Санкт-Петербургский государственный политехнический университет

Институт информационных технологий и управления

Кафедра информационных и управляющих систем

Работа допущена к защите

Зав. кафедрой ИУС

\_\_\_\_\_\_\_\_И.Г. Черноруцкий

«\_\_\_\_\_»\_\_\_\_\_\_\_\_ 2015 г.

**ВЫПУСКНАЯ РАБОТА БАКАЛАВРА**

Тема: Разработка протокола канального уровня с прямым исправлением ошибок

Направление**:** 230100 – Информатика и вычислительная техника

Санкт-Петербург

2015 г.

Содержание

[Введение 3](#_Toc420433620)

[1. Анализ методов передачи данных. 7](#_Toc420433621)

[1.1 Базовая эталонная модель OSI 7](#_Toc420433622)

[1.2 Канальный уровень базовой эталонной модели OSI 10](#_Toc420433623)

[1.3 Обзор проколов канального уровня 12](#_Toc420433624)

[1.3.1 Высокоуровневый протокол управления каналом(HDLC) 12](#_Toc420433625)

[1.3.2 Протокол стандарта IEEE 802.3 15](#_Toc420433626)

[Семейство протоколов стандарта IEEE 802.3 – это самое распространенное семейство протоколов в данный момент. 15](#_Toc420433627)

[В первых версиях стандарта указано, что в качестве передающий среды указан коаксиальный кабель, в дальнейшем появилась возможность использовать витую пару и оптический кабель. Таким образом данный стандарт предлагает крайне надежную физическую среду передачи данных. 15](#_Toc420433628)

[1.3.3 Протокол стандарта IEEE 802.11 16](#_Toc420433629)

[IEEE 802.11 — набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9, 2,4, 3,6 и 5 ГГц. 16](#_Toc420433630)

[1.3.4 Протокол стандарта IEEE 802.16 17](#_Toc420433631)

[1.3.5 Постановка задачи 20](#_Toc420433632)

[2. Исследование существующих методов исправления ошибок 21](#_Toc420433633)

[**2.1. Коды Боуза—Чоудхури—Хоквингема (БЧХ-коды)** 21](#_Toc420433634)

[**2.2. Коды Соломона Рида** 23](#_Toc420433635)

[**2.3.** **Код Хэмминга** 24](#_Toc420433636)

[**2.4.** **Набор исследуемых кодов** 25](#_Toc420433637)

[**2.5.** **Обеспечение требуемой вероятности приема** 26](#_Toc420433638)

[**2.6.** **Минимизация времени задержки приема** 26](#_Toc420433639)

[3. Разработка и программная реализация канальных протоколов 27](#_Toc420433640)

[3.1. Обобщённая структура кадра 27](#_Toc420433641)

[3.2. Выбор способа реализации канальных протоколов для исследования. 27](#_Toc420433642)

[3.3 Алгоритм оценочного моделирования 29](#_Toc420433643)

[3.4 Реализация инструмента оценочного моделирования 30](#_Toc420433644)

[3.4 Проверка инструмента оценочного моделирования. 31](#_Toc420433645)

[4. Разработка архитектуры и реализация протокола передачи данных с исправлением данных. 32](#_Toc420433646)

[**3.1. Модель p a** 32](#_Toc420433647)

[**3.3. Двоичный симметричный канал** 35](#_Toc420433648)

[**3.4. Параметры исследования протоколов канального уровня** 37](#_Toc420433649)

[5. Анализ результатов. 38](#_Toc420433650)

[Таблица : лучшие протоколы с одним криптоблоком на кадр по потокам ошибок 39](#_Toc420433651)

[Таблица : лучшие протоколы с одиннадцатью криптоблоками на кадр по потокам ошибок 39](#_Toc420433652)

[Таблица : лучшие протоколы с шестнадцатью криптоблоками на кадр по потокам ошибок 40](#_Toc420433653)

[5. Заключение 41](#_Toc420433654)

[6. Список литературы 42](#_Toc420433655)

[**7. Приложение 1 Исходный код** 43](#_Toc420433656)

[**Приложение 2 Файл результатов** 53](#_Toc420433657)

[**Приложение 3 Интерфейс программы** 54](#_Toc420433658)

# Введение

Каналом передачи информации (каналом связи)называют совокупность устройств, обеспечивающих передачу сигналов с определёнными свойствами с одного пункта к другому. При построении системы канал, как правило, является заданным звеном, с которым источники и получатели должны быть согласованы посредством передатчиков и приёмников.

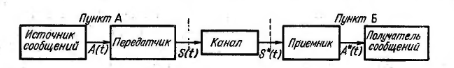


Рис. 1: система передачи информации от одного источника к одному получателю по одному каналу

A(t) – сообщение поступающее от источника.

S(t) – сигнал полученный после преобразования сообщения A(t) передатчиком.

S\*(t) – сигнал полученный на выходе канала (выходной или принимаемый).

A\*(t) – сообщение преобразованное из сигнала S\*(t) приёмником.

Каналы связи характеризуются по различным признакам:

* По используемым линиям связи:
  + Кабельные;
  + Радиорелейные;
  + Тропосферные;
  + И др.
* По полосе частот сигнала в линии:
  + Тональные;
  + Высокочастотные;
  + Коротковолновые;
  + Световые;
  + И др.
* По техническому характеру сигналов и назначению систем связи:
  + Телефонные;
  + Звукового вещания;
  + Телевизионные;
  + Телеграфные;
  + Передачи цифровой информации;
  + И др.

При математическом описании каналы различают, в первую очередь, по типу множеств которым принадлежат входные и выходные сигналы (непрерывные и дискретные), и по характеру изменения этих сигналов во времени (каналы непрерывного и дискретного времени).

Среди непрерывных каналов непрерывного времени можно выделить два наиболее типичных:

1. Непосредственно линия связи, часто с усилительным или переприёмным (ретрансляционным) оборудованием. Такой канал входит в состав всех других каналов связи.
2. Отличается от первого наличием модуляционного и демодуляционного оборудования (часто многоступенного) и полосой пропускания. Примерами таких каналов могут служить телевизионные каналы, тракты систем высокочастотного телефонирования и т.п.

Дискретный канал чаще всего дискретен и по времени. Он состоит из непрерывного канала и подключенных к нему формирователя сигналов (дискретного модулятора) и решающего устройства. Последние и обуславливают дискретность множества входных и выходных элементарных сигналов. В идеальном случае эти два устройства действуют синхронно.

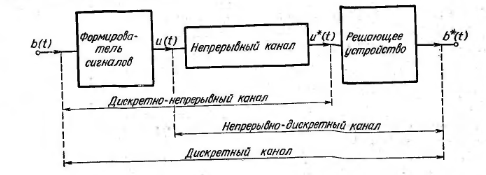


Рис.2: Дискретный канал

Дискретный канал связи предназначен для передачи дискретных сигналов (символов). При передаче по такому каналу сообщение S(t) представляется некоторой последовательностью элементарных дискретных сообщений X(t), принадлежащих конечному множеству. В результате кодирования последовательность X(t) заменяется другой последовательностью Y(t), которая ставится в соответствие E(t). Последовательность Y(t) подаётся на вход дискретного канала.

Основной характеристикой дискретного канала является вероятность того или иного изменения символа на данной позиции. Эта характеристика определяется теми изменениями, которые претерпевает символ при передаче по каналу:

* Смещение во времени;
* Отличие на некоторых позициях выходных символов от входных(аддитивные ошибки);
* Смещение номеров позиций выходной последовательности символов от позиций входной последовательности символов (ошибки синхронизации);
* Появление на некоторых ошибках символов стирания.

При действии рассмотренных факторов основная характеристика дискретного канала зависит от номера позиции, от значения, передаваемого и всех ранее переданных символов.

Поток ошибок представляет собой дискретный случайный процесс E. Каждая позиция E по определённому правилу складывается соответствующей позицией Y (сообщение на выходе).

Представляется логичным и достаточно удобным рассматривать поток ошибок дискретного канала связи как ступенчатый случайный процесс. Такой подход позволяет при исследовании каналов связи использовать многочисленные важные результаты, полученные для случайных процессов.

# Анализ методов передачи данных.

# Базовая эталонная модель OSI

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Модель OSI | | | | |
| Уровень | | Тип данных | Функции | Примеры |
| Host layers | Прикладной (applicaiton) | Данные | Доступ к сетевым службам | HTTP, FTP, SMTP |
| Представительский(представления) (presentation) | Представление и шифрование данных | ASCII, EBCDIC, JPEG |
| Сеансовый(session) | Управление сеансом связи | RPC, PAP |
| Транспортный(transport) | Сегменты | Прямая связь между конечными пунктами и надежность | TCP, UPD |
| Media layers | Сетевой(network) | Пакеты, дейтаграммы | Определение маршрута и логическая адресация | [IPv4](https://ru.wikipedia.org/wiki/IPv4), IPv6, IPsec, [AppleTalk](https://ru.wikipedia.org/wiki/AppleTalk) |
| Канальный(data link) | Биты, Кадры | Физическая адресация | [PPP](https://ru.wikipedia.org/wiki/Point-to-Point_Protocol), 802.2, L, [ARP](https://ru.wikipedia.org/wiki/ARP) |
| Физический(physical) | Биты | Работа со средой передачи, сигналами и двоичными данными | DSL, USB |

Сетевая модель OSI(англ. *open systems interconnection basic reference model*— базоваяэталонная модельвзаимодействия открытых систем, сокр.ЭМВОС; 1978 год) —сетевая модельстекасетевых протоколовOSI/ISO (ГОСТ Р ИСО/МЭК 7498-1-99).

Любой протокол модели OSI должен взаимодействовать либо с протоколами своего уровня, либо с протоколами на единицу выше и/или ниже своего уровня. Взаимодействия с протоколами своего уровня называются горизонтальными, а с уровнями на единицу выше или ниже — вертикальными. Любой протокол модели OSI может выполнять только функции своего уровня и не может выполнять функций другого уровня, что не выполняется в протоколах альтернативных моделей.

Каждому уровню с некоторой долей условности соответствует свой операнд — логически неделимый элемент данных, которым на отдельном уровне можно оперировать в рамках модели и используемых протоколов: на физическом уровне мельчайшая единица — бит, на канальном уровне информация объединена в кадры, на сетевом — в пакеты (датаграммы), на транспортном — в сегменты. Любой фрагмент данных, логически объединённых для передачи — кадр, пакет, датаграмма — считается сообщением. Именно сообщения в общем виде являются операндами сеансового, представительского и прикладного уровней. К базовым сетевым технологиям относятся физический и канальный уровни.

