, И НА ОТЛИЧНОГО ПАРНЯ С ДРУГОГО КОНТИНЕНТА А В ЭТО ВРЕМЯ ТЕ, НА БАЗЕ, ЖИЛИ В СВОЕ УДОВОЛЬСТВИЕ, СПАЛИ НА ЧИСТЕНЗЫЗИХ ПРОСТЫНКАХ В КОНДИЦИОНИРОВАННОЙ ПРОХЛАДЕ, ПРИНИМАЛИ ДУШ, ЖРАЛИ НА ЗАВТРАК ФРУКТЫ, ДЖЕМ И БИФШТЕКСЫ В ТРИ ПАЛЬЦА ТОЛЩИНОЙ, И ОКНА ТАК УЮТНО СВЕТИЛИСЬ, И МУЗЫКА ИГРАЛА, И ФУТБОЛ ПО ТЕЛЕВИЗОРУНИЧЕГО В ЭТОЙ ЗЛОСТИ НЕ БЫЛО ПЛОХОГО, НАОБОРОТ - ТАКОЙ НАСТРОЙ КАК РАЗ И ПРИДАЕТ БОЕВОГО КУРАЖА…

А ПОТОМ ПРИШЕЛ КОНЕЦ И ПОСТОРОННИМ МЫСЛЯМ И БЕЗДЕЛЬЮ. МОРСКОЙ ЗМЕЙ НАКОНЕЦ-ТО ПОДАЛ ЗНАК, КОТОРОГО ОНИ ЖДАЛИ ЧЕТВЕРО СУТОК, И ЭТО БЫЛО СЛОВНО МЕДНЫЙ РЕВ БОЕВОЙ ТРУБЫ, ЭТО ОЗНАЧАЛО, ЧТО НАЧАЛИСЬ РАБОТЫ, И НИЧЕГО УЖЕ НЕ ИЗМЕНИТЬ, НЕ ОСТАНОВИТЬ, НЕ ПЕРЕИГРАТЬ…

ПРИЛОЖЕНИЕ 3.
ЗАДАНИЯ НА САМОСТОЯТЕЛЬНУЮ РАБОТУ

"Криптоанализ шифротекстов полученных методом гаммирования"[27]

Заданием для данной лабораторной работы является отыскание открытого текса зашифрованного методом гаммирования при помощи сдвигового регистра с линейной обратной связью. Для сдачи работы необходимо предоставить текст файла отчета. **После получения верного открытого текста необходимо по найденной части ключа вручную определить положение отводов в регистре при помощи алгоритма Берлекэмпа-Месси** и представить таблицу вывода для проверки. Необходимо заметить, что это является обязательным шагом уже после нахождения верного открытого текста. Для промежуточных нахождений положений отводов в регистре алгоритм Берлекэмпа-Месси использовать необязательно, можно воспользоваться методом, основанным на нахождении обратной матрицы.

Общее описание лабораторной работы

Целью работы является приобретение практических навыков криптоанализа аддитивных шифров.

Результатом работы является получение осмысленного открытого текста из зашифрованного сообщения при помощи учебной программы, называемой «Криптоанализ аддитивного шифра LSR». Лабораторная работа представляет собой исполняемый файл LSR.exe (учебная программа) и набор из 25 вариантов задания (зашифрованный текст).

Общий вид окна учебной программы

Программа LSR.exe представляет собой исполняемый файл, который запускается двойным нажатием на пиктограмму

Рис П3.1. Пиктограмма LSR

После чего на экране появляется диалоговое окно, представляющее собой окно лабораторной работы (рабочее окно).

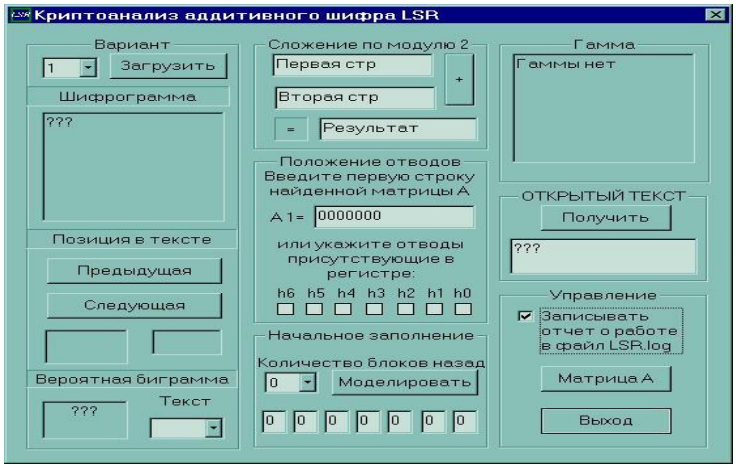


Рис П3.2. Внешний вид окна LSR

Рабочее окно лабораторной работы разделено на 7 блоков, которые представляют собой отдельно последовательно выполняемые шаги лабораторной работы и блок управления. Работа последующих блоков базируется на результатах работы предыдущих.

