МИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное ГОСУДАРСТВЕННОЕ бюджетное ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информатики

и вычислительной техники

Кафедра информационной

безопасности

**Расчетно-графическая работа**

по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем»

на тему: «Разработка проводной защищенной системы передачи информации»

Выполнил: ст. гр. БИс-41

Баженов А.В.

Проверил: Тюкаев А.Ю.

Йошкар-Ола

2016 г.

Содержание

[Введение 3](#_Toc437894410)

[1. Проводные системы передачи информации 4](#_Toc437894411)

[1.1. Обобщённая структура телекоммуникационные системы 4](#_Toc437894412)

[1.2. Особенности проводных систем передачи информации 5](#_Toc437894413)

[1.3. Угрозы безопасности информации проводной системы связи 6](#_Toc437894414)

[1.3.1. Структура канала утечки информации 7](#_Toc437894415)

[1.3.2. Структура канала искажения информации 9](#_Toc437894416)

[2. Защита информации в проводной системе связи 11](#_Toc437894417)

[2.1. Методы защиты информации от влияния помех 11](#_Toc437894418)

[2.1.1. Скремблирование 12](#_Toc437894419)

[2.1.2. Помехоустойчивое кодирование 17](#_Toc437894420)

[3. Криптографическая защита 18](#_Toc437894421)

[3.1. Структура криптографической системы защиты информации 18](#_Toc437894422)

[3.1. Классификация криптографических алгоритмов 18](#_Toc437894423)

[3.2. Описание алгоритма RSA 20](#_Toc437894424)

[3.2.1. Нахождение взаимно простых чисел 21](#_Toc437894425)

[3.2.2. Решение уравнения a \* x + b \* y = 1 22](#_Toc437894426)

[4. Структура канала передачи 22](#_Toc437894427)

[4.1. Классификация каналов передачи информации 22](#_Toc437894428)

[4.2. Выбор типа проводной линии связи 23](#_Toc437894429)

[4.4. Линейное кодирование 25](#_Toc437894430)

[5. Моделирование и анализ компонентов системы 26](#_Toc437894431)

[5.1. Моделирование и анализ криптографической системы защиты 26](#_Toc437894432)

[5.2. Синтез и анализ помехоустойчивого кода 27](#_Toc437894433)

[5.3. Моделирование линейного кода 29](#_Toc437894434)

[Моделирование работы системы передачи информации 31](#_Toc437894435)

[Заключение 31](#_Toc437894436)

[Список используемых источников 34](#_Toc437894437)

# Введение

В наше время проводные линии связи получили широкое развитие и применяется в различных областях науки и производства (связь, радиоэлектроника, энергетика, термоядерный синтез, медицина, космос, машиностроение, летающие объекты, вычислительные комплексы и т. д.). Темпы роста волоконной оптики и оптоэлектроники на мировом рынке опережают все другие отрасли техники и составляют 40% в год. С их помощью решаются такие задачи, как:

* объединение локальных сетей подразделений.

Это позволяет значительно ускорить обмен информацией, а значит сделать бизнес более эффективным; сократить количество управляющих серверных станций, и, соответственно, необходимое для их обслуживания количество персонала; уменьшить число копий однотипных программ за счет установки одной сетевой версии (программы управления предприятием (ERP-системы), материального учета (MRP-системы), бухгалтерия (1C), Консультант плюс и т.п.), то есть сэкономить деньги на их покупку для каждого компьютера.

* перевод телефонии на оптические каналы связи.

При таком подходе во всех офисах телефонные аппараты могут получить внутренний номер, в результате будет достигнута экономия за счет снижения внешнего телефонного трафика.

* скоростной доступ к Интернету по отдельной линии связи.

Существенно повышает безопасность работы сети, обеспечивает высокую скорость и уменьшает трудозатраты по разделению внутренних и внешних информационных потоков.

Защита информации – одна из самых актуальных проблем в наше время. Не зря родилась поговорка «Кто владеет информацией – тот владеет миром». Съем информации по побочным электромагнитным излучениям и наводкам является основным способом кражи информации. И один из самых незащищенных участков – это линии передачи информации.

# Проводные системы передачи информации

# 1.1. Обобщённая структура телекоммуникационные системы

Система передачи информации (система связи) – это совокупность технических средств и среды распространения, обеспечивающая передачу информации.

Обобщённая структурная схема и основные элементы цифровой системы связи показана на рисунке 1.

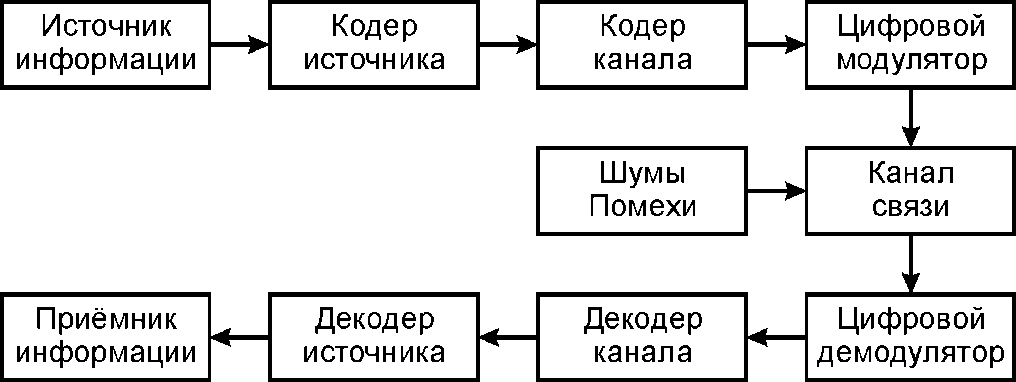


Рис. 1 – Обобщённая структурная схема цифровой системы связи.

В общем случае ИИ выдает непрерывный сигнал S(t). В цифровой системе передачи сообщение выданное источником преобразуется в последовательность двоичных символов. В идеале сигнал с выхода источника необходимо представить небольшим числом двоичных символов (необходимо найти эффективное представление сигналов с выхода источника с наименьшей избыточностью или полным ее отсутствием). Процесс эффективного преобразования выхода источника как аналогового, так и цифрового называют кодированием источника или сжатием данных.

Кодер источника (КИ) преобразует входной сигнал S(t) в последовательность двоичных символов, то есть последовательность m-разрядных кодовых комбинация

Обобщенная структурная схема кодера источника представлена на рисунке 2.