Прикладной уровень (уровень приложений; англ. *application layer*) — верхний уровень модели, обеспечивающий взаимодействие пользовательских приложений с сетью:

* позволяет приложениям использовать сетевые службы:
  + удалённый доступ к файлам и базам данных,
  + пересылка электронной почты;
* отвечает за передачу служебной информации;
* предоставляет приложениям информацию об ошибках;
* формирует запросы к уровню представления.

Представительский уровень (уровень представления; англ. *presentation layer*) обеспечивает преобразование протоколов и кодирование/декодирование данных. Запросы приложений, полученные с прикладного уровня, на уровне представления преобразуются в формат для передачи по сети, а полученные из сети данные преобразуются в формат приложений. На этом уровне может осуществляться сжатие/распаковка или шифрование/дешифрование, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально. Обычно представляет собой промежуточный протокол для преобразования информации из соседних уровней. Это позволяет осуществлять обмен между приложениями на разнородных компьютерных системах прозрачным для приложений образом. Уровень представлений обеспечивает форматирование и преобразование кода. Форматирование кода используется для того, чтобы гарантировать приложению поступление информации для обработки, которая имела бы для него смысл. При необходимости этот уровень может выполнять перевод из одного формата данных в другой. Уровень представлений имеет дело не только с форматами и представлением данных, он также занимается структурами данных, которые используются программами. Таким образом, уровень 6 обеспечивает организацию данных при их пересылке.

Сеансовый уровень (англ. *session layer*) модели обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений.

Транспортный уровень (англ. *transport layer*) модели предназначен для обеспечения надёжной передачи данных от отправителя к получателю. При этом уровень надёжности может варьироваться в широких пределах. Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции (например, функции передачи данных без подтверждения приема), и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных. Например, UDP ограничивается контролем целостности данных в рамках одной датаграммы, и не исключает возможности потери пакета целиком, или дублирования пакетов, нарушение порядка получения пакетов данных; TCP обеспечивает надёжную непрерывную передачу данных, исключающую потерю данных или нарушение порядка их поступления или дублирования, может перераспределять данные, разбивая большие порции данных на фрагменты и наоборот склеивая фрагменты в один пакет.

Сетевой уровень (англ. *network layer*) модели предназначен для определения пути передачи данных. Отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и «заторов» в сети. Протоколы сетевого уровня маршрутизируют данные от источника к получателю. Работающие на этом уровне устройства (маршрутизаторы) условно называют устройствами третьего уровня (по номеру уровня в модели OSI).

Канальный уровень (англ. *data link layer*) предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля за ошибками, которые могут возникнуть. Полученные с физического уровня данные, представленные в битах, он упаковывает в кадры, проверяет их на целостность и, если нужно, исправляет ошибки (формирует повторный запрос поврежденного кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Физический уровень (англ. *physical layer*) — нижний уровень модели, который определяет метод передачи данных, представленных в двоичном виде, от одного устройства (компьютера) к другому. Составлением таких методов занимаются разные организации, в том числе: Институт инженеров по электротехнике и электронике, Альянс электронной промышленности, Европейский институт телекоммуникационных стандартов и другие. Осуществляют передачу электрических или оптических сигналов в кабель или в радиоэфир и, соответственно, их приём и преобразование в биты данных в соответствии сметодами кодирования цифровых сигналов. Функции физического уровня реализуются на всех устройствах, подключенных к сети. Со стороны компьютера функции физического уровня выполняются сетевым адаптером или последовательным портом. К физическому уровню относятся физические, электрические и механические интерфейсы между двумя системами. Физический уровень определяет такие виды сред передачи данных как оптоволокно, витая пара, коаксиальный кабель, спутниковый канал передач данных и т. п. Стандартными типами сетевых интерфейсов, относящимися к физическому уровню, являются: V.35, RS-232, RS-485, RJ-11, RJ-45, разъемы AUI и BNC.

# Канальный уровень базовой эталонной модели OSI

Канальный уровень (англ. *Data Link layer*) — второй уровень сетевой модели OSI, предназначенный для передачи данных узлам, находящимся в том же сегменте локальной сети. Также может использоваться для обнаружения и, возможно, исправления ошибок, возникших на физическом уровне. Примерами протоколов, работающих на канальном уровне, являются: Ethernet для локальных сетей (много узловой), Point-to-Point Protocol (PPP), HDLC и ADCCP для подключений точка-точка (двух узловой).

Канальный уровень отвечает за доставку кадров между устройствами, подключенными к одному сетевому сегменту. Кадры канального уровня не пересекают границ сетевого сегмента. Функции межсетевой маршрутизации и глобальной адресации осуществляются на более высоких уровнях модели OSI, что позволяет протоколам канального уровня сосредоточиться на локальной доставке и адресации.

Заголовок кадра содержит аппаратные адреса отправителя и получателя, что позволяет определить, какое устройство отправило кадр и какое устройство должно получить и обработать его. В отличие от иерархических и маршрутизируемых адресов, аппаратные адреса одноуровневые. Это означает, что никакая часть адреса не может указывать на принадлежность к какой-либо логической или физической группе. Когда устройства пытаются использовать среду одновременно, возникают коллизии кадров. Протоколы канального уровня выявляют такие случаи и обеспечивают механизмы для уменьшения их количества или же их предотвращения.

Многие протоколы канального уровня не имеют подтверждения о приёме кадра, некоторые протоколы даже не имеют контрольной суммы для проверкицелостности кадра. В таких случаях протоколы более высокого уровня должны обеспечивать управление потоком данных, контроль ошибок, подтверждение доставки и ретрансляции утерянных данных.

В программировании доступ к этому уровню предоставляет драйвер сетевой платы. В операционных системах имеется программный интерфейс взаимодействия канального и сетевого уровней между собой, это не новый уровень, а просто реализация модели для конкретной ОС. Примеры таких интерфейсов: ODI, NDIS.

Длина пакета, формируемого протоколом канального уровня, ограничена сверху посредством MTU. MTU может быть изменено. Минимальная длина кадра прописывается в стандартах и не может быть изменена.

Спецификация IEEE 802 разделяет этот уровень на 2 подуровня. MAC (Media Access Control) регулирует доступ к разделяемой физической среде, LLC (Logical Link Control) обеспечивает обслуживание сетевого уровня.

Функции канального уровня:

1. Получение доступа к среде передачи. Обеспечение доступа — важнейшая функция канального уровня. Она требуется всегда, за исключением случаев, когда реализована полно связная топология (например, два компьютера, соединенных через кроссовер, или компьютер со свичом в полнодуплексном режиме).
2. Выделение границ кадра. Эта задача также решается всегда. Среди возможных решений этой задачи — резервирование некоторой последовательности, обозначающей начало или конец кадра.
3. Аппаратная адресация (или адресация канального уровня). Требуется в том случае, когда кадр могут получить сразу несколько адресатов. В локальных сетях аппаратные адреса (MAC-адреса) применяются всегда.
4. Обеспечение достоверности принимаемых данных. Во время передачи кадра есть вероятность, что данные исказятся. Важно это обнаружить и не пытаться обработать кадр, содержащий ошибку. Обычно на канальном уровне используются алгоритмы контрольных сумм, дающие высокую гарантию обнаружения ошибок.
5. Адресация протокола верхнего уровня. В процессе декапсуляции указание формата, вложенного PDU существенно упрощает обработку информации, поэтому чаще всего указывается протокол, находящийся в поле данных, за исключением тех случаев, когда в поле данных может находиться один-единственный протокол.

# Обзор проколов канального уровня

# Высокоуровневый протокол управления каналом(HDLC)

Во всех бит-ориентированных протоколах используется формат кадра, показанный на рис.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 8 | 8 | 8 | 10 | 16 | 8 |
| 0 1 1 1 1 1 1 0 | Адрес | Управляющее поле | Данные | Контрольная  сумма | 0 1 1 1 1 1 1 0 |

Поле *Address* (адрес) чрезвычайно важно для линий с несколькими терминалами, где оно используется для идентификации одного из терминалов. В двухточечных сетях это поле иногда используется, чтобы отличать команды от ответов.

Поле *Control* (управляющей информации) используется для хранения порядковых номеров, подтверждений и других служебных данных.

Поле Data(данные) может содержать произвольную информацию. Оно может быть любой длины, хотя эффективность контрольной суммы снижается с увеличением длины кадра из-за увеличения вероятности многочисленных пакетов ошибок.

Поле Checksum(контрольная сумма) является разновидностью циклического избыточного кода.

В качестве заголовка и концевика кадра используется флаговый байт (01111110).

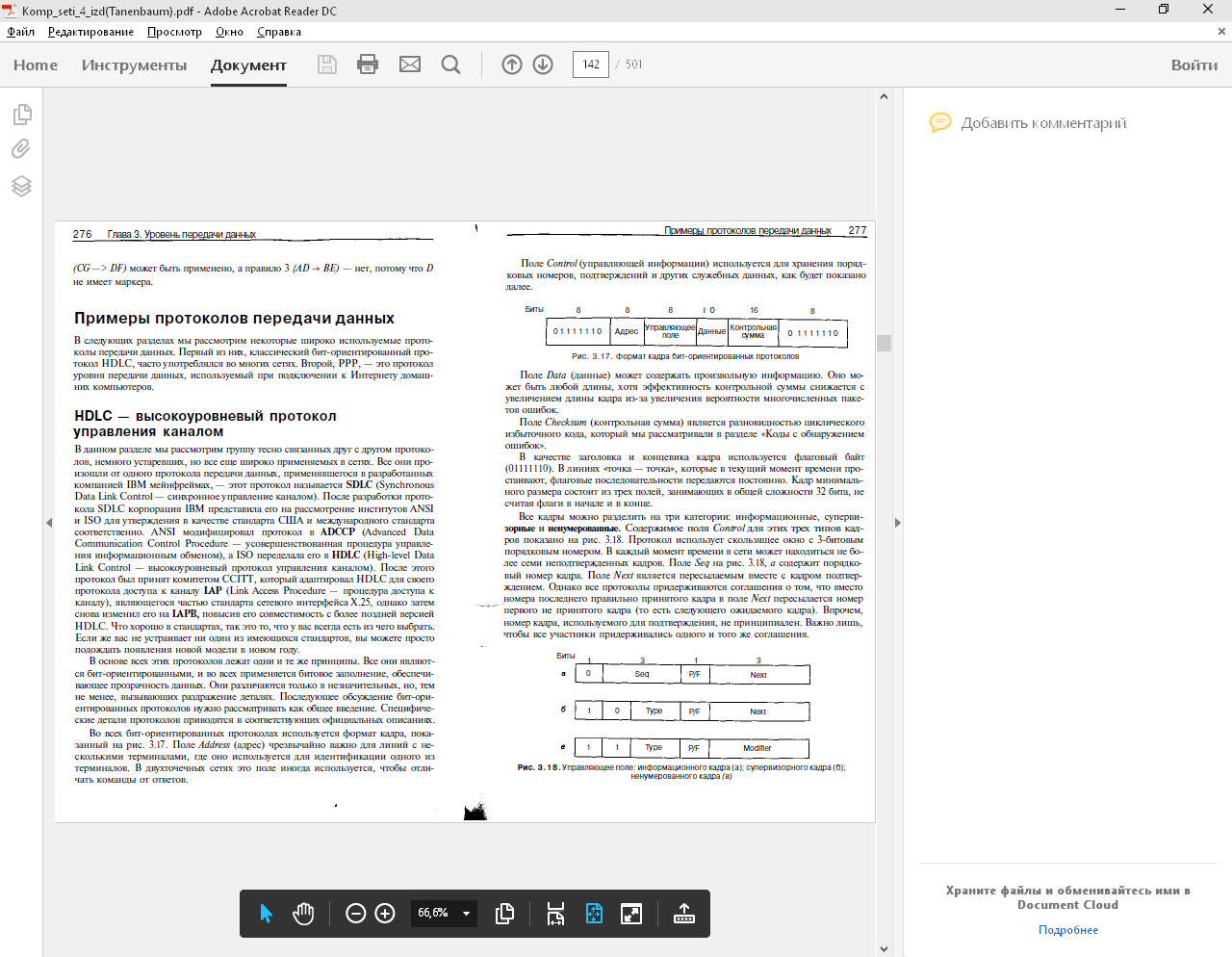
В линиях ≪точка — точка≫, которые в текущий момент времени проcтаивают, флаговые последовательности передаются постоянно. Кадр минимального размера состоит из трех полей, занимающих в общей сложности 32 бита, не считая флаги в начале и в конце.