Кратко перечислим и поясним эти блоки:

- Вариант. Блок предназначен для загрузки внешнего файла варианта в соответствии с выбранным номером, отображения текста задания (подзаголовок Шифрограмма) в зашифрованном виде в битовом представлении и выбора одной из наиболее вероятных биграмм (подзаголовок Вероятная

биграмма). Кроме того в блоке находятся кнопки управления «Предыдущая» и «Следующая» для перехода к соответственно предыдущий и последующей позиции, которая является вероятной позицией для биграммы;

- Сложение по модулю два. Блок предназначен для отыскания части вероятной гаммы путем сложения по модулю два битового представления вероятной биграммы и битового представления выбранной части зашифрованного текста;
- Положение отводов. Блок предназначен для ввода строки матрицы А, которая определяет положение отводов в регистре, или указания положения отводов путем заполнения соответствующих полей. **Положение отводов определяется студентом используя подпрограмму**, которая вызывается нажатием кнопки «Матрица А». **Выполняющий составляет вектора S(1),…,S(8)** и подпрограмма, используя метод основанный на нахождении обратной матрицы (с помощью метода Гаусса), находит матрицу обратную к X1 и матрицу А (значение первой строки, которой необходимо для определения положения отводов).
- Начальное заполнение. Блок предназначен для поиска начального заполнения выбранного регистра в соответствии с частью вероятной гаммы. Блок позволяет моделировать работу регистра на некоторое число блоков назад (1 блок=8 шагов) и получать таким образом нужное начальное заполнение, которое так же представлено в этом блоке;
- Гамма. Блок предназначен для получения и отображения гаммы, которая получается используя вид регистра и его начальное заполнение;
- Открытый текст. Блок необходим для получения текстового представления открытого текста, который получен сложением шифрованного текста и гаммы по модулю 2 и последующей перекодировкой;
- Управление. Блок является вспомогательным. Он предназначен для управлением автоматическим созданием файла отчета, нахождения матрицы А (имеется кнопка «Матрицап А», вызывающая подпрограмму поиска матрицы А) и для завершения работы (в данном блоке имеется кнопка «Выход», предназначенная для завершения лабораторной работы и закрытия рабочего окна).

Требования к размещению файлов

Для запуска лабораторной работы необходимо наличие файла LSR.exe, для ее выполнения нужен файл соответсвующего варианта (всего 25 различных вариантов $\Rightarrow$ 25 файлов). Файлы вариантов должны располагаться в том же каталоге, что и LSR.exe. Заметим, что файл отчета lsr.log будет создаваться так же в том же каталоге.

Необходимые знания

Для успешного выполнения лабораторной работы требуются базовые знания в области аддитивных шифров, в частности общие понятия о принципе действия линейного сдвигового регистра, а также пользовательские навыки работы с ОС Windows. Изложенный ранее краткий теоретический материал является достаточным для выполнения лабораторной работы.

Загрузка варианта

Каждому студенту преподавателем назначается вариант, и в соответствии со своим вариантом студент выполняет лабораторную работу.

Для загрузки соответствующего варианта предназначено поле выбора и кнопка «Загрузить» в верхней части блока «Вариант»

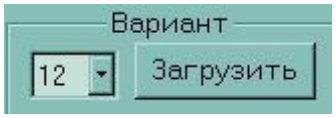


Рис. П3.3.Часть блока вариант

Выполняющий работу (студент) выбирает один из предложеных 25 номеров варианта и нажимает кнопку «Загрузить»

Рис. П3.4. Кнопка «Загрузить»

После нажатия кнопки в поле для чтения «Шифрограмма» появляется зашифрованный текст в битовом представлении или возникает сообщение об ошибке (см. Сообщения выдаваемые в процессе работы). Задачей выполняющего является расшифровка данного текста.

Рис. П3.5. Поле для чтения «Шифрограмма»

В поле для чтения «Шифрограмма» располагается двоичное представление зашифрованного текста. Каждые восемь бит в совокупности представляют собой одну закодированную букву. Ознакомиться с кодировкой можно в Приложении 1.

Всего в поле для чтения «Шифрограмма» представлено 16 закодированных букв (128 бит), таким образом зашифрованный текст представляет собой слово или фразу из 16 символов.

Выбор вероятных составляющих

Поскольку для дальнейшего расшифрования текста (а именно отыскания начального заполнения еще неопределенного регистра) нам требуется 2*L бит гаммы (L – разрядность регистра, в работе n=7 ⇒ требуется 14 бит), то следующим шагом в выполнении работы является определение вероятной биграммы и ее положения в зашифрованном тексте. Для этого предназначено поле выбора «Вероятная биграмма»

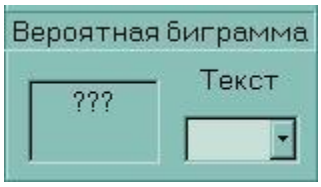


Рис. П3.6. Поле «Вероятна биграмма»

На выбор выполняющему работу предлагается 8 биграмм (ЕН, ЕТ, НА, НИ, ПР, РА, СТ, ТО). Эти биграммы являются наиболее вероятными в русском языке, следовательно хотябы одна из них должна содержатся в зашифрованном сообщении (см. полную таблицу вероятностей биграмм в тексте в Приложении 2).