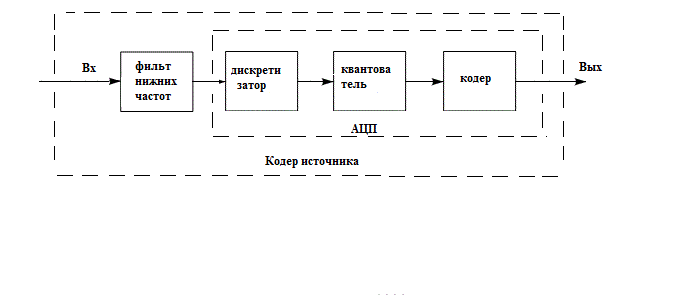


Рис. 2. Обобщенная структурная схема кодера источника

Преобразование аналогового сигнала S(t) в цифровой происходит в аналого-цифровом преобразователе (АЦП) и включает последовательное выполнение 3-х основных операций:

1. дискретизация непрерывного сигнала по времени, в результате чего формируется импульсный сигнал, промодулированный по амплитуде;
2. квантование амплитудно-импульсного модулированного сигнала по уровню;
3. кодирование отчетов амплитудно-импульсного модулированного сигнала, в результате чего формируется импульсно кодированный модулированный сигнал.

В процессе формирования цифровых сигналов осуществляется дискретизация непрерывного сигнала S(t), в соответствии с теоремой отсчетов.

# 1.2. Особенности проводных систем передачи информации

Проводные системы передачи (системы связи) – это системы связи, использующие искусственную среду распространения (линию связи) т.е. металлические провода.

Линия связи обеспечивает соединение передатчика и приёмника. Передатчик, линия связи и приемник образуют канал связи.

Источник сообщений, передатчик, линия связи, приемник и получатель образуют систему связи (Рис. 3). Системы связи, предназначенные для передачи непрерывных сообщений, называются аналоговыми, а для передачи цифровых сообщений — цифровыми.

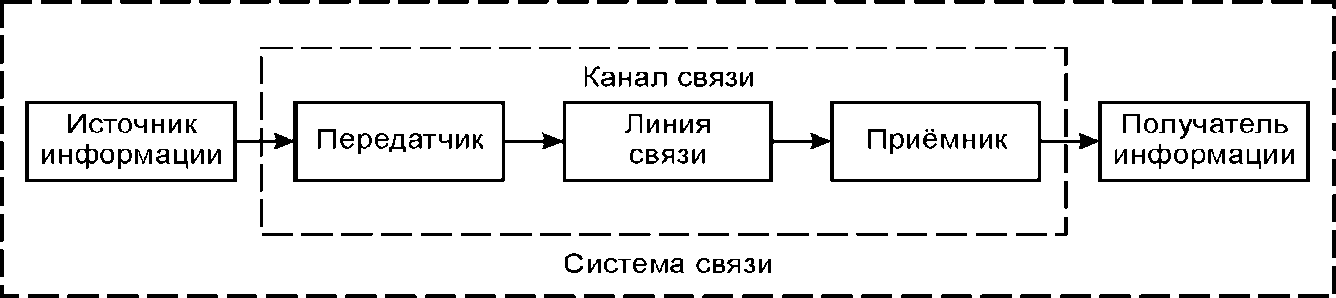


Рис. 3. Обобщённая структурная схема системы связи.

Тенденцией последних лет в развитии систем связи является переход к цифровым системам связи. Это вызвано тем, что ЦСП имеют ряд преимуществ перед аналоговыми, среди которых можно выделить следующие:

1. Высокая помехоустойчивость.

2. Слабая зависимость качества передачи от длины линии связи.

3. Стабильность параметров каналов.

4. Эффективность использования пропускной способности каналов для передачи дискретных сигналов.

5. Возможность построения цифровой сети связи.

6. Высокие технико-экономические показатели.

## 1.3. Угрозы безопасности информации проводной системы связи

Угроза безопасности - потенциально возможное событие, процесс или явление, которые могут привезти к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Как правило, наиболее уязвимой в автоматической системе обработки данных является подсистема передачи информации. В общем случае все угрозы безопасности информации делятся на:

1. угрозы утечки информации;
2. угрозы искажения информации.

### 1.3.1. Структура канала утечки информации

Утечка информации – это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Существуют определенные условия, при которых возможно образование канала передачи информации несанкционированного с источником и получателем. Такой канал в явном виде не проявляет себя, а передача информации по нему осуществляется только в одну сторону от источника к злоумышленнику. По аналогии с каналом связи такой канал называют техническим каналом утечки информации.

Под техническим каналом утечки информации будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможно несанкционированное получение информации. Для создания такого канала необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства для обработки полученной информации.

Технические каналы утечки информации в проводной системе связи можно разделить на электромагнитные и электрические.

Электромагнитный канал утечки информации возникает вследствие побочных электромагнитных излучений, образующихся по тем или иным причинам конструкторско-технологического характера. Каждое радиоэлектронное устройство системы связи является источником электромагнитных полей широкого частотного спектра. Характер электромагнитного поля изменяется в зависимости от дальности его приема. Условно можно выделить ближнюю и дальнюю зоны. Для ближней зоны расстояние значительно меньше длины волны и поле имеет явно выраженный магнитный характер, а для дальней зоны поле носит электромагнитный характер и распространяется в виде плоской электромагнитной волны, энергия которой делится поровну между электрической и магнитной составляющей. С учетом этого можно считать возможным образование канала утечки информации за счет магнитной составляющей и электромагнитного излучения.

Рассмотренные выше каналы утечки информации не требуют контактного подключения к линии связи, поэтому широко применяются в случае использования сигнальных устройств контроля целостности линии связи, устройств измерения активного (сопротивление резистивного элемента) и реактивного (индуктивного или емкостного) сопротивлений.

Структуру электромагнитного канала утечки представлена на Рис. 4.

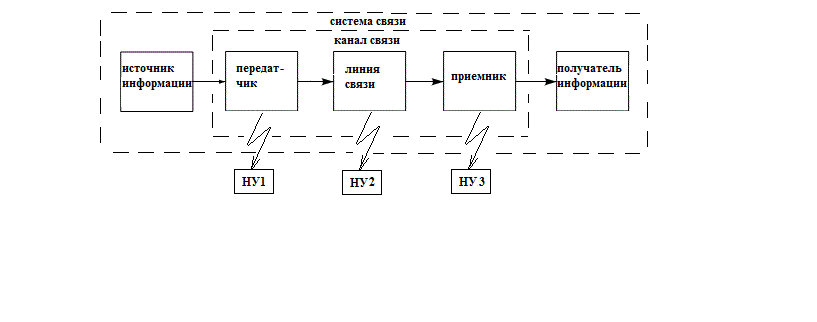


Рис.4. Структура э/м канала утечки информации.

