ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙНАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК

КАФЕДРАИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МЕТОДА КРИПТОЗАЩИТЫ ПРИ СУБПОЛОСНОЙ ПЕРЕДАЧЕ В БЕСПРОВОДНЫХ СЕТЯХ СВЯЗИ

Выпускная квалификационная работа
обучающегося по направлению подготовки 11.03.02
Инфокоммуникационные технологии и системы связи
очной формы обучения, группы 07001410
Воротынцева Валентина Валентиновича

Научный руководитель
канд. техн. наук, доцент
кафедры
Информационно-
телекоммуникационных
систем и технологий
НИУ «БелГУ» Урсол Д.В

Рецензент
доктор тех. наук, доцент,
профессор кафедры
Прикладной информатики и
информационных технологий
НИУ «БелГУ» Черноморец А.А

БЕЛГОРОД 2018

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
(НИУ «БелГУ»)
ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХНАУК
КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
Направление *11.03.02 Инфокоммуникационные технологии и системы связи*

Утверждаю
Зав. кафедрой
«____» _____ 201_ г.

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

____ Воротынцева Валентина Валентиновича
(фамилия, имя, отчество)

1. Тема ВКР «Разработка и исследование метода криптозащиты при субполосной передаче в беспроводных сетях связи»

Утверждена приказом по университету от «____» _____ 201_ г. № _____

2. Срок сдачи студентом законченной работы ___._____

3. Исходные данные:
Исследуемая технология – LTE;
Применяемые математические базисы –FFT и SB;
Количество поднесущих -150:1200

4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов):
4.1. Постановка задачи исследования;
4.2. Исследование базиса Фурье
4.3. Исследование базиса с оптимальными канальными сигналами с частотным уплотнением
4.4. Сравнение двух подходов реализации криптозащиты
4.5. Технико-экономическое обоснование проекта;

5. Перечень графического материала:
5.1. Схема сети LTE ;
5.2. Канал с базисом Фурье;
5.3. Канал с базисом оптимальных канальных сигналов с частотным плотнением;
5.4. Сравнение двух базисов;

6. Консультанты по работе с указанием относящихся к ним разделов

Раздел	Консультант	Подпись, дата	
		Задание выдал	Задание принял
4.1-4.4	*канд. тех. наук, доцент каф. ИТСиТ Урсол Д.В*		
4.5	*канд. техн. наук доцент каф. ИТСиТ Болдышев А.В.*		

7. Дата выдачи задания _____

Руководитель

канд. тех. наук, доцент
кафедры Информационно-телекоммуникационных
систем и технологий»
НИУ «БелГУ» _____*Д.В. Урсол*
(подпись)

Задание принял к исполнению _____
(подпись)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Беспроводные технологии прочно заняли свое место в повседневной жизни человечества. Количество трафика в беспроводных сетях нисколько не уступает количеству трафика в проводных сетях, поэтому его объемы исчисляются йоттабайтами[1].

Учитывая столь колоссальные объемы информации следует позаботится о ее гарантированной доставке и о ее защите. Выбор технологий для этого достаточно велик, и каждый может защитить свой трафик так, как посчитает нужным (все зависит от того, насколько важна информация). Если брать какие либо крупные компании или корпорации, то для передачи каких либо конфиденциальных данных, скажем, из одного офиса в одном конце города в другой офис другого конца города следует позаботиться о конфиденциальности на премиальном уровне:

1. Надежный помехоустойчивый код для защиты от потери данных;
2. Стеганографические методы сокрытия информации;
3. Криптографические методы защиты информации.

Комбинация вышеперечисленных способов защиты при должной конфигурации позволит защитить свои данные чуть ли не на 100%.

Но во всех технологиях есть свои бреши, уязвимости, и не стоит полагаться на них со 100% уверенностью, так как хорошо подготовленный злоумышленник, владеющий соответствующими техническими навыками, может не только перехватить конфиденциальные данные, но и расшифровать их, что в некоторых случаях может привести к весьма нежелательным последствиям.

Конечно, если говорить о крупных организациях, то в них за защиту информации отвечают целые отделы подготовленных специалистов, имеющих доступ к передовым технологиям, что существенно снижает риск возникновения кражи или взлома данных. Но даже в таком случае нельзя быть на 100% уверенным в том, что система защиты информации функционирует надежно.

А если речь идет об обычном оборудовании рядовых пользователей (смартфоны, ноутбуки, стационарные пк, планшеты и т.д), то в них, как правило, установлен ограниченный («заводской») набор технологий защиты информации, который явно не обеспечивает желаемого уровня безопасности. Конечно, этот набор можно изменить во своему желании, либо усложнить алгоритмы криптографии и стеганографии, но это может ударить по карману, поэтому большая часть пользователей не особо уделяет внимание вопросам защиты информации[2].

Актуальность данного проекта прежде всего в обеспечении конфиденциальности информации при ее передаче по беспроводным сетям. Сделать это можно множеством способов, одним из которых является внедрение в процесс передачи суб-полосного преобразования(SubBand) вместо обычного быстрого преобразования Фурье (Fast Fourier Transform), что позволить увеличить надежность передачи данных не только для крупных организаций, но и для рядовых пользователей беспроводных технологий связи.

Целью данной работы является разработка комплексного метода обеспечения информационной безопасности, качественные показатели эффективности которого будут превышать показатели эффективности стандартных методов, применяемых в беспроводных системах связи.

Для достижения цели будут выполнены следующие задачи:

– Исследование существующих технологий обеспечения информационной безопасности в беспроводных сетях связи;

– Разработка и исследование более эффективного алгоритма обеспечения информационной безопасности;

– Сравнение получившихся результатов.

1 УЯЗВИМОСТИ В ТЕХНОЛГИЯХ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ

Сегодня беспроводные сети прочно заняли свое место в нашей жизни, превратившись из новой технологии в повседневность. Зайдя выпить кофе в кафе или присев на лавочку в сквере многие начинают искать ближайшую точку доступа, нисколько не задумываясь о вопросах безопасности. Практика показала, что не только рядовые пользователи, а так же и часть сетевых администраторов имеют слабое представление о различных сетевых угрозах.

Беспроводные сети в силу особенностей среды передачи не могут обеспечить разграничения доступа к данным, пакеты, передаваемые клиентом или точкой доступа могут быть получены любым устройством в зоне действия сети.

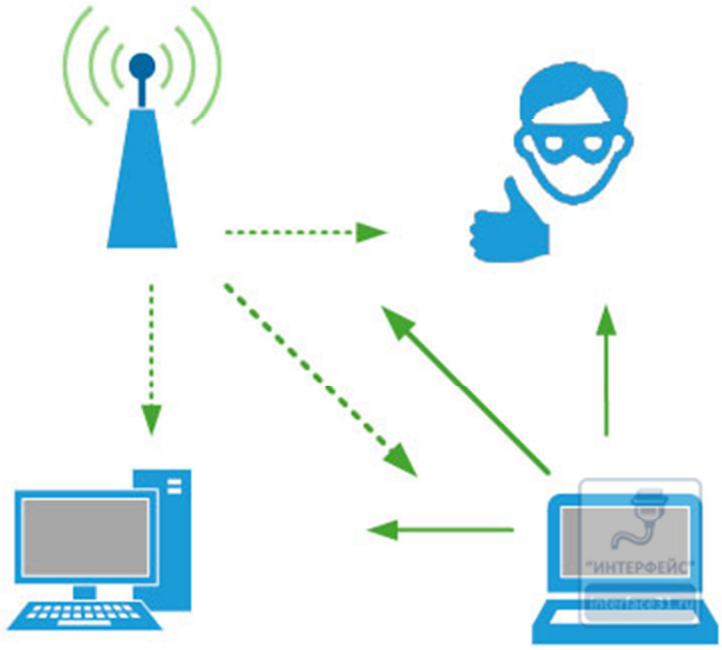

Рисунок 1 – Способ работы беспроводных сетей

Сетевое оборудование при передаче/приеме информации работает только с данными, предназначенными конкретно ему, однако существует ПО, которое позволяет осуществлять перехват и анализ всего сетевого трафика.

Даже если это гостевая Wi-Fi и она надежно изолирована от корпоративной сети, все равно она подвержена тем же угрозам, особенно если ею пользуются сотрудники с персональных устройств, а если они при этом еще обращаются к корпоративным сервисам, то риски возрастают многократно.

Доступность соответствующего ПО и инструкций делают эту задачу доступной даже для скучающих школьников.

Кроме того, сети с шифрованием WEP открытые, и при наличии сетевой активности в сети для ее взлома требуется 5-10 минут, причем делается это специализированным ПО в автоматическом режиме и не требует от злоумышленника никаких специальных знаний.

В WPA / WPA2 стеях при выборе надежного ключа и отказе от скомпрометированной технологии TKIP (в пользу AES) взломать такие сети без применения спецсредств и глубоких знаний несколько тяжелее. Опять-таки не следует забывать о защищенных сетях, ключ которых известен злоумышленнику.

Существует ПО, например, «CommView for WiFi», которое позволяет осуществлять перехват и расшифровку пакетов даже в закрытых сетях. Поэтому защищенные сети, ключ от которых известен широкому кругу лиц, следует также рассматривать как открытые, со всеми вытекающими из этого мерами предосторожности.

Основная угроза открытых сетей - это перехват и анализ трафика.

Вполне может быть, что злоумышленник при помощи ноутбука и 3G модема поднявший точку доступа, собирает из проходящего трафика пароли, cookie и прочую "интересную" информацию, поэтому, используя открытые сети не следует авторизовываться ни на каких ресурсах, передающих авторизационные данные в открытом виде. Злоумышленнику даже не нужен пароль, который может быть передан в зашифрованном виде, вполне достаточно перехватить cookie, после чего можно без проблем авторизоваться под чужой учетной записью.

Другая опасность подстерегает там, где принадлежность точки доступа вроде бы известна. Злоумышленник может использовать еще одно свойство сетей

Wi-Fi – автоматически переключаться на точку доступа с лучшим уровнем сигнала при наличии сетей.

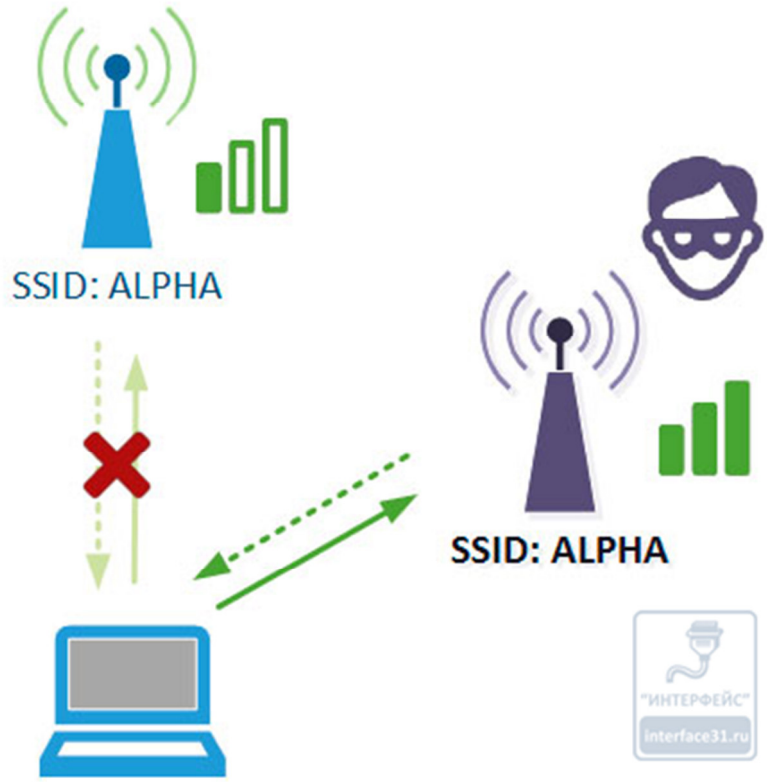

Рисунок 2 – Переключение на точку доступа с более мощным сигналом

Схема атаки предельно проста, злоумышленником создается точка доступа с таким же SSID, как у существующей сети, после чего, все устройства, находящиеся в радиусе действия подключаться к точке доступа злоумышленника, без малейших подозрений о перехвате трафика. В итоге посиделки с планшетом в любимом кафе могут закончиться очень невесело и хорошо еще, если пострадает личная информация, а не будут утрачены реквизиты доступа к корпоративной сети.

Здесь в полный рост встает проблема безопасного доступа к корпоративным ресурсам, даже если в организации не используется Wi-Fi. Где гарантия, что сотрудник сидя в парке или кафе не решит проверить корпоративную почту?

Но даже если есть уверенность, что точка доступа одна и принадлежит тому, кому надо, не стоит радоваться. Существует тип атаки **ARP-spoofing**, который способен направить трафик через устройство злоумышленника.

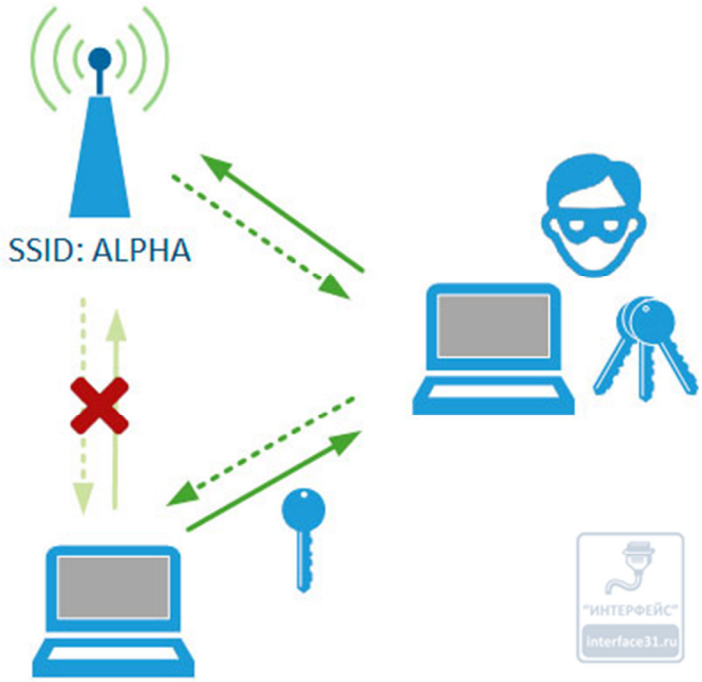

Рисунок 3 – ARP-Spoofing

Наконец злоумышленник может просто собирать и анализировать Wi-Fi трафик не вмешиваясь в работу беспроводной сети, переведя свой Wi-Fi адаптер в режим мониторинга, что позволит перехватывать практически всю информацию, проблемой в данном случае будет лишь отсоритровать большой объем данных.

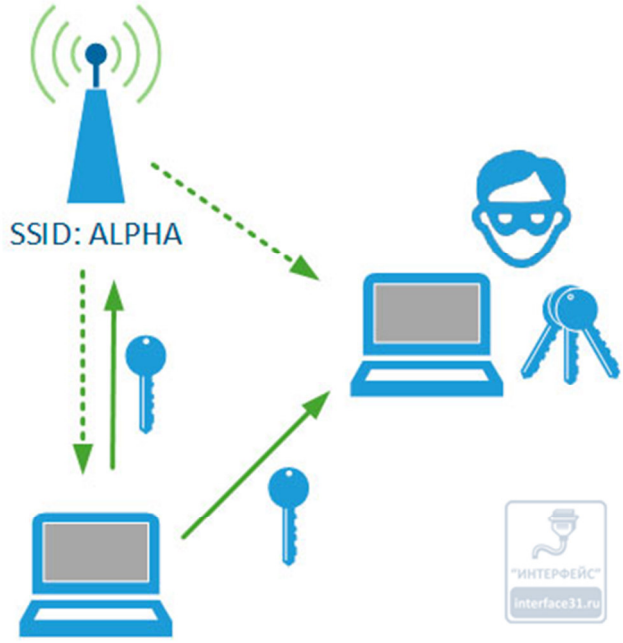

Рисунок 4 – Режим мониторинга

Понятно, что повлиять на возможность перехвата пакетов в сетях Wi-Fi не представляется возможным в силу особенностей среды распространения. Отказ от использования Wi-Fi в организации также никак не обезопасит инфраструктуру. К каждому сотруднику сторожа не приставишь и использовать корпоративные ресурсы через открытые сети не запретишь. [3]

В целом можно сказать, что существует проблема уязвимости защищенности информации в беспроводных сетях (это касается не только точек доступа Wi-Fi, а и сетей доступа типа WiMax и LTE). Она связана с тем, что сети радиодоступа являются открытыми в большинстве случаев, поэтому перехватить трафик в такой сети не составляет большого труда (в связи с универсальностью и доступностью современного ПО). Даже не смотря на современные алгоритмы криптозащиты, «умельцы» умудряются получать необходимую информацию. В связи с сложившейся плачевной ситуацией предусмотрены некоторые комплексные методы борьбы с информационной уязвимостью. Таких методов огромное множество и даже они не всегда помогают каким либо образом улучшить ситуацию, так как не существует «идеальной» защиты, и все можно взломать и получить ко всему доступ имея соответствующие навыки и

вычислительные и временные ресурсы, но можно свести к минимуму угрозы информационной безопасности. [4]

1.1 Проблемы уязвимости и средства защиты в сетях LTE

В качестве проверяемой беспроводной технологии связи в данной выпускной квалификационной работе будет рассмотрена технология LTE.

