На правах рукописи

Е С И П О В Антон Владимирович

СИНТЕЗ УСТРОЙСТВ ЗАЩИТЫ ОТ ОШИБОК ПРИ ПЕРЕДАЧЕ ДАННЫХ ПО КАНАЛАМ СВЯЗИ

Специальность 05.13.05. Элементы и устройства вычислительной техники и систем управления

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург – 2012

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Санкт-Петербургский государственный политехнический университет» (ФГБОУ ВПО «СПбГПУ»)

Научный руководитель: кандидат технических наук, доцент **Хромов Валентин Васильевич.**

Официальные оппоненты: доктор технических наук, профессор **Лыпарь Юрий Иванович,** кандидат технических наук **Кравец Леонид Залманович**

Ведущая организация: Федеральное государственное унитарное предприятие ”Научно производственное объединение «Импульс»”

Защита состоится 31 мая 2012 года на заседании диссертационного совета Д212.229.18 ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет» по адресу: 195251, Санкт-Петербург, ул. Политехническая, д.21, корпус 9, ауд. 325

С диссертацией можно ознакомиться в фундаментальной библиотеке ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан

Ученый секретарь
диссертационного совета Д212.229.18
к.т.н., доцент  **Васильев А. Е.**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В настоящее время имеется некоторое отставание в реализации новейших достижений теории помехоустойчивого кодирования в устройствах, призванных обеспечивать защиту информации при передаче в каналах связи. Между тем развитие новой элементной базы позволяет применить на практике все более сложные алгоритмы.

Одним из основных вопросов теории помехоустойчивого кодирования является разработка алгоритмов кодирования и декодирования, а также устройств, их реализующих. Полезность теоретических достижений определяется тем, возможно ли их воплотить в устройстве. Задачам разработки и технической реализации новых способов и алгоритмов помехоустойчивого кодирования посвящаются многочисленные монографии, статьи в таких научных изданиях, как «IEEE Transactions on Communications», «IEEE Transactions on Information Theory», они обсуждаются на регулярных научных конференциях, что подчеркивает актуальность всех проводимых в этой области исследований. Внесли свой вклад в развитие теории помехоустойчивого кодирования и разработку новых устройств, реализующих их идеи, такие видные ученые, как А.Витерби, Р.Галлагер, М.Голей, В.Золотарев, В.Котельников, Д.Месси, Е.Мирончиков, У.Питерсон, Э.Уэлдон, Р.Хэмминг и др.

Принципы, которыми следует руководствоваться при выборе того или иного кода для применения в конкретном канале, зависят от требований, которые предъявляются к системе связи. Если требуется высокая скорость передачи и не критична задержка при передаче потока данных, то задачу можно считать решенной, например, в рекомендации V.42 Международного Телекоммуникационного Союза (ITU). Однако во многих ситуациях, когда требуется передать команду управления по каналу, использование обратной связи в котором невозможно или нежелательно, эта рекомендация неприменима. В данной работе ставится задача разработать методику синтеза устройств, призванных гарантировать исправление ошибок в передаваемом сообщении, его достоверный прием, синхронизацию. Синтез зависит от характеристик канала, причем акцент сделан на каналах плохого качества, передача в которых ведется без обратной связи, а критерием оптимальности является минимизация времени передачи блока данных (команды). Данный критерий актуален для систем связи со значительной задержкой, например, для связи через высокоорбитальные спутники или в системах связи сверхдлинноволнового и коротковолнового диапазона. Каналом плохого качества является канал с вероятностью ошибки бита $5 \cdot 10^{-2} \sim 5 \cdot 10^{-3}$, хотя некоторые авторы

расширяют нижнюю границу до 10^{-3}, а также любой канал на который наводится активные электронные помехи.

Цель диссертационной работы – разработка устройств для передачи данных в каналах плохого качества, которые позволили бы значительно уменьшить время передачи блока данных за счет исправления ошибок канала связи. Эта цель определила следующие задачи исследования:

1. Провести анализ существующих методов помехоустойчивого кодирования и выявить наиболее перспективные из них для передачи данных в каналах плохого качества.
2. Разработать методику синтеза устройств защиты от ошибок при передаче данных в каналах плохого качества, ориентированную на критерий эффективности – время передачи.
3. Разработать способы оценки вероятностно-временных характеристик приема информации устройством, в зависимости от способов передачи.
4. Разработать программные средства для исследования предлагаемых устройств и выбора наиболее эффективного из них.
5. Создать, согласно разработанной методике синтеза, устройство обработки сигналов передачи данных для конкретного канала, характеристики которого зарегистрированы экспериментально.

Положения, выносимые на защиту и их научная новизна:

1. Методика синтеза устройств защиты от ошибок при передаче данных в каналах плохого качества, отличающаяся от известных применяемым критерием эффективности.
2. Способ идентификации процесса приема в виде цепи Маркова и получения аналитических выражений для расчета, из литературы не известных. Выражения позволяют оценить вероятностно-временные характеристики приема информации на этапе проектирования устройства.
3. Конкретный вариант устройства для канала, параметры которого экспериментально зарегистрированы. Устройство позволяет обеспечить аппроксимацию к заданным вероятностно-временные характеристикам приема информации (вероятности верного приема, ложного приема, ложной синхронизации сообщений и кодовых слов, потери синхронизации сообщений и кодовых слов); оно отлично от известных спецификой использования избыточности помехоустойчивых кодов для исправления ошибок.
4. Новый способ синхронизации сообщений, отличающийся от известных тем, что сам вид синхросигнала несет в себе служебную информацию, что позволяет сделать процесс приема более эффективным.

Методы исследования. Для анализа, разработки и исследования использовались методы теории вероятности, математической статистики, математического моделирования и технологии программирования.

Практическая ценность работы. Разработанное устройство позволяет увеличить помехоустойчивость и сократить время доставки блока данных. Предлагается методика разработки таких устройств, включающая способ комбинирования кодов, обеспечивающий повышение достоверности приема. Методика включает набор прикладных программных средств, позволяющий производить исследование эффективности устройств передачи данных и способ синхронизации сообщений, обеспечивающий высокую надежность передачи служебной информации.