После выбора в поле «Текст» выроятной биграммы в соседнем поле для чтения появится битовое представление этой биграммы, кроме того тоже битовое представление появится в поле ввода «Вторая стр» блока «Сложение по модулю 2».

Рис. П3.7. Выбранная биграмма

На этом выбор вероятной биграммы закончен. Теперь необходимо определить ее положение в тексте. Будем последовательно перебирать все возможные положения данной биграммы при помощи двух управляющих кнопок «Предыдущая» и «Следующая» (подзаголовок Позиция в тексте).

Рис. П3.8. Позиция в тексте и управляющие кнопки

При нажатии на кнопку «Следующая» или «Предыдущая» в левом поле рис 7 появится часть шифрограммы, которая соответствует позициям, номера которых появятся в правом поле для чтения. Одновременно с этим поизойдет заполнение первого поля в блоке «Сложение по модулю 2» содержимым левого поля.

После того как выбрана биграмма и ее положение (то есть заполнены два верхних поля в блоке «Сложение по модулю 2»), в поле «=» блока «Сложение по модулю 2» появится результат сложения.

На этом определение вероятного местоположения вероятной биграммы и части вероятной гаммы закончен. Таким образом мы имеем предполагаемую биграмму, ее предполагаемое местоположение и, вероятно, часть ключа. Дальнейшие шаги покажут нам правильность или ошибочность выбора предполагаемых компонентов.

Нахождение вероятной части ключа

Данный шаг необходим для ручного сложения по модулю 2 собственных компонентов, то есть на предыдущем шаге вероятная часть ключа была найдена автоматически. Таким образом данное описание можно пропустить.

Для определения вероятной части ключа мы будем использовать блок «Сложение по модулю 2» с внесенными в него на предыдущем шаге начальными данными (вероятной

биграммой и соответствующей ей части зашифрованного текста).

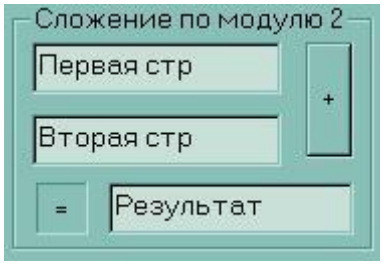


Рис. П3.9. Блок «Сложение по модулю 2»

Поскольку для определения вероятной части гаммы достаточно простого сложения по модулю два вероятной биграммы и соответствующей ей части зашифрованного текста, то для получения необходимо нажать кнопку «+».

Рис. П3.10. Кнопка «+» (сложить)

После чего в поле «=» появится искомая часть вероятной гаммы.

Рис. П3.11. Поле «=» - результат сложения

Таким образом мы определили 16 бит ключевой последовательности, которые нужны нам для отыскания положения отводов в регистре, начального заполнения регистра и, как следствие, всей гаммы и открытого текста. Строго говоря, 2 бита из этой последовательности являются избыточными, поскольку для определения положения отводов нужно 2*7=14 бит, а для получения начального заполнения всего 7 бит, но в связи с выбранной кодировкой символов приходится учитывать и эти 2 бита.

Определение положения отводов

Одним из ключевых шагов в выполнении работы является нахождение положения отводов в регистре. В данной работе предполагается определение положения отводов при помощи метода основанного на нахождении обратной матрицы методом Гаусса, используя подпрограмму для обращения матрицы и нахождения матрицы А.

Для определения положения отводов выполняющему необходимо вызвать подпрограмму нахождения матрицы А, нажатием кнопки «Матрица А».

Рис. П3.12. Кнопка «Матрица А»

Затем в появившемся диалоговом окне необходимо заполнить поля представляющие собой поля для ввода векторов-столбцов S(1)…S(8) (см. Теоретическое введение).