Электрический канал утечки информации возникает по следующим причинам:

1. Незащищенность линии связи сигнальными устройствами контроля целостности линии связи ее активного и реактивного сопротивлений
2. Наводки электромагнитных излучений элементов системы связи на соединительной линии и посторонние проводники, выходящие за пределы контролируемой зоны
3. Проникновение информационных сигналов в цепи электропитания элементов систем связи
4. Проникновение информационных сигналов в цепи заземления элементов систем связи

Электрический канал утечки информации предполагает непосредственное подключение устройств съема информации к источнику сигнала.

Структура электрического канала утечки информации представлена на Рис. 5.

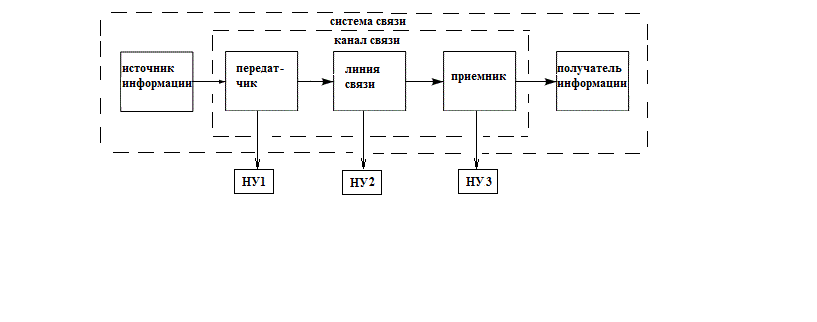


Рис.5. Структурная схема электрического КУИ.

### 1.3.2. Структура канала искажения информации

Искажение информации - событие, процесс или явление, которые могут привести к уничтожению, утрате целостности информации или появлению ложной информации при определенных пространственных, энергетических и временных условиях, возникающих в проводной системе связи. Возможно возникновение канала, по которой распространяется некоторое воздействие, искажающее информацию.

Технический канал искажения информации - физический путь, по которой распространяется некоторое воздействие (преднамеренное, случайное), вследствие которого происходит искажение информации.

Угрозы искажения информации:

1) случайные;

2) преднамеренные.

Угрозы, которые не связаны с преднамеренными действиями злоумышленника и реализуются в случайный момент времени, относят к случайным угрозам. К случайным угрозам искажения информации относят различного рода шумы и помехи, возникающие в системе связи. Все шумы и помехи можно разделить:

1. По характеру воздействия на информацию - помехи проявляются как задержка передачи импульсов, искажение уровней передаваемых потенциалов, уменьшение амплитуд передаваемых сигналов, постоянное смещение уровней напряжения питания.
2. По источнику создания - помехи разделяют на внешние и внутренние.
3. По месту проявления - помехи, как правило, разделяются на помехи в линиях связи и помехи в цепях питания.

Рассмотрим преднамеренные угрозы искажения информации. Преднамеренные угрозы искажения информации возникают вследствие преднамеренных действий злоумышленника и реализуются в известные злоумышленнику моменты времени. В общем случае можно выделать 3 вида преднамеренных угроз искажения информации:

* Утрата доступности – это утрата информацией при ее хранении, обработке и передаче техническими средствами доступности, выражающаяся в затруднении или прекращении санкционированного доступа к ним.
* Утрата целостности информации – это утрата информацией свойства целостности, т.е. часть информации удалена.
* Утрата подлинности – это утрата информацией свойства подлинности, вызванная умышленной заменой истинной информации ложной.

Как правило, вышеперечисленные преднамеренные угрозы искажения информации возможны вследствие физического или логического разрыва линии связи, что позволяет злоумышленнику подключить несанкционированное устройство, которое искажает или заменяет истинную информацию ложной.

Структура канала искажения информации в проводной системе связи путем физического или логического разрыва линии связи представлена на Рис. 6.

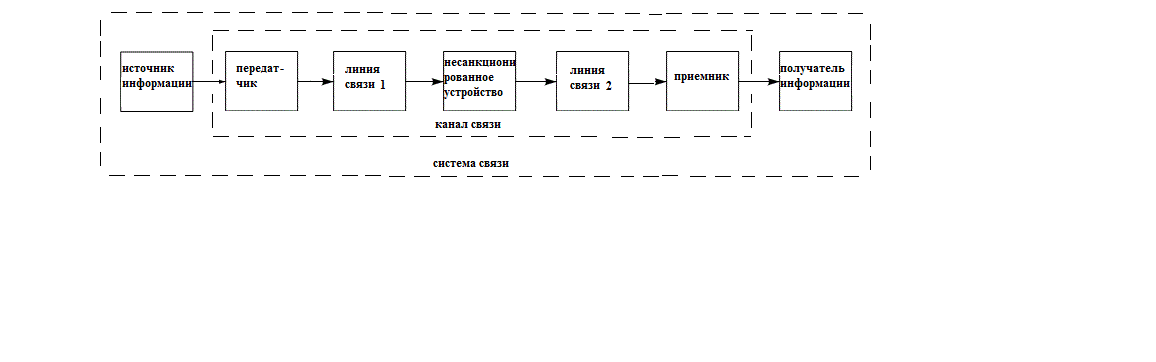


Рис.6. Структурная схема канала искажения информации.

Можно выделить случайный и преднамеренный технический канал искажения информации, которые могут возникнуть независимо друг от друга и действовать как на отдельные элементы системы, так и на всю систему в целом.

Обобщенная структура канала искажения информации путем зашумления (преднамеренного или случайного) представлена на Рис. 7.

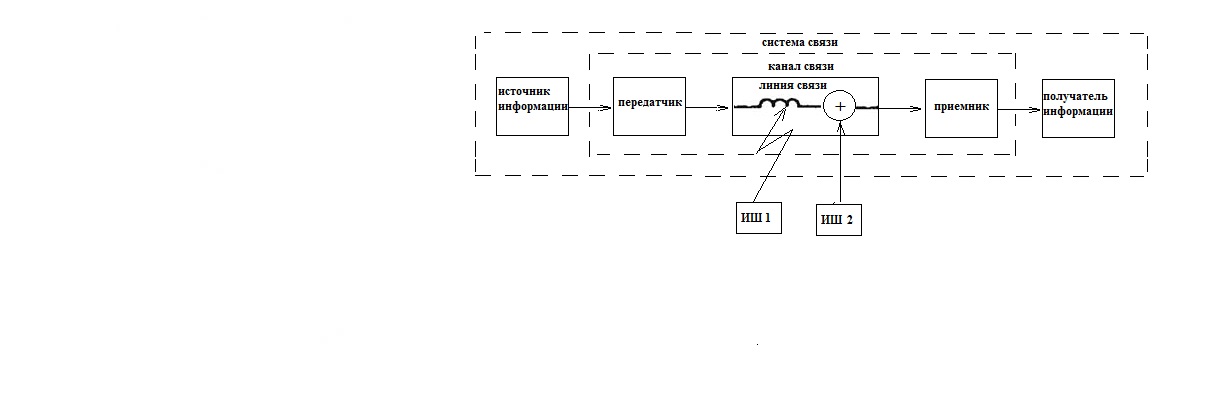


Рис.7. Обобщенная структура канала искажения информации.