Публикации. По теме диссертации опубликовано четыре работы, из них три – в соавторстве, одна статья в журнале из перечня, рекомендованного ВАК РФ для публикации результатов диссертационных работ.

Внедрение результатов. Полученные результаты используются в опытно-конструкторских работах НПО «Импульс», а также в учебном процессе СПбГПУ по дисциплине «Сети ЭВМ и телекоммуникации». Разработанное устройство реализовано в НПО «Импульс» на базе процессора TMS 6713.

Структура и объем работы. Диссертация состоит из введения, пяти глав, заключения, библиографического списка из 129 наименований, изложена на 138 страницах, содержит 28 таблиц и 44 рисунка.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, определены цель и задачи исследований, представлены основные положения диссертационной работы, выносимые на защиту.

В первой главе «Анализ методов помехоустойчивого кодирования» дан обзор основных положений теории кодирования, принципов защиты информации от искажения в канале передачи данных при помощи избыточных кодов.

Применение на практике того или иного кода определяется совокупностью имеющихся в наличии технических средств, способных этот код реализовать, требованиями к качеству и скорости передачи, и условиями передачи. Такие элементы устройства, как декодеры помехоустойчивых кодов, могут различаться по сложности реализации, по числу операций совершаемых для декодирования определенного блока данных, и также по корректирующим способностям.

Из большого разнообразия способов помехоустойчивого кодирования в данной работе решено использовать блоковые коды, допускающие простую техническую реализацию. Подобный вывод определяется спецификой передаваемой информации в виде разрозненного потока коротких сообщений типа команд управления. Сверточное кодирование и турбокодирование не перспективно, поскольку демонстрируют высокую эффективность только на пакетах данных порядка тысяч бит.

Во второй главе «Методика синтеза устройств передачи данных» предложена методика синтеза устройств, призванных решать поставленную задачу. Описано устройство, которое позволяет уменьшить время передачи блока данных посредством существующего оборудования за счет исправления ошибок канала связи. Разработан способ синхронизации сообщений за счет М-последовательностей (последовательностей максимальной длины, сформированная генератором на основе регистров сдвига с линейными обратными связями) в качестве синхропосылки и способ синхронизации кодовых слов сообщения.

В системах, передающих управляющую информацию, а также связанных с обменом информацией между компьютерами, требования к допустимой вероятности ложного приема сообщения предъявляются очень высокие. Корректирующий код, за счет исправления наиболее часто встречающихся ошибок, повышает верность приема сообщения в десятки раз. Но повышение верности в тысячу и более раз коды, исправляющие ошибки, обеспечить не могут. Для обеспечения заданной вероятности ложного приема сообщения традиционно применяют коды обнаруживающие ошибки, причем их избыточность существенно меньше, чем у корректирующих. Однако, когда заданная верность гарантирована, применяют код, исправляющий ошибки для повышения вероятности приема сообщения. Таким образом, разрабатываемое устройство должно использовать протокол передачи данных, который не только исправлял бы ошибки, но и гарантировал заранее заданную вероятность ложного приема сообщения.

Традиционная комбинация двух кодов, каскадный код, не дает весомого выигрыша в защищенности по сравнению с обычным кодом той же длины $N = n_1 n_2$, где n_1, n_2 – длина кодовых слов составляющих кодов. Главная цель каскадирования – существенно упростить процедуру декодирования за счет применения двух декодеров кодов с длинами всего лишь n_1 и n_2. Однако в данной работе предлагается скомбинировать два кода с иной целью. Один код должен наиболее эффективно исправлять данные, исказившиеся в канале передачи данных. Второй код призван отслеживать, были ли исправлены все ошибки. Кроме того, код, обнаруживающий ошибки, будет применяться для того, чтобы увеличивать также и вероятность приема сообщения за счет использования его в схеме вероятностного

декодирования комбинаций криптоблоков кода или комплекса кодов, исправляющих ошибки. Ранее коды, обнаруживающие ошибки, в таком режиме не применялись.

Код обнаруживающий ошибки выбирается так, чтобы его характеристики при уровне ошибок в заданном канале обеспечивали требуемую верность приема сообщения.

Вероятность ошибочного приема определяется по формуле

$$P_{err} = \sum_{i=d}^{n} p_i k_i \ ,$$

где d – кодовое расстояние, n – длина кода, p_i – вероятность ошибки в i символах кодового слова, а k_i – доля ошибок кратности i, обнаруживаемых этим кодом. Определенную трудность представляет нахождение p_i. Описаны способы нахождения этой величины для ряда моделей каналов – ДСК, ОПП, модель (p, α). Для каналов, которые могут быть описаны моделями, не позволяющими достаточно просто и эффективно рассчитать вероятность ошибки кратности i, методика предлагает программно реализовать модель канала и просто накопить статистику того, какие ошибки как часто встречаются.

Еще более сложной задачей при выборе кода, обнаруживающего ошибки, является отыскание значений k_i. Для этого необходимо знать спектр кода. Это трудно решаемая задача для длинных кодов и к тому же подобный подход оставляет единственный вариант анализа – перебор.

Поэтому для выбора кода, обнаруживающего ошибки предлагается использовать оценку допустимой вероятности. В случае независимых ошибок в канале можно задаться такой длиной информационного блока k, чтобы число ошибок последующей кратности было меньше, чем предыдущей. В таком случае вероятность неверного приема сообщения кодом, обнаруживающим все ошибки кратности не более i равна:

$$P_{err} = 1 - p_0 - p_1 - \ldots - p_i.$$

При некотором значении t_0 указанная вероятность выйдет на заданное значение требуемой верности, и, следовательно, код, обнаруживающий все ошибки кратности не более t_0 (т.е. код с кодовым расстоянием $d = t_0 + 1$) можно рекомендовать в качестве кода, обнаруживающего ошибки в предлагаемом протоколе. Такой код (код Боуза-Чоудхури-Хоквингхема) легко находится при известных d и k. В действительности, подобная методика подбора кода содержит в себе некоторую избыточность, поскольку выбранный код будет также обнаруживать и некоторые ошибки кратности выше t_0. Однако подобная методика надежна только для каналов с независимыми ошибками.