Архитектура сетей LTE (Long Term Evolution) имеет явные расхождения с сетями 3 поколения. В связи с этим появляется необходимость совершенствовать механизмы безопасности. Ключевым требованием является наличие того же уровня безопасности, который присутствовал в 3G сетях. Все различия представлены далее:

1. Структура ключей, которые используются в различных ситуациях;

2. Разделение механизмов безопасности для слоя без доступа (NAS), на котором осуществляется поддержка связи между узлом ядра сети и мобильным терминалом (UE), и для слоя с доступом (AS), обеспечивающего взаимодействие между оконечным сетевым оборудованием (включая набор базовых станций NodeB (eNB)) и мобильными терминалами;

3. Концепция превентивной безопасности, которая способна снизить масштабы урона, наносимого при компрометации ключей;

4. Внедрение дополнительного алгоритма безопасности при взаимодействии LTE и 3G

Существуют четыре основных требования к механизмам безопасности технологии LTE:

1. Обеспечение такого же уровня безопасности, как и в сетях 3 поколения;

2. Обеспечение защищенности от угроз из интернета;

3. Данные механизмы не должны мешать переходу между 3G и LTE;

4. Возможность продолжать использовать модуль USIM (Universal Subscriber Identity Module, универсальная сим-карта).

2 последних требования достигаются при помощи 3GPP AKA (Authentication and Key Agreement). Требования же безопасности к компоненту Evolved Packet Core, т.е. к ядру сети LTE, достигаются применением технологии безопасной доменной зоны (NDS – Network Domain Security) на сетевом уровне, как это описано в стандарте TS33.210, так-же как и для сетей 3G.

В качестве основного алгоритма в сетях LTE используется потоковое шифрование, которое формирует определенную ПСП, которая затем накладывается на исходную информацию аналогично процедур в 3G. Стоит так же отметить, что формируемая ПСП никогда не повторяется и имеет фиксированный размер. В сетях 3G для генерации сеансового ключа необходимо использование механизма аутентификации и обмена ключами (AKA). Работа механизма AKA занимает доли секунды, необходимые для выработки ключа в приложении USIM и для установления соединения с Центром регистрации (HSS). Таким образом, для достижения скорости передачи данных сетей LTE, необходимо добавить функцию обновления ключевой информации без инициализации механизма AKA. Решается данная проблема путем использования ключевой структуры, показанной на рисунке 5:

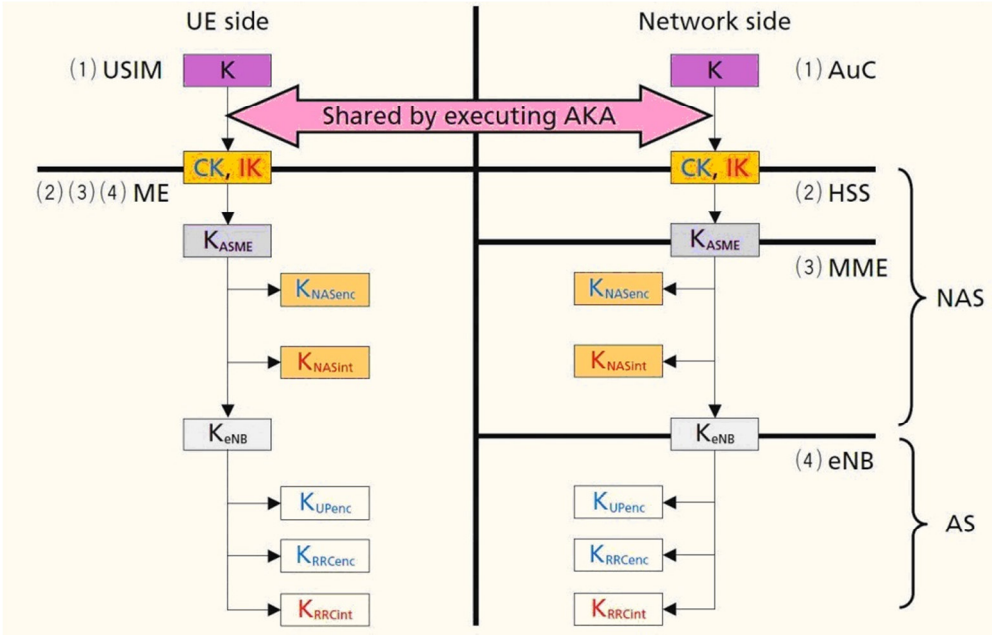

Рисунок 5 – Применение иерархической ключевой инфраструктуры для обеспечения безопасности в сетях LTE

В сетях LTE алгоритмы шифрования и обеспечения комплексной безопасности основаны на технологии Snow 3G и стандарте AES. Помимо этих двух алгоритмов, технология 3GPP использует два дополнительных алгоритма таким образом, что даже если один из алгоритмов будет взломан, оставшиеся должны обеспечить безопасность сети LTE. [5]

Хотя данные методы и средства и позволяют частично устранить проблему защищенности информации, существует более хитрый и простой способ улучшить защищенность информации не прибегая при этом даже к сложному шифрованию или стеганографии. Основывается данный метод на замене математического базиса FFT(Fast Fourier Transform)[6], который активно используется во многих беспроводных технологиях передачи на ортогональный субполосный базис (Sub Band)[7], и после его внедрения выполнение обычного перемешивания несущих частот. Описание данного метода будет рассмотрено в главе 3.

2. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ БЕСПРОВОДНОЙ СВЯЗИ

2.1 Технология ортогонального частотного уплотнения (OFDM)

Так как в технологии доступа LTE используется OFDM канал, то целесообразно составить на его основе математическую модель а так же отыскать возможность улучшить качество обеспечения информационной безопасности еще не уровне формирования сигнала.

Способ модуляции с одновременным использованием нескольких несущих частот, имеющий название OFDM (способ с мультиплексированием ортогональных частот), известен более 30 лет, однако в последние годы, с развитием цифрового ТВ вещания, преимущества этого способа модуляции оказались актуальны.

Основная идея, положенная в основу этого способа, заключается в следующем. Передаваемый цифровой поток модулирующего сигнала демультиплексируется, передаваясь по нескольким каналам - путем модуляции нескольких несущих. Число несущих выбирается из соображений сокращения скорости передачи на каждой из них. В результате достигается главное - на передачу одного символа на каждой отдельной несущей отводится большее времени. Настолько больше, чтобы сделать передачу каждого символа независимой от наличия отраженных сигналов, обусловленных так называемым «многолучевым» распространением радиоволн, что достаточно характерно для городских условий.

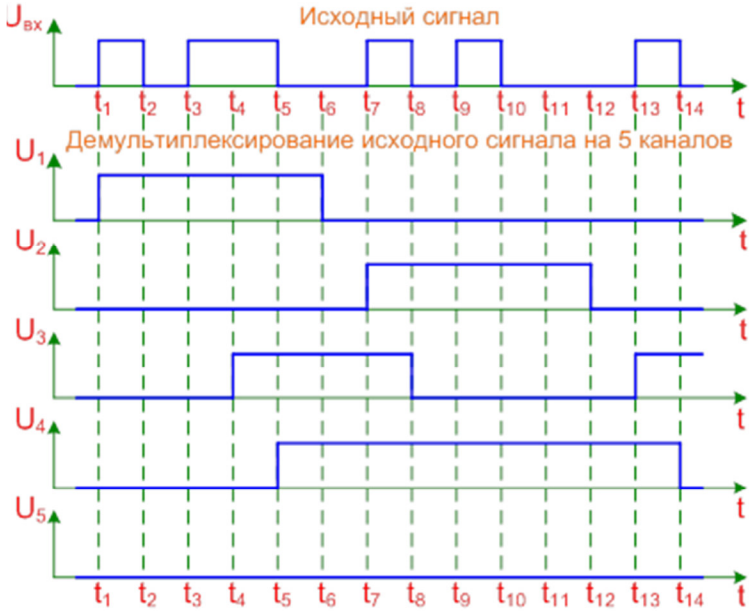

Рисунок 6 - Пример демультиплексирования цифрового сигнала

На рисунке 6 показан процесс демультиплексирование одного цифрового потока на пять составляющих что позволяет увеличить длительность передачи символа в каждом из пяти сигналов в пять раз. Затем каждый из полученных путем демультиплексирования сигналов модулирует свою собственную несущую, число которых равно числу модулирующих сигналов. Каждая несущая при этом модулируется либо QAM либо PSK методом. Несущие частоты выбираются из следующих соображений:

- число несущих, при неизменной скорости потока данных на входе модулятора OFDM должно увеличивать до требуемой величины время передачи одного символа на каждой несущей;
- несущие на частотной полосе должны находиться близко друг к другу чтобы сократить занимаемую полосу;
- выбор частот несущих необходимо делать учитывая возможность взаимного влияния.

Последнее условие достигается при достижении требования ортогональности. Физический смысл этого требования заключается в следующем: спектр каждой несущей после модуляции должен иметь «нули» на частотах, на которых расположены остальные несущие. Выполнение этого условия

обеспечивает отсутствие взаимных помех и независимую передачу информации на каждой несущей.

На рисунке 7 показан спектр одной несущей в результате модуляции ее сигналом прямоугольной формы.

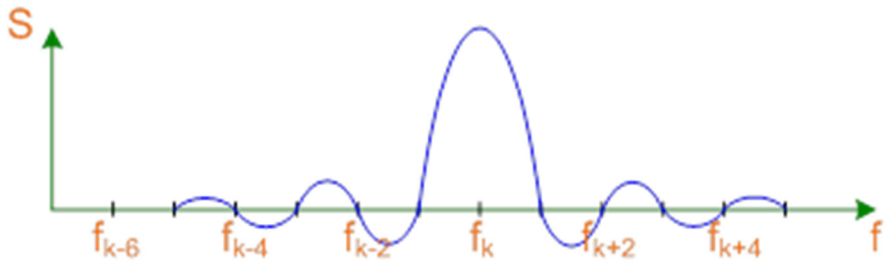

Рисунок 7 - Огибающая спектра одной несущей с номером k при модуляции OFDM

По условию ортогональности, частоты несущих должны располагаться на оси частот на расстоянии 1/Ts друг от друга- времени передачи одного символа. При этом значения каждой частоты определяются выражением:

$$f_k = f_0 + k * \frac{1}{T_s} \quad (1)$$

где k = 0, 1, 2, ..., n - 1, N.

Таким образом, получается ряд частот, расположенных равномерно и с общим спектром, достаточно близко приближающимся к прямоугольной форме, что позволяет эффективно использовать частотный канал передачи (рисунок 8).

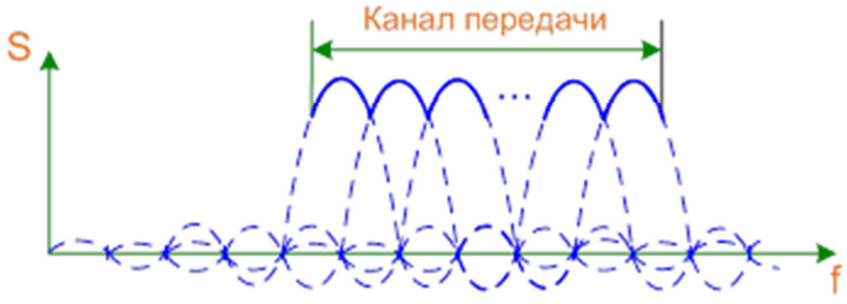

Рисунок 8 - Спектр передаваемого сигнала при модуляции OFDM

Весьма весомым фактором при таком способе модуляции является так называемая «межсимвольная интерференция» (ISI). В OFDM для борьбы с таким явлением предусмотрен простой механизм: увеличение времени передачи одного символа при увеличении количества частот. Это увеличение позволяет ввести между символами на частотной полосе «защитный интервал» (GI) (рисунок 9).

Исходя из этого время, затрачиваемое на передачу одного символа OFDM, состоит из интервала передачи полезной информации и защитного интервала:

$$T_{GS} = T_G + T_S, \quad (2)$$

где T_{GS}- времяпередачи одного символа; T_G- защитный интервал; T_S - время передачи полезной информации.

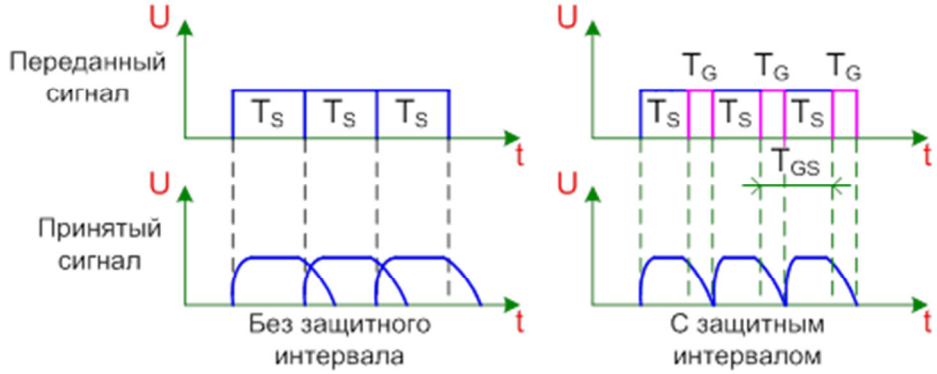

Рисунок 9 - Назначение защитного интервала при модуляции OFDM

Процесс формирования полного символа OFDM, включающего защитный интервал, схематично показан на рисунок 10.

Рисунок 10 - Пояснение формирования полного символа OFDM

Оптимальная длина защитного интервала позволяет устранять помехи, называемые «эхо-сигнал». На рисунке 11 показаны временные интервалы для основного сигнала и двух его эхосигналов. Задержка первого эхо-сигнала не превышает допускаемых параметров и переходные процессы, которые происходят в месте стыка двух сигналов происходят в защитном интервале основного сигнала, не искажая его полезную часть. Если же длительность второго эхосигнала будет слишком высока, то его переходная зона повлияет на часть следующего за ним основного сигнала и защита не будет обеспечена.