Все кадры можно разделить на три категории: информационные, супервизорные и ненумерованные**.**

Содержимое поля *Control* для этих трех типов кадров показано на рис. 3.18. Протокол использует скользящее окно с 3-битовым порядковым номером. В каждый момент времени в сети может находиться не более семи неподтвержденных кадров. Поле *Seq* на рис. 3.18, *а* содержит порядковый номер кадра. Поле *Next* является пересылаемым вместе с кадром подтверждением. Однако все протоколы придерживаются соглашения о том, что вместо номера последнего правильно принятого кадра в поле *Next* пересылается номер

первого не принятого кадра (то есть следующего ожидаемого кадра). Впрочем,

номер кадра, используемого для подтверждения, не принципиален. Важно лишь,

чтобы все участники придерживались одного и того же соглашения. 

**Рис. . Управляющее поле: информационного кадра (а); супервизорного кадра (б);**

**ненумерованного кадра *(в)***

Бит *P/F* означает *Poll/Final* (Опрос/Финальный). Он используется, когда компьютер (или концентратор) опрашивает группу терминалов. В случае значения *Р* компьютер предлагает терминалу посылать данные. Во всех кадрах, кроме последнего, посылаемых терминалом, бит *P/F* устанавливается в Р. В последнем кадре этот бит устанавливается в *F.*

Некоторые протоколы используют бит *P/F,* чтобы заставить другую машину послать супервизорный кадр немедленно, не ожидая попутного потока данных. Этот бит также изредка используется в ненумерованных кадрах. Тип супервизорного кадра указывается с помощью значения поля *Туре.*

Если *Туре* = 0, значит, данный кадр является подтверждением. Он официально называется RECEIVE READY (к приему готов). Такой кадр сообщает номер следующего ожидаемого кадра и применяется при отсутствии попутного потока данных для передачи подтверждения.

*Туре* = 1 является признаком отрицательного подтверждения, официально называющегося REJECT (отказ). Он применяется для сообщения об обнаружении ошибки передачи. Поле *Next* в этом случае содержит номер первого неверно полученного кадра (то есть первого кадра, который следует переслать повторно). Отправитель должен переслать повторно все неподтвержденные кадры, начиная

с кадра с номером *Next.*

*Туре -* 2 означает RECEIVE NOT READY (к приему не готов). При этом, как и в случае RECEIVE READY, подтверждается прием всех кадров вплоть до *Next-i,* однако отправителю сообщается, что передачу следует приостановить. Сигнал неготовности к приему предназначен не для использования в качестве альтернативы схеме скользящих окон, а для обозначения наличия у получателя каких-либо временных проблем, например отсутствия свободной памяти в буферах. Когда получатель сможет продолжить работу, он пошлет сигнал готовности, отказа или другой управляющий кадр.

*Туре =* 3 означает SELECTIVE REJECT (выборочный отказ). Такой байт представ-

ляет собой запрос повторной передачи только указанных кадров. Наиболее полезен, когда

размер окна отправителя не превышает половины количества используемых порядковых номеров. Таким образом, если получатель хочет сохранить в буфере несвоевременные кадры для последующего использования, он может запросить повторную передачу любого кадра с помощью SELECTIVE REJECT.

Протоколы HDLC и ADCCP поддерживают этот тип кадра, а протоколы SDLC и LAPB — нет, то есть в этих протоколах нет команды выборочного отказа, а кадры типа 3 не используются.

Третий класс кадров составляют ненумерованные кадры. Иногда они применяются для служебных целей, но могут переносить и данные, когда требуется ненадежный, не требующий соединения сервис. В отличие от предыдущих двух классов, в которых различные бит-ориентированные протоколы были почти идентичными, в вопросе использования ненумерованных кадров они очень сильно различаются. Для обозначения типа кадра зарезервировано 5 бит, однако используются значительно меньше, чем 32 возможных комбинации.

Все протоколы поддерживают команду DISC (DISConnect — прервать связь),

позволяющую предупредить, что машина скоро будет выключена (например, для профилактического обслуживания). Также имеется команда, позволяющая машине, только что вернувшейся в подключенный режим (on-line), заявить о своем присутствии и принудительно обнулить все порядковые номера.

Эта команда называется SNRM (Set Normal Response Mode — установить нормальный режим ответа). К сожалению, этот ≪нормальный режим≫ является чем угодно, но не нормой. Это несбалансированный (то есть асимметричный) режим, при котором один конец линии является ведущим (master), а другой — ведомым (slave). Команда SNRM появилась еще в те времена, когда обмен данными означал общение примитивного терминала с компьютером, которое, конечно, было асимметричным. Чтобы лучше учитывать ситуацию равноправных партнеров, в протоколы HDLC и LAPB была добавлена команда SABM (Set Asynchronous Balanced Mode — установить асинхронный сбалансированный режим), которая инициализирует линию и объявляет равенство сторон. Кроме того, в этих протоколах имеются дополнительные команды SABME и SNRME, которые отличаются от SABM и SNRM только тем, что вводят расширенный формат кадров с 7-битовым порядковым номером вместо 3-битового.

Третьей командой, поддерживаемой всеми этими протоколами, является FRMR

(FRaMe Reject — отклонить кадр), применяющаяся, когда приходит кадр с верной контрольной суммой, но недопустимой семантикой. Например, супервизорный кадр типа 3 в протоколе LAPB, кадр длиной менее 32 бит, недопустимый управляющий кадр или подтверждение кадра, находящегося вне пределов окна и т. д. Данные включают управляющее поле неправильного кадра, параметры окна и набор битов, указывающих тип ошибки.

Управляющие кадры могут быть повреждены или потеряны так же, как и информационные кадры, поэтому им также нужны подтверждения. Для этой цели предназначен специальный служебный кадр, называемый UA (Unnumbered Acknowledgement — ненумерованное подтверждение). Поскольку неподтвержденным может быть только один управляющий кадр, то не возникает вопроса о том, какой именно служебный кадр подтверждается.

Остальные управляющие кадры занимаются инициализацией, опросом и сообщением состояния. Есть также управляющий кадр, который может содержать произвольную информацию, UI (Unnumbered Information). Эта информация не передается на сетевой уровень, но получается и обрабатывается самим уровнем передачи данных.

# Протокол стандарта IEEE 802.3

# Семейство протоколов стандарта IEEE 802.3 – это самое распространенное семейство протоколов в данный момент.

# В первых версиях стандарта указано, что в качестве передающий среды указан коаксиальный кабель, в дальнейшем появилась возможность использовать витую пару и оптический кабель. Таким образом данный стандарт предлагает крайне надежную физическую среду передачи данных.

Стандарт 802.3 определяет восемь полей заголовка:

* *Поле преамбулы*состоит из семи байтов синхронизирующих данных. Каждый байт содержит одну и ту же последовательность битов - 10101010. При манчестерском кодировании эта комбинация представляется в физической среде периодическим волновым сигналом. Преамбула используется для того, чтобы дать время и возможность схемам приемопередатчиков (transceiver) прийти в устойчивый синхронизм с принимаемыми тактовыми сигналами.
* *Начальный ограничитель* кадра состоит из одного байта с набором битов 10101011. Появление этой комбинации является указанием на предстоящий прием кадра.
* *Адрес получателя*- может быть длиной 2 или 6 байтов (MAC-адрес получателя). Первый бит адреса получателя - это признак того, является адрес индивидуальным или групповым: если 0, то адрес указывает на определенную станцию, если 1, то это групповой адрес нескольких (возможно всех) станций сети. При широковещательной адресации все биты поля адреса устанавливаются в 1. Общепринятым является использование 6-байтовых адресов.
* *Адрес отправителя* - 2-х или 6-ти байтовое поле, содержащее адрес станции отправителя. Первый бит - всегда имеет значение 0.
* Двухбайтовое *поле длины* определяет длину поля данных в кадре.
* *Поле данных* может содержать от 0 до 1500 байт. Но если длина поля меньше 46 байт, то используется следующее поле - поле заполнения, чтобы дополнить кадр до минимально допустимой длины.
* *Поле заполнения* состоит из такого количества байтов заполнителей, которое обеспечивает определенную минимальную длину поля данных (46 байт). Это обеспечивает корректную работу механизма обнаружения коллизий. Если длина поля данных достаточна, то поле заполнения в кадре не появляется.
* *Поле контрольной суммы*- 4 байта, содержащие значение, которое вычисляется по определенному алгоритму (полиному CRC-32). После получения кадра рабочая станция выполняет собственное вычисление контрольной суммы для этого кадра, сравнивает полученное значение со значением поля контрольной суммы и, таким образом, определяет, не искажен ли полученный кадр.

Кадр 802.3 является кадром MAС-подуровня, в соответствии со стандартом 802.2 в его поле данных вкладывается кадр подуровня LLC с удаленными флагами начала и конца кадра.

# Протокол стандарта IEEE 802.11

# IEEE 802.11 — набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9, 2,4, 3,6 и 5 ГГц.

Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с и, опционально, на скорости 2 Мбит/с. Один из первых высокоскоростных стандартов беспроводных сетей — IEEE 802.11a — определяет скорость передачи уже до 54 Мбит/с брутто. Рабочий диапазон стандарта — 5 ГГц.