В случае, если ошибки пакетируются, используется известная приближенная формула расчета ошибочного приема сообщения P_{err}:

$$P_{err} \approx \frac{1}{2^r} P(N_{err} \geq d, n),$$

где N_{err} - число ошибок в сообщении, d – кодовое расстояние, r – избыточность кода и n – длина кодового слова. Величина $P(N_{err} \geq d,n)$ для каждой модели рассчитывается соответственно:

для модели (p, α) справедлива оценочная формула $P(i \geq d, n) \approx p\left(\frac{n}{d}\right)^{1-\alpha}$.

для модели обобщенного пуассоновского потока, в случае, если распределение интервалов задается обобщенной гиперболой $G(t) = \left(\frac{\alpha}{\alpha + t}\right)^{v}, v > 1, \alpha > 0$, справедлива рекуррентная формула

$$P(i,t) = \frac{v + i - 2}{i} \frac{t}{\alpha + t} P(i-1, n), i = 1,2,...$$

$$P(0,t) = \left(\frac{\alpha}{\alpha + t}\right)^{v-1}.$$

для модели Гилберта-Эллиота, описываемой набором параметров $\{p,\ q,\ \varepsilon_0,\ \varepsilon_1\}$, справедлива формула

$$P(i,n) \approx P_i(t = n) = \frac{1}{i!}\left[p\left(\frac{n}{2}\right)^i e^{-\frac{n}{2}} + (1-p)(\varepsilon n)^i e^{-\varepsilon n} \right].$$

В случае, если рассматривается не математическая модель канала, а реальный канал, статистику ошибок кратности i можно просто накопить.

Выбор кода, обнаруживающего ошибки, производится в несколько итераций.

На первом шаге в качестве кода, обнаруживающего ошибки, предлагается проверка на четность, т.е. $n = k + 1$, $d = 2$. Отыскивается оценка значения избыточности r.

На втором шаге выбора кода по найденному числу избыточных битов r выбирается код БЧХ так, чтобы максимизировалось кодовое расстоянием d.

Выбор кода, исправляющего ошибки производится по требуемой согласно техническому заданию вероятности достоверного приема сообщения за контрольный срок. Если канал представлен в виде теоретической модели, то расчет вероятности приема ведется по соответствующим формулам. Если имеется статистика потока ошибок реального канала передачи данных, то целесообразно моделировать процесс передачи данных и оценить соответствие полученной опытным путем вероятности достоверного приема заранее требуемой величине.

Важнейшим компонентом протокола передачи данных является синхронизация данных при приеме. Методика выбора оптимального способа синхронизации должна предлагать наилучшие решение следующих задач:

- Синхронизация сообщений
- Синхронизация кодовых блоков в сообщении

Для синхронизации сообщений предлагается использовать М-последовательности. Отсутствие синхронизации сообщений М-последовательностью рассчитывается по формуле:

$$P''_{false} = P_{miss} + P'_{false} = \left(1 - \sum_{i=0}^{Q} C_L^i p^i q^{L-i}\right) + \left(1 - \left[1 - \frac{1}{2^L}\sum_{i=0}^{Q} C_L^i\right]^N\right),$$

где p – вероятность ошибки бита, $q = 1 - p$, L – длина М-последовательности, выбирается такой, чтобы обеспечить заданную вероятность синхронизации сообщения. Следует отметить, что $L = 2^S - 1$, и существует S М-последовательностей длины L. Выбор той или иной последовательности позволяет передать S служебных бит, и это соображение также влияет на выбор длины синхропоследовательности. N – длина преамбулы в битах. Поскольку в равной степени не желательно как пропускать истинную синхропоследовательность, так и ложно опознать ее во фрагменте данных, синхропоследовательностью не являющемся, то параметр Q – число допустимых ошибок в синхропосылке – должен выбираться таким, чтобы оба слагаемых приведенной формулы были примерно равны.

В случае независимости ошибок адекватной моделью функционирования блокового синхронизатора является марковская цепь. Она позволяет оценить вероятностные характеристики процесса синхронизации и задать необходимые параметры.

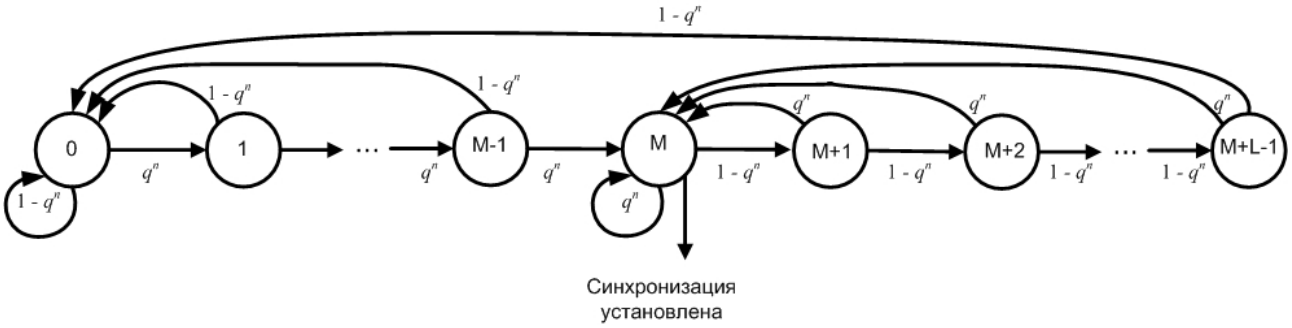

Рис.1. Синхронизация кодовых слов (M/M – L).