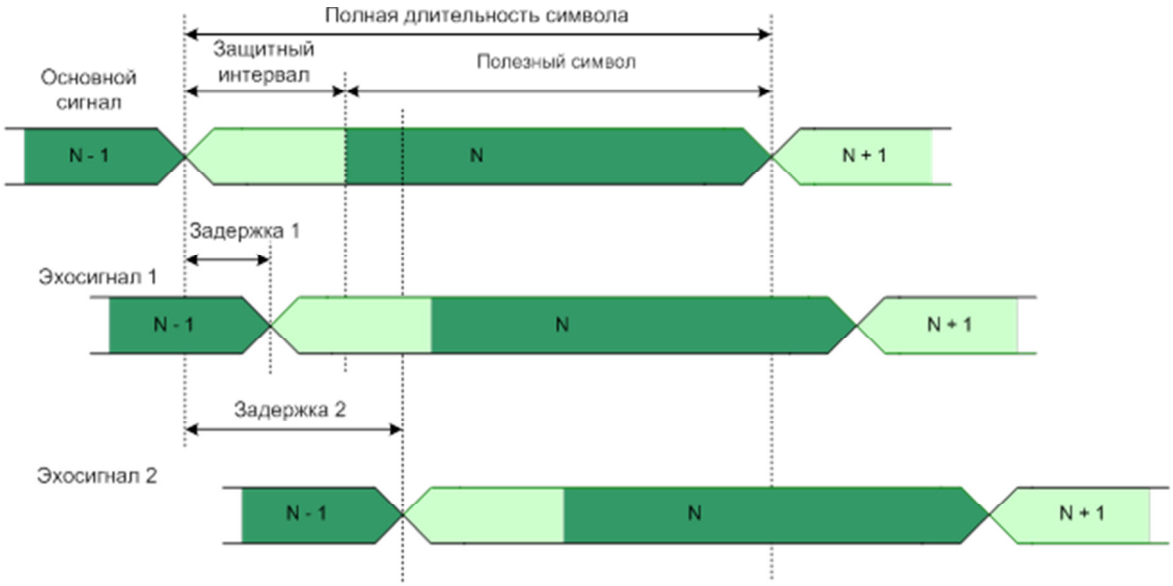

Рисунок 11 - Временные интервалы основного и двух эхосигналов

На рисунке 12 показан процесс устранения мешающего сигнала при суммировании всех сигналов. На рисунке 12 помимо основного сигнала показаны отраженные эхосигналы 1, 2 и сигнал соседнего передатчика одночастотной сети (эхосигнал 3). В приемник поступает сумма этих четырех сигналов. При выборе времени T_G больше времени импульсной реакции канала или времени задержки распространения, МСИ существенно снижается, потому как все нежелательные переходные процессы завершаются на протяжении защитных интервалов. К сожалению, даже наличие защитных интервалов не полностью устраняет эффект влияния сигналов друг на друга. Зачастую, на практике длина защитного

интервала не превышает четверти длительности сигнала, так как при его увеличении занимаемая полоса так же становится больше.

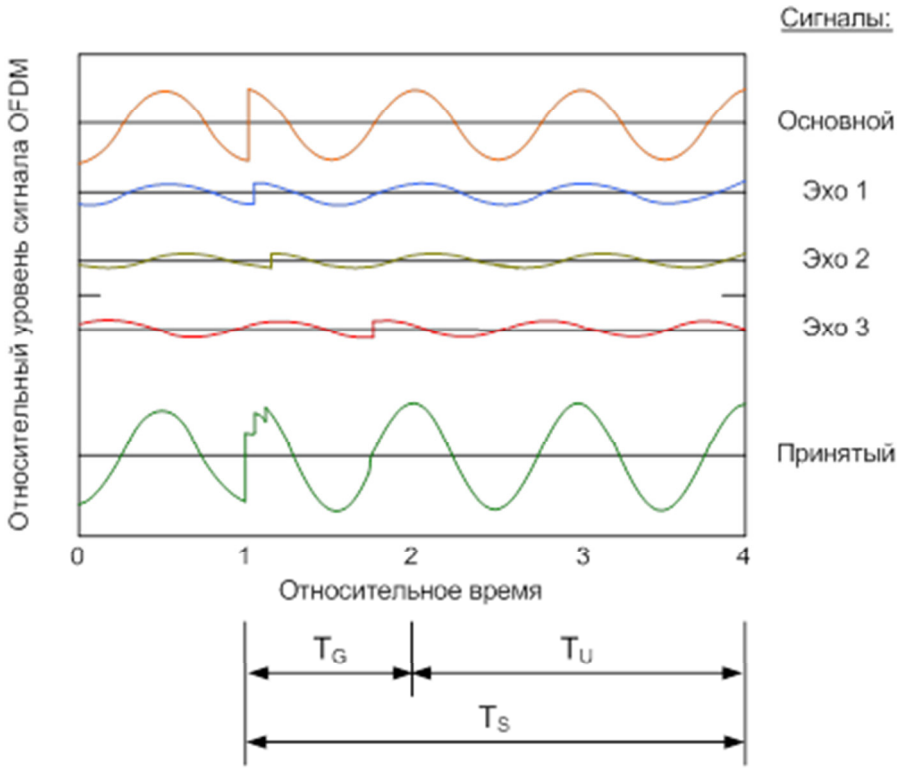

Рисунок 12 - Защитный интервал в символе OFDM

Примерная структурная схема модулятора OFDM показана на рисунке 13.

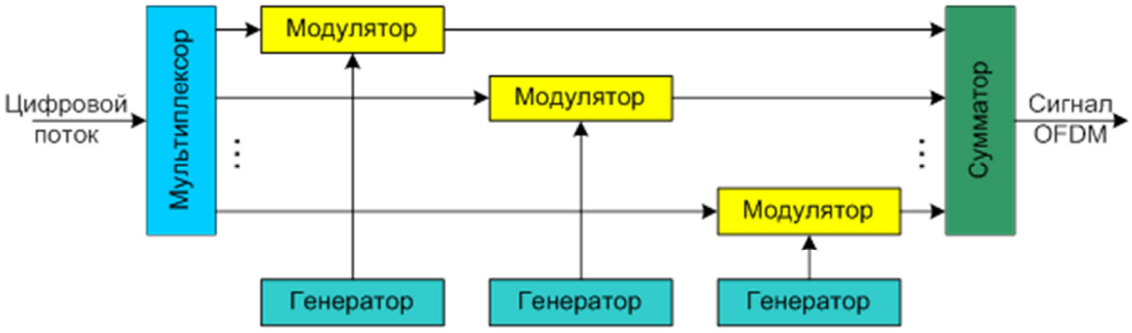

Рисунок 13 - Формирование сигнала OFDM

Каждая несущая частота формируется своим собственным задающим генератором. Данный способ уместен при небольшом количестве несущих. В случае телевизионного сигнала – на выходе модулятора может оказаться несколько тысяч таких несущих, поэтому при построении модулятора было

найдено оригинальное решение, позволившее избежать изготовления такой многоканальной системы передачи. Каждая несущая является частью общего спектра на выходе модулятора. В радиотехнике существует способ приема сложного сигнала, состоящего из отдельных гармонических составляющих. Таким приемом является обратное преобразование Фурье. Уже разработаны эффективные алгоритмы таких преобразований, позволяющие это делать без существенных затрат времени и вычислительных ресурсов.

На рисунке 14 показан пример формирования сигнала OFDM с помощью обратного быстрого преобразования Фурье (ОБПФ), которому подвергается входной цифровой поток. После ОБПФ вычисленные мнимая и вещественные части переводятся в аналоговую форму, проходя ЦАП и ФНЧ для отсеивания высокочастотных составляющих, затем поступают в преобразователь частоты, где происходит умножение на квадратурный и основной сигналы - гармоническое колебание частоты f_0. Это позволяет после сумматора получить спектр сигнала OFDM, смещенный на частоту f_0.

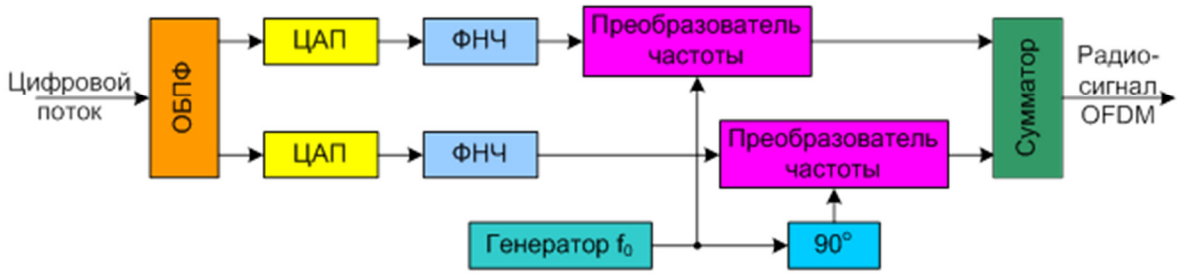

Рисунок 14 - Формирование радиосигнала OFDM с помощью обратного быстрого преобразования Фурье

Стоит упомянуть об еще одном «резерве помехоустойчивости» при данном способе. В процессе формирования передаваемого сигнала, состоящего из нескольких несущих, может возникнуть ситуация, когда следующие друг за другом последовательно во времени символы модулируют соседние по частоте несущие. Это обстоятельство неблагоприятно влияет на устойчивость такой

системы передачи к помехам, поражающим сразу определенный диапазон частот (рисунок 15).

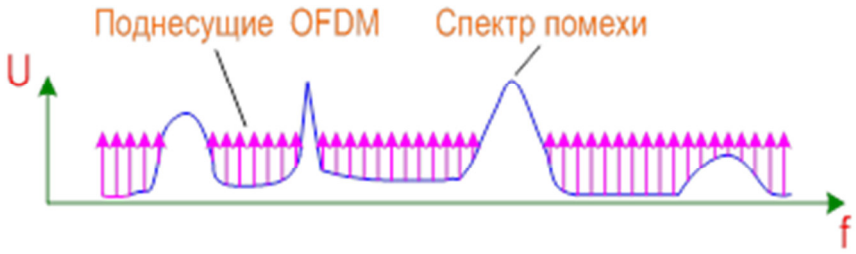

Рисунок 15 - Воздействие помех при передаче сигнала OFDM

Одним из вариантов способа модуляции OFDM, является COFDM, который «перемешивает» передаваемые символы во времени так, что следующие друг за другом символы полезной информации на передающей стороне модулируют те несущие, номера которых предписываются специальной заранее определенной последовательностью. Эта последовательность точно выдерживается на передающей стороне и, в обратном порядке - в приемном устройстве. Данный механизм позволяет свести практически на 0 чувствительность сигнала к замираниям, а также помехам, исключающим на короткое время возможность использования какого-либо участка диапазона частот.

Особенностью модуляции OFDM является повышенная неравномерность уровня мощности группового модулированного сигнала. На рисунке 16 показан результат суммирования пяти немодулированных несущих различных частот. Их суммарный сигнал имеет сильную неравномерность амплитуды. Отношение пиковой к средней мощности в каждом субканале системы OFDM также как и для систем с одиночной несущей зависит только от вида сигнального созвездия и коэффициента скругления спектра α. Теоретически различие в значениях отношений пиковой мощности к средней для полного спектра системы COFDM и системы с одиночной несущей составляет $\Delta(P_M/P_0) = 10\lg(N)$, где N - число несущих. При N = 1000 разница должна составить 30 дБ.

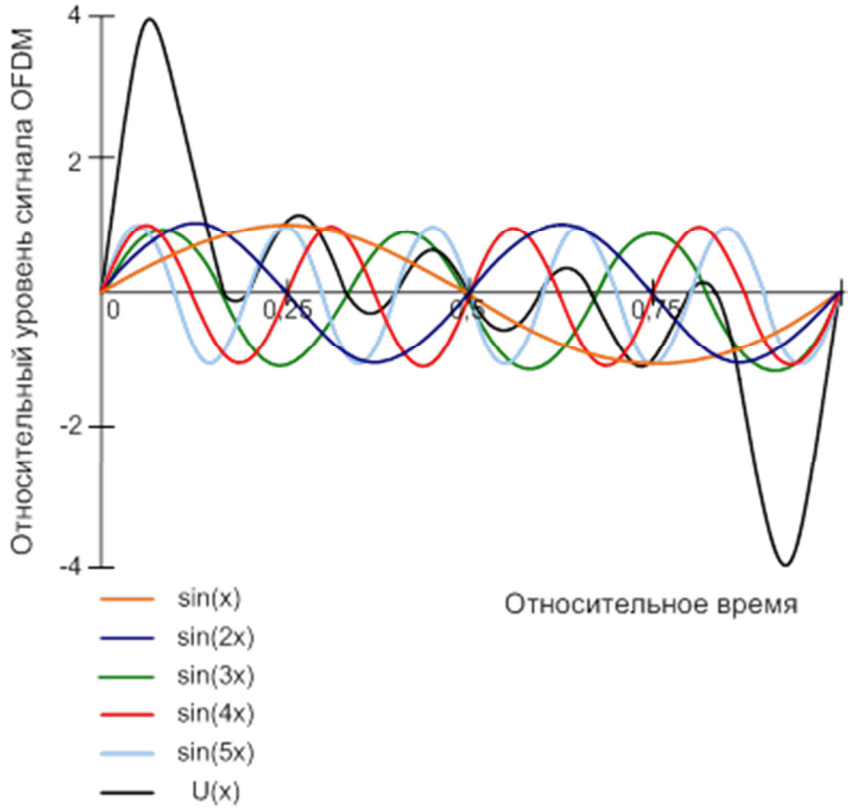

Рисунок 16 - Сумма несущих OFDM

Хотя за счет скремблирования информации теоретическое значение достигается лишь в случаях большого размера сигнального созвездия Т.к. скремблированный сигнал OFDM может рассматриваться как последовательность независимых одинаково распределенных несущих, то согласно центральной предельной теореме теории вероятностей при большом числе несущих ($N \geq 20$) их распределение приближается к гауссовскому. При этом вероятность того, что превышение пиковой мощности над средней мощностью составит 9,6 дБ, равна 0,1%, а что превышение составит 12 дБ - менее 0,01%. [8]

Из описания данной технологии можно сделать вывод, что при увеличении числа несущих частот будет страдать помехоустойчивость всего сигнала, что в случае требовательных высокоточных систем может оказать значительное влияние на работу системы в целом, если по каким либо причинам не получается устранить влияние помех (т.е в данном случае необходимым решением будет дополнительно вводить в процесс формирования и передачи сигнала сложный и надежный метод помехоустойчивого кодирования что, конечно же, отразиться на

стоимости оборудования для реализации такой технологии). Однако, если требования системы к обеспечению надежности конфиденциальной передачи информации играют более важную роль (будь то банковские данные, или информация, представляющая важность на уровне государства), то в данном случае следует выбрать компромиссный вариант между защищенной информацией и помехоустойчивость канала. Все, как это зачастую происходит, упирается в затраты на реализацию подобных технологий.

2.2 Стандарт Long Term Evolution (LTE)

LTE - это стандарт мобильной связи, разработанный консорциумом 3GPP. Он является усовершенствованием технологий мобильной передачи данных CDMA и UMTS, что и следует из его названия: Long Term Evolution, долговременная эволюция. Развитие сотовых сетей схематично представлено на рисунке 17.

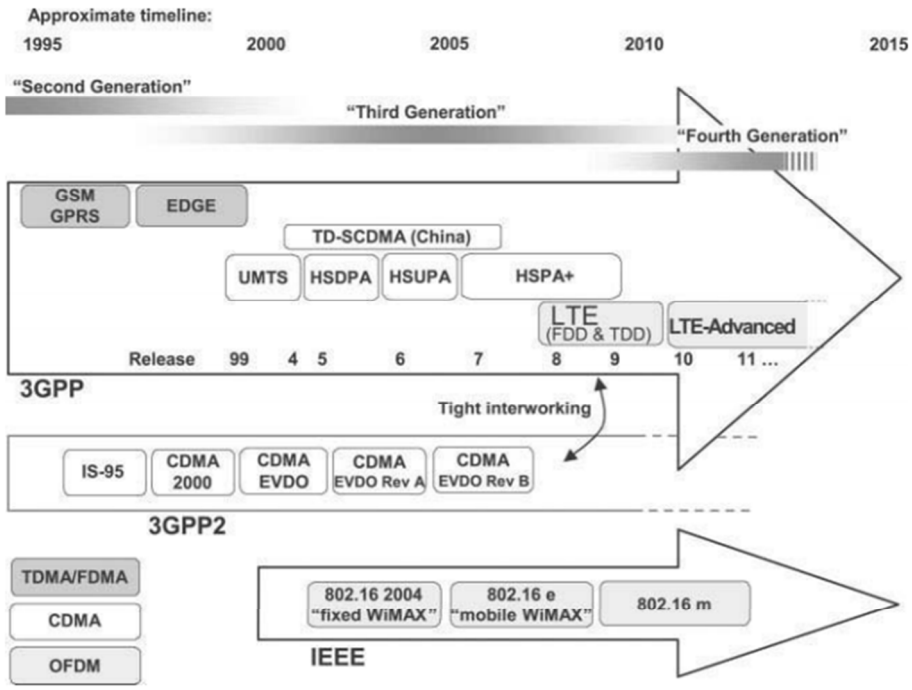

Рисунок 17 - Эволюция сетей сотовой связи

LTE является следующим этапом развития сетей 3G (HSDPA, HSUPA, HSPA+), но к 4 поколению сотовой связи относится только LTE-Advanced, (начиная с Rel.10). Вся коммутация в сетях LTE - пакетная, для передачи голоса необходимо использование технологии передачи голоса по IP-сетям (VoIP).