Вопреки своему названию, принятый в 1999 году стандарт IEEE 802.11b не является продолжением стандарта 802.11a, поскольку в них используются различные технологии: DSSS (точнее, его улучшенная версия HR-DSSS) в 802.11b против OFDM в 802.11a. Стандарт предусматривает использование нелицензируемого диапазона частот 2,4 ГГц. Скорость передачи — до 11 Мбит/с. Обеспечивает сервис с потверждением без установки соединения.

Стандарт 802.11 может использовать различные методы обработки ошибки. Версия 802.11b предполагает лишь обнаружение ошибок с использованием циклического избыточного кода. Версия 802.11a и 802.11g предполагает использование сверточных кодов для прямого исправления ошибок. Однако прямое исправление ошибок реализовано не на канальном, а на физическом уровне.[]

# Протокол стандарта IEEE 802.16

**WiMAX** (англ. ***W****orldwide****I****nteroperability for****M****icrowave****A****ccess*) — телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов). Основана на стандарте IEEE 802.16, который также называют Wireless MAN (WiMAX следует считать жаргонным названием, так как это не технология, а название форума, на котором Wireless MAN и был согласован).

Название «WiMAX» было создано WiMAX Forum — организацией, которая была основана в июне 2001 года с целью продвижения и развития технологии WiMAX. Форум описывает WiMAX как «основанную на стандарте технологию, предоставляющую высокоскоростной беспроводной доступ к сети, альтернативный выделенным линиям и DSL». Максимальная скорость — до 1 Гбит/сек на ячейку.

WiMAX подходит для решения следующих задач:

* Соединения точек доступа Wi-Fi друг с другом и другими сегментами Интернета.
* Обеспечения беспроводного широкополосного доступа как альтернативы выделенным линиям и DSL.
* Предоставления высокоскоростных сервисов передачи данных и телекоммуникационных услуг.
* Создания точек доступа, не привязанных к географическому положению.
* Создания систем удалённого мониторинга (monitoring системы), как это имеет место в системе SCADA.

WiMAX позволяет осуществлять доступ в Интернет на высоких скоростях, с гораздо большим покрытием, чем у Wi-Fi-сетей. Это позволяет использовать технологию в качестве «магистральных каналов», продолжением которых выступают традиционные DSL- и выделенные линии, а также локальные сети. В результате подобный подход позволяет создавать масштабируемые высокоскоростные сети в рамках городов.

В общем виде WiMAX сети состоят из следующих основных частей: базовых и абонентских станций, а также оборудования, связывающего базовые станции между собой, с поставщиком сервисов и с Интернетом.

Для соединения базовой станции с абонентской используется высокочастотный диапазон радиоволн от 1,5 до 11 ГГц. В идеальных условиях скорость обмена данными может достигать 70 Мбит/с, при этом не требуется обеспечения прямой видимости между базовой станцией и приёмником.

Как уже говорилось выше, WiMAX применяется как для решения проблемы «последней мили», так и для предоставления доступа в сеть офисным и районным сетям.

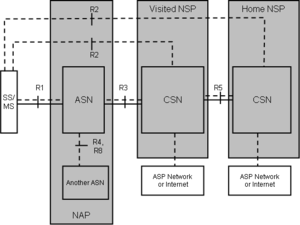
Между базовыми станциями устанавливаются соединения (прямой видимости), использующие диапазон частот от 10 до 66 ГГц, скорость обмена данными может достигать 140 Мбит/c. При этом, по крайней мере одна базовая станция подключается к сети провайдера с использованием классических проводных соединений. Однако, чем большее число БС подключено к сетям провайдера, тем выше скорость передачи данных и надёжность сети в целом.

Структура сетей семейства стандартов IEEE 802.16 схожа с традиционными GSM сетями (базовые станции действуют на расстояниях до десятков километров, для их установки не обязательно строить вышки — допускается установка на крышах домов при соблюдении условия прямой видимости между станциями).

В Wi-Fi сетях все пользовательские станции, которые хотят передать информацию через точку доступа (АР), соревнуются за «внимание» последней. Такой подход может вызвать ситуацию, при которой связь для более удалённых станций будет постоянно обрываться в пользу более близких станций. Подобное положение вещей делает затруднительным использование таких сервисов как Voice over IP (VoIP), которые очень сильно зависят от непрерывного соединения.

Что же касается сетей 802.16, в них MAC использует алгоритм планирования. Любой пользовательской станции стоит лишь подключиться к точке доступа, для неё будет создан выделенный слот на точке доступа, недоступный другим пользователям.

WiMAX Forum разработал архитектуру, которая определяет множество аспектов работы WiMAX сетей: взаимодействия с другими сетями, распределение сетевых адресов, аутентификация и многое другое. Приведённая иллюстрация даёт некоторое представление об архитектуре сетей WiMAX.

[](https://commons.wikimedia.org/wiki/File:WiMAXArchitecture.png?uselang=ru)

WiMAX Форум WiMAX Архитектура

SS/MS: (the Subscriber Station/Mobile Station)

ASN: (the Access Service Network)[4]

BS: (Base station), базовая станция, часть ASN

ASN-GW: (the ASN Gateway), шлюз, часть ASN

CSN: (the Connectivity Service Network)

HA: (Home Agent, часть CSN)

NAP:(a Network Access Provider)

NSP: (a Network Service Provider)

ASN (Access Service Network) — сеть доступа.

ASN Gateway — предназначен для объединения трафика и сообщений сигнализации от базовых станций и дальнейшей их передачи в сеть CSN.

BS (Base Station) — базовая станция. Основной задачей является установление, поддержание и разъединение радио соединений. Кроме того, выполняет обработку сигнализации, а также распределение ресурсов среди абонентов.

CSN (Connectivity Service Network) — сеть обеспечения услуг.

HA (Home Agent) — элемент сети, отвечающий за возможность роуминга. Кроме того, обеспечивает обмен данными между сетями различных операторов.[5]

Следует заметить, что архитектура сетей WiMax не привязана к какой-либо определённой конфигурации, обладает высокой гибкостью и масштабируемостью.

# 1.3.5 Постановка задачи

# 2. Исследование существующих методов исправления ошибок

### **2.1. Коды Боуза—Чоудхури—Хоквингема (БЧХ-коды)**

БЧХ-код является циклическим кодом, который задается порождающим полиномом. Для его нахождения в случае БЧХ-кода необходимо заранее определить длину кода n  и требуемое минимальное расстояние d \leqslant n. Найти порождающий полином можно следующим образом.

Пусть ~\alpha — примитивный элемент поля ~GF(q^m) (то есть \alpha^{q^m-1}=1, \alpha^i \neq 1, i< q^m-1), пусть ~\beta=\alpha^s , — элемент поля ~GF(q^m) порядка ~n, \quad s = (q^m-1) / n . Тогда нормированный полином g(x) минимальной степени над полем GF(q), корнями которого являются ~d-1 подряд идущих степеней ~\beta^{l_0}, \beta^{l_0+1},\ldots,\beta^{l_0+d-2}элемента ~\beta для некоторого целого ~l_0 (в том числе 0 и 1), является порождающим полиномом БЧХ-кода над полем ~GF(q) с длиной n и минимальный расстоянием ~d_0 \geqslant d. Поясним почему у получившегося кода будут именно такие характеристики (длина кода ~n , минимальное расстояние ~d_0). Действительно, как показано в [1] , длина БЧХ кода равна порядку элемента ~\beta, если ~d>2 и равна порядку элемента ~\beta^{l_0}, если ~d=2, тогда, так как случай ~d=2нам не интересен (такой код не может исправлять ошибки, только обнаруживать), то длина кода будет равна порядку элемента ~\beta ,то есть равна ~n. Минимальное расстояние ~d_0 может быть больше ~d, когда корнями минимальных функций(стр.83[2]) от элементов ~\beta^{l_0}, \beta^{l_0+1},\ldots,\beta^{l_0+d-2} будут элементы расширяющие последовательность, то есть элементы ~\beta^{l_0+d-1},\beta^{l_0+d},\ldots,\beta^{l_0+d_0 - 2}.

Число проверочных символов r равно степени g(x), число информационных символов k = n - r, величина d называется конструктивным расстоянием БЧХ-кода. Если n = qm - 1, то код называется примитивным, иначе не примитивным.

Так же, как и для циклического кода, кодовый полином c(x) может быть получен из информационного полинома m(x), степени не больше k-1, путём перемножения m(x) и g(x):

Для нахождения порождающего полинома необходимо выполнить несколько этапов:

* выбрать q, то есть поле GF(q), над которым будет построен код;
* выбрать длину n кода из условия:

где m,s — целые положительные числа;

* задать величину d конструктивного расстояния;

1) построить циклотомические классы элемента \beta=\alpha^s поля GF(q^m) над полем GF(q), где \alpha — примитивный элемент GF(q^m);

2) поскольку каждому такому циклотомическому классу соответствует неприводимый полином над GF(q), корнями которого являются элементы этого и только этого класса, со степенью равной количеству элементов в классе, то выбрать \beta^{l_0}, \beta^{l_0+1},\ldots, \beta^{l_0+d-2} таким образом, чтобы суммарная длина циклотомических классов была минимальна; это делается для того, чтобы при заданных характеристиках кода ~n и ~d минимизировать количество проверочных символов ~k;

3) вычислить порождающий полином g(x)=f_1(x)f_2(x)\ldots f_h(x), где f_i(x) — полином, соответствующий i-ому циклотомическому классу; или вычислить g(x), как НОК минимальных функций от элементов \beta^{l_0}, \beta^{l_0+1},\ldots,\beta^{l_0+d-2} .

При несистематическом кодировании кодовое слово получается в виде произведения информационного полинома на порождающий:

Оно может быть реализовано при помощи перемножения полиномов.

При систематическом кодировании кодовое слово формируется в виде информационного подблока и проверочного

Пусть информационное слово образует старшие степени кодового слова, тогда

Тогда из условия  , следует

Главной идеей в декодировании БЧХ кодов является использование элементов конечного поля для нумерации позиций кодового слова (или, эквивалентно, в порядке коэффициентов ассоциированного многочлена).

### **2.2. Коды Соломона Рида**

Коды Рида-Соломона – недвоичные циклические коды, позволяющие исправлять ошибки в блоках данных. Элементами кодового вектора являются группы битов(блоки). Часто на практике используют варианты данного кода, работающего с байтами(октетами).