Код, используемый для исправления ошибок, может быть использован и для синхронизации. Однако если он является циклическим кодом, то это создает некоторые сложности, поскольку сдвиг кодового слова циклического кода есть также кодовое слово. Классический подход предполагает серьезное расширение циклических кодов, решающее

эту проблему. Но в рамках данной работы предлагается просто инвертировать последний бит кодового блока. Тогда попытка синхронизироваться в неправильном месте будет приводить сразу к двум ошибкам – к одной за счет заранее инвертированного бита, ко второй – за счет неверно инвертированного бита в ошибочном конце блока.

Если бы в канале передачи данных отсутствовали помехи, этого было бы достаточно. Однако, определенное количество ошибок может привести к тому, что правильная синхронизация будет утрачена, или комбинация ошибок создаст кодовое слово – и начало блока будет идентифицировано в неверном месте. Для предотвращения подобных ситуаций предлагается применить критерий (M/N – L). Если при поиске синхронизации маркер границ блока предполагается найденным, то дальнейшее сканирование последовательности блоков производится не посредством проверки побитового сдвига, а через отсчет сразу на несколько блоков вперед. Для того, чтобы синхронизация считалась сохраняющейся, требуется деления нацело после инверсии проверочного бита M блоков из N (M < N). Возврат к сканированию побитовым сдвигом происходит при отсутствии делимости на протяжении L блоков (L >> M). Варьирование параметров M, N и L призвано обеспечить скорейшее достижение синхронизма в различных потоках ошибок в каналах передачи данных.

Структура разработанного устройства приведена на рисунке 2. Косвенным признаком наличия такого устройства исправления ошибок для пользователя было бы значительное уменьшение времени передачи в канале плохого качества за счет того, что не приходилось бы передавать повторы сообщений, искаженных в канале.

Рис.2. Структура устройства.

В общем виде разработанная методика синтеза устройств приведена на рисунке 3.

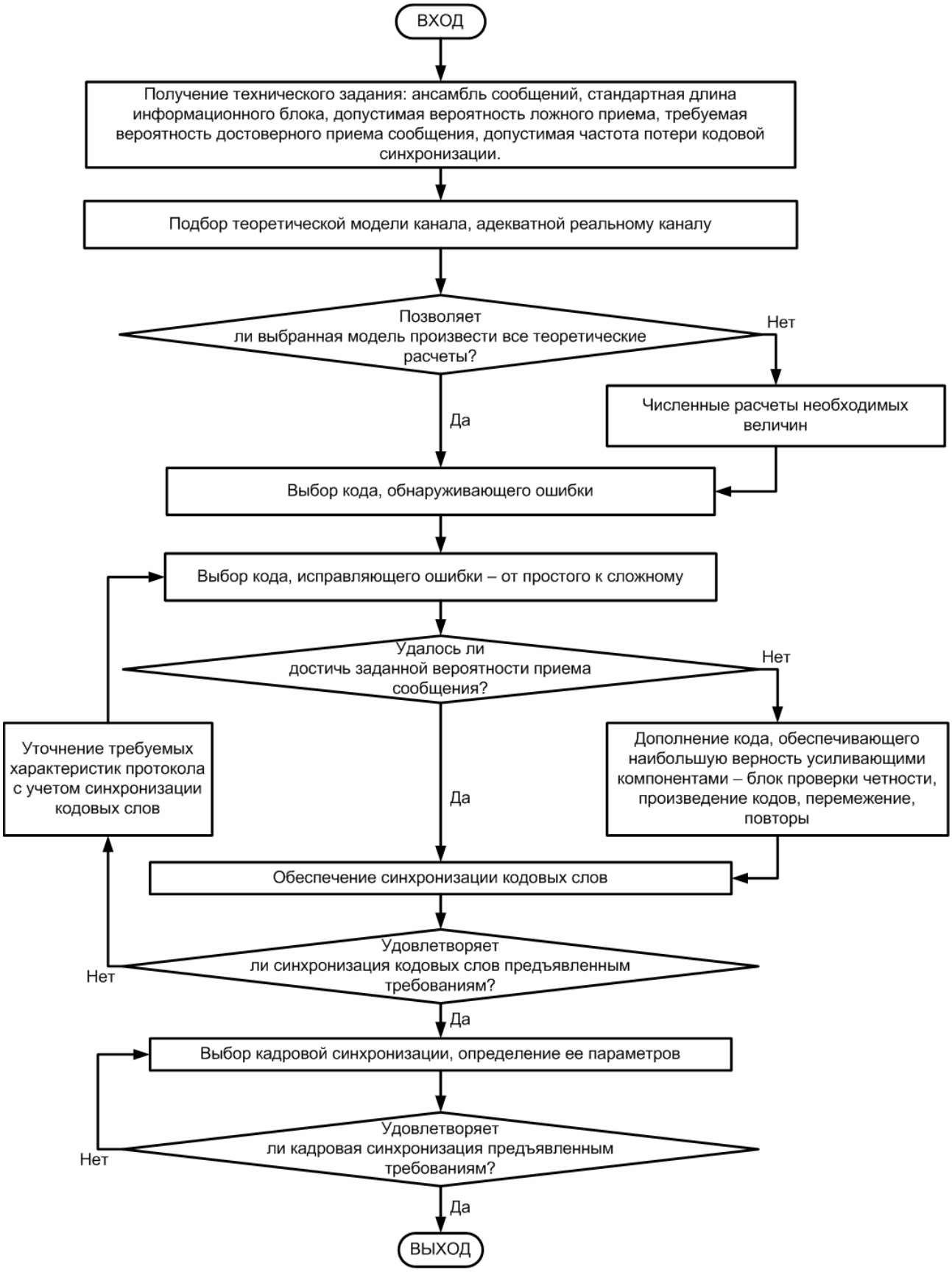

Рис.3. Методика синтеза устройства.