Требования к стандарту LTE и цели его создания:

– Уменьшение задержек установления соединения и передачи данных;

– Увеличение скорости передачи как около базовых станций так и на границе зоны покрытия;

– Увеличение спектральной эффективности, уменьшение стоимости передачи одного бита;

– Более гибкое использование спектра, как в новых, так и в существующих диапазонах частот;

– Упрощение архитектуры сети;

– Бесшовная передача обслуживания, в том числе между различными технологиями.

Данные цели достигаются использованием в LTE трех основных технологий:

– ортогональное частотное мультиплексирование (OFDM),

– многоантенные системы MIMO[9]

– эволюционная системная архитектура (SAE) [10].

Как и во всех современных технологиях беспроводной связи, в LTE поддерживаются много-антенные системы (MIMO). Так как данная технология ориентируется на простые абонентские устройства, то и технологи MIMO здесь существенно упрощена.

В стандарте применяется комбинация из 1, 2 и 4 антенн в различной конфигурации. В MIMO-системах предусмотрено 2 вида передачи:

– пространственное мультиплексирование;

– диверсифицированная передача.

В первом случае каждый канал будет передавать свой цифровой поток, и будет при этом некореллирован с другими каналами. Существует два способа пространственно-мультиплексированной передачи:

– для одного АУ (SU-MIMO)

– для группы АУ (MU-MIMO).

В первом случае базовая станция передает несколько потоков одному аппаратному устройству, количество антенн которого должно совпадать с количеством антенн самой БС. Так как в один момент времени может передаваться лишь 2 потока, то система даже с наличием 4 антенн может работать одновременно лишь с двумя потоками.

При диверсифицированной передаче несколько антенн используются для передачи одного потока. Данный метод в основном направлен для улучшения качества передачи и борьбы с замираниями в канале. Скорость передачи в данном случае будет повышаться в зависимости от качества канала. В восходящем канале применяется техника пространственного мультиплексирования MU-MIMO. Несколько АУ в данном случае могут использовать идентичные частотно-временные ресурсы, но за счет декорелляции каждого из них базовая станция работает одновременно с каждым в отдельности.

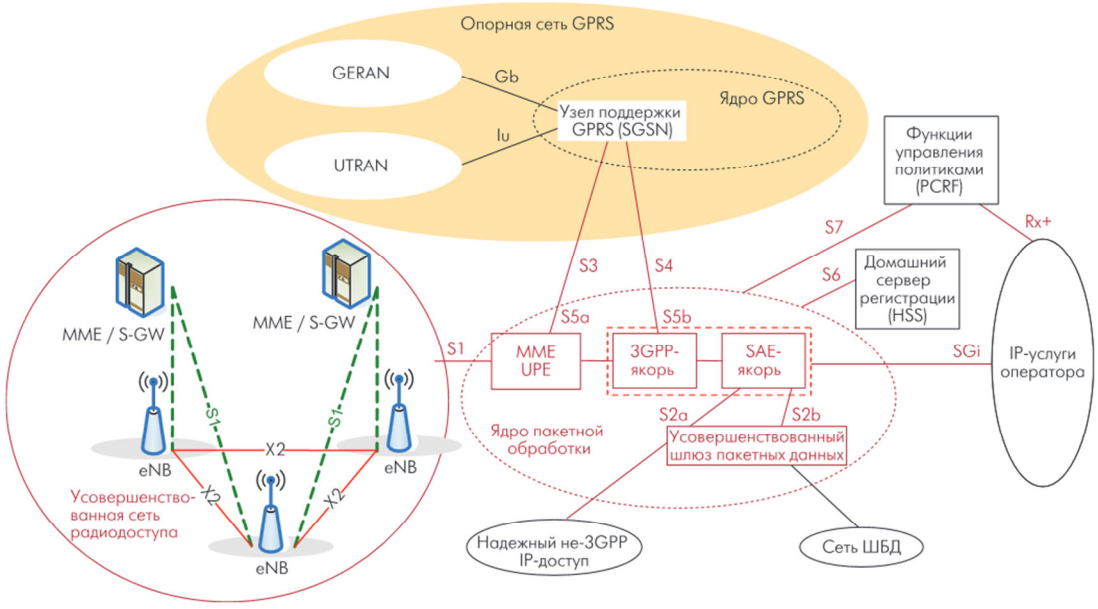

Рисунок 18 – Основные компоненты архитектуры SAE

LTE архитектура SAE (System Architecture Evolution - Эволюция системной архитектуры) значительно отличается от сетей стандартов 2G и 3G. Схематично она изображена на рисунке 19. Основные отличия:

– упрощенная архитектура, новая, плоская модель;

– целиком построена на IP;

– обеспечивает большую пропускную способность на сети радиодоступа (RAN);

– обеспечивает меньшую задержку RAN;

– поддерживает мобильность между несколькими гетерогенными RAN (в том числе не-3GPP системы).

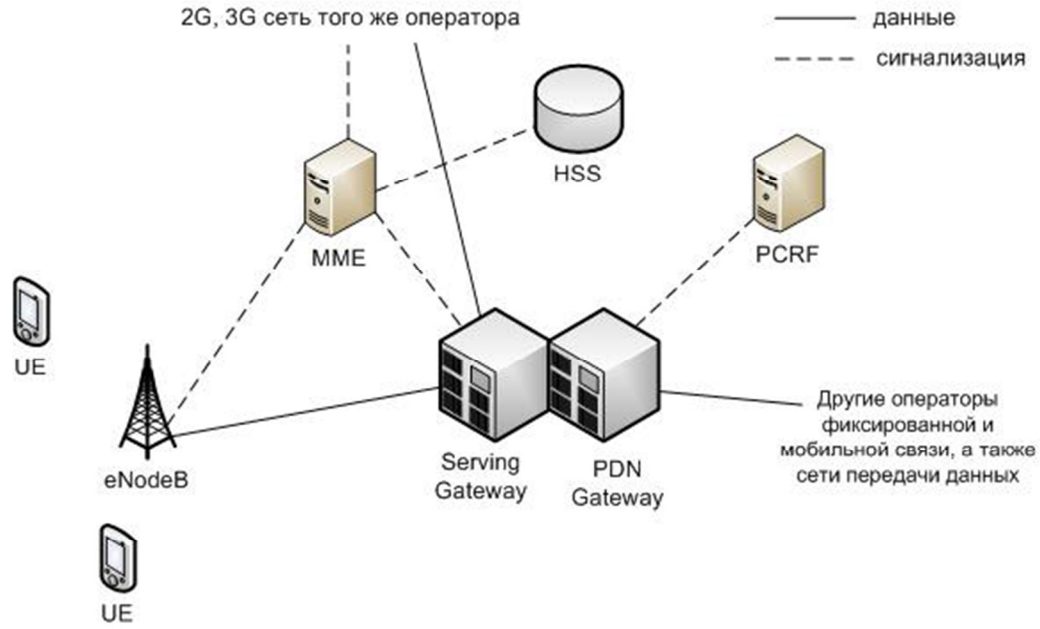

Рисунок 19 - Структура сети стандарта LTE

Цель SAE – поддержка широкого спектра информационных услуг на базе технологии IP и непрерывное обеспечение этими услугами абонентов, которые перемещаются между беспроводными сетями не обязательно соответствующими стандартам 3GPP (GSM, UMTS, WCDMA и т.д.). В сети с архитектурой SAE применяются 2 типа узлов:

– базовые станции (evolved NodeB, eNodeB);

– и шлюзы доступа (Access Gateway, AGW).

Ядро SAE сети состоит из 4 компонентов:

1. Модуль управления мобильностью (Mobility Management Entity, MME) хранит служебную информацию об абоненте и управляет мобильностью абонента;

2. Модуль управления абонентом (User Plane Entity, UPE) устанавливает нисходящие соединение, обеспечивает шифрование и маршрутизацию;

3. 3GPP-якорь является шлюзом между 2G/3G и LTE;

4. SAE-якорь поддерживает непрерывное обслуживание абонента при его перемещении как между сетями спецификации 3GPP, так и нет (I-WLAN и т.п.).

Последние 2 компонента являются новшеством архитектуры ядра мобильной сети связи (Evolved Packet Core) и появились благодаря необходимости поддержки непрерывности обслуживания абонента при его перемещении. Конфигурацию же функциональных элементов такой сети можно выбирать по своему усмотрению. Еще одной особенностью SAE является то, что она может пересылать пользовательские данные непосредственно как по беспроводным так и по проводным линиям связи (интерфейс X2). Это особенно важно при хендовере, для быстрого бесшовного переключения пользователя между БС. Допускается передача данных между базовыми станциями по ip шлюзам. Функционал mesh-сети позволяет осуществлять непосредственную передачу между БС. Так же особое место в 3GPP занимает обеспечения качества обслуживания сетей с архитектурой SAE. Многомодовые терминалы позволяют обслуживать абонентов с разными способами доступа, которые определяет из необходимости сам абонент. Так же из преимуществ следует выделить уменьшение количества задержек в таких типах трафика как VoIP или мультимедийный трафик реального времени, которые являются наиболее чувствительными к задержкам Значения этих задержек по крайней мере на 50% меньше, чем в аналогичных сетях 3G.

Технология ортогонального частотного мультиплексирования OFDM (Orthogonal Frequency Division Multiplexing) основана на формировании многочастотного сигнала, состоящего из множества поднесущих частот, отличающихся на величину Δf, которая выбирается из соображений условия ортогональности сигналов на соседних поднесущих. При формировании OFDM сигнала поток последовательных информационных символов длительностью разбивается на блоки, содержащие N символов. Далее блок последовательных информационных символов преобразуется в параллельный, в котором каждый из символов соответствует определенной поднесущей многочастотного сигнала. Причем при этом длительность символов увеличивается в N раз. Таким образом, суммарная ширина спектра многочастотного сигнала соответствует ширине спектра исходного последовательного сигнала.

Целью такого преобразования является защита от узкополосных помех (либо от частичных искажений спектра в результате переотражений и многолучевого распространения). Это достигается тем, что параллельные символы многочастотного сигнала представляют собой кодовое слово помехоустойчивого кода (например, кода Рида-Соломона), который позволяет их восстановить в случае ошибочного приема за счет искажений спектра. Частотно-временное представление OFDM сигнала представлено на рисунке 19. Преобразование сигнала из временной в частотную область обеспечивается дискретным преобразованием Фурье (DFT - Discrete Fourier Transform).

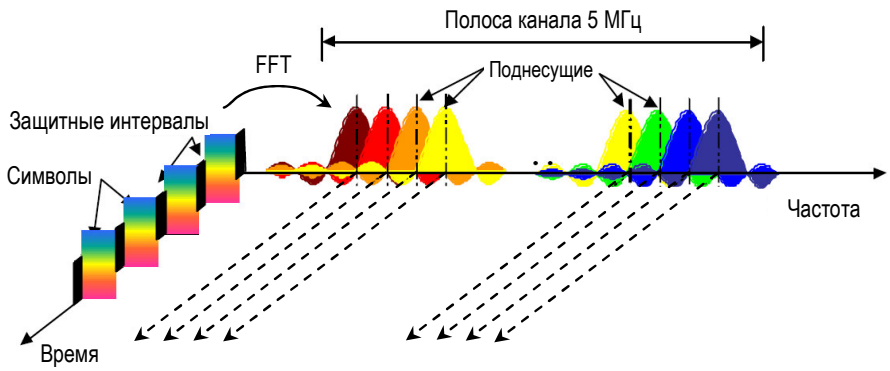

Рисунок 19 - Частотно-временное представление OFDM сигнала

Так же следует упомянуть об уменьшении количества защитных интервалов в OFDM. При последовательном сигнале защитные интервалы добавляются между каждыми символами, а при многочастотном – между группами символов (OFDM-символами).

Принцип формирования OFDM-сигнала показан на рисунке 20 [8].

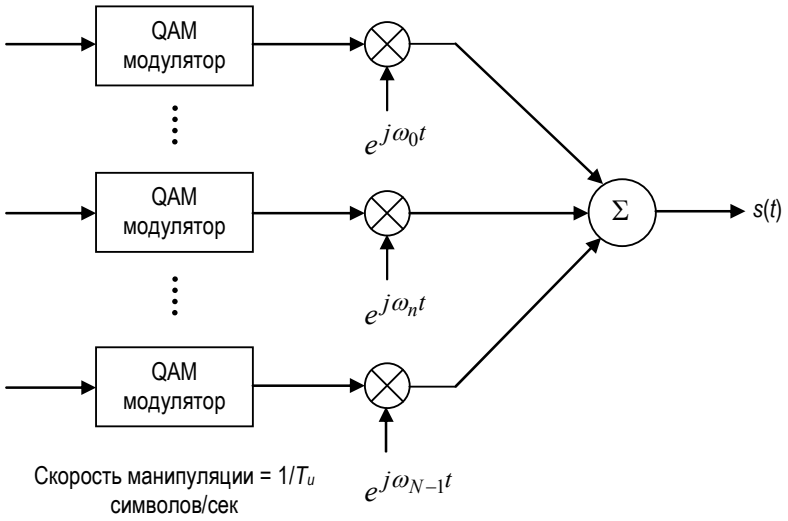

Рисунок 20 - Принцип формирования OFDM-сигнала

Особенностями сигналов OFDM являются:

– Мультиплексирование несущих колебаний (называемых поднесущими), модулированных информационными символами по выбранному закону (QPSK, 16QAM, 64QAM);

– Поднесущие ортогональны, или, по крайней мере, квазиортогональны (на практике);

– Каждый OFDM-символ имеет защитный временной интервал для исключения межсимвольной интерференции. Этот защитный интервал выбирается с учетом импульсной характеристики линии связи (физической среды распространения радиосигнала).

2.3 Технологии множественного доступа SC-FDMA

Особенностью линии «вниз» сети LTE является использование технологии множественного доступа SC-FDMA (Single Carrier - Frequency Division Multiple Access) с одной несущей частотой и средней мощностью передачи PAPR. Взаимное влияние исключается при помощи использования циклических префиксов и эффективных эквалайзеров. Основная конфигурация предполагает использование 4 антенн (двух на пользовательском терминале и двух на передающей станции).

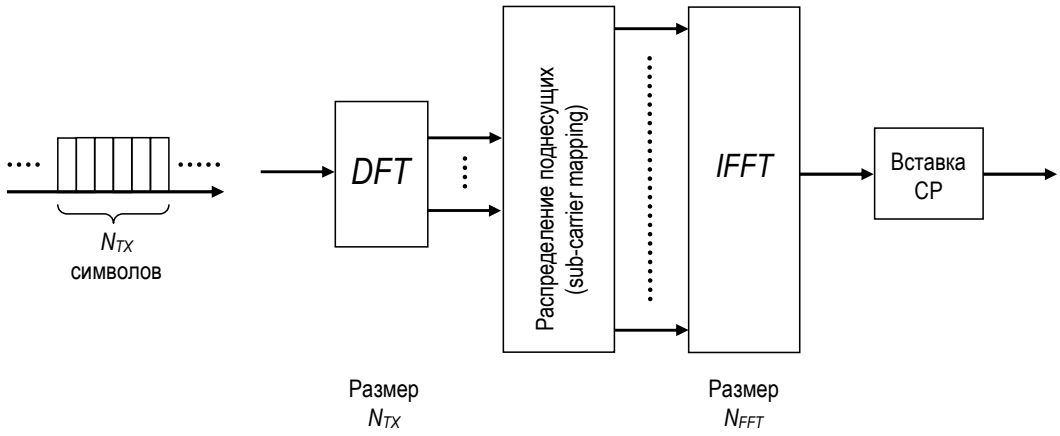

Рисунок 21 - Структурная схема передающего устройства SC-FDMA

В процессе модуляции OFDM в технологии множественного доступа SC-FDMA используется дискретное преобразование Фурье DFT (рисунок 22).