Коды Рида-Соломона являются частным случаем кодов БЧХ, для которых количество слов в символе m = m0 = 1. Данный вид кода характеризуется следующими параметрами:

* Длина блоков n = q -1, выраженная числом q-ичных символов;
* Количество информационных символов k от 1 до n – 1;
* Минимальное кодовое растояние dmin = n – k + 1.

Для задания кодов Рида-Соломона использую порождающий полином вида:

Поскольку данным полином имеет степень 2t, то возможно использование всего 2t проверочных символов для исправления пакетов из t ошибок. Согласно теореме о границе Рейгера, данный код является оптимальным с точки зрения соотношения длины пакета и возможности исправления ошибок.

Для декодирования кодов Рида-Соломона существуют эффективные алгоритмы декодирования жестких решений, что позволяет использовать относительно длинные коды во многих практических задачах, особенно в системах с q-ичной модуляций.

В настоящий момент коды Рида — Соломона используется при записи и чтении в контроллерах оперативной памяти, при архивировании данных, записи информации на жесткие диски, записи на CD/DVD диски. Даже если поврежден значительный объем информации, испорчено несколько секторов дискового носителя, то коды Рида — Соломона позволяют восстановить большую часть потерянной информации. Также используется при записи на такие носители, как магнитные ленты и штрих коды.

### **Код Хэмминга**

Код Хэмминга представляет собой блочный код, который позволяет выявить и исправить ошибочно переданный бит в пределах переданного блока. Обычно код Хэмминга характеризуется двумя целыми числами, например, (11,7) используемый при передаче 7-битных ASCII-кодов. Такая запись говорит, что при передаче 7-битного кода используется 4 контрольных бита (7+4=11). При этом предполагается, что имела место ошибка в одном бите и что ошибка в двух или более битах существенно менее вероятна. С учетом этого исправление ошибки осуществляется с определенной вероятностью. Например, пусть возможны следующие правильные коды (все они, кроме первого и последнего, отстоят друг от друга на расстояние 4):

00000000  
11110000  
00001111  
11111111

При получении кода 00000111 не трудно предположить, что правильное значение полученного кода равно 00001111. Другие коды отстоят от полученного на большее расстояние Хэмминга. Расстояние Хэмминга для двух кодов равной длины равно числу разных бит в этих кодах.

В общем случае код имеет N=M+C бит и предполагается, что не более чем один бит в коде может иметь ошибку. Тогда возможно N+1 состояние кода (правильное состояние и n ошибочных). Пусть М=4, а N=7, тогда слово-сообщение будет иметь вид: M4, M3, M2, C3, M1, C2, C1. Теперь попытаемся вычислить значения С1, С2, С3. Для этого используются уравнения, где все операции представляют собой сложение по модулю 2:

С1 = М1 + М2 + М4  
С2 = М1 + М3 + М4  
С3 = М2 + М3 + М4

Для определения того, доставлено ли сообщение без ошибок, вычисляем следующие выражения (сложение по модулю 2):

С11 = С1 + М4 + М2 + М1  
С12 = С2 + М4 + М3 + М1  
С13 = С3 + М4 + М3 + М2

Результат вычисления интерпретируется следующим образом.

|  |  |  |  |
| --- | --- | --- | --- |
| С11 | С12 | С13 | Значение |
| 1 | 2 | 4 | Позиция бит |
| 0 | 0 | 0 | Ошибок нет |
| 0 | 0 | 1 | Бит С3 не верен |
| 0 | 1 | 0 | Бит С2 не верен |
| 0 | 1 | 1 | Бит М3 не верен |
| 1 | 0 | 0 | Бит С1 не верен |
| 1 | 0 | 1 | Бит М2 не верен |
| 1 | 1 | 0 | Бит М1 не верен |
| 1 | 1 | 1 | Бит М4 не верен |

Число возможных кодовых комбинаций М помехоустойчивого кода делится на n классов, где N - число разрешенных кодов. Разделение на классы осуществляется так, чтобы в каждый класс вошел один разрешенный код и ближайшие к нему (по расстоянию Хэмминга) запрещенные коды. В процессе приема данных определяется, к какому классу принадлежит пришедший код. Если код принят с ошибкой, он заменяется ближайшим разрешенным кодом. При этом предполагается, что кратность ошибки не более qm.

### **Набор исследуемых кодов**

**Таблица 1: параметры исследуемых кодов**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код | Длина кода n, символов | Длина данных k, символов | Корректирующая способность t, символов | Бит на символ |
| БЧХ | 31 | 11 | 5 | 1 |
| БЧХ | 31 | 16 | 3 | 1 |
| Рида-Соломона | 23 | 17 | 3 | 8 |
| Хемминга | 63 | 57 | 1 | 1 |
| Хемминга | 31 | 26 | 1 | 1 |
| БЧХ | 31 | 21 | 2 | 1 |

### **Обеспечение требуемой вероятности приема**

Помехоустойчивое кодирование позволяет повысить вероятность приема кадра в десятки раз, но повышение в большее количество раз коды, исправляющие ошибки обеспечить не могут. Для обеспечения необходимого уровня приема кадров применяют коды обнаруживающие ошибки. Избыточность таких кодов существенно меньше, чем у кодов исправляющие ошибки. Таким образом, используется комбинация двух кодов: коды обнаруживающие ошибки обеспечивают требуемую вероятность приема, а корректирующий код минимизацию времени задержки приема.

Вероятность не выявления ошибки в случае использования циклического избыточного кода, если ошибка на самом деле есть, в худшем случае равна , где r – степень образующего полинома. Таким образом, для обеспечения должно быть , т.е. . Такой циклический код позволит обнаружить пакеты ошибок длиной до r.

Таким образом выбираем код CRC-30 длиной 30 бит, задаваемый полиномом:

### **Минимизация времени задержки приема**

Использование помехоустойчивого кодирования способно значительно уменьшить время задержки приема данных в плохих каналах связи. Однако, имеется возможность дальнейшей минимизации задержки путем создания необходимой структуры кадра. Проверочные данные в структуре кадра можно передавать после всех блоков с информационными данными, включающих контрольные суммы этих блоков. В таком случае правильность приема данных можно определить до приема всего кадра. Если данные приняты верно, их можно передать на обработку, а проверочные данные игнорировать и таким образом минимизировать время задержки приема. Для реализации такой структуры кадра нужно использовать разделимые коды для помехоустойчивого кодирования.

# Разработка и программная реализация канальных протоколов

# 3.1. Обобщённая структура кадра

Предполагается к исследованию семейство канальных протоколов с потверждением приема кадра, с возможносьбю переспроса кадра. При повторной отправке кадра все последующие кадры, если они уже были переданы отбрасываются.

Кадр данного семейства канальных протоколов состоит из следующих частей:

* 1. Последовательность Голда длиной 63 бита – отделяет один кадр от другого и определяет количество исходных криптоблоков в кадре.
  2. Поле данных, длина которого определяется как l = (120+30)\*c, где 120 – длина криптоблока (задана), 30 – длина CRC, c – количество криптоблоков в сообщении.
  3. Поле проверочных кодов – длина, которых зависит от используемого кода.

Поле данных разделено на блоки, длина которых зависит от используемого кода. Если при приеме данных не выявлено ошибок, то декодер не принимает кадр до конца, а передает данные на обработку и отсылает подтверждение об успешном приеме.

Поле проверочных кодов, как и поле данных, разделено на блоки, длина которых зависит от используемого кода. Количество блоков в поле данных и в поле проверочных символов совпадает; при обнаружении ошибки в первом блоке данных для востановления используется первый блок проверочных символов и т.д.

# 3.2. Выбор способа реализации канальных протоколов для исследования.

Самым очевидным способом исследованием системы цифровой передачи данных является создание такой системы с последующим ее испытанием в реальных условиях или в специально физически смоделированной среде. Однако, такой способ исследования является затратным. Для его реализации для каждого варианта протокола необходимо реализовать кодер и декодер.

В настоящий момент задачу исследования, могут облегчить системы математического моделирования, в которых существуют библиотеки компонентов, из которых можно создавать модели кодера и декодера, а также моделировать поток ошибок. Система математического моделирования MATLAB является одним из популярных средств для решения таких задач.

Главная особенность среды MATLAB – проработанность и отлаженность всего богатейшего арсенала средств и методов. Возможности MATLAB закрывают большую часть потребностей разработчиков все возможнох систем. Обширный набор численных методов в сочетании с средствами графической визуализации делает MATLAB универсальным инструментов для инженерных расчетов и научных исследований.

Однако MATLAB основана на интерпритируемом языке программирования, что обуславливает ее главный недостаток – низкую скорость вычислений. Помимио этого в таких системах приходится создавать громоздкие многоуровневые блок-схемы, не отражающие естественной структуры моделируемой системе.

Таким образом системы типа MATLAB имеет смысл использовать для проверки отдельных алгоритмов и отладки компонентов проектируемой системы передачи данных, но при необходимости выполнить большой обьем статистического моделирования за короткое время, чтобы получить при использовании минимума ресурсов максимально быстро отбросить большое количество плохих вариантов, целесообразно использовать грубый метод оценочного моделирования.

Целью данного исследования является получения следующих характеристик для различных вариантов протокола и различных потоков ошибок:

* 1. Скорость передачи данных.
  2. Распределение вероятности доставки кадров по времени.

Скорость передачи данных – это отношение количества правильно принятых полезных бит к общему количеству переданных бит. Полезные биты – это сумма длины криптоблока и длины контрольной суммы этого криптоблока, умноженная на количество криптоблоков в кадре. Определив зависимость скорости передачи от количества полезных бит в кадре можно выбрать оптимальное количество криптоблоков на кадр для данного варианта протокола.

Вероятность доставки кадра за определенное время – это отношение успешно принятых кадров за данное время к общему количеству отправленных кадров за это же время.

Количество попыток ограничено, т.к. в некоторых условиях один кадр может постоянно приниматься неверно, даже с его переспросом. Из-за лимита попыток распределения будет достигать единицы в случае, если верятность потери кадра равна нулю, в противном случае максимальная вероятность доставки равна:

# 3.3 Алгоритм оценочного моделирования

При оценочном моделировании эффективности протокола в качестве передаваемых данных используют нули, а единицы считают за ошибки.

Варианты протокола задаются следующими характеристиками:

1. Параметры кадра:
   1. Длина начальной флаговой последовательности (бит);
   2. Длина криптоблока (бит);
   3. Длина контрольной суммы для криптоблока (бит);
   4. Количество криптоблоков в кадре;
2. Параметры коды для прямого исправления ошибок:
   1. Длина кода n (бит);
   2. Длина информационной последовательности k (бит);
   3. Количество исправляемых кодов ошибок;
   4. Количество бит в слове.