Поскольку оконечным оборудованием данных как правило является компьютер, целесообразной является программная реализация устройства. В случае, если требуется высокая отказоустойчивость устройства, оно может быть выполнено отдельно, например на

основе программируемой логической интегральной схемы. Кроме того, возможности современных микропроцессоров модемов позволяют передать им часть функций устройства, таких как кодирование/декодирование данных. Компонентами передающей части устройства являются: кодер обнаруживающего ошибки кода, кодер исправляющего ошибки кода и генератор синхропосылки. Компонентами принимающей части устройства являются: синхронизатор сообщений, синхронизатор кодовых слов исправляющего кода, декодер исправляющего ошибки кода, декодер обнаруживающего ошибки кода и система верификации данных.

В третьей главе «Синтез устройства» решена задача создания оптимального устройства передачи данных для заранее заданных реального канала, значений приемлемой достоверности и вероятности ложного приема. Синтез устройства ведется для потока ошибок реального канала передачи данных, полученного посредством длительной тестовой работы двух радиомодемов. Задан уровень достоверности приема 0,999 и вероятность ложного приема $P_{err} = 10^{-6}$, длина информационного сообщения k – 120 символов.

Используется критерий оптимальности, отличающийся от общепринятого – время. Критерий актуален для случаев, когда нужно передать команду за как можно более короткое время. Код, обнаруживающий ошибки выбирается согласно формуле

$$P_{err} \approx \frac{1}{2^r} P(N_{err} \geq d, n)$$

Для реального канала, а также его аппроксимаций основными теоретическими моделями каналов производится расчет вероятности ложного приема в зависимости от значений r и d.

Таблица 1. Расчет P_{err} в зависимости от значений r и d.

Канал	Реальный	Реальный	ДСК	ОПП	(p, α)
d	5	6	6	6	6
$\boldsymbol{P(N_{err} \geq d, n)}$	0,5584	0,51565	0,461597	0,256931	0,381889
r	16	20	20	20	20
$\boldsymbol{P_{err}}$	$8{,}5205\times10^{-06}$	$4{,}9176\times10^{-07}$	$4{,}4021\times10^{-07}$	$2{,}4503\times10^{-07}$	$3{,}642\times10^{-7}$

В результате этого расчета для обнаружения ошибок принимается код БЧХ с кодовым расстоянием 6 и избыточностью 20 символов. Вычисления в теоретических моделях каналов показали, что в отсутствие статистики реального канала оценка аппроксимированных моделей также позволяет выбрать код, обнаруживающий ошибки, который обеспечит требуемую вероятность ложного приема.

Код, исправляющий ошибки выбирается путем анализа эффективности имеющихся классов кодов, начиная с простых по технической реализации, с последующим

подключением дополнительных средств исправления ошибок – блоков проверки на четность, перемежителей, повторений сообщений.

Таблица 2. Выбор метода исправления ошибок.

Способ исправления ошибок	*P* приема	Способ исправления ошибок	*P* приема
Код БЧХ (15, 11)	0,327084	Дополнение кода Голея блоком проверки четности	0,905187
Код БЧХ (15, 7)	0,635967	Произведение двух кодов Голея	0,990735
Код Голея (23, 12)	0,772166	Двукратное повторение кодированного по Голею сообщения с блоком четности	**0,99909**
Код БЧХ (31, 16)	0,697841	Двукратное повторение самоортогонального кода с блоком четности	0,952976
Код БЧХ (63, 24)	0,862098	Сверточный код с мажоритарным исправлением	0,967702
Код БЧХ (255, 71)	0,969763	Турбо-код с мажоритарным исправлением	0,940792

Произведено сравнение разработанного устройства со способом передачи данных, реально применяемым на практике, показано преимущество разработанного.

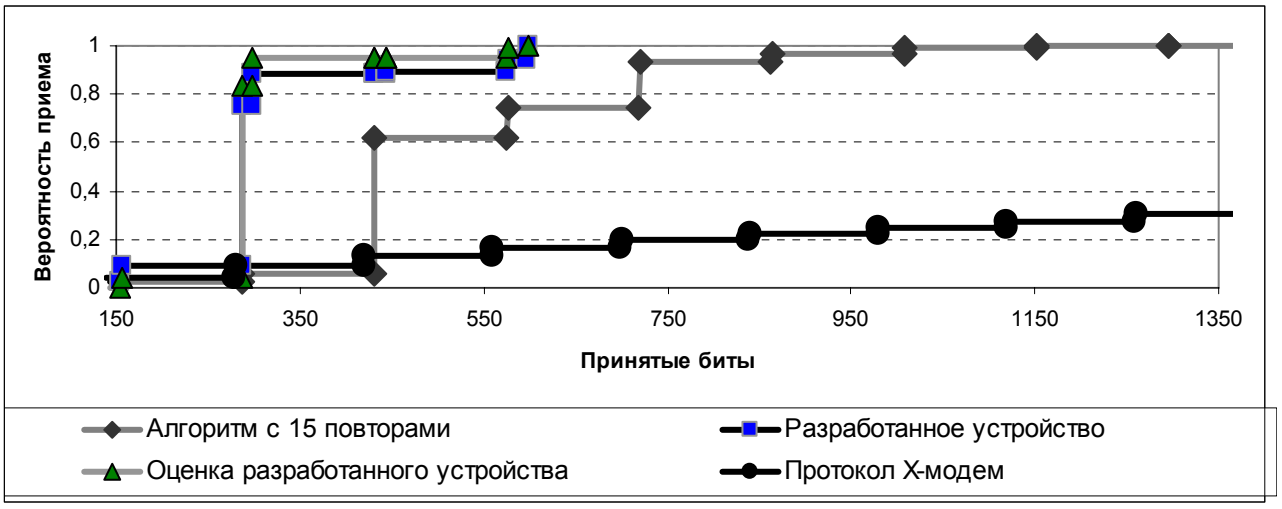

Рис.4. Временные характеристики разработанного и применяемого алгоритмов.

Необходимым компонентом методики является разработанный способ оценки вероятностно-временных характеристик приема данных. В канале с независимыми ошибками, с вероятностью ошибки бита p, $q = 1 - p$, вероятность приема незащищенного блока данных из k символов равна $P_{block} = q^k$.

Если блок k символов дополнен символом проверки на четность, то вероятность приема блока равна $P_1 = q^k + C_k^1 pq^k$.