А **Б**

Рисунок 22 – Метод формирования OFDM поднесущих:
А-последовательный; Б-параллельный

Во время формирования группового сигнала в восходящей линии принимается решение о том, какая часть поднесущих будет использоваться для передачи, а какая будет заполняться нулями Между каждыми выходами дискретного Фурье вставляется L-1 нулевых символов.

При последовательном распределении поднесущих L=1 (рисунок 22а), то есть между сигналами с выхода преобразователя DFT не вставляются нулевые поднесущие (L-1=0). При смешанном распределении (рисунок 22б), L>1 .

Структура SC-FDMA-сигнала идентична сигналу с OFDM. Точно так же модулируется множество поднесущих, расположенных с шагом Δf. Отличием является то, что все несущие модулируются одинаково, то есть в один момент времени передается один модуляционный символ (рисунок 23). При этом ресурсная сетка полностью аналогична нисходящему каналу. Получается, что каждый ресурсный блок занимает по 12 поднесущих с шагом Δf =15 кГц (всего 180 КГц в частотной области) и во временной области 0.5 мс. Ресурсным блоком являются 7 SC-FDMA-символов при стандартном циклическом префиксе и 6 – при расширенном. Длительность SC-FDMA-символа (без префикса) равна длительности OFDMA-символа и составляет 66,7мкс (длительности соответствующих циклических префиксов также равны). Сетка может содержать от 6 до 105 ресурсных блоков. Единственным условием является кратность числа ресурсных блоков 2, 3 или 5, что связано с процедурой ДПФ. Очередная

особенность данной системы – опциональная поддержка модуляции 64-QAM в АУ.

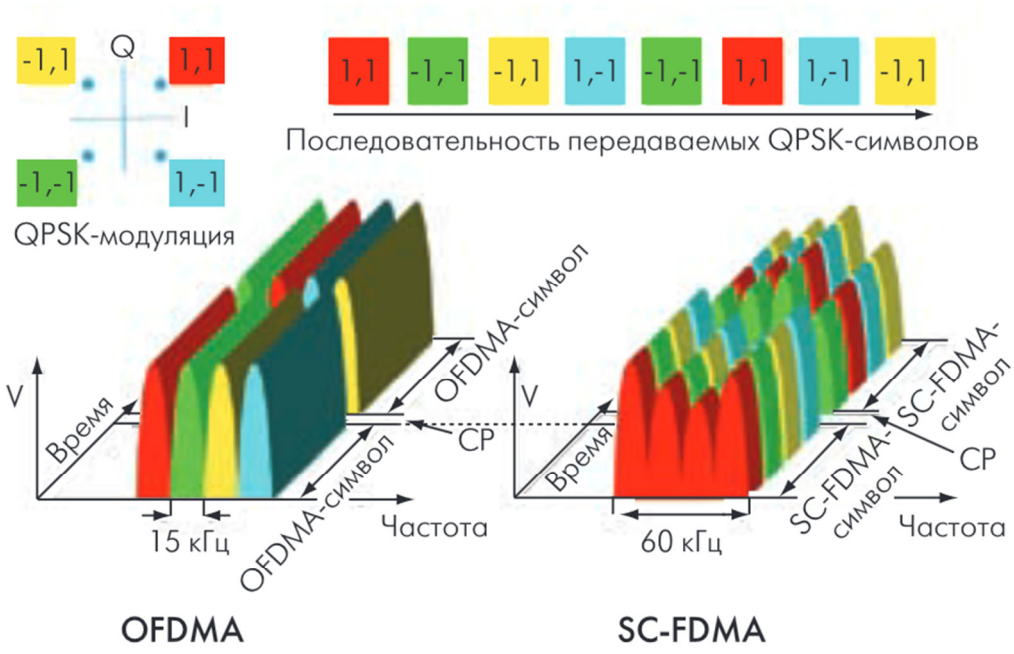

Рисунок 23 – Различие между OFDMA и SC-FDMA при передаче последовательности QPSK символов

Каждому абоненту сети на передачу данных выделятся определенное время. Расписание этого времни передается абонентам по служебным каналам в нисходящем радиоканале. Однако если при OFDMA один модуляционный символ (QPSK, 16- или 64-QAM) соответствует OFDM-символу на одной поднесущей (15 кГц, 66,7 мкс), то при SC-OFDMA ширина модуляционного символа занимает всю полосу (то есть он передается на всех несущих одновременно), при этом один такой символ содержит несколько модуляционных символов – в идеале такое же количество, как и количество несущих но в определенное число раз больше ем в OFDM, что соответствует условиям теоремы Котельникова-Шеннона. Сама процедура формирования SC-FDMA-сигнала отличается от схемы OFDMA. После того как такие символы закодируются в канале, перескремблируются и сформируют модуляционные символы они группируются в блоки по M символов – субсимволов SC-FDMA (рисунок 24). Поэтому перенести их на поднесущие с шагом в 15 КГц невозможно – требуется в N раз более высокая частота, где N –

это число доступных для передачи поднесущих. Поэтомупосле формирования группы M модуляционных символов (M < N), они подвергаются M-точечному (ДПФ), т.е. формируют аналоговый сигнал. А уже затем с помощью стандартной процедуры обратного N-точечного Фурье-преобразования синтезируют сигнал, соответствующий независимой модуляции каждой поднесущей, добавляют циклический префикс и генерируют выходной ВЧ-сигнал. В результате такого подхода передатчик и приемник OFDMA- и SC-FDMA-сигналов имеют схожую функциональную структуру. АУ при этом может использовать как фиксированный частотный диапазон (используются смежные ресурсные блоки, т.е. смежные поднесущие), так и распределенный –режим скачкообразной перестройки частоты (FH). В последнем случае для каждого слота восходящего канала используется новый ресурсный блок из доступной ресурсной сетки. Сетевое оборудование в данном случае определяет параметры этой частотной перестройки при инициализации абонентской станции в сети, так и по ходу работы в канале управления. В случае распределенного способа – информация от каждого абонента распложена во всем спектре сигнала (рисунок 24), поэтому данный способ устойчив к частотно-избирательному замиранию. Хотя при локализованном способе появляется возможность определения необходимой для абонента полосы. Поскольку области замирания сигнала для всех абонентов различны, то можно достичь общую максимальную эффективность использования радиоканала. Однако в данном случае канал нуждается в диспетчеризации. В восходящем канале помимо информации так же генерируются опорные сигналы, которые помогают БС настраиваться на определенное АУ. Кроме того, эти сигналы выполняют функцию диспетчеризации ресурсов. В восходящем канале существует 2 вида опорных сигналов:

- демодулированные;
- зондовые.

Демодулированные опорные сигналы аналогичны опорным сигналам нисходящего канала. Они передаются на постоянной основе. Так, в общем информационном канале последовательность демодулированного опорного

сигнала передается в четвертом SC-FDMA-символе каждого слота при стандартом CP. Зондовые сигналы апериодичны. Их основное назначение – дать БС возможность оценить качество канала, если передача еще не ведется.

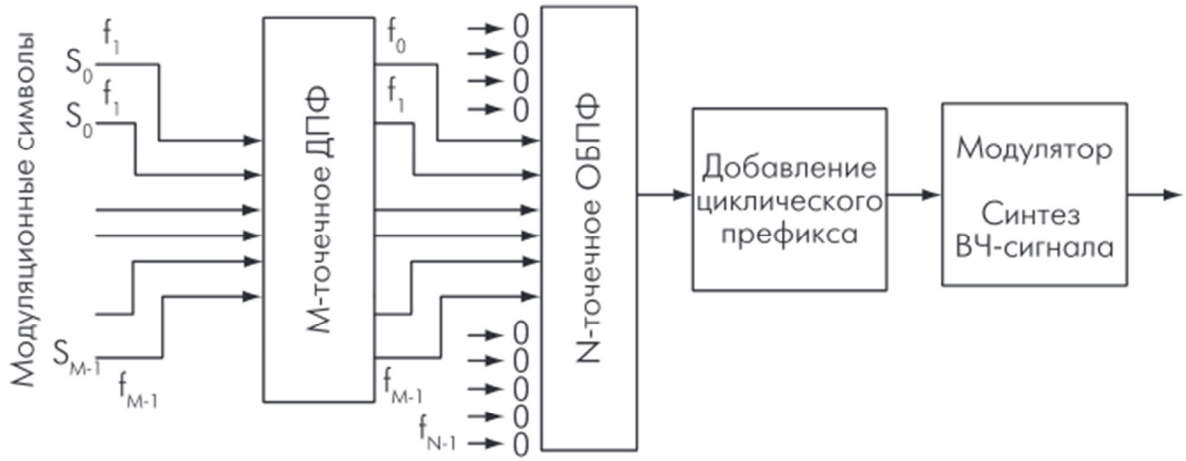

Рисунок 24- особенность формирования выходного сигнала в случае с SC-FDMA

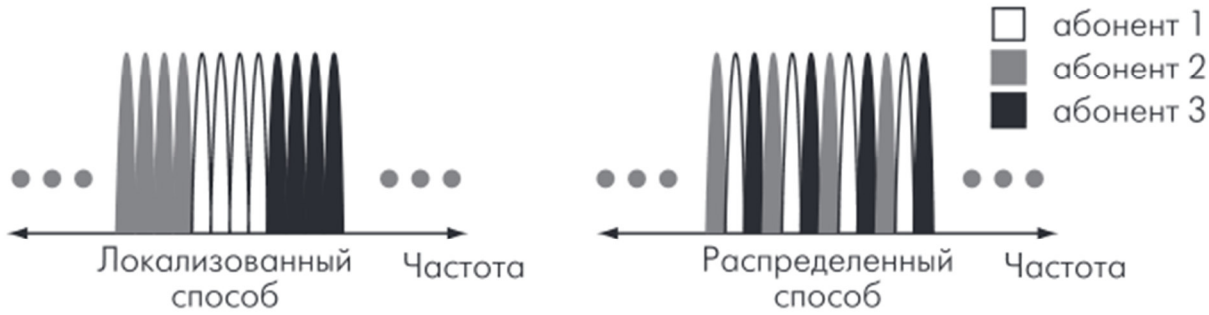

Рисунок 25 – Способы распределения поднесущих в SC-FDMA

До сих пор речь шла о формировании физического канала между абонентом и БС. Однако, как в восходящем, так и в нисходящем каналах передаются различные типы информационных потоков. В случае восходящего канала это:

- канал общего пользования назначения (PUSCH);
- управляющий канал (PUCCH) ;
- канал произвольного доступа (PURCH).

В первом канале передается информация пользователей. Управляющий канал содержит индикатор качества канала, сообщения подтверждения доставки (ACK/NACK) и запрос на получение расписания (о доступных ресурсах). Канал

общего пользования и управляющий канал никогда не транслируются одновременно одним АУ. Управляющий канал передается в одном из ресурсных блоков в каждом слоте каждого субкадра. В зависимости от формата PUCCH возможно четыре варианта его расположения на ресурсной сетке, определяемые переменной m. Канал произвольного доступа отвечает за начальную инициализацию сети, при хендовере, при выходе из режима ожидания в активный режим и т.п. АС в данном случае будет назначаться интервал в ресурсной сетке, в течении которого необходимо передать преамбулу произвольного доступа. Преамбула генерируется на основе последовательностей Задова-Чу с нулевой зоной корреляции, всего определено 64 различных преамбулы на одну ячейку. БС, приняв запрос доступа, отвечает в том же самом канале произвольного доступа (но уже нисходящем) подтверждением. Если подтверждение не получено, АУ повторяет запрос. Количество каналов больше в нисходящем направлении::

1. общий канал (Physical Downlink Shared Channel – PDSCH);
2. канал управления (Physical Downlink Control Channel – PDCCH);
3. канал групповой передачи (Physical Multicast Channel – PMCH);
4. широковещательный канал (Physical Broadcast Channel – PBCH);
5. индикаторный канал управления форматом (Physical Control Format Indicator Channel– PCFICH) и индикаторный канал гибридной процедуры повторного запроса (HARQ) Physical Hybrid ARQ Indicator Channel (PHICH).

Назначение общего канала очевидно – передача данных конкретным абонентским устройствам. В канале управления PDCCH передаются таблицы с назначением канальных ресурсов абонентским устройствам – как в нисходящем, так и в восходящем каналах. В канале PCFICH, который передается в каждом субкадре, указываются номера OFDM-символов, которые используются для трансляции сообщений канала управления PDCCH. Канал PHICH предназначен для подтверждения доставки данных в восходящем канале. Назначение каналов групповой передачи и широкого вещания также очевидны. Отметим особенность широковещательного канала – каждый блок транспортного широковещательного канала (с верхних уровней протокола) транслируется в четырех субкадрах,

следующих с жестко фиксированным интервалом в 40 мс. Это исключает необходимость в дополнительных указателях на расположение этих субкадров.

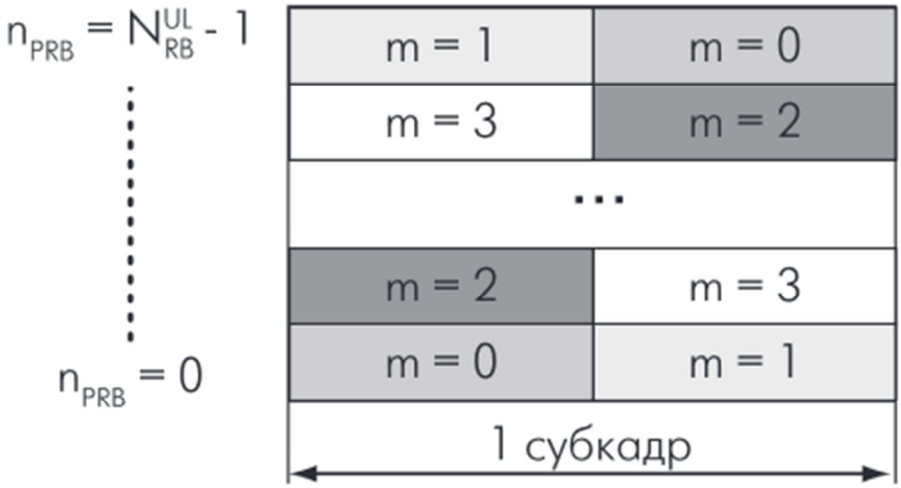

Рисунок 26 – Варианты расположения канала управления PUCHH в нисходящем канале

3 ИССЛЕДОВАНИЕ ОРТОГОНАЛЬНОГО СУБПОЛОСНОГО БАЗИСА В ЗАДАЧЕ ПОЫШЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

В ходе выполнения выпускной квалификационной работы необходимо анализировать и исследовать реальные технологии с конкретными параметрами. В качестве исследуемой беспроводной технологии было принято использовать модель LTE, так как в связи с бурным развитием технологий передачи и ее перспективами в этой отрасли на ближайшее будущее она является наиболее оптимальным вариантом среди других беспроводных технологий передачи.

Естественно, в ходе исследования параметры, математическая модель, базис, и необходимые результаты, которые будут при этом отражаться будут постоянно меняться, из чего можно сделать вывод, что при выполнения данной выпускной квалификационной работы необходимо прибегнуть к использованию имитационного моделирования, так как оно в наибольшей степени подходит для процесса исследования тематики работы.

Наиболее оптимальной с точки зрения инженера «не программиста» средой имитационного моделирования является программный продукт Matrix Laboratory, он же далее – MatLab. Широкий набор разнообразных встроенных инструментов и функций, а так-же возможность пользователя самостоятельно добавлять необходимые опции позволяет обширно и эффективно подходить к решению многих задач, используя MatLab.

В состав данного ПО уже входит OFDM канал с анализатором помехоустойчивости и скремблером поднесущих, что очень удобно, так как нет необходимости с нуля моделировать уже существующие методы, так как некоторые из параметров системы LTE не являются открытыми и, возможно, некоторых частей технологии в открытом доступе вообще нет, так как она не является разглашенной и открытой. В случае же данного инструмента можно проводить исследования LTE меняя дефолтные параметры, либо, при желании

добавлять свои или изменять структуру программного кода самого инструмента под нужды пользователя.