# Защита информации в проводной системе связи

## Методы защиты информации от влияния помех

Все методы защиты информации от влияния помех можно разделить на физические и логические.

Под физическими методами защиты информации от влияния помех будем понимать комплекс технических мер, применение которых позволяет избавиться или снизить уровень помех и шумов в системе связи. К физическим методам защиты можно отнести:

1. Экранирование элементов системы
2. Согласование разнородных линий связи
3. Рациональный выбор кабелей для различных систем передачи
4. Подавление помех в цепях питания
5. Использование сигнального и межприборного заземления
6. Уменьшение емкостной и магнитной связи между элементами системы передач

Физические методы защиты информации от влияния помех и шумов достаточно эффективны, как правило, всегда используются при проектировании автоматических систем.

Однако данные методы не позволяют достичь высокого уровня защиты информации от влияния помех и шумов. И используются в основном для снижения уровня мешающих воздействий на элементы системы.

Под логическими методами защиты информации от влияния помех и шумов будем понимать комплекс мер, заключающихся в изменении структуры передаваемых сигналов (передаваемой информации) с целью уменьшения взаимного влияния в соседних линиях связи и повышение их помехоустойчивости.

К основным логическим методам можно отнести: скремблирование, помехоустойчивое кодирование, перемежение.

### 2.1.1. Скремблирование

Скремблирование – это шифрация потока данных, в результате которой он выглядит как поток случайных битов. В результате скремблирования последовательности бит в исходном массиве данных вероятности появления логической единицы- 1 и логического нуля – 0 становятся одинаковым и независимым.

Обычно скремблирование осуществляется перед модуляцией с помощью скремблера. Основной частью скремблера является генератор псевдослучайной последовательности.

На рис.8. представлена схема генератора псевдослучайной последовательности в виде M- разрядного сдвигового регистра с обратными связями.

****

Рис.8. Генератор псевдослучайной последовательности.

Генератор формирует псевдослучайную последовательность максимальной длины -1. Регистр сдвига изначально устанавливается в некоторое ненулевое состояние.

Под действием фронтов синхросигнала CLK хранимый в регистре код непрерывно циркулирует в нем и одновременно видоизменяется благодаря преобразованию бит элементам исключающих «или».

В общем случае при использовании M-разрядного регистра цепь обратной связи подключается к разрядам с номерами M и N. Для того чтобы на выходе формировалась псевдослучайная последовательность с периодом 2M - 1 следует выбирать точки подключения согласно таблице 1.

Таблица 1. Точки подключения к цепи обратной связи

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **M** | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 15 | 17 | 18 | 20 | 21 | 22 | 23 | 25 | 28 | 29 | 31 |
| **N** | 2 | 3 | 3 | 5 | 6 | 5 | 5 | 7 | 9 | 14 | 14 | 11 | 17 | 19 | 21 | 18 | 22 | 25 | 27 | 28 |

Различают 2 основных вида скремблирования - самосинхронизирующееся и с установкой (аддитивное).

Структурная схема самосинхронизирующейся системы скремблер-дескремблер представлена на Рис. 9.

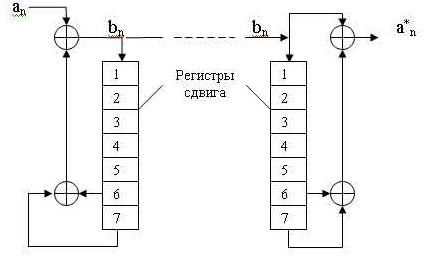


Рис.9. Структурная схема скремблера и дескремблера.

В данной работе скремблер-дескремблер содержит элементы рассмотренного генератора псевдослучайной последовательности. В скремблере цепь обратной связи на основе сдвигового регистра RG1 дополнительно содержит элемент ИСКЛЮЧАЮЩЕЕ ИЛИ XOR2. В дескремблере дополнительно применен аналогичный генератор RG2 с разомкнутой цепью обратной связи. Все процессы, протекающий в системе, синхронизируются от генератора тактовых импульсов ГТИ. ГТИ формирует синхросигнал CLK, т.е. непрерывную последовательность тактовых импульсов со скважностью равной 2 (длительность тактового импульса = половине периода). В каждом такте по фронту синхросигнала на вход скремблера передается новый бит данных DT. А код в сдвиговом регистре RG1 продвигается на один разряд вправо (1 становится 2, 2 становится 3), причем в этот же момент в освободившийся разряд заносится старый вид данных, просуммированный по модулю 2 со старым битом Y1 с выхода элемента XOR1. Если от источника данных поступает произвольная битовая последовательность, то она взаимодействует с последовательностью бит с выхода элемента XOR1. В результате формируется скремблированная последовательность бит, близкая к случайной. Эта последовательность в свою очередь продвигается по регистру 1, формирует поток данных Y1, и т.д.

При дескремблировании с помощью блока выделения тактовой частоты БВТЧ из скремблированного сигнала выделяется синхросигнал CLK, который передается на синхронизирующие входы регистра 2 и приемника данных. БВТЧ предназначен для формирования высокостабильного сигнала CLK\* на основе непрерывного смещения за входным скремблированным сигналом. Сдвиг данных в регистре 2 и прием очередного бита в его освободившийся разряд происходят по фронту сигнала CLK\*. Дескремблированные данные DT\* поступают в приемник данных и фиксируются в нем по фронтам сигнала CLK\*. Потоки данных DT и DT\* совпадают с точностью до задержки передач.

Рассмотренный способ скремблирования-дескремблирования не требует применения какой-либо процедуры начальной кодовой синхронизации, после которой коды в обоих регистрах становятся одинаковыми. Синхронизация достигается автоматически после заполнения регистров одинаковыми данными. Данный метод обладает следующими недостатками:

1. Плохая устойчивость по отношению к некоторым битовым потокам данных (например, длинные последовательности 0)
2. Размножение одиночной ошибки

Недостатки, присущие данному методу, практически отсутствуют при аддитивном скремблировании. Структурная схема аддитивной системы показана на рисунке 10:

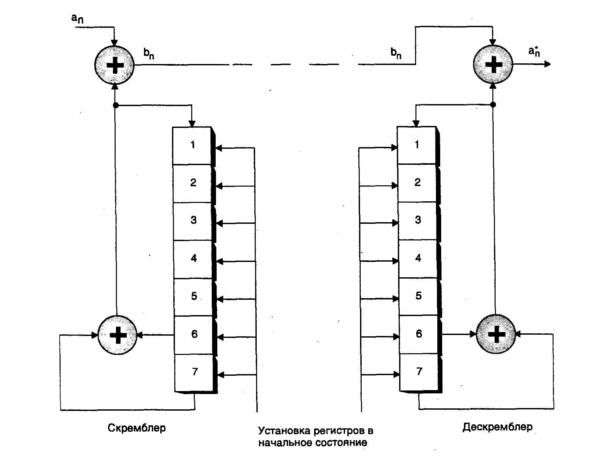


Рис.10. Структурная схема аддитивной системы.