Вероятность приема пакета из i блоков, дополненных блоком проверки на четность:

$$P_{pack} = P_{block}^i + C_i^1 P_{block}^i (1 - P_{block}) = P_{block}^i \left[1 + i(1 - P_{block})\right].$$

Следующая оценка рассматривает прием двойного пакета i блоков кода Голея, дополненных блоком четности, но легко может быть обобщена для любого блочного кода. Решение о приеме пакета выносится в следующем порядке:

1. Проверка первой информационной части. Вероятность приема P_{pack}, сообщение не принято с вероятностью $Q_{pack} = 1 - P_{pack}$.
2. Проверка того, не исправилась ли первая информационная часть первой проверочной частью. Вероятность приема на этом этапе $P_{correct} = P_{Goley}^{i}\left[1 + i(1 - P_{Goley})\right]$, где $P_{Goley} = \sum_{i=0}^{3} C_{23}^{i} p^{i} q^{23-i}$. Сообщение не принято с вероятностью $Q_{correct} = 1 - P_{correct}$.
3. Проверка второй информационной части вероятность приема на этом этапе P_{pack}, сообщение не принято с вероятностью Q_{pack} .
4. Проверка того, не исправилась ли вторая информационная часть второй проверочной частью. Вероятность приема на этом этапе $P_{correct}$, неприема – $Q_{correct}$.
5. Проверка того, не исправилась ли первая информационная часть второй проверочной частью, при условии что в объединении первой информационной и первой проверочной частей есть хотя бы один блок с четырьмя или более ошибками. Вероятность приема $P'_{correct} \le P_{correct}$, вероятность неприема – $Q'_{correct}$.
6. Проверка того, не исправилась ли вторая информационная часть первой проверочной частью. Вероятность приема $P'_{correct}$, вероятность неприема – $Q'_{correct}$.

Таким образом, можно указать оценку вероятности неприема сообщения:

$$Q = Q_{pack}^{2} Q_{correct}^{2} Q'^{2}_{correct} \ge Q_{pack}^{2} Q_{correct}^{4}$$

Если длина сообщения превышает 120 символов, то оно делится на 120-битные порции, которые кодируются и последовательно передаются. Для моделирования приема многоблочного сообщения может быть использована цепь Маркова. Матрица переходных вероятностей восьмиблочного сообщения выглядит следующим образом:

$$\begin{bmatrix}
P_{00} & P_{01} & P_{02} & P_{03} & P_{04} & P_{05} & P_{06} & P_{07} & P_{08} \\
0 & P_{11} & P_{12} & P_{13} & P_{14} & P_{15} & P_{16} & P_{17} & P_{18} \\
0 & 0 & P_{22} & P_{23} & P_{24} & P_{25} & P_{26} & P_{27} & P_{28} \\
0 & 0 & 0 & P_{33} & P_{34} & P_{35} & P_{36} & P_{37} & P_{38} \\
0 & 0 & 0 & 0 & P_{44} & P_{45} & P_{46} & P_{47} & P_{48} \\
0 & 0 & 0 & 0 & 0 & P_{55} & P_{56} & P_{57} & P_{58} \\
0 & 0 & 0 & 0 & 0 & 0 & P_{66} & P_{67} & P_{68} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{77} & P_{78} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{88}
\end{bmatrix}$$

Вероятности перехода между состояниями в канале ДСК с вероятностью ошибки бита p:

$P_{0i} = C_8^i P^i Q^{8-i}$, $i = 0,\ldots,8$,

$P = P_{simple} + (1 - P_{simple})(P_{Goley}{}^{13} + 13 P_{Goley}{}^{12}(1 - P_{Goley}))$, $Q = 1 - P$;

$P_{simple} = q^{156} + 13q^{144}(1 - q^{12})$ - вероятность приема сообщения или сразу, или после исправления блоком проверки на четность, а

$P_{Goley} = \sum_{i=0}^{3} C_{23}^i p^i q^{23-i}$ - вероятность исправления ошибок в блоке кода Голея

$P_{1i} = C_7^{8-i} P^{i-1} Q^{8-i}$, $i = 1,\ldots,8$;

$P_{2i} = C_6^{8-i} P^{i-2} Q^{8-i}$, $i = 2,\ldots,8$;

$P_{3i} = C_5^{8-i} P^{i-3} Q^{8-i}$, $i = 3,\ldots,8$;

$P_{4i} = C_4^{8-i} P^{i-4} Q^{8-i}$, $i = 4,\ldots,8$;

$P_{5i} = C_3^{8-i} P^{i-5} Q^{8-i}$, $i = 5,\ldots,8$;

$P_{6i} = C_2^{8-i} P^{i-6} Q^{8-i}$, $i = 6,\ldots,8$;

$P_{7i} = C_1^{8-i} P^{i-7} Q^{8-i}$, $i = 7,\ldots,8$;

$P_{88} = 1$.

Для выбранного способа исправления ошибок проведена оптимизация расположения компонентов в составе сообщения. Сравнение вариантов устройства позволило определить наилучшую компоновку, обеспечивающую минимальное время доставки команды.

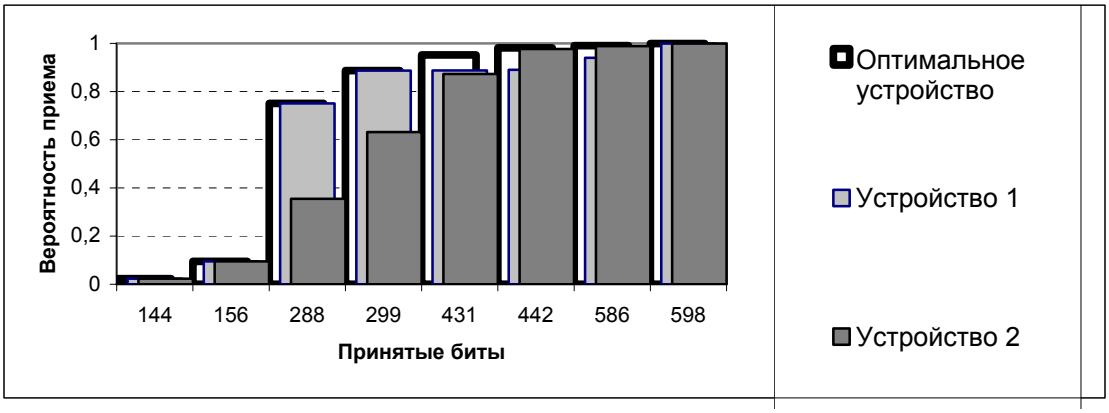

Рис.5. Выбор оптимального устройства по минимуму времени доставки команды.