Со стороны пользователя при использовании LTE System Toolbox необходимо лишь указать некоторые из базовых параметров канала, такие как:

- Модуляционный алфавит;
- Число поднесущих;
- Количество передаваемых символов;
- Циклический префикс;
- Количество бит в одном символе;
- Количество ошибочных бит.

Так же следует указать тип модуляции (в ходе данной работы будут применяться QPSK для базиса оптимальных канальных сигналов с частотным уплотнением и OFDM для базиса Фурье) и ширину защитных интервалов (в нашем случае это 106 бит). После чего можно моделировать канал LTE с различными базисами. Отличительной особенностью подобных систем является то, что при необходимости можно добавить в основной скрипт программы несколько пользовательских функций или правок для более подробного рассмотрения технологии. В нашем случае необходимо формировать не один символ (как это установлено по умолчанию в данной функции) а несколько и исследовать спектр данных сигналов, что возможно сделать, немного подредактировав скрипт программы.

3.1 Формирование канального сигнала на основе базиса FFT в технологии LTE

При формировании сигналов с OFDM потом информационных символом для начала обрабатывается в блоке помехоустойчивого кодирования, после чего обработанная последовательность подается на модулятор. Модулятор в данном случае преобразовывает поступившую в него последовательность в двоичные модуляционные символы основываясь на принципе манипуляции. Затем

полученный поток данных преобразуется из последовательного в параллельный. Групповой сигнал формируется при помощи ОБПФ; так же на данном этапе к сигналу добавляются пилотные поднесущие, которые позволяют оценивать параметры канала. Обратное преобразование в аналоговую форму производится при помощи ЦАП.

Спектр дискретного сигнала является периодической функцией с периодом, равным частоте дискретизации Fs. Восстановление аналогового сигнала осуществляется с помощью ЦАП и фильтра нижних частот (ФНЧ) с полосой пропускания $\Delta Fз$. Амплитудно-частотная характеристика ФНЧ должна быть плоской в области основного лепестка спектра сигнала с OFDM и быстро спадать вне основного лепестка, чтобы эффективно подавить копии спектра дискретного сигнала.

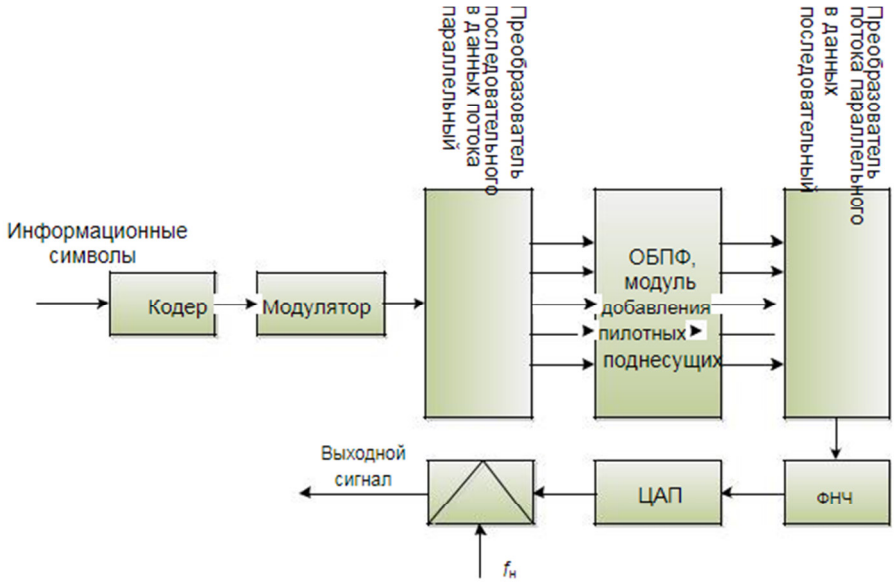

Рисунок 27 - Обобщенная структурная схема устройства формирования сигналов с OFDM

В реальных условиях аппаратура формирования сигналов с OFDM включает в себя блоки помехоустойчивого кодирования, перемежения, блоки тактовой и цикловой синхронизации, блоки введения защитного интервала и другое. [12]

В нашем случае задаются такие параметры как:

– Модуляционный алфавит - M = 4; k = log2(M);

– Количество несущих частот - N=512;

– Число информационных поднесущих OFDM - numSC = 300;

– Циклический префикс OFDM - cpLen = N/16;

– Количество ошибочных бит - maxBitErrors = 100;

– Количество передаваемых бит - maxNumBits = 1e3;

– Ширина полосы пропускания – 5Мгц;

Результатом будет сформированный в OFDM канале сигнал, основанный на базисе Фурье. Для более подробного исследования необходимо поместить данный сигнал в канал с шумом (встроенная в MatLab функция awgn [13]), с соотношением сигнал шум, равным 10%. Спектры чистого и зашумленного сигналов с базисом Фурье показаны на рисунке 28:

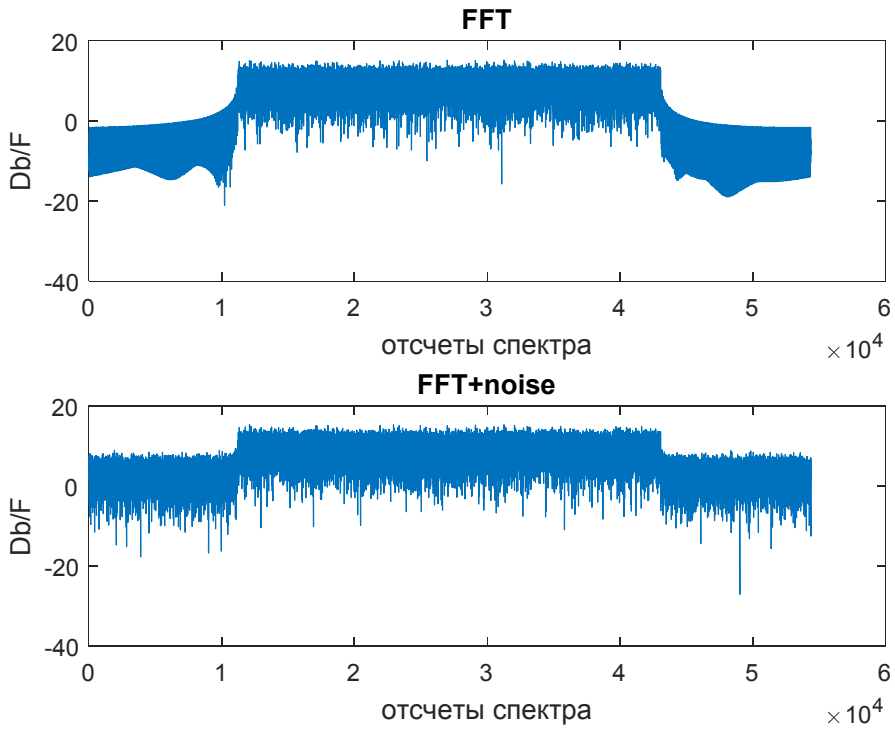

Рисунок 28 – Спектры чистого и зашумленного сигналов на основе базиса FFT при полосе 5 МГц с циклическим префиксом равным 32

Стоит заметить, что на данном этапе не присутствует никакого шифрования или стеганографии. Безопасность информации обеспечивается в данном случае

простым перемешиванием несущих частот. Для злоумышленника в данном случае, число таких перемешиваний будет равно:

$$C_{300}^{1} = \frac{300!}{1 * (300 - 1)!} * 4 = 300 * 4 = 1200$$

Так как на каждой поднесущей передается не один бит а один символ, содержащий исходя из QAM модуляции 4 бита, то необходимо 300*4=1200 переборов чтобы получить полный доступ к данным, что составляет трудности при попытке декодирования информации. Так как помимо «вскрытия» основного алгоритма шифрования данных (какой-нибудь AES или WPA) и в некоторых случаях, устранения влияния методов стеганографии придется еще покопаться.

Данный механизм не требует каких-либо дополнительных затраты на свою реализацию, существенным образом не меняет структуру беспроводной технологии передачи данных, что выглядит весьма перспективным и заманчивым (в случае каких-либо крупных операторов либо же организаций, активно и в широких масштабах пользующихся такого рода технологиями не придется тратиться на модернизацию своей существующей сети либо кардинальным образом усложнять уже имеющиеся сегменты сети).

В таблице 1 отражены результаты моделирования системы с базисом FFT при различной ширине рабочей полосы:

Таблица 1 – Параметры системы с базисом FFT

Ширина полосы	Число ошибочных бит	Число передаваемых бит	Длина циклического префикса	Длина частотного защитного интервала	Количество переборов
2.5 МГц	50000	500000	16	53	600
5 МГц	100000	1000000	32	106	1200
10 МГц	200000	2000000	64	212	2400
20 МГц	400000	4000000	128	424	4800

Из таблицы 1 можно сделать вывод, что параметры системы, такие как:

– Криптостойкость;

– Помехоустойчивость;

– Количество несущих частот;

– Количество информационных поднесущих;

– Число передаваемых бит;

– Число ошибочных бит;

– Длина циклического префикса;

– Длина защитного интервала.

будут зависеть от ширины рабочей полосы (чем шире полоса, тем больше потребуется несущих, информационных поднесущих, передаваемых и ошибочных бит, длина циклического префикса и защитного частотного интервала и наоборот, чем меньше полоса, тем меньше и значения вышеперечисленных параметров).

3.2 Формирование оптимального канального сигнала с частотным уплотнением на основе ортогонального субполосного базиса

Суть метода состоит в формировании канального сигнала на основе собственных векторов (далее SubBand) с определенными коэффициентами, которыми являются информационные биты исходного сигнала. Последовательность бит должна иметь биполярный вид. Такой вид исходной последовательности исключает возможность потери собственного вектора при перемножении на нулевой коэффициент.

Для формирования оптимального канального сигнала, прежде всего, следует вычислить элементы субполосной матрицы A для заданного частотного интервала по формуле (5).

Количество собственных чисел близких или равных единице определяют сколько собственных векторов удовлетворяют условию по оптимальному занятию выделенной полосы частот, тем самым можно определить количество бит *J*,

которые можно передать в выбранной последовательности, при том что один бит соответствует одному собственному вектору.

Формируем матрицу $Q = \{q_1, q_2, \dots, q_j\}$ размерностью [*N*x*J*], состоящую из собственных векторов q, соответствующие собственные числа которых близки или равны единице.

На приемной стороне регистрируются N значений, и осуществляется перемножение на заранее известную транспонированную матрицу собственных векторов q и исходя из условия (8) можно восстановить переданный информационный вектор.

$$e = Q^t * x = Q^t * Q * e = 1 * e$$

где e - восстановленный информационный вектор.

Таким образом, имея идеальный канал связи, т.е. передача канального сигнала осуществляется без искажений и помех, восстановленный вектор будет совпадать с первоначальным.

Если $x = x + \varepsilon$ где ε - помехи в канале связи, то необходимо использовать решающую процедуру отнесения символа e_i к 1 или к 0, на основе скалярных произведений $e_i = e_i + (\varepsilon_i * q_i)$

Решающее устройство с порогом $h=0$, принимает решение о наличии логической единицы, если $e_i > 0, i = 1 \dots . J$ или логического нуля, если $e_i < 0, i = 1 \dots . J$ таким образом восстанавливая исходный информационный вектор. Безопасность передачи информации обеспечивается за счет перестановок собственных векторов перед формированием канального сигнала, что потребует знание точного расположения переставленных собственных векторов при восстановлении данных на приемной стороне, ключом данного метода защиты будет являться карта точного расположения собственных векторов.

Здесь A - квадратная, симметричная субполосная матрица:

$$\mathrm{A} = \{\mathrm{a_{ik}}\}, \mathrm{i}, \mathrm{k} = 1, \dots, \mathrm{N} \qquad (3)$$

$$a_{ik} = \int_{v\epsilon V} \frac{exp[-jv(i-k)]dv}{2\pi},\ j = \sqrt{-1} \quad (4)$$

Элементы матрицы А вычисляются исходя из:

$$a_{ik} = \frac{\{sin[v_2(i-k)]-sin[v_1(i-k)]\}}{[\pi(i-k)]}, i \neq k \quad (5)$$

$$a_{ik} = \frac{v_2 - v_1}{\pi}, i = k$$

V- заданный частотный интервал

$$V = [-v_2, -v_1) \cup (v_1, v_2] \quad (6)$$

границы которого удовлетворяют условию $0 \leq v_1 < v_2 \leq \pi$

После вычисляются собственные вектора и числа данной матрицы где для определённости предполагается, что собственные числа упорядочены по убыванию и обладают следующими свойствами:

$$\lambda_1 > \lambda_2 > \cdots > \lambda_N > 0$$
$$\|q_i\|^2 = \sum_{k=1}^{N} q_{ki}^2 = 1$$
$$(q_k, q_i) = \sum_{r=1}^{N} q_{ri} q_{rk} = 0, i \neq k \quad (7)$$

Исходя из условия (7) значения собственных чисел соответствующих собственных векторов не превышают единицу, поскольку

$$\lambda_i = \frac{1}{2\pi}\int_{w\epsilon V} |Q_i(w)|^2 dw \leq \sum_{k=1}^{N} q_{ik}^2 \quad (8)$$

$$Q_i = \sum_{k=1}^{N} q_{ik} e^{-jw(k-1)} \quad (9)$$

Таким образом, из условия (9) следует, что собственные векторы, энергия которых максимально сосредоточенна в заданной полосе, обладают

соответствующими собственными числами, значения которых равны или близки к единице.

Исходя из исследований, проведенных в [7] можно сделать вывод, что данный метод позволяет существенно повысить эффективность использования частотных ресурсов путем минимизации доли энергии за переделами заданного частотного интервала, также при этом существенно понизить интерференцию между соседними каналами. Более подробно вопросы исследования формирования оптимальных канальных сигналов с частотным уплотнением рассмотрены в [7].

После проведения всех необходимых вычислений имеем спектр сигнала с использованием метода SubBand который показан на рисунке 29:

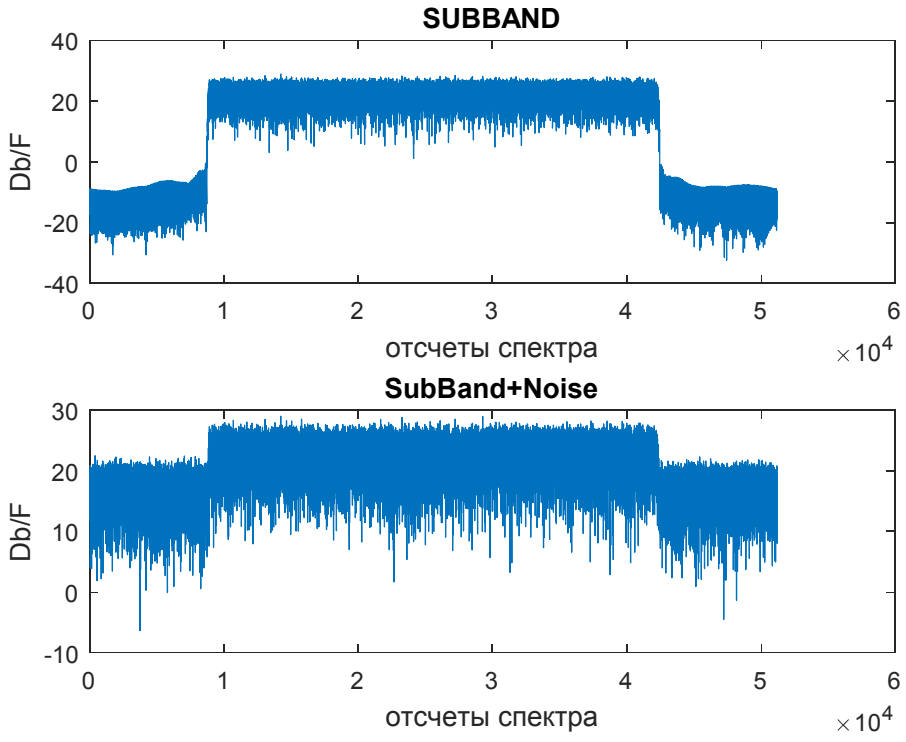

Рисунок 29 – Спектр сигнала с SubBand полосе 5 МГц с циклическим префиксом равным 32

Так как количество поднесущих (в сравнении с обычным FFT) увеличено на 10% (т.е 330 а не 300) то и число перестановок поднесущих будет так же выше. В качестве информационных несущих можно по прежнему использовать 300, а в

новообразовавшиеся 30 поднесущих можно передавать липовые данные для того, чтобы сильнее запутать злоумышленника.

$$C_{300}^{1} = \frac{330!}{1*(330-1)!}$$=330*4=1320.