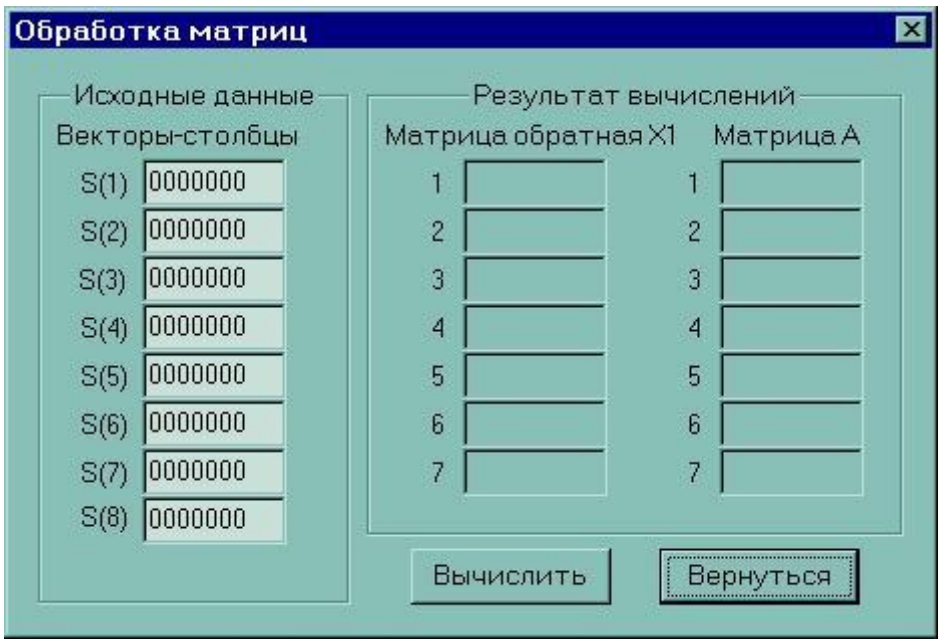


Рис. П3.13. Окно подпрограммы для нахождения матрицы А

После корректного заполнения вышеуказанных полей, необходимо нажать кнопку «Вычислить» и в соответствующих полях окна подпрограммы появятся строки соттветствующие матрицам X^{-1} и А.

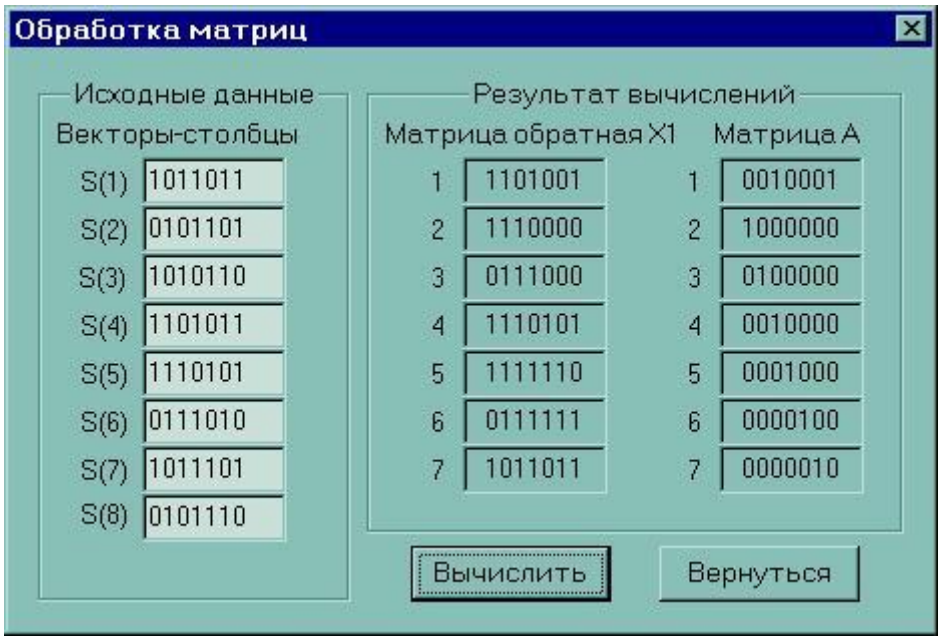


Рис. П3.14. Результат работы после нажатия на кнопку «Вычислить»

Следует отметить, что **матрица А должна иметь специальный вид**: первая строка – определяет положение отводов, в остальных строках под главной диаганалью находятся единицы, остальные нули. Если найденная матрица отличается по виду от вышеописанной, то была допущена ошибка на ранних шагах (например выбрана ошибочная биграмма). Строка 1 подраздела «Матрица А» является определяющей, то есть именно ее вид определяет положение отводов и именно ее необходимо заносить в поле А1 блока положение отводов, после выхода из подпрограммы (нажатием кнопки «Вернуться»).

Рис. П3.15. Блок положение отводов

Поскольку для определение отводов существует, по крайней мере, два способа определения положения отводов, то возможно 2 способа заполнения положения отводов. Рассмотрим эти способы.

1) Если отводы были определены при помощи нахождения обратной матрицы, то удобно ввести в поле «A1=» первую строку матрицы A, что будет являться заданием положения отводов и будет продублировано в нижней части блока.

Регистр по условию лабораторной работы является 7-разрядным, то есть первая строка матрицы A является последовательностью из 7 бит, каждый из которых говорит о наличии (если бит равен 1) или отсутствии (если бит равен 0) отвода в регистре.

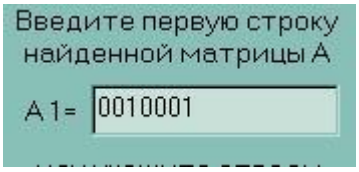


Рис. П3.16. Строковое задание положения отводов

2) Если положение отводов были найдены другим способом, то удобно непосредственно указать отводы присутствующие в регистре, то есть активировать чек-бокс соответствующий присутствующему отводу, введенные данные продублируются в строке «A1=»

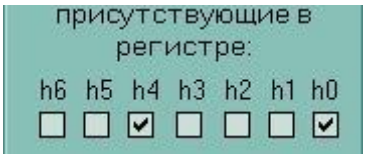


Рис. П3.17. Непосредственный выбор отводов

Необходимо внимательнее подходить к проблеме поиска отводов в регистре, так как неправильное определение положения отводов влечет за собой неправильный результат.

Поиск начального заполнения

Для того, чтобы расшифровать текст необходима гамма такой же длины как и зашифрованный текст. Для получения гаммы нам нужно знать начальное заполнение регистра. Для определения начального заполнения в лабораторной работе используется блок «Начальное заполнение».