<u>В четвертой главе</u> «Оценка вероятностных характеристик» предложена оценка характеристик синхронизации сообщений 63-разрядной М-последовательностью по формуле

$$P''_{false} = P_{miss} + P'_{false} = \left(1 - \sum_{i=0}^{Q} C_{63}^i p^i q^{63-i}\right) + \left(1 - \left[1 - \frac{1}{2^{63}} \sum_{i=0}^{Q} C_{63}^i\right]^N\right),$$

где p – вероятность ошибки бита, $q = 1 - p$, N – длина преамбулы в битах. Произведен расчет порога синхронизации Q – числа ошибок в синхропосылке, до превышения которого синхронизация считается установленной. Для рассматриваемого реального канала и

синхронизации сообщений посредством 63 символьной М-последовательности порог ошибок согласно разработанной методике будет равен 21.

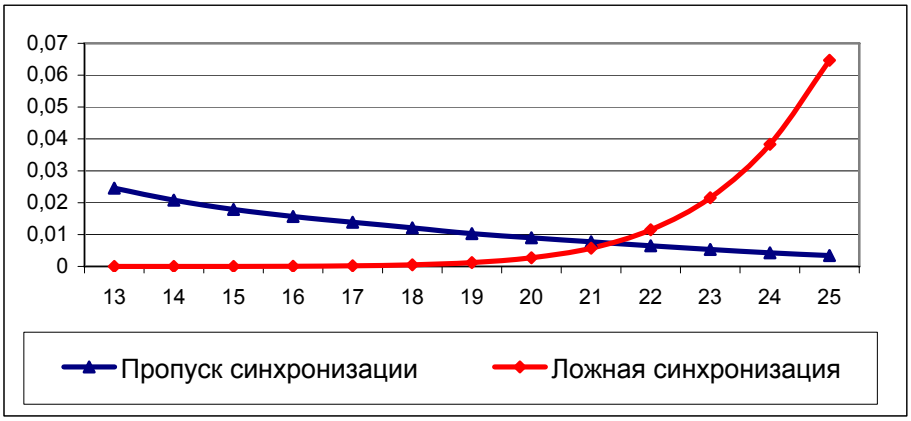

Рис.6. Выбор порога синхронизации как ближайшего целого к точке пересечения.

Вероятности достоверного и ложного приема сообщений могут быть получены через представление процесса приема цепью Маркова. Вероятность правильного и ложного приема при обработке *i* повторений находится возведением матрицы переходных вероятностей в степень, равную *i*. Получены численные оценки вероятностей достоверного и ложного приема для разработанного устройства.

Получено выражение стационарной вероятности установления синхронизации кодовых слов. Согласно методике выбора значений M и L в зависимости от условий передачи данных, если допустимая вероятность ложной синхронизации кодовых слов равна 10^{-7}, то для рассматриваемого реального канала связи M=2. Выбор параметра L определяется заранее заданной частотой потерь синхронизации за единицу времени. Чтобы потери синхронизации случались не чаще одного раза в час для модемного оборудования с информационной скоростью 1200 бит/с, M = 2, N = 3, параметр L должен быть равен 8.

В пятой главе «Программные средства разработки устройства и моделирования его работы» рассматриваются вопросы построения программного обеспечения, необходимого для моделирования процесса приема сообщения разработанным устройством. Для всех компонентов устройства были созданы модели с помощью пакета математических программ Matlab. Разработанные посредством MathWork Simulink модели устройства затем могут быть при помощи DSP Builder Signal Compiler преобразованы в программный код формата VHDL и далее реализованы аппаратно в виде программируемой логической интегральной схемы с помощью набора средств компании «Альтера».