В данной системе применены изолированные от линии связи генераторы псевдослучайной последовательности. К недостаткам данной схемы можно отнести сложность установления кодовой синхронизации, однако разработаны методы, которые позволяют исключить данный недостаток.

Применительно к цифровым системам передачи информации скремблирование позволяет:

1. уменьшить уровень помех, излучаемых на соседние линии многожильного кабеля
2. повысить надежность синхронизации устройств, подключенных к линии связи
3. обеспечить защиту информации от НСД

При распространении сигнала по линии связи неизбежна передача части его энергии в окружающее пространство. Наибольшему влиянию со стороны активной линии связи подвержены соседние линии многожильного кабеля. Это влияние проявляется в том, что появляются помехи, обусловленные в основном индуктивными и емкостными паразитными связями между соседними линиями связи. Для уменьшения взаимного влияния в соседних линиях связи следует по возможности исключить из передаваемого сигнала выраженные периодические компоненты. Это достигается за счет применения скремблирования, в результате которого последовательность бит становится псевдослучайной.

### 

### 2.1.2. Помехоустойчивое кодирование

Помехоустойчивое кодирование – это шифрация потока данных, заключающаяся во введении управляемым способом некоторой избыточности в информационную двоичную последовательность, которая может использоваться в приемнике, чтобы преодолеть влияние шума и интерференции, с которой сталкиваются при передаче сигнала через канал. Добавленная избыточность улучшает вероятность воспроизведения принятого сигнала. Говоря о помехоустойчивом кодировании, выделяют 2 стратегии использования помехоустойчивого кода:

1. С непосредственным исправлением ошибок за счет избыточности;
2. С обнаружением ошибок с последующими запросами на повторную передачу ошибочно принятой информации.

Классификация помехоустойчивых кодов:

1. Блоковые / непрерывные
2. Двоичные / недвоичные
3. Составные
4. Арифметические
5. Для пакетов ошибок / для одиночных ошибок
6. Циклические / квазициклические / нециклические
7. Систематические / несистематические
8. Корреляционные
9. Производные
10. Линейные / нелинейные

# Криптографическая защита

## Структура криптографической системы защиты информации

Самый надежный технический метод защиты информации основан на использовании криптосистем. Криптосистема включает:

алгоритм шифрования;

набор ключей (последовательность двоичных чисел), используемых для шифрования;

систему управления ключами.

Общая схема работы криптосистемы показана на рис. 11.

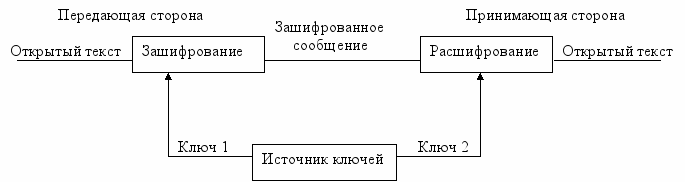


Рис.11 Общая схема работы криптосистемы

Криптосистемы решают такие проблемы информационной безопасности, как обеспечение конфиденциальности, целостности данных, а также аутентификацию данных и их источников.

Криптографические методы защиты являются обязательным элементом безопасных информационных систем. Особое значение криптографические методы получили с развитием распределенных открытых сетей, в которых нет возможности обеспечить физическую защиту каналов связи.

## Классификация криптографических алгоритмов

Известны несколько классификаций криптографических алгоритмов. Одна из них подразделяет КА в зависимости от числа ключей, применяемых в конкретном алгоритме:

* бесключевые КА — не используют в вычислениях никаких ключей;
* одноключевые КА — работают с одним ключевым параметром (секретным ключом);
* двухключевые КА — на различных стадиях работы в них применяются два ключевых параметра: секретный и открытый ключи.

Существуют более детальные классификации, одна из которых Приведена на рис. 12.



Рис.12 Классификации

Охарактеризуем кратко основные типы КА.

Хеширование — это метод криптозащиты, представляющий собой контрольное преобразование информации: из данных неограниченного размера путем выполнения криптографических преобразований вычисляется хеш-значение фиксированной длины, однозначно соответствующее исходным данным.

Симметричное шифрование использует один и тот же ключ как для зашифровывания, так и для расшифровывания информации.

Симметричное шифрование подразделяется на два вида: блочное и поточное, хотя следует отметить, что в некоторых классификациях они не разделяются и считается, что поточное шифрование — это шифрование блоков единичной длины.

Блочное шифрование характеризуется тем, что информация предварительно разбивается на блоки фиксированной длины (например, 64 или 128 бит). При этом в различных КА или даже в разных режимах работы одного и того же алгоритма блоки могут шифроваться как независимо друг от друга, так и «со сцеплением», т. е. когда результат шифрования текущего блока данных зависит от значения предыдущего блока или от результата шифрования предыдущего блока.

Поточное шифрование применяется, прежде всего, тогда, когда информацию невозможно разбить на блоки — скажем, есть некий поток данных, каждый символ которых требуется зашифровать и отправить, не дожидаясь остальных данных, достаточных для формирования блока. Алгоритмы поточного шифрования шифруют данные побитно или посимвольно.

Асимметричное шифрование характеризуется применением двух типов ключей: открытого — для зашифровывания информации и секретного — для ее расшифровывания. Секретный и открытый ключи связаны между собой достаточно сложным соотношением.

Электронная цифровая подпись (ЭЦП) используется для надежного подтверждения целостности и авторства данных.

## Описание алгоритма RSA

RSA относится к так называемым асимметричным алгоритмам, у которых ключ шифрования не совпадает с ключом дешифровки. Один из ключей доступен всем (так делается специально) и называется открытым ключом, другой хранится только у его хозяина и неизвестен никому другому. С помощью одного ключа можно производить операции только в одну сторону. Если сообщение зашифровано с помощью одного ключа, то расшифровать его можно только с помощью другого. Имея один из ключей невозможно (очень сложно) найти другой ключ, если разрядность ключа высока.

