

# **ТЕМА 2.1.4 ИСКАЖЕНИЕ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ**



**Контроль ошибок** состоит в обнаружении и исправлении ошибок в данных при их записи и воспроизведении или передаче по линиям связи.

В системах связи возможны несколько стратегий **борьбы с ошибками**:

- Обнаружение ошибок в блоках данных и автоматический запрос повторной передачи повреждённых
- Обнаружение ошибок в блоках данных и отбрасывание повреждённых блоков (такой подход иногда применяется в системах потокового мультимедиа, где важна задержка передачи и нет времени на повторную передачу)
- Упреждающая коррекция ошибок добавляет к передаваемой информации такие дополнительные данные, которые позволяют исправить ошибки без дополнительного запроса.



# Стратегии исправления ошибок.

Упреждающая коррекция ошибок (также прямая коррекция ошибок, англ. **Forward Error Correction, FEC**) — техника помехоустойчивого кодирования и декодирования, позволяющая исправлять **ошибки методом упреждения**. Применяется для исправления **сбоев и ошибок** при передаче данных путём передачи избыточной **служебной информации**, на основе которой может быть восстановлено первоначальное содержание.

На практике широко используется в сетях передачи данных в **телекоммуникационных технологиях**.



# Автоматический запрос повторной передачи

Распространены следующие методы автоматического запроса:

## Запрос ARQ с остановками (англ. stop-and-wait ARQ)

**Передатчик** ожидает от **приемника** подтверждения успешного приема предыдущего блока данных перед тем, как начать передачу следующего. В случае, если блок данных был принят с ошибкой, **приемник передает отрицательное подтверждение** и **передатчик повторяет передачу блока**. Его недостатком является низкая скорость из-за высоких накладных расходов на ожидание.

## Непрерывный запрос ARQ с возвратом (continuous ARQ with pullback)

**Передача данных** от передатчика к приемнику производится **одновременно**. В случае ошибки **передача возобновляется, начиная с ошибочного блока** (то есть передается ошибочный блок и все последующие). Осуществляется передача только ошибочно принятых блоков данных.



**Корректирующий код (также помехоустойчивый код)** — код, предназначенный для обнаружения и исправления ошибок.

**Коды обнаружения ошибок** - могут только установить факт ошибки. Применяются в сетевых протоколах.

**Коды, исправляющие ошибки** - могут установить факт ошибки и исправить ее (при этом он будет способен обнаружить большее число ошибок, чем был способен исправить).

**Применяются** в системах цифровой связи, в том числе: спутниковой, радиорелейной, сотовой, передаче данных по телефонным каналам, а также в системах хранения информации, в том числе магнитных и оптических.



По способу работы с данными коды, исправляющие ошибки, бывают:

## **Блочные**

Делят информацию на фрагменты постоянной длины и обрабатывают каждый из них в отдельности. Блочные коды делятся на:

- **Линейные коды общего вида** (Коды Хэмминга)
- **Линейные циклические коды** (Коды CRC, Коды BCH)

## **Свёрточные**

Работают с данными как с непрерывным потоком.

**Кодирование** производится с помощью **регистра сдвига**

**Декодирование** производится по **алгоритму Витерби**

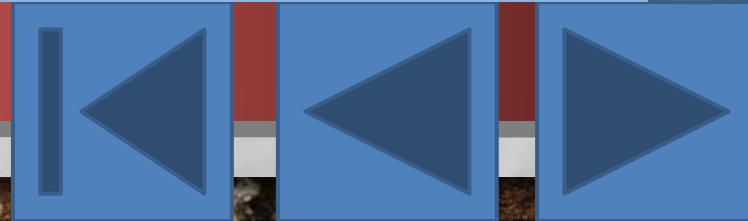


# Методы защиты информации при передаче по каналам связи

**Криптография** — наука о методах обеспечения **конфиденциальности** (невозможности прочтения информации посторонним), **целостности данных** (невозможности незаметного изменения информации), **аутентификации** (проверки подлинности авторства или иных свойств объекта), **шифрования** (кодировка данных).

Известные **криптографические методы** защиты информации можно разбить на два класса:

- 1) **Шифрование** - обработка информации путем замены и перемещения букв, при котором объем данных не меняется
- 2) **Кодирование** - сжатие информации с помощью замены отдельных сочетаний букв, слов или фраз.



# Требования алгоритмам шифрования

- Высокий уровень **защиты данных** против дешифрования и возможной модификации;
- Защищенность информации должна основываться только на **знании ключа** и не зависеть от того, известен алгоритм или нет (**правило Киркхоффа**)
- **Малое изменение** исходного текста или ключа должно приводить к **значительному изменению** зашифрованного текста (**эффект «обвала»**)
- Область значений ключа должна **исключать возможность дешифрования** данных путем перебора значений ключа
- **Экономичность** реализации алгоритма при достаточном быстродействии
- **Стоимость дешифрования** данных без знания ключа должна превышать **стоимость данных**





# Современные алгоритмы шифрования

- Симметричное шифрование
- Стандарт ГОСТ 28147-89
- Стандарт AES
- Асимметричное шифрование
- Алгоритм RSA



# Стеганография

Способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения).

В отличие от **криптографии**, которая скрывает содержимое тайного сообщения, **стеганография** скрывает сам факт его существования.



# Классификация стеганографии

Классическая

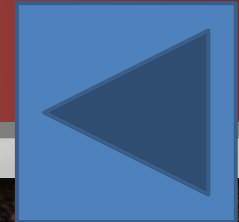
Компьютерная

Цифровая



# Классическая стеганография

- Использование симпатических (невидимых) чернил
- Запись на боковой стороне колоды карт, расположенных в условленном порядке
- Запись внутри варёного яйца
- «Жаргонные шифры», где слова имеют другое обусловленное значение;
- Геометрическая форма — метод, в котором отправитель старается скрыть ценную информацию, поместив её в сообщение так, чтобы важные слова расположились в нужных местах или в узлах пересечения геометрического рисунка
- Семаграммы — секретные сообщения, в которых в качестве шифра используются различные знаки, за исключением букв и цифр
- Узелки на нитках



# Компьютерная стеганография

**Использование зарезервированных полей компьютерных форматов файлов** (часть поля расширений, не заполненная информацией о расширении, по умолчанию заполняется нулями. Соответственно мы можем использовать эту «нулевую» часть для записи своих данных.)

**Недостаток:** низкая степень скрытности и малый объём передаваемой информации.

**Метод скрытия информации в неиспользуемых местах гибких дисков** (информация записывается в неиспользуемые части диска)

**Недостатки:** маленькая производительность, передача небольших по объёму сообщений.

**Метод использования особых свойств полей форматов, которые не отображаются на экране** основан на специальных «невидимых» полях для получения сносок, указателей. К примеру, написание чёрным шрифтом на чёрном фоне.

**Недостатки:** маленькая производительность, небольшой объём передаваемой информации.



# Цифровая стеганография

Направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов.

Данные объекты являются мультимедиа-объектами и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов.

В оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования; далее, при воспроизведении этих объектов появляется дополнительный аналоговый шум и нелинейные искажения аппаратуры, все это способствует большей незаметности сокрытой информации.