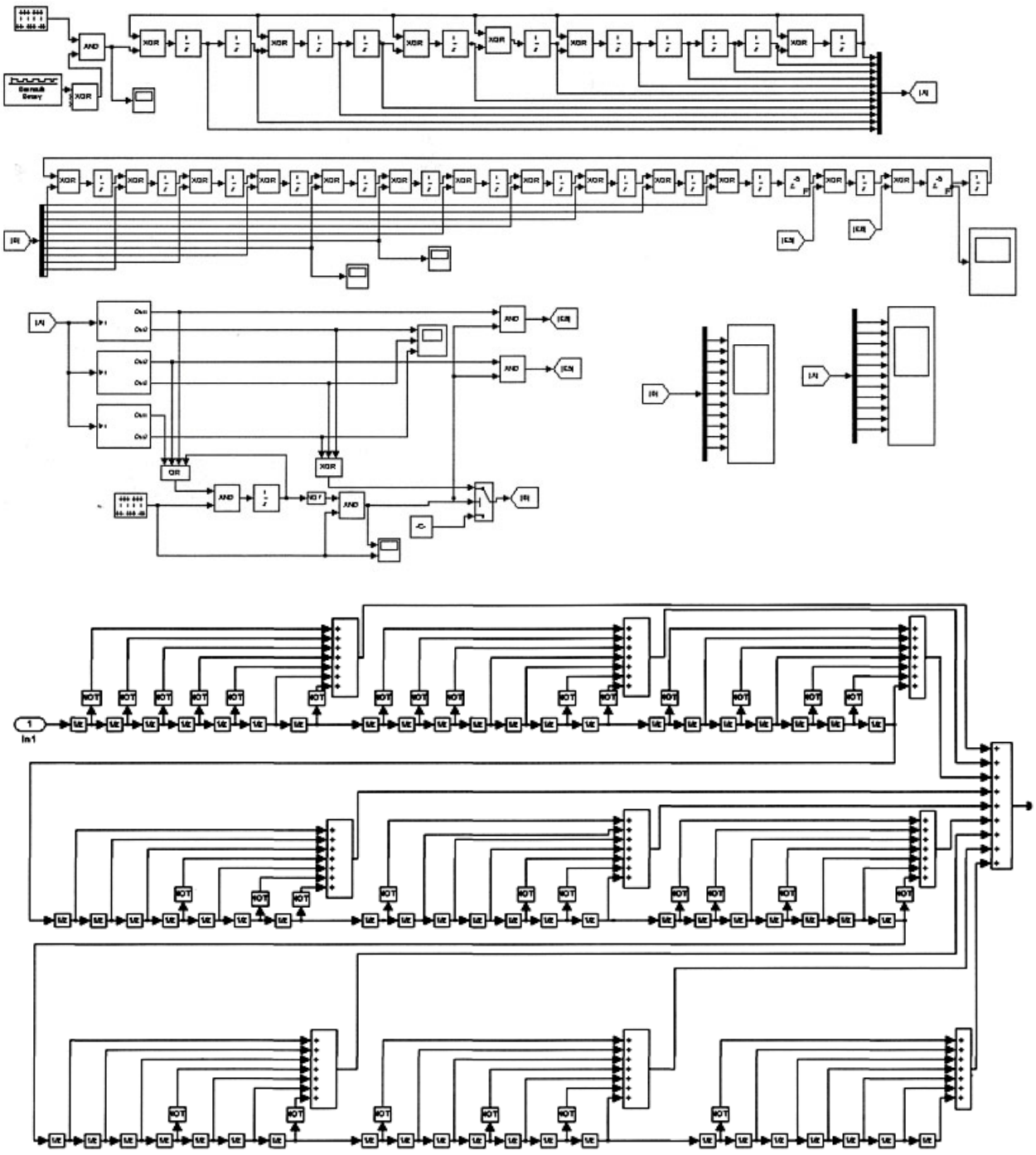

Рис. 7. Модели устройства, разработанные в программном комплексе Matlab

Для оценки достоверности приема сообщения разработан способ моделирования передачи данных в канале, представленном как поток ошибок, а именно как поток нулей и единиц, где ноль соответствует безошибочному прохождению передаваемого бита, а единица – искаженному. Предполагается передача в канал закодированного пакета, состоящего исключительно из нулей, а затем – декодирование полученного из канала набора нулей и единиц с целью получить информационную часть пакета, по-прежнему состоящего

только из нулей. Способ опирается на общеизвестное свойство линейных систем – реакция на сумму воздействий равна сумме реакций на каждое из воздействий. Достоинством подобного подхода является возможность уклониться от процедур кодирования и декодирования сообщения, которые требуют значительных временных и вычислительных ресурсов. В то же время основные схемы кодирования-декодирования были проверены на реальных данных, с тем, чтобы убедиться в корректной работе программно описанных декодеров.

Основным языком программирования, на котором осуществлялось моделирование, был выбран C/C++. Главным достоинством кода, написанного на C, является высокая степень его переносимости, то есть возможность переноса программного обеспечения, написанного для одной операционной системы и даже одного типа компьютеров на другие операционные системы и типы компьютеров.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

Основные результаты диссертационной работы заключаются в следующем:

1. Проведен анализ существующих помехоустойчивых кодов, выявлены наиболее перспективные из них для использования при передаче данных в каналах плохого качества.
2. Разработана методика проектирования устройств передачи данных в каналах плохого качества, включающая в себя выбор кодера кода, обнаруживающего ошибки, кодера кода, исправляющего ошибки, способа синхронизации сообщений и кодовых слов. В рамках методики предложен способ комбинирования кодов, обеспечивающий повышение вероятности достоверного приема и разработан способ оценки вероятностно-временных характеристик создаваемых устройств.
3. Предложен новый способ синхронизации сообщений, сочетающий в себе два метода: маркер начала в виде М-последовательности или последовательности Голда и указание длины сообщения в виде вариантов М-последовательностей
4. Созданы устройство и конкретный вариант протокола для него, обеспечивающий в заданном канале прием сообщения с требуемой вероятностью за время, составляющее 46% от времени, которое требуется для решения этой задачи по протоколу, применяемому в настоящее время, и 0,8% от времени по протоколу X-модем.
5. Предложен способ моделирования передачи данных, отличающийся от известных тем, что минимизирует затраты ресурсов на кодирование/декодирование данных.

ПУБЛИКАЦИИ ПО ОСНОВНЫМ РЕЗУЛЬТАТАМ ДИССЕРТАЦИИ

Хромов В.В., Есипов А.В. Оценка вероятностно-временных характеристик класса алгоритмов передачи данных по каналу с независимыми ошибками // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. – 2008. – Т.6.– СПб.: Изд-во Политехн. ун-та, 2008 – С. 69-74.

Есипов А.В., Хромов В.В. Программное обеспечение описания и моделирования работы протокола передачи данных в канале с большим уровнем шума // Вычислительные, измерительные и управляющие системы: сборник научных трудов / Под ред. Ю.Б.Сениченкова. – СПб.: Изд-во Политехн. ун-та, 2008 – С. 54-60.

Хромов В.В., Есипов А.В. Расчет вероятности ложного приема при передаче информации по каналу с независимыми ошибками. //Вычислительные, измерительные и управляющие системы: сборник научных трудов / Под ред. Ю.Б.Сениченкова. – СПб.: Изд-во Политехн. ун-та, 2007 – С. 10-18.

Есипов А.В. Геоинформационная система ЕИСТ: архитектура и информационная безопасность. //Территориальное стратегическое планирование: измеряя результаты. Выпуск №6. – СПб, 2006 – С. 90-93.