При оценочном моделировании протоколов с прямым исправлением ошибок необходимо вести подсчет ошибок, приходящиеся на отдельные блоки кадра. Рассмотрим протокол, в котором используется Голея с 5 криптоблоками по 120 бит на кадр. Каждый криптоблок снабжается контрольной суммой длиной 30 бит, поэтому длина полезных данных равна 750 бит. Длина информационной последовательности для кода Голея равна 12 битам, поэтому для передачи данных необходимо 63 кодовых блока. Данный код обеспечивает исправление до 3 ошибок. При анализе потока ошибок нужно определить номер кадра и номер блока внутри кадра, на который приходится ошибка и увеличить на единицу. Если счетчик ошибок превысит порог ошибок для данного кода, то следует признать, что блок не будет восстановлен при приеме, и кадр будет принят неверно.

Данный алгоритм легко обощается для работы с недвоичными кодами. Для этого необходимо дополнительно определить слово в блоке, на которое приходиться ошибка. Если в слово попали еще ошибки, это ничего не меняет – декодер будет исправлять слово целиком.

# 3.4 Реализация инструмента оценочного моделирования

Инструмент оценочного моделирования представляет собой приложения с консольным интерфейсом. Программа выполнена на языке C++ и не зависит от программно.

Пользователь с помощью встроенного генератора смоделировать поток ошибок одним из алгоритмов: ДСК и ОПП.

Пользователь должен установить параметры моделирования:

1. Общее количество информации;
2. Размер блока и длина контрольной суммы для него;
3. Количество криптоблоков в кадре;
4. Установить параметры кода для прямого исправления ошибок(см. Раздел 3.3)
5. Установить модель потока ошибок и ее параметры.

Результатов работы программы является текстовый файл. Имя этого файла формируется из названия модели потока ошибок, ее параметра и параметров кода используемого для моделирования. Например,:

OPP\_model A = 1, V = 0.98 code(63, 57, 1, 1).txt,

Где

OPP\_model – тип потока ошибок;

A и V – параметры данного потока ошибок;

code(63, 57, 1 ,1) – параметры кода.

Пример файла приведен в приложении 2. Интерфейс программы приведен в приложении 3.

# 3.4 Проверка инструмента оценочного моделирования.

# Разработка архитектуры и реализация протокола передачи данных с исправлением данных.

## **3.1. Модель p a**

Основным понятием, положенным в основу данной модели, является плотность ошибка порядка t. Это неслучайная функция от n и t:

.

В числитель является средним числом ошибок на блоке длинной n, содержащих t или больше ошибок. Значения плотности порядка t ограничены снизу величиной t/n, а сверху единицей, т.е. . Значения v(t,n) не убывают с ростом t; . При величине плотности v(1,n) можно судить о степени группирования ошибок, если считать, что увеличение доли ошибок высших кратностей идентично увеличению степени группирования. Для многих каналов, было установлено:

*.*

Параметр α носит название показатель группирования . При значении α равного нулю получаем модель канала с независимыми ошибками, при значении α равного единице канал с “жестким” пакетированием ошибок.

Вероятность приема блока с t ошибками равна:

Использую приближение

Но, на практике обычно применяют более простое соотношение:

Это верхняя граница вероятности . При t/n < 0,3 точные значения близки к верхней границе.

Таким образом, модель(p, a) задается соотношением:

Параметр модели p – вероятность ошибки символа, находится как и для канала ДСК[Надо вставить метод вычисления].

Параметр a вычисляется из уравнения

Данная модель учитывает факт пакетирования ошибок, что возникает в большинстве реальных каналов, имеется возможность единообразно описывать различные типа каналов. Так значения a в кабельных каналах достигает максимального значения(>0.5), а в радиоканалах минимально(~0.3 – 0.45). Но, модель имеет недостаток, заключающейся в вопросе на уровне блоков.

**3.2. Модель ОПП**

Наблюдаемое пакетирование ошибок в каналах связи при предположении о пуассоновском характере потока можно объяснить, если считать параметр  не константой, а случайной величиной или процессом. Получающийся путем рандомизации  новый случайный процесс называют обобщенным пуассоновским . Будем считать  случайной величиной, закон распределения которой известен . Тогда канал задается как поток ошибок первым способом:



Поскольку вид и параметры закона распределения для реальных каналов обычно неизвестны, указанной выше формулой воспользоваться не удается.

По экспериментальным данным относительно легко можно найти закон распределения интервалов между ошибками – функцию Пальма-Хинчина , которая полностью определяет ОПП (второй способ здания потока).

Справедлива формула:

,

где - параметр потока,

 и 

 - вероятность отсутствия ошибок за время .

Таким образом, для ОПП, зная функцию распределения интервалов между ошибками или , вычисляются вероятности , т.е. приходим к конструктивному заданию потока первым способом. Для моделирования будем считать распределение интервалов, заданное обобщенной гиперболой:

, .

Тогда для параметра потока тогда получается:

.

 и

.

Для расчетов вероятностей наиболее удобна рекуррентная формула:



.

Неизвестные параметры  и  легко находятся, например, методом моментов, поскольку обобщенная гипербола для интервалов между ошибками приводит к гамма-распределению параметра .

К недостаткам этой модели можно отнести более трудоемкие формулы для расчета, чем у модели ДСК и тот факт, что не все каналы имеют обобщенную гиперболу в качестве закона распределения между ошибочных интервалов.

Алгоритмы, необходимые для генерации потока ошибок модели ОПП:

|  |  |
| --- | --- |
|  |  |
| **Рис. : Алгоритм генерации потока ошибок** | **Рис. : Алгоритм функции генерации позиции ошибки в потоке битов.** |

**3.3. Двоичный симметричный канал.**

В рамках данной модели дискретный канал связи может быть представлен как симметричный канал без памяти (ДСК), т.е. такой стационарный дискретный канал, в котором вероятности искажения любого из символов 0 или 1 одинаковы. В этом канале вероятность передачи не зависит от статистики передаваемой последовательности. Воздействие помехи можно представить, как позиционное суммирование входной последовательности символов, выдаваемых условным источником помехи, статистическая характеристика которой полностью определяет канал. В ДСК ошибки кратности t подчиняются биномиальному закону распределения, поток ошибок задается через вероятность ошибки бита *р.* Вероятность -кратной ошибки на блоке из символов равна:



Поток ошибок в ДСК без памяти является процессом восстановления с геометрическим распределением интервалов между ошибками .

Параметр  легко находится по экспериментальным данным

, здесь  - число ошибочных символов за сеанс связи,  - число символов переданных за этот сеанс.

К сожалению, число реальных каналов, ошибки которых описываются моделью ДСК весьма мало. Это обычно каналы высокого качества локальных сетей. Основное достоинство данной модели – простота и возможность оценки по ней потенциальных границ вероятностных характеристик качества доставки сообщений в системе.

Генерация потока ошибок для ДСК осуществляется по следующему алгоритму:

Начало

Задание длины сеанса связи N,

Вероятности ошибки символа p

//Счетчик

Counter = 0

R<p

//случайная величина от 0 до 1

R

Бит = 1

Бит = 0

Counter++

Counter<N

Возврат потока битов

Конец

Рисунок 1 Алгоритм генерации потока ошибок для ДСК

## **3.4. Параметры исследования протоколов канального уровня**

**Таблица : параметры потоков ошибок ОПП**

|  |  |  |
| --- | --- | --- |
| Средняя вероятность ошибки p | A | V |
| **0.00487** | **0.9** | **0.8** |
| **0.0132** | **0.9** | **0.9** |
| 0,0439 | **1** | **0.98** |

**Таблица : параметры потоков ошибок ДСК**

|  |
| --- |
| **0,001** |
| **0,01** |
| **0,05** |

# Анализ результатов.

Результатами моделирования являются две характеристики:

* 1. Скорость передачи данных
  2. Распределение вероятности доставки кадра по времени

Лучшим протоколом по критерию “скорость передачи данных” выбирается, такой протокол, который обеспечивает максимальное соотношение количества правильно принятых бит к общему числу отправленных бит.

Лучшим протоколом по критерию “минимальная задержка при передаче” выбирается:

1. В случае, если для потока ошибок, существуют протоколы у которых максимально накопленная вероятности приема кадра превышает 0.95, то выбирается протокол, который достиг данную вероятность раньше других вариантов;
2. В случае , если ни один из вариантов протокола не достиг вероятность приема кадра большую 0.95, то выбирается протокол с максимально накопленной вероятностью.

В ходе моделирования, было получено, что лучший протокол по критерию “скорость передачи” редко совпадает с лучшим протоколом по критерию “минимальная задержка”.

Для потока ошибок, полученным по ОПП показывает код .

Для потока ошибок, полученным по ДСК показывает код .

Во многих случаях код , обеспечивает наивысшую скорость передачи, но при этом часто вероятность безошибочного приема кадра не превышает 0.95. Это озночает, что используя код с большей корректирующей способностью, можно сократить задержку, но такой код дает снижение скорости передачи.

Для протоколов с сильным группированием ошибок вполне может быть эффективным использованием кода БЧХ(63,57,1) – этот код обеспечивает высокую скорость передачи, исправляет редкие одиночные ошибки, а длинные группы ошибок в любом случае приведут к потере кадра, какой бы корректирующий способностью код не обладает.

Ниже приведены таблицы лучших протоколов с одним, одиннадцатью и шестнадцатью криптоблоками на кадр. Отсутствие результата в таблице, означает, что невозможно получить протокол, который будет обладать вероятностью доставки кадра минимум 0,5.

**Таблица : лучшие протоколы с одним криптоблоком на кадр по потокам ошибок**

|  |  |  |  |
| --- | --- | --- | --- |
| Тип потока ошибок | Средняя вероятность ошибки | Скорость передачи | Минимальная задержка |
| ДСК | 0,001 |  |  |
| 0,01 |  |  |
| 0,05 |  |  |
| ОПП | 0,0439 |  |  |
| 0.0132 |  |  |
| 0.00487 |  |  |

**Таблица : лучшие протоколы с одиннадцатью криптоблоками на кадр по потокам ошибок**

|  |  |  |  |
| --- | --- | --- | --- |
| Тип потока ошибок | Средняя вероятность ошибки | Скорость передачи | Минимальная задержка |
| ДСК | 0,001 |  |  |
| 0,01 |  |  |
| 0,05 |  |  |
| ОПП | 0,0439 |  |  |
| **0.0132** |  |  |
| **0.00487** |  |  |

**Таблица : лучшие протоколы с шестнадцатью криптоблоками на кадр по потокам ошибок**

|  |  |  |  |
| --- | --- | --- | --- |
| Тип потока ошибок | Средняя вероятность ошибки | Скорость передачи | Минимальная задержка |
| ДСК | 0,001 |  |  |
| 0,01 |  |  |
| 0,05 |  |  |
| ОПП | 0,0439 | БЧХ (31, 26, 1, 1) | БЧХ (31, 11, 5, 1) |
| 0.0132 |  |  |
| 0.00487 |  |  |

# 5. Заключение

В рамках данной работы для решения задачи разработки протокола канального уровня с прямым исправлением ошибок был осуществлен анализ существующих алгоритмов и способов помехоустойчивой передачи данных и предложена архитектура для семейства протоколов. В ходе решения поставленной задачи был разработан инструмент оценочного моделирования в виде компьютерной программы, позволяющий провести моделирование протокола при использовании различных потоков ошибок. С использованием программы был проведен анализ и для каждого потока ошибок были предложены оптимальные параметры протокола.