Алгоритм RSA состоит из следующих пунктов:

* Выбрать простые числа p и q
* Вычислить n = p \* q
* Вычислить m = (p - 1) \* (q - 1)
* Выбрать число d взаимно простое с m
* Выбрать число e так, чтобы e \* d = 1 (mod m)

Числа e и d являются ключами RSA. Шифруемые данные необходимо разбить на блоки - числа от 0 до n - 1. Шифрование и дешифровка данных производятся следующим образом:

* Шифрование: b = ae (mod n)
* Дешифровка: a = bd (mod n)

Следует также отметить, что ключи e и d равноправны, т.е. сообщение можно шифровать как ключом e, так и ключом d, при этом расшифровка должна быть произведена с помощью другого ключа.

### Нахождение взаимно простых чисел

На шаге 4 алгоритма RSA необходимо найти число d взаимно простое с m, т.е. не имеющее общих делителей с ним, кроме единицы. Число d должно быть меньше m, т.о. разрядность числа d равна сумме бит в числах p и q. Для нахождения взаимно простых чисел используется алгоритм Евклида, который находит наибольший общий делитель двух чисел. Если найденный делитель больше единицы, то необходимо выбрать другое число d и повторить проверку.

Алгоритм Евклида

Исходные числа a и b

Вычислить r - остаток от деления a на b: a = b \* q + r

Если r = 0, то b - искомое число (наибольший общий делитель), конец

Заменить пару чисел <a, b> парой <b, r>, перейти к пункту 2

При вычислении наибольшего общего делителя с помощью алгоритма Евклида будет выполнено не более 5 \* p операций деления с остатком, где p есть количество цифр в десятичной записи меньшего из чисел a и b. На практике алгоритм работает очень быстро.

### Решение уравнения a \* x + b \* y = 1

В 5-м пункте алгоритма RSA предполагается нахождение такого числа e, чтобы e \* d = 1 (mod m). Для этого нужно использовать модифицированный алгоритм Евклида, который работает только если числа d и m взаимно просты. Вычисление числа e сводится к решению уравнения m \* x + d \* e = 1 в натуральных числах. Число x не существенно.

http://www.paveldvlip.ru/images/rsa/matrix1.pngАлгоритм решения уравнения a \* x + b \* y = 1

Необходимо определить матрицу E =

http://www.paveldvlip.ru/images/rsa/matrix2.pngВычислить r - остаток от деления a на b: a = b \* q + r

http://www.paveldvlip.ru/images/rsa/matrix3.pngЕсли r = 0, то второй столбец матрицы дает решение: конец

E = E \*

Заменить пару чисел <a, b>, парой <b, r>, перейти к пункту 2

В данном алгоритме все вычисления можно производить по модулю большего из чисел a и b. Отрицательное число -q заменяется положительным, полученным путем вычитания числа q из числа, взятого в качестве модуля. Например, если из чисел a и b большим является число b, то все вычисления можно производить по модулю числа b, при этом -q будет представлено как b - q. Скорость работы алгоритма и количество производимых им операций примерно равно соответствующим параметрам алгоритма Евклида, описанного выше.

# Структура канала передачи

## Классификация каналов передачи информации

Каналы передачи информации можно классифицировать по следующим признакам:

1. В зависимости от способа представления информации различают аналоговые и цифровые каналы
2. По природе физической среды распространения (линии связи)
3. В зависимости от направления передачи различают симплексные каналы, дуплексные, полудуплексные
4. В зависимости от числа каналов различают одно – и много канальные системы связи. В настоящее время используются многоканальные.

## Выбор типа проводной линии связи

Линии связи предъявляются требования:

1. Осуществление связи на практически требуемое расстояние
2. Широкополосность и пригодность для передачи различных видов сообщений
3. Защищенность цепей от взаимных влияний и помех, а также от физических воздействий
4. Стабильность параметров линии, устойчивость и надежность связи

В настоящее время для создания среды распространения в проводных системах связи используют симметричный, коаксиальный и оптоволоконный кабель.

Симметричный кабель представляет собой 2 изолированных провода, спиралевидно сплетенных друг с другом (витая пара).

Различают экранированные и неэкранированные симметричные провода. Кабели данного типа обеспечивают передачу данных на сравнительно низких скоростях (несколько мегабит в секунду) и небольших расстояниях (несколько десятков метров).

Коаксиальный кабель содержит 2 проводника. Один служит для передачи сигналов, второй для заземления. Роль заземления всегда играет внешний цилиндрический проводник. Пространство между проводниками заполнено изоляционным материалом. Коаксиальный кабель способен передавать широкополосные сигналы, т.е. возможно одновременно передавать много сигналов каждый на своей чистоте. Кабели такого типа обеспечивают передачу данных на расстояние 2,5 км.

Оптоволоконный кабель представляет собой световод на кремниевой или пластмассовой основе, который защищен материалом с низким коэффициентом преломления. Оптоволоконный кабель обеспечивает скорость передачи до 50 мегабит/с, отличается практически полным отсутствием потерь при передаче, отсутствием ограничений на расстояние передачи, полосу пропускания и практически полной невосприимчивостью к помехам.

* 1. **Особенности передачи цифровых сигналов по линии связи**

Линия связи (канал связи) состоит из физической среды, по которой передается сигнал, несущий информацию, аппаратуры передачи, приема сигналов и промежуточной аппаратуры. В зависимости от физической среды передачи данных линии связи разделяются на следующие:

- проводные (воздушные),

- кабельные (медные и волоконно-оптические),

- радиоканалы наземной и спутниковой связи,

- беспроводные оптические.

Характеристики физической среды передачи во многом определяют качество предоставляемых пользователю услуг. Поэтому важно понимание процессов, происходящих при прохождении сигнала по физической среде. Физические среды передаче в радиоэлектронной аппаратуре можно разделить на внутренние и внешние. На основе внутренних построен любой радиоэлектронный блок (печатные проводники, соединительные провода). Внешние среды связи предназначены для соединения разнесенных в пространстве радиоэлектронных устройств и систем, которые могут находиться на расстоянии от нескольких метров до десятков, сотен и тысяч километров. Внешние среды отличаются от внутренних своей протяженностью. В дальнейшем под линиями связи будем понимать именно внешние линии связи. Проводные (воздушные) линии связи представляют собой провода без каких-либо изолирующих или экранирующих оплеток. По таким линиям связи передаются телефонные или телеграфные сигналы.

Такие линии не обладают помехозащищенностью. Имеют низкие скоростные качества. Кабельные линии состоят из проводников заключенных в несколько слоев изоляции: электрической, электромагнитной, механической. В настоящее время применяются три основных типа кабеля: на основе скрученных пар медных проводов (витая пара), коаксиальные кабели с медной жилой, волоконно-оптические кабели. Витая пара может существовать как в экранированном, так и в неэкранированном вариантах. Витая пара за счет скрученности проводов обладает повышенной помехоустойчивостью. Коаксиальный кабель имеет несимметричную конструкцию и состоит из внутренней медной жилы и оплетки. Волоконно-оптический кабель состоит из тонких волокон, по которым распространяются световые сигналы. Такой тип кабеля обеспечивает повышенную защищенность от электромагнитных помех. Радиоканалы наземной и спутниковой связи образуются с помощью передатчика и приемника радиоволн. Радиоканалы различаются по диапазону используемых частот или длиной волн (ДВ, СВ, КВ, УКВ, СВЧ и т.д.). Беспроводные оптические каналы основаны на передаче электромагнитных волн в инфракрасном, ультрафиолетовом и видимом оптических диапазонах. В качестве источника излучения используется лазер. Такие каналы уступают по дальности действия радиоканалам, но имеют низкую стоимость и не требуют лицензии на выделение диапазона частот.