Из этого можно сделать вывод, что 1320 перестановок вместо 1200 необходимо больше времени и вычислительного ресурса, чтобы получить искомую комбинацию поднесущих и расшифровать данные. Исходя из этого защищенность информации возрастает на 10% в сравнении с использованием метода формирования канального сигнала с FFT базисом.

3.3 Оценка сигналов с различной ортогональной базой

Для определения эффективности разработанного метода необходимо сравнить его параметры с параметрами сигнала с базисом FFT при различной ширине полосы в ходе моделирования. На рисунке 30 отражен результат моделирования двух сигналов с различной ортогональной базой:

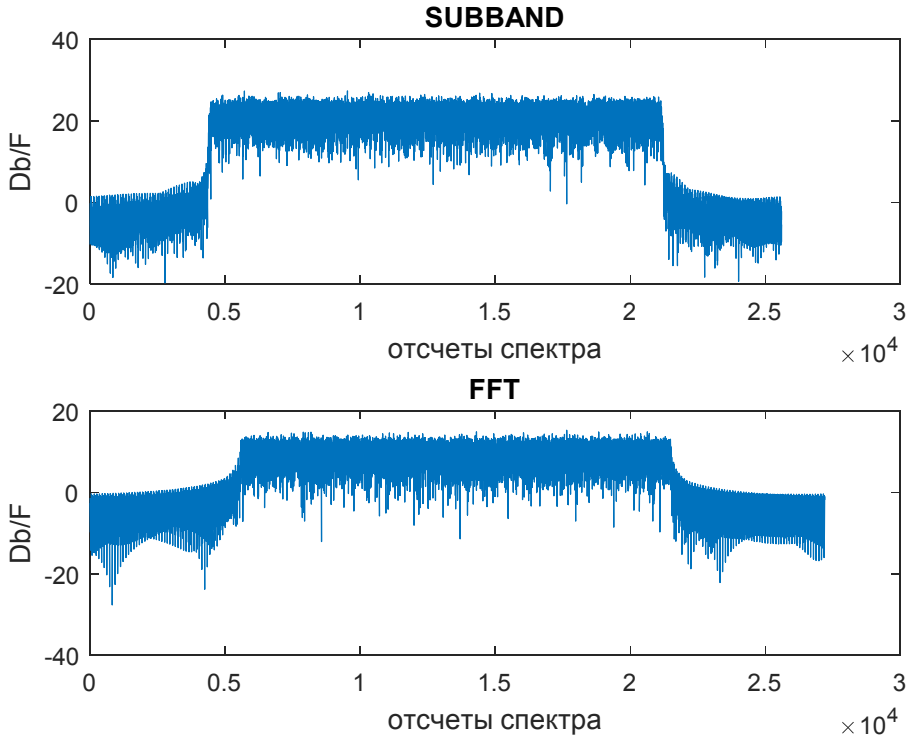

Рисунок 30 – Энергетический спектр сигналов с различной ортогональной базой при ширине полосы 2.5 МГц с циклическим префиксом равным 16

На рисунке 30 видно, что метод формирования оптимальных канальных сигналов более эффективно использует частотно-временные ресурсы, из чего следствием является возможность добавления в процесс передачи дополнительных поднесущих за счет использования защитных частотных полос. Следствием увеличения объема передаваемой информации является снижение помехоустойчивости такой системы, что отражено на рисунке 31:

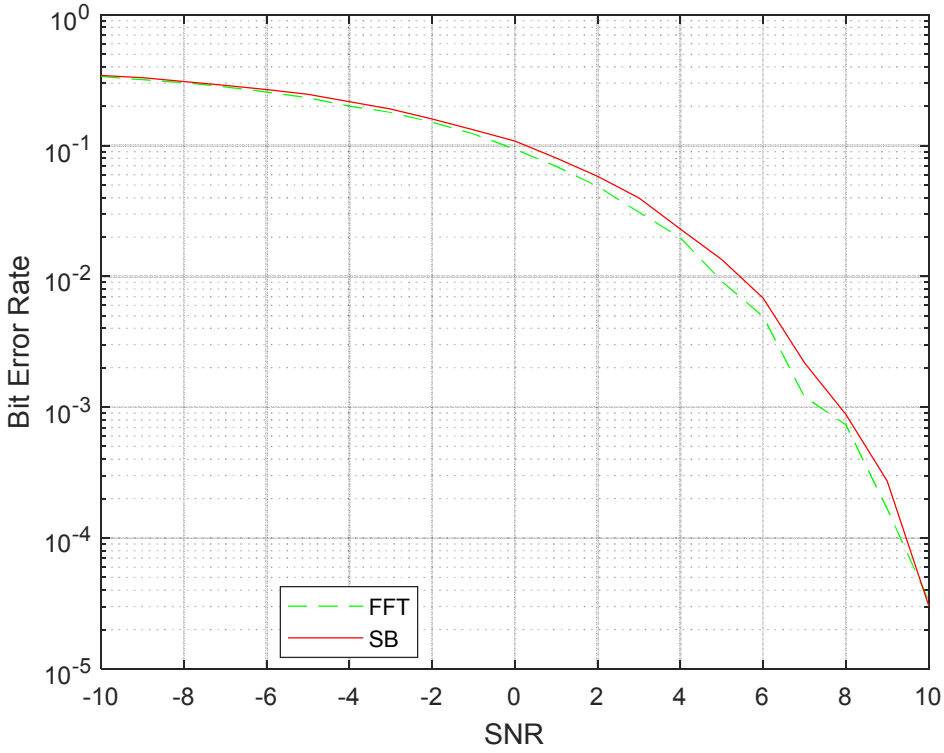

Рисунок 31 – Помехоустойчивость систем с различной ортогональной базой при ширине полосы 2.5 МГц с циклическим префиксом равным 16

Рисунок 31 показывает что помехоустойчивость системы при использовании метода SubBand меньше чем у системы, в которой применяется метод FFT, как было сказано выше, связано это с тем, то при использовании базиса SubBand в одной и той же полосе передается на 10% больше информации, что влечет за собой дополнительные затраты энергетического ресурса канала, что в свою очередь сказывается на помехоустойчивости. Хотя показатель в 2-4% не является критичным, если его можно так назвать, в некоторых случаях он может в значительной степени повлиять на работу всей системы беспроводной передачи данных. Однако если в случае полосы в 2.5 МГц при использовании FFT для передачи полезной информации используется 150 поднесущих, то в случае базиса SubBand в той же полосе 2.5 МГц будет передаваться 165 поднесущих, 15 из которых заполняются «липовыми» данными, что позволит повысить защищенность информации, так как количество переборов этих поднесущих будет увеличено на 10%.. Если вычислительный ресурс системы позволяет реализовать данный алгоритм допуская влияние на помехоустойчивость (можно

просто добавить в процесс передачи надежный помехоустойчивый код для устранения возможных возникающих ошибок в процессе передачи), то это может обеспечить выигрыш в защищенности информации такой системы в 10% в сравнении с стандартным применяемым базисом FFT без существенного изменения структуры системы.

Таблица 2 – Параметры системы с базисом SubBand

Ширина полосы	Число ошибочных бит	Число передаваемых бит	Длина циклического префикса	Длина частотного защитного интервала	Количество переборов
2.5 МГц	50	500000	16	53	660
5 МГц	100	1000000	32	106	1320
10 МГц	200	2000000	64	212	2640
20 МГц	400	4000000	128	424	5280

Если сравнить результаты, отраженные в таблицах 1 и 2, то можно сделать вывод, чт применение ортогонального субполосного базиса действительно позволяет повысить защищенность информации на 10% при различной ширине занимаемой полосы ценой снижения помехоустойчивости системы на 2-4% в сравнении с стандартным базисом FFT. Однако показатель в 10% не является пороговым и защищенность информации можно повысить в еще большей степени, изменив условие (9) из которого следует, что собственные векторы, энергия которых максимально сосредоточенна в заданной полосе, обладают соответствующими собственными числами, значения которых равны или близки к единице. Для максимального увеличения защищенности информации предлагается сделать следующее: использовать все собственные векторы, значения собственных числел которых больше 0.5. Результаты такого моделирования отражены в таблице 3.

Таблица 3 – Сравнение криптостойкости систем с различными базисами

Ширина полосы	Количество переборов		
	Базис FFT	Базис SubBand	
		L=1	L>0.5
2.5 МГц	600	660	674
5 МГц	1200	1320	1348
10 МГц	2400	2640	2697
20 МГц	4800	5280	5396

Исходя из данных, полученных в ходе исследования в пунктах 3.1 и 3.2, которые отражены в таблицах 1,2 и 3 можно сделать вывод, что при использовании метода формирования оптимальных канальных сигналов с частотным уплотнением количество переборов поднесущих (т.е криптостойкость системы) выше на 10% чем у системы с использованием базиса FFT и OFDM модуляции при практически одинаковой помехозащищенности систем. Важным моментом является то, что собственные вектора матрицы A, формируемой по (5) выбираются из соображений, что все собственные числа данной матрицы равны 1, поэтому количество дополнительных поднесущих и определяется как 10%. Можно сделать количество поднесущих большим, изменив условие с L=1 на L>0.5 что в среднем даст на 2.15% больше переборов в результате, но еще сильнее понизит помехоустойчивость системы, что не целесообразно, поэтому показатель в 10% является наиболее оптимальным.

4 ЭКОНОМИЧЕСКАЯ ЧАСТЬ

В реализации исследования были заняты следующие специалисты:

-Старший научный сотрудник(заведующий лабораторией);

-Младший научный сотрудник (проводящий исследование);

-Экономист (дающий оценку эффективности технико-экономических показателей исследования).

Расчет сроков проведения и трудоемкости представлен в таблице 4.

Таблица 4- Планирование работ по исследованию

Наименование этапов работ	**Исполнитель**	**Трудоемкость, час**	**Продолжительность, дней**
1	**2**	**3**	**4**
1.Подготовительный			
1.1.Сбор информации	Младший научный сотрудник	64	8
1.2.Выработка идеи	Старший научный сотрудник	16	2
1.3.Определение объема исследовательских работ	Младший научный сотрудник	32	4
1.4.Формирование исследовательской работы	Младший научный сотрудник	8	1
1.5.Обработка и анализ информации	Младший научный сотрудник	64	8
Итого:		184	23
2.Основной (экономический анализ)			
2.1.Обоснование целесообразности работы	Старший научный сотрудник	8	1
2.2.Выполнение работы	Младший научный сотрудник	160	20
Итого:		168	21
3.Заключительный			
3.1.Технико-экономическое обоснование	Экономист	8	1
3.2.Оформление и утверждение документации	Младший научный сотрудник	40	5
Итого:		48	6

Подводя итоги (основываясь на данных из таблицы) можно сделать вывод, что исследовательская работа провелась в течении 50 рабочих дней (по 8 часов) усилиями трех специалистов (старшего и младшего научных сотрудников и экономиста, оценившего эффективность работы).

4.1 Расчет расходов на оплату труда на исследование

Расчет расходов на оплату труда разработки исследования представлен в таблице 5.

Таблица 5 - Расчет расходов на оплату труда

Должность Исполнителей	**Трудоемкость, час**	**Оклад, руб**
1	**2**	**3**
Младший научный сотрудник	400	10000
Старший научный сотрудник	80	16000
Экономист	20	12000
Итого:	500	

Часовая тарифная ставка ($Ч_{ТС}$) рассчитывается по формуле:

$$Ч_{ТС} = \frac{P}{F_{мес}} \quad (10)$$

где $F_{мес}$ – фонд рабочего времени месяца, составляет 176 часов (22 рабочих дня по 8 часов в день); Р – оклад сотрудника.

Расход на оплату труда ($Р_{ОТ}$) находится следующим образом:

$$Р_{ОТ} = Ч_{ТС} * Т_{СУМ} \quad (11)$$

где $Т_{СУМ}$ – суммарная трудоемкость каждого из исполнителей.

Результаты расчетов сведены в таблицу 6.

Таблица 6 - Расчет расходов на оплату труда

Должность Исполнителей	**Трудоемкость, час**	**Оклад, руб**	**$Ч_{ТС}$, руб/час**	**$Р_{от}$, руб**
1	**2**	**3**	**4**	**5**
Младший научный сотрудник	400	10000	56,81	22724
Старший научный сотрудник	80	16000	90.9	7272
Экономист	20	12000	68.18	1363
Итого:	500			31359

4.2 Расчет продолжительности исследования

Согласно расчетам трудоемкость исследования составила 500 часа. Продолжительность исследования составит:

$$Т_{ИССЛ} = \frac{Т_{СУМ}}{Т_{РД}} \quad (12)$$

где $Т_{СУМ}$ = 500 часа суммарная трудоемкость исследования

$Т_{РД}$ = 8 часов – продолжительность рабочего дня

$$Т_{ИССЛ} = 500/8 = 63 \text{ дней.}$$

Продолжительность исследования составила 63 дня.

4.3 Расчет стоимости расходных материалов

В разделе стоимости расходных материалов учитываются расходы на приобретение основных материалов необходимых для проведения исследования, оформления соответствующей документации, а также учитывается стоимость картриджа. Расчет стоимости расходных материалов приведен в таблице 7.

Таблица 7 - Стоимость расходных материалов

Наименование расходных материалов	**Цена за единицу, руб.**	**Количество, шт.**	**Сумма, руб.**
1	**2**	**3**	**4**
Бумага	150	2	300
Канцтовары	180	-	180
Расходные материалы для принтера (картридж)	2000	-	2000
Итого:			2480

Исходя из таблицы 13 можно сделать вывод, что для проведения исследования на приобретение расходных материалов потребуется 2480 рублей.

4.4 Расчет сметы расходов на исследование

С учетом часового тарифной ставки рассчитаем общие расходы на разработку и проведение исследования. В данную статью расходов включаются премиальные выплаты, районный коэффициент и страховые взносы. Для оценки затрат на исследование составляем смету на разработку и проведение исследования.

Произведем расчет расходов:

Премиальные выплаты рассчитываются по формуле:

$$ПВ = Р_{ОТ}/К_{ПВ} \quad (13)$$

где $К_{ПВ}$ - коэффициент премиальных выплат, составляет 20 %, в случае если премии не предусмотрены $К_{ПВ}$=1.

$$ПВ = 31359 \cdot 0{,}2 = 6271.8 \text{ руб.}$$

Дополнительные затраты на проведение исследования можно определить как:

$$З_{ДОП} = К * Р_{ОТ} \quad (14)$$

где К - коэффициент дополнительных затрат (К=14%).

$$З_{ДОП} = Р_{ОТ} \cdot 14\ \%.$$

$$З_{ДОП} = 31359 \cdot 0{,}14 = 4390.26 \text{ руб.}$$

В заработной плате может быть предусмотрен районный коэффициент, которых характеризует доплату при работе в трудных условиях. Величина коэффициента определяется в зависимости от характера производства:

$$РК = Р_{ОТ} * К_{РВ} \quad (15)$$

где $К_{РВ}$ – коэффициент районных выплат, для примера составляет 15 % от суммы.

$$РК = (31359) \cdot 0{,}15 = 4703 \text{ руб.}$$

Общие расходы на оплату труда вычисляются по формуле:

$$Р_{ОБЩ} = Р_{ОТ} + РВ + РК + З_{ДОП} \quad (16)$$

где $Р_{ОТ}$ - основная заработная плата; ПВ - премиальные выплаты; $З_{ДОП}$ - дополнительные затраты; РК - районный коэффициент.

$$\Sigma\ Р_{ОТ} = 31359 + 6271.8 + 4390.26 + 4703 = 46724.06 \text{ руб.}$$

Из таблицы 13 берется итоговая сумма стоимости расходных материалов по статье расходных материалов.

$$\Sigma\ Р_{РМ} = 2480 \text{ руб.}$$

Страховые взносы рассчитываются по формуле:

$$СВ = Р_{ОТ} * 0.3 \quad (17)$$

$$СВ = 31359 \cdot 0{,}30 = 9407.7 \text{ руб.}$$

Амортизационные исчисления на использование компьютера составляют 25% от стоимости компьютера:

$$АО = 0.25 * С_{ПК} \quad (18)$$

$$АО = 20000 \cdot 0{,}25 = 5000 \text{ руб.}$$

Расходы на использование Интернета берутся из расчета месячной абонентской платы для предприятия. Пусть:

$$Р_{ИНТ}=350 \text{ руб.}$$

Административно-хозяйственые расходы составляют 50% от основной заработной платы ($Р_{ОТ}$).

$$Р_{АХ} = 0.5 * Р_{ОТ} \quad (19)$$

$$Р_{АХ}=31359 \cdot 0,5=15679.5 \text{ руб.}$$

Результаты расчета расходов сведем в таблицу. Смета расходов на разработку и проведение исследования представлена в таблице 8. **[14]**

Таблица 8 - Смета расходов на разработку и проведение исследования

Наименование статей расходов	**Сумма, руб.**	**Удельный вес статей, %**
1	**2**	**3**
1.Стоимость расходных материалов	2480	3.11
2. Расходы на оплату труда 2.1. Основная заработная плата	46724.06 31359	58.66
2.2. Дополнительные затраты	4390.26	5.51
2.3. Премиальные выплаты	6271.8	7.87
2.4 Районный коэффициент	4703	5.9
3. Единый социальный налог	9407.7	11.81
4. Амортизационные исчисления на использование компьютера	5000	6.27
5. Расходы на использование Интернет	350	0.43
6.Административно-хозяйственные расходы	15679.5	19.68
Итого:	79641.3	100

Исходя из данных таблицы 14 можно сделать вывод, что:

- продолжительность исследовательских работ составила 50 дней;
- сметы расходов на исследование – 79641.3 рублей.

ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы исследовались вопросы обеспечения информационной безопасности в беспроводных системах передачи. В частности, целью данной работы было увеличить защищенность информации в таких системах не прибегая к существенному изменению технологии либо применения дополнительных затрат. Задачами было исследование существующих методов обеспечения информационной безопасности и попытка их усовершенствования.

Как выяснилось, сделать это возможно если изменить математический аппарат системы еще на этапе формирования сигнала – то есть на физическом уровне. Безопасность передачи информации при этом обеспечивается за счет перестановок собственных векторов перед формированием канального сигнала, что потребует знание точного расположения переставленных собственных векторов при восстановлении данных на приемной стороне, ключом данного метода защиты будет являться карта точного расположения собственных векторов. Но, как следствие, при увеличении защищенности информации таким способом будет страдать помехозащищенность канала (выигрыш в защищенности составит 10 % а проигрыш в помехоустойчивости в 2-4%). Если такие показатели для каких-либо систем являются допустимыми, то данную технологию можно применять и даже совершенствовать.

Как показало исследование максимальным показателем защищенности, которого можно достичь является 12.15% но достигается это путем доплнительного снижения помехоустойчивости, что менее оптимально в сравнении с отношением защищенность/помехоустойчивость при 10%.

Так же следует заметить, что планируется дальнейшее более глубокое исследование уже с добавлением методов шифрования и стеганографии, которые теоретически еще больше увеличат показатель защищенности информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Наибольшая единица измерения информации, [Электронный ресурс] //rhish777.livejournal.com/ Основы информатики - Режим доступа: https://rhish777.livejournal.com/29327.html/ (дата обращения 19.02.2018)
2. Незащищенные Wi-Fi сети по всему миру, [Электронный ресурс] // https://securelist.ru/ Особенности Wi-Fi системы - Режим доступа: https://securelist.ru/research-on-unsecured-wi-fi-networks-across-the-world/29731/(дата обращения 19.02.2018)
3. Безопасность в сетях Wi-Fi, [Электронный ресурс]// https://interface31.ru/ Особенности шифрования в Wi-Fi - Режим доступа: https://interface31.ru/tech_it/2014/05/bezopasnost-v-setyah-wi-fi-chast-1-otkrytye-seti.html/ (дата обращения 19.02.2018)
4. Защита данных в беспроводных сетях Wi-Fi, WiMAX, LTE,[Электронный ресурс]// http://mirtelecoma.ru /Механизмы обеспечения информационной безопасности - Режим доступа: http://mirtelecoma.ru/magazine/elektronnaya-versiya/18/
   (дата обращения 9.03.2018)
5. Шифрование в сетях LTE, [Электронный ресурс]// http://1234g.ru /Криптография в сетях 4 поколения - Режим доступа: http://1234g.ru/4g/lte/printsip-raboty-seti-lte/bezopasnost-v-setyakh-lte/ (дата обращения 1.03.2018)
6. Алгоритм быстрого преобразования Фурье, [Электронный ресурс]// http://ru.dsplib.org /Основные математические алгоритм-Режим доступа: http://ru.dsplib.org/content/fft_introduction/fft_introduction.html/ (дата обращения 10.03.2018)
7. Оптимальные канальные сигналы с частотным уплотнением при цифровой передаче, [Электронный ресурс]// https://cyberleninka.ru/ Цифровые системы передачи- Режим доступа: https://cyberleninka.ru/article/v/optimalnye-kanalnye-

signaly-pri-tsifrovoy-peredache-s-chastotnym-uplotneniem / (дата обращения 12.03.2018)

8. Способ модуляции OFDM, [Электронный ресурс]// http://life-prog.ru /Описание модуляций- Режим доступа: http://life-prog.ru/1_39606_sposob-modulyatsii-OFDM.html/ (дата обращения 10.03.2018)
9. Много-антенные системы, [Электронный ресурс]]// http://1234g.ru/ Особенности LTE - Режим доступа: http://1234g.ru/4g/lte/fizicheskij-uroven-standarta-lte/mnogoantennye-tekhnologii-mimo-v-lte/ (дата обращения 15.03.2018)
10. Архитектура SAE, [Электронный ресурс]// http://pro3gsm.com /Особенности LTE-Режим доступа: http://pro3gsm.com/arhitektura-seti-lte/ (дата обращения 15.03.2018)
11. Описание LTE System Toolbox в Matlab, [Электронный ресурс]// https://matlab.ru /Официальный сайт MatLab-Режим доступа: https://matlab.ru/products/LTE-System-Toolbox/ (дата обращения 04.04.2018)
12. Формирование OFDM канала с базисом FFT, [Электронный ресурс] // https://studfiles.net/ Практическое применение OFDM - Режим доступа: https://studfiles.net/preview/2426815/page:11/ (дата обращения 5.04.2018)
13. Функция канала с шумом в MatLab, [Электронный ресурс]// http://matlab.exponenta.ru/ Официальный сайт MatLAb - Режим доступа: http://matlab.exponenta.ru/ communication/book2/9/awgn.php / (дата обращения 5.04.2018)
14. А.В. Болдышев «Методические рекомендации для ТЭО проекта» [текст], НИУ «БелГУ» 2017 – 25с.
15. С.Н. Девицына, С.Л. Бабаринов «Методические рекомендации по подготовке и защите выпускных квалификационных работ» [текст] НИУ «БелГУ» 2017 – 27с.
16. Б. Скляр «Цифровая связь. Теоретические основы и практическое применение» [Текст] Изд. 2-е, испр. Перевод с английского – издательский дом «Вильямс», 2003 - 1104 с. Парал.тит.англ

17. В.Олифер, Н.Олифер «Компьютерные сети: принципы, технологии, протоколы» [Текст] Изд. 5-е: «Питер» 2017, 963с.
18. Описание технологии LTE , [Электронный ресурс]// http://window.edu.ru /Сайт образовательного портала- Режим доступа: http://window.edu.ru/resource/169/75169/files/popov3.pdf/ (дата обращения 5.04.2018)
19. Алгоритмы формирования и приема OFDM сигналов на основе манипуляции с минимальным сдвигом частоты [Электронный ресурс]// http://jre.cplire.ru/ Разделение каналов -Режим доступа: http://jre.cplire.ru/jre/aug16/1/text.html/(дата обращения 5.04.2018)
20. Почему WiFi и LTE используют OFDM [Электронный ресурс]// https://habrahabr.ru /Описание радиосистем 3 и 4 поколения - Режим доступа: https://habrahabr.ru/post/129101/(дата обращения 5.04.2018)
21. Технология сотовой связи LTE [Электронный ресурс]// http://lvk.cs.msu.su /Описание LTE - Режим доступа:http://lvk.cs.msu.su/~vbabernov/.pdf / (дата обращения 5.04.2018)

ПРИЛОЖЕНИЕ 1

```
%МАТРЦИА ФУРЬЕ
clc
clear
M = 4;                  % Модуляционный алфавит
k = log2(M);
N=512;                  % Общее число несущих частот
numSC = 300;            % Число информационных поднесущих
maxBitErrors = 100;     % Число ошибочных бит
maxNumBits = 1e6;       % Число передаваемых бит
Fs=5000000;             %ПОЛОСА
GI=(N-numSC)/2;         %РАЗМЕР ЗАЩИТНОГО ЧАСТОТНОГО ИНТЕРВАЛА
f = 1000*(0:511)/Fs;
qpskMod = comm.QPSKModulator('BitInput',true);
qpskDemod = comm.QPSKDemodulator('BitOutput',true);

%Защитные интервалы устанавливаются в модуляторе и демодуляторе
ofdmMod=comm.OFDMModulator('FFTLength',N,'CyclicPrefixLength',N/16,'NumGuardBandCa
rriers',[GI;GI]);
ofdmDemod=comm.OFDMDemodulator('FFTLength',N,'CyclicPrefixLength',N/16,'NumGuardBa
ndCarriers',[GI;GI]);
errorRate = comm.ErrorRate;
ofdmDims = info(ofdmMod);
numDC = ofdmDims.DataInputSize(1);
frameSize = [k*numSC 1];
EbNoVec =(10)';
snrVec=(-10:10);

errorStats = zeros(1,3);
OO=zeros(N+N/16,40);
for m = 1:length(snrVec)
    for numS = 1:100
        dataIn = randi([0,1],frameSize);          %Рандомная последовательность
        qpskTx = step(qpskMod, dataIn);           % QPSK модуляция
        txSig=step(ofdmMod,qpskTx);               % OFDM модуляция
        OO(:,numS)=txSig;                         %ЧИСТЫЙ СИМВОЛ
        rxSig = awgn(txSig,snrVec(m),'measured');
        OON(:,numS)=rxSig;                        %ЗАШУМЛЕННЫЙ СИМВОЛ
        qpskRx = step(ofdmDemod,rxSig);           % OFDM ddемодуляция
         dataOut = step(qpskDemod,qpskRx);
         errorStats(numS,:) = step(errorRate,dataIn,dataOut);% ПОДСЧЕТ ВЕРОЯТНОСТИ
ОШИБКИ
         errorRate.reset;
    end
      berVec(m,:,1) = errorStats(:,1); %ВЕКТОР ОШИБОК
end
berTheory = berawgn(snrVec,'psk',M,'nondiff');
txSig1 = reshape(OO,[],1);
rxSig11 =  reshape(OON,[],1);
F=fft(txSig1);
F=F(1:25600);
N1=fft(rxSig11);

%СПЕКТР ФУРЬЕ
figure (1),
subplot(2,1,1)
plot(10*log10(abs(fftshift(F))));
title('FFT');
xlabel('отсчеты спектра');
ylabel('Db/F');
subplot(2,1,2);
```

```
plot(10*log10(abs(fftshift(N1))));
title('FFT+noise');
xlabel('отсчеты спектра');
ylabel('Db/F');
berVec=berVec';
m1=mean(berVec);

%Зависимость вероятности ошибки от snr
figure (2),
semilogy(snrVec,m1,'r')
hold on
legend('FFT','Location','Best')
xlabel('SNR')
ylabel('Bit Error Rate')
grid on
hold off

%СУБПОЛОСНАЯ МАТРИЦА
numSC2=numSC+0.1*numSC;
V=[-0.9, -0.1, 0, 2.07];
%Формирование субполосной матрицы A
for j=1:N
    for i=1:N
        if i~=j
            A(i,j)=(sin((V(4)*(i-j))-sin(V(3)*(i-j))))/(pi*(i-j));
        end
        if i==j
            A(i,j)=(V(4)-V(3))/pi;
        end
    end
end
[Q,L]=eig(A);%Собственные вектора субполосной матрицы A
Qmy = Q(:,183:end);%СОБСТВЕННЫЕ ВЕКТОРА СОБСТВЕННЫЕ ЧИСЛА КОТОРЫХ РАВНЫ ИЛИ ОКОЛО
1
Qmy2=Q(:,175:end); %Для SBmax
CP2=zeros(N/8,1);
CP2=step(qpskMod,CP2);
frameSize2=[k*numSC2 1];
frameSize22=[k*338 1]; %Для SBmax
for m = 1:length(snrVec)
    for numS = 1:100
        dataIn2 = randi([0,1],frameSize2);
        dataIn22 = randi([0,1],frameSize22);%Для SBmax
        qpskTx2 = step(qpskMod, dataIn2);
        qpskTx22 = step(qpskMod, dataIn22); %Для SBmax
        txSig2 = Qmy*qpskTx2;
        txSig22 = Qmy2*qpskTx22;            %Для SBmax
        OO2(:,numS)=txSig2;   %ВСЕ 100 СИМВОЛОВ
        OO22(:,numS)=txSig22;   %Для SBmax
        rxSig5 = awgn(txSig2,snrVec(m),'measured');          %ЗАШУМЛЕНИЕ
        rxSig55 = awgn(txSig22,snrVec(m),'measured');          %Для SBmax
        OON2(:,numS)=rxSig5;  %ВСЕ 100 СИМВОЛОВ ЗАШУМЛЕННЫЕ
        OON22(:,numS)=rxSig55;  %%Для SBmax
        otvet = Qmy.'*rxSig5;
        otvet2 = Qmy2.'*rxSig55; %Для SBmax
        dataOut2=step(qpskDemod,otvet);
        dataOut22=step(qpskDemod,otvet2); %Для SBmax
        errorStats2(numS,:) = step(errorRate,dataIn2,dataOut2);
        errorStats22(numS,:) = step(errorRate,dataIn22,dataOut22);%Для SBmax
        errorRate.reset
    end
    berVec2(m,:,1) = errorStats2(:,1);
    berVec22(m,:,1) = errorStats22(:,1); %Для SBmax
end
```

```
txSig2 = reshape(OO2,[],1);
rxSig22 = reshape(OON2,[],1); %Для SBmax
F2=fft(txSig2);
N2=fft(rxSig22);
berVec2=berVec2';
m2=mean(berVec2);
txSig22 = reshape(OO22,[],1); %Для SBmax
rxSig222 = reshape(OON22,[],1); %Для SBmax
F22=fft(txSig22); %Для SBmax
N22=fft(rxSig222); %Для SBmax
berVec22=berVec22'; %Для SBmax
m22=mean(berVec22); %Для SBmax

%SB  и SB+Noise
figure (4),
subplot(2,1,1)
plot(10*log10(abs(fftshift(F2))));
title('SUBBAND');
xlabel('отсчеты спектра');
ylabel('Db/F');
subplot(2,1,2)
plot(10*log10(abs(fftshift(N2))));
title('SUBBAND+NOISE');
xlabel('отсчеты спектра');
ylabel('Db/F');

%SB и SBmax
figure (5),
semilogy(snrVec,m2,'g--')
hold on
semilogy(snrVec,m22,'r')
hold on
legend('SB при L=1','SB при L>0.5','Location','Best')
xlabel('SNR')
ylabel('Bit Error Rate')
grid on
hold off

%FFT и SB
figure (6),
semilogy(snrVec,m1,'g')
hold on
semilogy(snrVec,m2,'r')
hold on
legend('FFT','SB','Location','Best')
xlabel('Eb/No (dB)')
ylabel('Bit Error Rate')
grid on
hold off
```

Выпускная квалификационная работа выполнена мной совершенно самостоятельно. Все использованные в работе материалы и концепции из опубликованной научной литературы и других источников имеют ссылки на них.

«___» _____ _____ г.

_____ _____

(подпись) *(Ф.И.О.)*