Так же в ходе данной работы была создана методика синтеза протокола, которую можно использовать повторно. Алгоритм синтеза описывается следующим образом:

1. Формулирование технического задания на разработку протокола (характеристики потоков ошибок; характеристики передаваемых данных; требования к скорости и надежности передачи данных).
2. Выбор необходимой архитектуры семейства протоколов. В данной работе, есть возможность выбора архитектуры протокола, что позволяет решать большое множество заданий.
3. На основе требований определить параметры протокола, которые однозначно определены.
4. Использую программу оценочного моделирования получить параметры протокола, которые невозможно определить однозначно.

# 6. Список литературы

**Р. Блейхут** Теория и практика кодов, контролирующих ошибки: Пер. с англ. [Книга]. - Москва : Мир, 1986.

**Э. Таненбаум** Компьютерные сети [Книга]. - СПб : Питер, 2003.

**Finneran, Michael F. WiMax versus Wi-Fi. A Comparison Technologies, Markets and Business Plans. 2004**

**Р. Блейхут** Теория и практика кодов, контролирующих ошибки: Пер. с англ. [Книга]. - Москва : Мир, 1986.

**Э. Таненбаум** Компьютерные сети [Книга]. - СПб : Питер, 2003.

**Finneran, Michael F. WiMax versus Wi-Fi. A Comparison Technologies, Markets and Business Plans. 2004.**

**Wikipedia.[В Интернете] http://ru.wikipedia.org/wiki/HDLC**

## **7. Приложение 1 Исходный код**

//  
// Created by Alexander on 12.05.2015.  
//  
#include "api.hpp"  
#ifndef DIPLOM\_PROTOCOL\_H  
#define DIPLOM\_PROTOCOL\_H  
  
class protocol {  
  
public:  
 protocol(const std::vector<Block> &bl, const Code &code) : bl(bl), code(code) {  
 protocol::blSize = (UINT) protocol::bl.begin()->size();  
 protocol::blocks = (UINT) protocol::bl.size();  
 }  
 virtual ~protocol() { }  
  
 const std::string &getResults() const {  
 return results;  
 }  
  
 void work(UINT type, UINT pkSize);  
private:  
 std::vector<Block>bl;  
 std::vector<Packet>pl;  
 std::string results;  
 Code code;  
 double speed = 0.0, delProbability = 0.0, singleTime = 0.0;  
 UINT blSize, blocks, pkSize, RecivedPackets = 0, SentPackets = 0;  
 UINT blErrors = 0, packetSize;  
  
 void datagramm();  
 void latency();  
 void Nstep();  
  
 bool isCorectable(Packet packet);  
 bool checkPacket(Packet packet);  
 UINT checkBlockErrors(Block bl);  
 bool isCorrectiableBlock(Block block);  
};  
  
  
#endif //DIPLOM\_PROTOCOL\_H

//  
// Created by Alexander on 12.05.2015.  
//  
//***TODO need implement Nstep and latency protocol***#include "protocol.h"  
#include <list>  
  
void protocol::work(UINT type, UINT pkSize) {  
 protocol::pkSize = pkSize;  
 UINT frames = blocks/pkSize;  
 pl = makePackets(pkSize,frames, bl);  
 packetSize = blSize\*pkSize;  
 switch (type){  
 case 1:  
 datagramm();  
 break;  
 case 2:  
 latency();  
 break;  
 case 3:  
 Nstep();  
 break;  
 default:  
 std::cout << "Set correct params" << std::endl;  
 break;  
 }  
 pl.erase(pl.begin(), pl.end());  
 RecivedPackets = 0; SentPackets = 0; delProbability = 0.0; speed = 0; singleTime = 0.0;  
}  
void protocol::datagramm() {  
 bool CoruptedPacket, CorrectablePacket;  
 for(auto packet : pl){  
 CoruptedPacket = checkPacket(packet);  
 if (CoruptedPacket){  
 CorrectablePacket = isCorectable(packet);  
 if(CorrectablePacket){  
 RecivedPackets+=1;  
 }  
 }  
 else{  
 RecivedPackets+=1;  
 }  
 SentPackets+=1;  
 }  
 std::cout << "Sent Packets = " << SentPackets << " RecivedPackets = " << RecivedPackets << std::endl;  
 delProbability = static\_cast<double >(RecivedPackets) / static\_cast<double>(SentPackets);  
 speed = delProbability\*RecivedPackets/SentPackets;  
 speed = speed\*packetSize;  
 std::cout << "Deleviring probability: " << delProbability << std::endl <<  
 "Speed: " << speed << std::endl;  
}  
//***TODO need hard fix***void protocol::latency() {  
 bool CoruptedPacket, CorrectablePacket;  
  
 for(auto packet : pl){  
 CoruptedPacket = checkPacket(packet);  
 if(CoruptedPacket){  
 CorrectablePacket = isCorectable(packet);  
 if(CorrectablePacket){  
 RecivedPackets += 1;  
 }  
 }  
 else{  
 RecivedPackets += 1;  
 }  
 SentPackets += 1;  
 }  
 double frameSize = blSize\*pkSize + (code.DataLength\*code.codeLength);  
 delProbability = static\_cast<double >(RecivedPackets) / static\_cast<double>(SentPackets);  
 speed = (static\_cast<double>(RecivedPackets)/ static\_cast<double>(SentPackets))\*frameSize;  
 singleTime = static\_cast<double>(SentPackets\*SentPackets)/ static\_cast<double>(RecivedPackets\*frameSize);  
 std::stringstream ss;  
 ss <<"Код (" << to\_str(code.codeLength) << ", " << to\_str(code.DataLength) << ", " << to\_str(code.errorsCorrection) << ", " << to\_str(code.bitsWord) << ")**\n**"  
 << "Размер блока, бит = " << blSize << "**\n**Количество блоков в кадре = " << pkSize  
 << "**\n**Отправлено кадров = " << to\_str(SentPackets)  
 << "**\n**Принято кадров = " << to\_str(RecivedPackets)  
 << "**\n**Скорость передачи = " << to\_str(speed)  
 << "**\n**Вероятность доставки кадра = " << to\_str(delProbability)  
 << " **\n**Среднее время задержки = " << to\_str(singleTime);  
 results = ss.str();  
}  
void protocol::Nstep() {  
}  
  
bool protocol::isCorectable(Packet packet) {  
 UINT corupted = 0;  
 for(auto block : packet) if(isCorrectiableBlock(block)) corupted += 1;  
 return corupted == 0;  
}  
bool protocol::checkPacket(Packet packet) {  
 UINT corupted = 0;  
 for(auto block : packet) if (checkBlockErrors(block) > 0) corupted+=1;  
 return corupted > 0;  
}  
UINT protocol::checkBlockErrors(Block bl) {  
 UINT errors = 0;  
 for(auto value : bl) if(value == 1) errors+=1;  
 return errors;  
}  
bool protocol::isCorrectiableBlock(Block block) {  
 UINT ipos = 0, epos = code.bitsWord;  
 blErrors = 0;  
 std::list<std::list<UINT> > words;  
 for (auto i = 0; i < block.size() / code.bitsWord; i++) {  
 std::list<UINT> word;  
 for (auto j = ipos; j < epos; j++) {  
 word.emplace\_back(block.at(j));  
 }  
 words.emplace\_back(word);  
 ipos += code.bitsWord;  
 epos += code.bitsWord;  
 }  
 for (auto word : words) {  
 for (auto value : word) {  
 if (value == 1) blErrors+=1;  
 }  
 }  
 return blErrors <= code.errorsCorrection;  
}

//  
// Created by Alexander on 28.04.2015.  
//  
#include "api.hpp"  
#include "protocol.h"  
#ifndef DIPLOM\_OPP\_H  
#define DIPLOM\_OPP\_H  
  
  
class opp {  
public:  
 opp(UINT BlockSize, UINT SessionSize):BlockSize(BlockSize), SessionSize(SessionSize) {  
 opp::Blocks = opp::SessionSize / opp::BlockSize;  
 opp::bytes = makeSession(opp::SessionSize);  
 }  
 virtual ~opp() { }  
 void setCode(UINT codeLength, UINT errosCor, UINT dataLength, UINT bitsWord) {  
 opp::code.errorsCorrection = errosCor;  
 opp::code.codeLength = codeLength;  
 opp::code.DataLength = dataLength;  
 opp::code.bitsWord = bitsWord;  
 }  
 void setParams(double A, double V) {  
 opp::A = A;  
 opp::V = V;  
 }  
 void setProtocolType(UINT ProtocolType, UINT PacketSize) {  
 opp::ProtocolType = ProtocolType;  
 opp::PacketSize = PacketSize;  
 }  
 void work();  
  
private:  
 UINT BlockSize, SessionSize, Blocks, ProtocolType, PacketSize;  
 double A,V;  
 Code code;  
 std::vector<UINT> bytes, errorsPos;  
 std::vector<Block> bl;  
 protocol\* pr;  
  
 UINT GenOppPos();  
 void saveToFile(std::string str);  
};  
  
  
#endif //DIPLOM\_OPP\_H

//  
// Created by Alexander on 28.04.2015.  
//  
#include "opp.h"  
  
UINT opp::GenOppPos(){  
 double R, a = 0, b = 1;  
 generator(a,b,R);  
 double X = (A/pow(R,(1/V))) - A;  
 return static\_cast<UINT>(X);  
}  
void opp::work()  
{  
 std::cout << "======Begin OPP model======" << std::endl;  
 int Pos = GenOppPos();  
  
 for(auto i = 0; i < bytes.capacity(); i++) {  
 if(Pos == i){  
 bytes[i] = 1;  
 errorsPos.emplace\_back(Pos);  
 Pos = i + 1 + GenOppPos();  
 }  
 else if( Pos != i){  
 bytes[i] = 0;  
 }  
 }  
  