## Линейное кодирование

Линейные коды отличаются от нелинейных замкнутостью кодового множества относительно некоторого линейного оператора, например, сложения или умножения слов кода, рассматриваемых как векторы пространства, состоящего из кодовых слов - векторов. Линейность кода упрощает его построение и реализацию. При большой длине практически могут быть использованы только линейные коды. Вместе с тем часто нелинейные коды обладают лучшими параметрами по сравнению с линейными. Для относительно коротких кодов сложность построения и реализации линейных и нелинейных кодов примерно одинакова.

Как линейные, так и нелинейные коды образуют обширные классы, содержащие много различных конкретных видов помехоустойчивых кодов. Среди линейных блочных наибольшее значение имеют коды с одной проверкой на четность, M-коды (симплексные), ортогональные, биортогональные, Хэмминга, Боуза-Чоудхури-Хоквингема, Голея, квадратично-вычетные (KB), Рида-Соломона. К нелинейным относят коды с контрольной суммой, инверсные, Нордстрома-Робинсона (HP), с постоянным весом, перестановочные с повторением и без повторения символов (полные коды ортогональных таблиц, проективных групп, групп Матье и других групп перестановок).

# Моделирование и анализ компонентов системы

## Моделирование и анализ криптографической системы защиты

При моделировании криптографической защиты был использован алгоритм шифрования RSA. RSA относится к так называемым асимметричным алгоритмам, у которых ключ шифрования не совпадает с ключом дешифровки

Стойкость алгоритма основывается на сложности вычисления обратной функции к функции шифрования

c=E(m)=m^{e}\mod n.

Для вычисления m по известным c,e,n нужно найти такой d, чтобы

e\cdot d\equiv 1{\pmod {\varphi (n)}},

то есть

d\equiv e^{-1}{\pmod {\varphi (n)}}.

Вычисление [обратного элемента](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%80%D0%B0%D1%82%D0%BD%D1%8B%D0%B9_%D1%8D%D0%BB%D0%B5%D0%BC%D0%B5%D0%BD%D1%82) по модулю не является сложной задачей, однако злоумышленнику неизвестно значение \varphi (n). Для вычисления [функции Эйлера](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_%D0%AD%D0%B9%D0%BB%D0%B5%D1%80%D0%B0) от известного числа n необходимо знать разложение этого числа на простые множители. Нахождение таких множителей и является сложной задачей, а знание этих множителей — «потайной дверцей» ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) backdoor), которая используется для вычисления d владельцем ключа. Существует множество алгоритмов для нахождения простых сомножителей, так называемой [факторизации](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D1%86%D0%B5%D0%BB%D1%8B%D1%85_%D1%87%D0%B8%D1%81%D0%B5%D0%BB), самый быстрый из которых на сегодняшний день — [общий метод решета числового поля](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%89%D0%B8%D0%B9_%D0%BC%D0%B5%D1%82%D0%BE%D0%B4_%D1%80%D0%B5%D1%88%D0%B5%D1%82%D0%B0_%D1%87%D0%B8%D1%81%D0%BB%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE_%D0%BF%D0%BE%D0%BB%D1%8F), скорость которого для k-битного целого числа составляет

\exp((c+o(1))k^{\frac {1}{3}}\log ^{\frac {2}{3}}k) для некоторого c<2.

В 2010 году группе учёных из Швейцарии, Японии, Франции, Нидерландов, Германии и США удалось успешно вычислить данные, зашифрованные при помощи криптографического ключа стандарта RSA длиной 768 бит. Нахождение простых сомножителей осуществлялось [общим методом решета числового поля](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%89%D0%B8%D0%B9_%D0%BC%D0%B5%D1%82%D0%BE%D0%B4_%D1%80%D0%B5%D1%88%D0%B5%D1%82%D0%B0_%D1%87%D0%B8%D1%81%D0%BB%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE_%D0%BF%D0%BE%D0%BB%D1%8F). По словам исследователей, после их работы в качестве надежной системы шифрования можно рассматривать только RSA-ключи длиной 1024 бита и более. Причём от шифрования ключом длиной в 1024 бит стоит отказаться в ближайшие три-четыре года. С 31 декабря 2013 года браузеры Mozilla перестали поддерживать сертификаты удостоверяющих центров с ключами RSA меньше 2048 бит.

Кроме того, при неправильной или неоптимальной реализации или использовании алгоритма возможны специальные криптографические атаки, такие как атаки на схемы с малой секретной экспонентой или на схемы с общим выбранным значением модуля.

## Синтез и анализ помехоустойчивого кода

При моделировании помехоустойчивого кода был использован Код Рида-Маллера.

Код Рида-Маллера — линейный двоичный блочный код. При определённом построении он может быть систематическим. В общем случае код Рида-Маллера не является циклическим.

Коды Рида-Маллера задаются следующими параметрами для любых значений m и r, называемого порядком кода, меньшего, чем m: — длина кодового слова n=2m; — длина информационной части k=1+Cm1+…+Cmr; — длина проверочной части n-k=1+Cm1+…+Cmm-r-1; — минимальное кодовое расстояние dmin=2m-r. Код Рида-Маллера определяется при помощи порождающей матрицы, состоящей из базисных векторов.

Строится по правилу: — пусть V0 — вектор, все компоненты которого равны 1; — пусть V1, V2,…, Vm — строки матрицы, столбцами которого являются все двоичные наборы длины m. Код Рида-Маллера r-го порядка содержит в качестве базиса векторы V0, V1,…, Vm и все компонентные произведения r или меньшего числа этих векторов.

Пусть m = 3, n = 8, k = 4. На вход кодера поступает сообщение a = 1101.

Чтобы получить зашифрованное сообщение u = a \* G, необходимо построить порождающую матрицу:

Для сообщения a = 1101 получим u = 11010100.

Пусть в процессе передачи была допущена ошибка e = 00010000. Тогда на выходе получим сообщение y = 11000100.

Чтобы на выходе получить сообщение без ошибок необходимо произвести следующие действия.