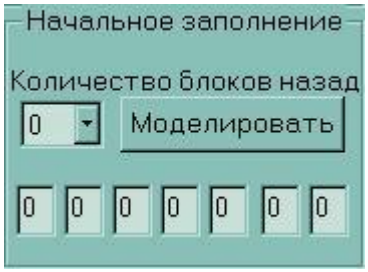


Рис. П3.18. Блок «Начальное заполнение»

Поскольку для получения начального заполнения необходимо промоделировать обратную работу регистра, то существует кнопка «Моделировать», при нажатии на которую происходит обратное моделирование работы регистра на заданное количество шагов, которое задается в поле выбора «Количество блоков назад».

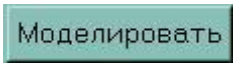


Рис. П3.19. Кнопка «Моделировать»

Поскольку нецелесообразно моделировать обратную работу на число шагов не кратное 8 (так как 1 символ закодирован 8 битами), то число шагов заменено числом блоков. То есть 1 блок = 8 шагов, и при моделировании на 1 блок производится обратная работа на 8 шагов. Выбор количества блоков назад ограничен 14 (для обеспечния отсутствия цикличности).

Выбор количества блоков на которое производится обратное моделирование важен для правильности определения начального заполнения. Количество блоков для обратного моделирования является первой цифрой в номере позиции вероятной биграммы (см. Подзаголовок «Позиция в тексте» блока «Вариант» правое поле для чтения). То есть если позиция представлена как 3-4 (то есть вероятная биграмма находится на позиции 3 и позиции 4), то обратное моделирование должно производиться на 3 блока назад.

После нажатия на кнопку «Моделировать» автоматически производится поиск начального заполнения регистра. Для этого используются первые 7 бит строки «=» блока «Сложение по модулю 2» и регистр из блока «Положение отводов» (точнее положение его отводов). Полученный результат отображается в схематичном представлении ячеек регистра, заполненных нулями или единицами.

Рис. П3.20. Схематичное представление ячеек регистра

Кроме того для удобства выполнения работы сразу после нажатия кнопки «Моделировать», если не произошло никаких ошибок заполняются поля в блоках «Гамма» и «Открытый текст». Таким образом после нажатия кнопки «Моделировать» **при правильном выборе вероятной биграммы, ее положения в тексте и правильного определения положения отводов получается открытый текст.**

Получение гаммы

Для расшифрования сообщения нам необходимо получить гамму, которая использовалась при зашифровке. Этот шаг выполняется автоматически при нажатии на кнопку «Моделировать» из блока «Начальное заполнение». Для контроля за правильностью гаммы предназначен блок «Гамма»

Рис. П3.21. Блок «Гамма»

Гамма представляет собой последовательность 128 двоичных символов, которые выводятся в поле для чтения «Гамма». Данная последовательность используется для последующего сложения по модулю 2 с шифрограммой и получения открытого текста в битовом представлении.

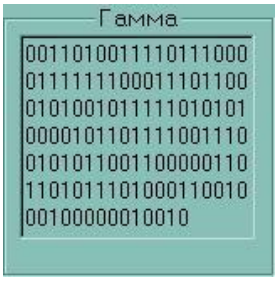


Рис. П3.22. Поле для чтения «Гамма»

Получение открытого текста

Открытый текст получается автоматически при нажатии на кнопку «Моделировать» блока «Начальное заполнение», однако для контроля предусмотрены дополнительный возможности.

Открытый текст представляется в программе перекодированным из битовой последовательности в символы и для этого используется блок «ОТКРЫТЫЙ ТЕКСТ».

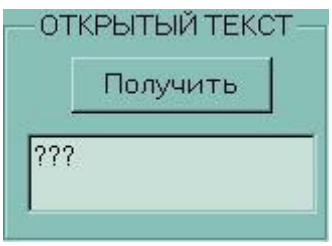


Рис. П3.23. Блок «Открытый текст»

Для получения открытого текста достаточно нажать кнопку «Получить». Программа автоматически произведет сложение гаммы и зашифрованного текста, а потом перекодирует битовый текст в символьный.

Рис. П3.24. Кнопка «Получить»

В результате в поле ввода появится некоторый текст, который либо представляет собой осмысленное сообщение (тогда работа успешно завершена), либо непонятный набор символов (увы, придется повторить некоторые шаги заново). Во втором случае наиболее вероятным местом ошибки является неправильно выбранное количество блоков для обратного моделирования (как следствие неправильные начальное заполнения и гамма). Если же вы уверены в своих действиях по выбору количества блоков, тогда неверно выбрана биграмма или ее положение (то есть придется вернуться к п 5.3.4), кроме того возможно неверное определение положения отводов (придется вернуться к п 5.3.5)

Если полученный открытый текст устраивает выполняющего то работа завершена.

Отчет о проделанной работе

Для контроля за выполнением работы предусмотрено специальное средство – отчет о проделанной работе. В данной лабораторной отчет представляется в форме файла отчета: файл отчета – необходим для предоставления проверяющему (преподавателю);

Форма отчета включаются путем выбора соответствующего элемента в блоке «Управление».