// std::cout << std::endl << "Errors" << std::endl;  
// print(errorsPos);  
  
 bl = makeBlocks(Blocks, BlockSize, bytes);  
 pr = new protocol(bl,code);  
 std::stringstream res;  
 //pr->work(ProtocolType, PacketSize);  
 for(UINT i = 1; i <= PacketSize; i+=5){  
 pr->work(ProtocolType, i);  
 res << pr->getResults() << "**\n**";  
 }  
 saveToFile(res.str());  
  
 std::cout << "======End OPP model======" << std::endl;  
}  
void opp::saveToFile(std::string str) {  
 std::stringstream ostr;  
 ostr << "Модель канала ОПП с параметрами A = " << A << ", V = " << V <<"**\n**"  
 << str << "**\n**";  
 std::cout << ostr.str() << std::endl;  
 std::ofstream fout;  
 std::stringstream fname;  
 fname << "OPP\_model A = " << A << ", V = " << V << " code(" << code.codeLength << ", " << code.DataLength <<  
 ", " << code.errorsCorrection << ", " << code.bitsWord << ")" <<".txt";  
 fout.open(fname.str());  
 fout.write(ostr.str().c\_str(), sizeof(char)\*ostr.str().size());  
 fout.close();  
}

#include "api.hpp"  
#include "protocol.h"  
#ifndef DIPLOM\_DSK\_H  
#define DIPLOM\_DSK\_H  
  
class dsk  
{  
private:  
public:  
 dsk(UINT BlockSize, UINT SessionSize) : BlockSize(BlockSize), SessionSize(SessionSize) {  
 dsk::Blocks = dsk::SessionSize / dsk::BlockSize;  
 dsk::bytes = makeSession(dsk::SessionSize);  
 }  
 virtual ~dsk() { }  
 void setP(double p) {  
 dsk::p = p;  
 }  
 void setCode(UINT codeleght, UINT correction, UINT data, UINT bitsWord){  
 dsk::code.codeLength = codeleght;  
 dsk::code.DataLength = data;  
 dsk::code.errorsCorrection = correction;  
 dsk::code.bitsWord = bitsWord;  
 }  
 void setProtocol(UINT protocol, UINT PacketSize) {  
 dsk::ProtocolType = protocol;  
 dsk::PacketSize = PacketSize;  
 }  
  
 void work();  
private:  
 UINT BlockSize, SessionSize, Blocks, ProtocolType, PacketSize;  
 double p;  
 Code code;  
 protocol\* pr;  
 std::vector<UINT>bytes, errors;  
 std::vector<Block>bl;  
 void saveToFile(std::string str);  
};  
  
#endif //DIPLOM\_DSK\_H

#include "dsk.hpp"  
  
void dsk::work() {  
 std::cout << "======Begin dsk model======" << std::endl;  
 double a = 0, b = 1, r;  
  
 for(auto i = 0; i < bytes.size(); i++){  
 generator(a,b,r);  
 r >= p ? bytes.at(i) = 0:1;  
 }  
 /\*  
 for(auto value : bytes){  
 std::cout << value << "";  
 }\*/  
 std::cout << std::endl;  
// std::cout << "Errors:" << std::endl;  
// print(errors);  
  
 bl = makeBlocks(Blocks, BlockSize, bytes);  
 pr = new protocol(bl,code);  
 pr->work(dsk::ProtocolType, dsk::PacketSize);  
 std::stringstream res;  
 for(UINT i = 1; i <= dsk::PacketSize; i+=5){  
 pr->work(dsk::ProtocolType, i);  
 res << pr->getResults() << "**\n**";  
 }  
 saveToFile(res.str());  
 std::cout << "======End dsk model======" << std::endl;  
}  
void dsk::saveToFile(std::string str) {  
std::stringstream ostr;  
 ostr << "Модель канала ДСК p = " << p <<"**\n**"  
 << str << "**\n**";  
 std::cout << ostr.str() << std::endl;  
 std::ofstream fout;  
 std::stringstream fname;  
 fname << "DSK\_model p = " << p << " code(" << code.codeLength << ", " << code.DataLength <<  
 ", " << code.errorsCorrection << ", " << code.bitsWord << ")" << ".txt";  
 fout.open(fname.str());  
 fout.write(ostr.str().c\_str(), sizeof(char)\*ostr.str().size());  
 fout.close();  
}

#ifndef DIPLOM\_API\_HPP  
#define DIPLOM\_API\_HPP  
  
#include <vector>  
#include <iostream>  
#include <algorithm>  
#include <cstdlib>  
#include <ctime>  
#include <string>  
#include <random>  
#include <sstream>  
#include <fstream>  
typedef unsigned int UINT;  
const UINT STRING\_LENGHT = 40;  
typedef std::vector<UINT> Block;  
typedef std::vector<Block> Packet;  
struct Code{  
 UINT codeLength;  
 UINT DataLength;  
 UINT errorsCorrection;  
 UINT bitsWord;  
};  
template<typename T>  
void print(T cont){  
 UINT conter = 0;  
 for(auto value : cont){  
 if(conter == STRING\_LENGHT){  
 std::cout << std::endl;  
 conter = 0;  
 }  
 std::cout << value << " ";  
 conter++;  
 }  
 std::cout << std::endl;  
}  
std::vector<UINT> makeSession(UINT SessionLenght);  
std::vector<Block> makeBlocks(UINT Blocks, UINT BlockSize, std::vector<UINT>bytes);  
std::vector<Packet> makePackets(UINT PacketSize, UINT Packets, std::vector<Block> v);  
void generator(double a, double b, double& num);  
template <typename T>  
void set2params(T& param1, T& param2, std::string message){  
 std::cout << message << std::endl;  
 std::cin >> param1;  
 std::cin >> param2;  
}  
template <typename T>  
void setparam(T& param, std::string message){  
 std::cout << message << std::endl;  
 std::cin >> param;  
}  
template <typename T>  
std::string to\_str(T value){  
 std::stringstream s;  
 s << value;  
 return s.str();  
}  
#endif //DIPLOM\_API\_HPP

//  
// Created by Alexander on 28.04.2015.  
//  
#include "api.hpp"  
  
std::vector<UINT> makeSession(UINT SessionLenght){  
 std::vector<UINT> ve;  
 ve.resize(SessionLenght);  
 std::fill(ve.begin(), ve.end(), 0);  
 return ve;  
}  
std::vector<Block> makeBlocks(UINT Blocks, UINT BlockSize, std::vector<UINT>bytes){  
 std::vector<Block> ve;  
 UINT IPOS = 0, EPOS = BlockSize;  
 ve.reserve(Blocks);  
 for(UINT i = 0; i < Blocks; i++){  
 Block bk;  
 for(auto j = IPOS; j < EPOS; j++){  
 bk.emplace\_back(bytes.at(j));  
 }  
 ve.emplace\_back(bk);  
 IPOS += BlockSize;  
 EPOS += BlockSize;  
 }  
 return ve;  
}  
std::vector<Packet> makePackets(UINT PacketSize, UINT Packets, std::vector<Block> v){  
 std::vector<Packet>ve;  
 UINT IPOS = 0, EPOS = PacketSize;  
 ve.reserve(Packets);  
 for(UINT i = 0; i < Packets; i++){  
 Packet pk;  
 for(auto j = IPOS; j < EPOS; j++){  
 pk.emplace\_back(v.at(i));  
 }  
 ve.emplace\_back(pk);  
 IPOS += PacketSize;  
 EPOS += PacketSize;  
 }  
 return ve;  
}  
void generator(double a, double b, double& num){  
 std::random\_device rd;  
 std::mt19937 gen(rd());  
 std::uniform\_real\_distribution<> dis(a, b);  
 num = dis(gen);  
}

//  
// Created by Alexander on 28.04.2015.  
//  
#include "main.h"  
  
int main(){  
 unsigned int SessionLenght = 0, BlockSize = 0, model = 0, protocol = 0, CRC;  
 unsigned int codeLenght = 0, dataLength = 0, errorsCorrection = 0, PacketSize = 0, bitsWord = 0;  
 double A = 0, V = 0, p = 0.0, a = 0.0;  
  
 setparam(protocol, "Chose protocol type**\n**"  
 "Enter 1 - datagramm, 2 - with latency, 3 - backNstep");  
 setparam(model, "Выберите поток ошибок**\n**"  
 "Enter 1 - ДСК,, 2 - PA, 3 - ОПП");  
 set2params(SessionLenght, BlockSize, "Установите длину сеанса связи и размер криптоблока");  
 set2params(CRC,PacketSize, "Установите длину CRC последовательности и количество криптоблоков в кадре");  
 BlockSize += CRC;  
  
 set2params(codeLenght, errorsCorrection, "Параметры кода:**\n**Установите длину кода n(бит) и"  
 " Количество исправляемых ошибок");  
 set2params(dataLength, bitsWord, "Установите длину информационной последовательности k(бит) и длину слова(бит)");  
  
 dsk\* dk = new dsk(BlockSize, SessionLenght);  
 pa\* pk = new pa(SessionLenght, BlockSize);  
 opp\* op = new opp(BlockSize, SessionLenght);  
 switch(model)  
 {  
 case 1:  
 setparam(p, "Enter p for single bit:");  
 dk->setP(p);  
 dk->setCode(codeLenght, errorsCorrection, dataLength, bitsWord);  
 dk->setProtocol(protocol, PacketSize);  
 dk->work();  
 break;  
 case 2:  
 set2params(p, a, "Установите p и a:");  
 pk->setCode(codeLenght, errorsCorrection, dataLength, bitsWord);  
 pk->setProtocol(protocol, PacketSize);  
 pk->setParams(a,p);  
 pk->work();  
 break;  
 case 3:  
 set2params(A, V, "Установите A и V:");  
 op->setProtocolType(protocol, PacketSize);  
 op->setCode(codeLenght, errorsCorrection, dataLength, bitsWord);  
 op->setParams(A, V);  
 op->work();  
 break;  
 default:  
 std::cout << "Введены некоректные параметры" << std::endl;  
 break;  
 }  
 return EXIT\_SUCCESS;  
}

## **Приложение 2 Файл результатов**

Модель канала ОПП с параметрами A = 1, V = 0.98

Код (63, 57, 1, 1)

Размер блока, бит = 150

Количество блоков в кадре = 6

Отправлено кадров = 11111

Принято кадров = 11073

Скорость передачи = 896.922

Вероятность доставки кадра = 0.99658

Среднее время задержки = 12.3879

Код (63, 57, 1, 1)

Размер блока, бит = 150

Количество блоков в кадре = 11

Отправлено кадров = 6060

Принято кадров = 6025

Скорость передачи = 1640.47

Вероятность доставки кадра = 0.994224

Среднее время задержки = 3.69406

Код (63, 57, 1, 1)

Размер блока, бит = 150

Количество блоков в кадре = 16

Отправлено кадров = 4166

Принято кадров = 4146

Скорость передачи = 2388.48

Вероятность доставки кадра = 0.995199

Среднее время задержки = 1.74421

## **Приложение 3 Интерфейс программы**