1. Найти , где
2. Построить вектор ошибок

|  |  |
| --- | --- |
| e | S |
| 00000001 | 0001 |
| 00000010 | 0010 |
| 00000100 | 0100 |
| 00001000 | 1000 |
| 00010000 | 0111 |
| 00100000 | 1011 |
| 01000000 | 1101 |
| 10000000 | 1110 |

1. По найденному S определить соответствующий ему ошибку e.
2. Из y вычесть е и получим сообщение без ошибок.

S = 0111 => e = 00010000. U = y – e = 11000100 – 00010000 = 11010100.

Таким образом, коррекция ошибок каждой ступенью декодирования обеспечивает более высокую достоверность исправления ошибок последующими ступенями декодирования. Следовательно, при оптимально выбранном количестве ступеней декодирования можно обеспечить высокую достоверность и скорость обработки информации при невысоких затратах на реализацию декодера.

## 5.3. Моделирование линейного кода

При моделировании линейного кода был использован код 2B1Q.

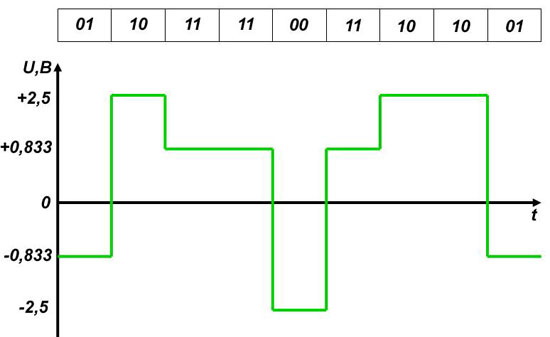
Линейное кодирование 2B1Q (2 Binary 1 Quandary) было разработано для использования в качестве протокола физического уровня в точке сопряжения U BRI-интерфейса сетей ISDN. Алгоритм 2B1Q представляет собой один из вариантов реализации амплитудно-импульсной модуляции с четырьмя уровнями выходного напряжения без возвращения к нулевому уровню. Алгоритм формирования кода приведен в табл. 2.

Таблица 2

|  |  |
| --- | --- |
| ***Кодовая группа*** | ***Кодовое напряжение*** |
| 00 | - 2,5 В |
| 01 | - 0,833 В |
| 10 | + 2,5 В |
| 11 | + 0,833 В |

Для формирования линейного кода входной информационный поток делится на кодовые группы по два бита в каждой. Положительная полярность означает, что первый бит равен 1, а отрицательная, что он равен 0. Второй бит интерпретируется как 1 при низких уровнях напряжения и как 0 при высоких уровнях.

Таким образом, закодированный в соответствии с правилами 2B1Q сигнал представляет собой последовательность скачкообразно изменяющихся напряжений с 4 возможными уровнями (рис. 10)

  
Рис. 10 Пример формирования кода 2В1Q

## Моделирование работы системы передачи информации

На языке программирования C# была написана программа, реализующая основные этапы проводной передачи информации:

* Шифрование
* Помехоустойчивое кодирование
* Линейное кодирование

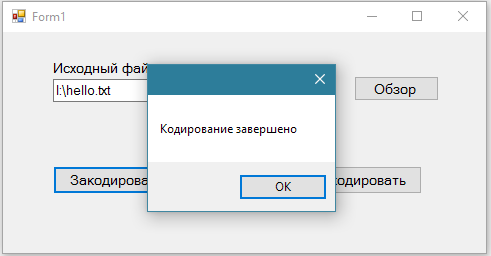


Рис. 11 Пример работы программы

# Заключение

Защищенная проводная система связи должна обеспечить гарантированную передачу конфиденциальной информации от отправителя до получателя. В общем случае комплекс мер по защите информации в проводной системе связи включает в себя защиту информации от утечки и искажения информации. Утечка информации является следствием направленных действий злоумышленника. Искажение информации может происходить вследствие намеренных действий злоумышленника, а также из-за действия различного рода шумов и помех.

В проводных системах связи основными каналами утечки и искажения информации следует считать электрический (за счет прямого контактного подключения к линии связи) и электромагнитный (за счет паразитных излучений нагруженных линий связи и других компонентов системы).

Основными направлениями защиты проводных каналов связи следует считать:

1. организационно-технические:
   1. оптимизация структуры системы, оптимальный выбор и размещение ее компонентов
   2. экранирование компонентов системы и линии связи (при наличии технической возможности)
   3. регулярный контроль состояния линии связи и оценка ее электрофизических характеристик
2. математические и программные:
   1. применение транспортных протоколов, обеспечивающих гарантии факта и качества доставки информации
   2. применение помехоустойчивых кодов с целью обнаружения и исправления ошибок
   3. применение методов резервирования и повторной передачи информации
   4. криптографическая защита информации, контроль целостности данных

Одним из важнейших элементов проводной системы связи является подсистема линейного кодирования, которая обеспечивает синхронность работы удаленных устройств в рамках единой системы. Таким образом можно выделить основные методы защиты информации в проводной системе связи:

1. Криптографические методы защиты
2. Помехоустойчивое кодирование
3. Конструкторско-технологические методы контроля состояния линии связи и обнаружения несанкционированных контактных подключений
4. Линейное кодирование

Защита информации – одна из самых актуальных проблем в наше время. Съем информации по побочным электромагнитным излучениям и наводкам является основным способом кражи информации. И один из самых незащищенных участков – это линии передачи информации. Именно поэтому данную проблему не стоит игнорировать.

## Список используемых источников

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. Москва. ИД "ФОРУМ" - ИНФРА - М. 2008 - 592стр.
2. Сердюк В.А. Системы обнаружения компьютерных атак и их роль в защите информационных сетей //BYTE/Россия. 2000. №10 - 24 стр.
3. Сердюк В.А., Технологии несанкционированных воздействий на Интернет, Приложение к журналу «Информационные технологии» //BYTE/Россия, №5, 2001, - 24 стр.
4. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979 г.
5. «Системы, сети и устройства телекоммуникаций». [Электронный ресурс]. URL: http://tekhnosfera.com/vak/sistemy-seti-i-ustroystva-telekommunikatsiy/17
6. «Википедия. Коаксиальный кабель». [Электронный ресурс]. URL: http://dic.academic.ru/dic.nsf/ruwiki/972168
7. «Википедия. Витая пара». [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Витая\_пара
8. «Особенности передачи сигналов по линиям связи». [Электронный ресурс]. URL: http://5fan.ru/wievjob.php?id=23870
9. «Краткая классификация помехоустойчивых кодов». [Электронный ресурс]. URL: http://studopedia.org/5-88021.html
10. «RSA» [Электронный ресурс]: свободная энциклопедия Википедия, URL: https://ru.wikipedia.org/wiki/RSA
11. «RSA» [Электронный ресурс]: URL: https://www.paveldvlip.ru /algorithms/rsa.html