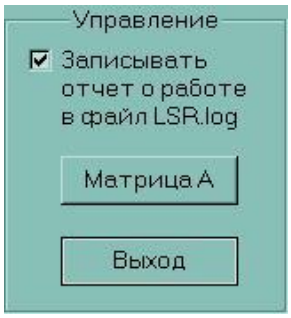


Рис. П3.25. Блок «Управление»

Выключатель «Записывать отчет о работе в файл LSR.log» включает\выключает режим записи произведенных действий в файл «lsr.log».

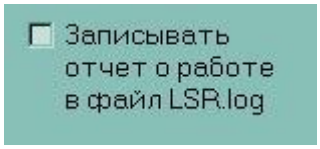


Рис. П3.26. Выключатель «Записывать отчет о работе в файл LSR.log»

При включении данного выключателя создается или перезаписываетя или дозаписывается (в зависимости от ситуации) файл «lsr.log», в который записываются действия пользователя по отысканию открытого текста.

Для составления отчета надо:

a) После запуска лабораторной работы включить переключатель «Записывать отчет о работе в файл LSR.log» (включен по умолчанию). Если уже существует lsr.log, то ответить на вопрос: «Переписывать?». Если такого файла нет, то он создастся;

b) Загрузить вариант. В файле появится запись «Начало LOG*********»;

c) Выполнить действия по поиску открытого текста;

d) Найти открытый текст.

e) Выйти из программы при помощи кнопки «Выход». В файле появится запись «Конец LOG*********».

Рис. П3.27. Кнопка «Выход»

В файле отчета будут задокументированны основные действия по поиску открытого текста. Отчет предоставляется в распечатанном виде от фразы «Начало LOG**********» до фразы «Конец LOG**********».

Сообщения выдаваемые в процессе работы

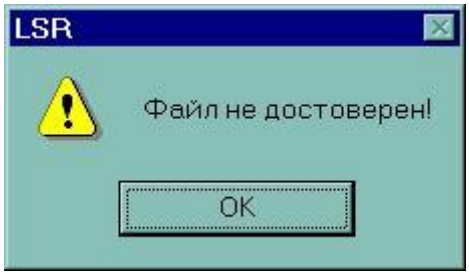
Во время выполнения лабораторной работы по мере возникновения исключительных ситуаций программа выдает сообщния, которые соответствуют определенному событию. Сообщения выводятся в отдельном окне. Программа перед продолжением работы ждет реакции пользователя на выведенное сообщение. Рассмотрим возможные сообщения.

Сообщения об ошибках

Это наиболее большая группа сообщений. Они возникают при вводе ошибочных или ложных данных в соответствующие поля ввода.

- *Файл не достоверен!*

Сообщение выдается, когда файл загружаемого варианта является недостоверным. То есть посчитанная контрольная сумма не совпадает с той которая записана в файле. Внешний вид окна сообщения:



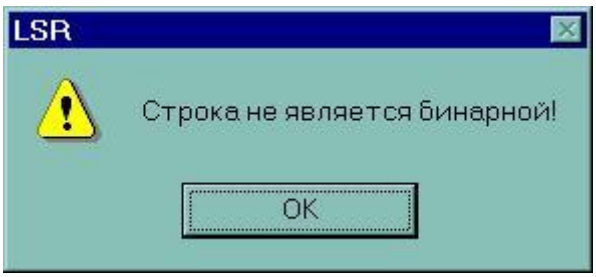
Действия пользователя:

- Нажать кнопку «ОК».

Найти правильный файл варианта или загрузить другой вариант.

- *Строка не является бинарной!*

Сообщение выдается при содержании в строке «=» блока «Сложение по модулю 2» хотя бы одной цифры отличной от нуля или единицы или при содержании в строке S1…S8 подпрограммы «Обработка матриц» хотя бы одной цифры отличной от нуля или единицы. Внешний вид окна сообщения:

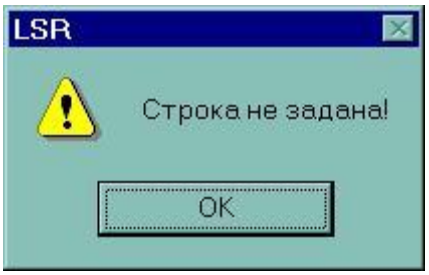


Действия пользователя:

- Нажать кнопку «ОК».
- Правильно заполнить строку «=» или строку S1…S8.

- *Строка не задана!*

Сообщение выдается, когда не задана (пустая) одна из двух строк (Первая стр или Вторая стр) в блоке «Сложение по модулю 2». Внешний вид окна сообщения:

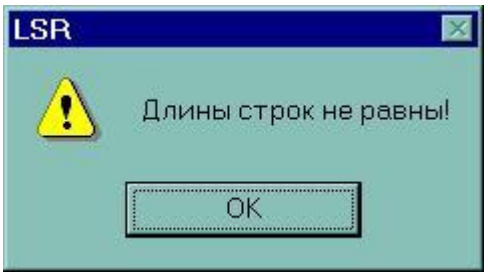


Действия пользователя:

- Нажать кнопку «ОК».
- Заполнить поля ввода «Первая стр» «Вторая стр».

- *Длины строк не равны!*

Сообщение выдается, когда длины строк складываемых в блоке «Сложение по модулю 2» различаются. Внешний вид окна сообщения:

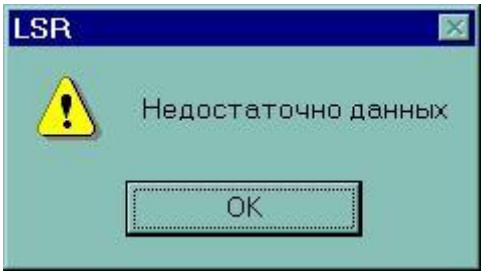


Действия пользователя:

- Нажать кнопку «ОК».
- Выравнять длину заполненных полей ввода «Первая стр» «Вторая стр».

- *Недостаточно данных*

Сообщение выдается, когда длина строки «=» блока «Сложение по модулю 2» меньше 14 бит или длина строки S1…S8 подпрограммы «Обработка матриц» менее 7 бит. Внешний вид окна сообщения:



Действия пользователя:

- Нажать кнопку «ОК».

- Увеличить длину последовательности данных в поле «=» или длину строк S1…S8.

- *Необходим 0 или 1*

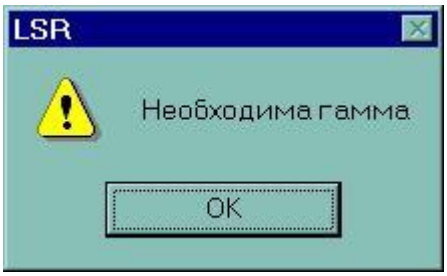
Сообщение выдается, когда одна из схематично изображенных ячеек регистра в блоке «Начальное заполнение» заполнена цифрой оличной от нуля ими единицы. Внешний вид окна сообщения:

Действия пользователя:

- Нажать кнопку «ОК».
- Правильно заполнить ячейки регистра.

- *Необходима гамма*

Сообщение выдается, когда необходимая гамма в поле «Гамма» не была получена, то есть не заполнено поле для чтения «Гамма». Внешний вид окна сообщения:



Действия пользователя:

- Нажать кнопку «ОК».
- Получить гамму нажатием кнопки «Получить гамму» в блоке «Гамма».

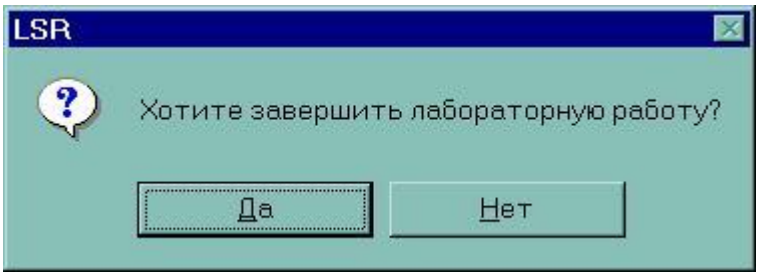
Сообщения-вопросы

Реакцией пользователя на сообщения данного типа должен стать выбор одного из предложенных вариантов ответа.

- *Хотите завершить лабораторную работу?*

Сообщение выдается при нажатии на кнопку «Выход» 

, то есть при желании выполняющего завершить выполнение работы. Внешний вид окна сообщения:



Действия пользователя:

- Нажать кнопку «Да», если действительно есть желание завершить лабораторную работу.
- Нажать кнопку «Нет», если нет желания завершать лабораторную работу.

- *Переписать лог?*

Сообщение выдается при включении режима записи файла-отчета, при условии, что файл уже существует. То есть при согласии на перезапись предыдущий вариант будет уничтожен. Внешний вид окна сообщения:

Действия пользователя:

- Нажать кнопку «Да», если необходимо создать новый отчет.
- Нажать кнопку «Нет» и отказаться от создания, если нужен файл старого отчета.

Критические ошибки

Система выдает сообщения данного типа, когда происходит ошибка препятствующая дальнейшему выполнению лабораторной работы.

- Не могу открыть файл!

Сообщение выдается в случае, когда программа не может в силу каких-либо причин открыть на чтение файл заданного варианта. Внешний вид окна сообщения:

Действия пользователя:

- Нажать кнопку «ОК».
- Рзрешить проблему доступа к файлу заданного варианта.

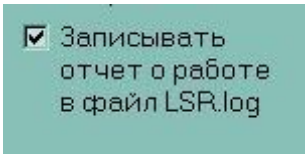
Пример

Рассмотрим для примера выполнение следующего задания:

Задание: Выриант №12

Решение: Начнем с нахождения открытого текста. Запускаем LSR.exe

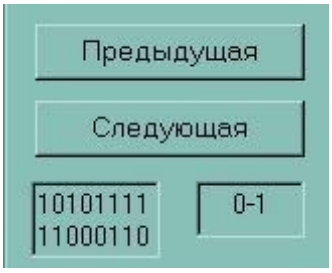
a) Включаем выключатель записи варианта в файл.



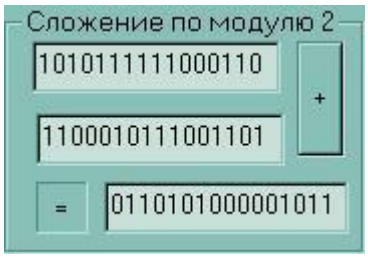
b) Загружаем файл для 12 варианта.

c) Выбираем вероятную биграмму – «ЕН». Получаем во второой строке блока «Сложение по модулю 2» строку «1100010111001101»

d) Предполагаем, что она стоит на месте 0-1. Таким образом, ничего не меняя, получаем в первой строке блока «Сложение по модулю 2» строку «0110101000001011»



e) Вероятная часть гаммы получена автоматически сложением двух строк.



f) Определим положение отводов в регистре при помощи метода основанного на нахождении обратной матрицы и введем первую строку матрицы A. Вызовем подпрограмму «Обработка матриц» кнопкой «Матрица A», заполним поля S1…S8 и нажмем кнопку «Вычислсть»

Как видно матрица A не имеет специального вида (см. выше), значит можно нажать кнопку «Вернуться» и выбрать следующее вероятное положение.

g) Выберем следующую позицию

Данная позиция также не даст положительных результатов.

Если продолжать выполнение, то мы переберем все возможные позиции вероятной биграммы (до 14-15) и не придем к удовлетворительному результату. Следовательно была ошибка в выборе биграммы.

h) Выберем новую биграмму и будем перебирать вероятные положения биграмм заново.

Перебирая положения и биграммы мы дойдем до вероятного положения биграммы 13-14 и биграммы ET. Остановимся на этом случае.

i) Вероятная часть гаммы найдена автоматически

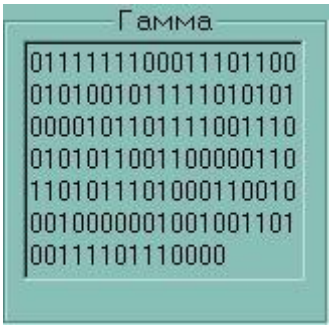
j) Определим положение отводов в регистре при помощи подпрограммы. То есть введем в поля ввода значения векторов S1…S8 (которые получаются из вероятной части ключа (см. поле ввода «=»)), нажмем кнопку «Вычислить» и получим значение строк обратной матрицы X^{-1} и значение строк матрицы A. В данном случае матрица A имеет специальный вид, значит первая строка представляет собой положение отводов в регистре.

k) Введем найденное положение отводов в блоке «Положение отводов»

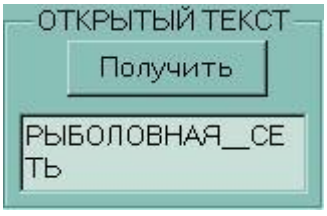
l) Промоделируем работу на 13 блоков назад и получим:

- Начальное заполнение регистра

- Гамму



- Открытый текст



Мы получили осмысленный текст и файл отчета «lsr.log», который содержит информацию о проделанной работе.

Теперь необходимо по части ключа «1001001101001111» с помощью алгоритма Берлекэмпа-Месси убедиться в правильности определения отводов регистра.

На вход алгоритма подаем битовую последовательность: «10010011010011», которая является частью ключа. На выходе мы получим минимальный регистр, который мог породить такую последовательность.

Составим таблицу для упрощения записей:

g_N	D	T(D)	C(D)	L	m	B(D)	N
-	-	-	1	0	-1	1	0
1	1	1	1+D	1	0	1	1
0	1	1+D	1	1	0	1	2
0	0	1+D	1	1	0	1	3
1	1	1	$1+D^3$	3	3	1	4
0	0	1	$1+D^3$	3	3	1	5
0	0	1	$1+D^3$	3	3	1	6
1	0	1	$1+D^3$	3	3	1	7
1	1	$1+D^3$	$1+D^3+D^4$	5	7	$1+D^3$	8
0	0	$1+D^3$	$1+D^3+D^4$	5	7	$1+D^3$	9
1	0	$1+D^3$	$1+D^3+D^4$	5	7	$1+D^3$	10
0	0	$1+D^3$	$1+D^3+D^4$	5	7	$1+D^3$	11
0	1	$1+D^3+D^4$	$1+D^3+D^4$	7	11	$1+D^3+D^4$	12
1	0	$1+D^3+D^4$	$1+D^3+D^7$	7	11	$1+D^3+D^4$	13
1	0	$1+D^3+D^4$	$\mathbf{1+D^3+D^7}$	7	11	$1+D^3+D^4$	14

Таким образом мы получили, что ячейки регистра, породившего заданную последовательность, задаются формулой $1+D^3+D^7$, если привести это выражение к уравнению, задающему положение отводов, то получим $H(X)=X^7+X^4+1$. Следовательно положение отводов в регистре, найденное двумя способами, оказалось одинаковым.

На этом выполнение работы завершено.

Ответ: РЫБОЛОВНАЯ__СЕТЬ

Теперь необходимо распечатать файл отчета, приложить решение алгоритмом Берлекэмпа-Месси и сдать на проверку преподавателю.