Тема лекции:
«ОСНОВНЫЕ ПРИНЦИПЫ КРИПТОГРАФИИ»

Одним из первых в истории документально засвидетельствованных примеров шифрования является шифр Цезаря (I в. до н.э.), который образовывался заменой одних букв другими соответствующими буквами по всему тексту.

В современной терминологии шифр Цезаря и его модификации относятся к **одноалфавитным** подстановкам или **одноалфавитным** заменам.

Предвестником возникновения криптографии стало появление ***криптоанализа***.

Значительной модификацией одноалфавитной замены является шифр, который называют квадратом Полибия.

В XVI столетии Д. Кардано изобрел новый тип шифра. Для шифрования Кардано предложил использовать квадрат с прорезанными в нем несколькими ячейками. Ячейки прорезались таким образом, чтобы при повороте квадрата вокруг своего центра.

При шифровании квадрат кладут на лист для послания сначала в исходном положении и пишут слева направо сверху вниз первую порцию сообщения. Для дешифрования необходимо иметь точную копию того квадрата.

Шифры, которые не модифицируют буквы сообщения, а только изменяют их размещение, называют ***перестановочными***.

После Д. Кардано французским дипломатом Виженером была предложена модификация шифра замен, получившая название таблицы Виженера.

Такой шифр получил название ***многоалфавитной*** *замены*.

Следующей модификацией этого способа стало шифрование по книге. При шифровании отправитель выбирает в ней произвольное место и записывает вместо пароля. Само кодирование выполняется по той же схеме, что и в методе Виженера. Получатель по другому каналу связи получает страницу и слово в книге, с которого началось шифрование.

С XIX века криптография перешла на качественно другой уровень: началась эра цифровой криптографии.

В 20-х годах XX века Г. Вернам предложил автоматизировать шифрование телетайпных сообщений по следующей схеме. Информация на телетайпной ленте представляет собой последовательность отверстий и не пробитых участков, соответствующих "0" и "1".

В момент передачи очередного импульса в канал связи лента-пароль сдвигается на одну позицию и с нее считывается текущее двоичное значение.

На принимающей стороне должна присутствовать точно такая же лента, и притом – в том же начальном положении, что и у отправителя.

Таким образом, тут впервые была применена операция сложения по модулю 2, которая стала базовой в цифровой криптографии.

Такая операция также называется "исключающее ИЛИ" и записывается как + или XOR (от английского "Exclusive OR").

Недостатком такой схемы является неудобство хранения большого пароля и его одноразовость.

КЛАССИФИКАЦИЯ ШИФРОВ

Первым принципиальным признаком, позволяющим провести разделение шифров, является объем информации, который неизвестен третьей стороне.

Если злоумышленнику совершенно неизвестен алгоритм выполненного над сообщением преобразования, то шифр называют ***тайнописью***.

В свое время А. Кергофф выдвинул идею о том, что раскрытие самого алгоритма не должно ни на шаг приближать к закрытому сообщению.

Эта идея получила название ***принцип Кергоффа***.

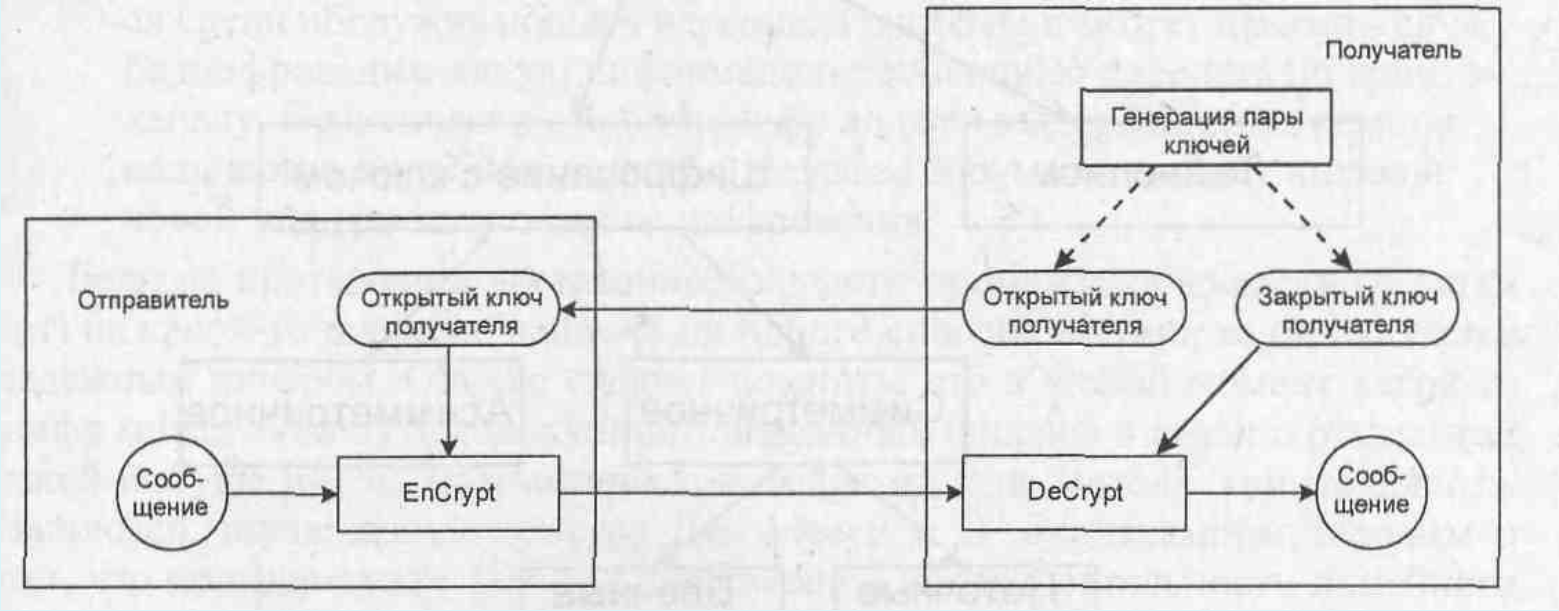
В противоположность тайнописи, ***криптографией с ключом*** называют сегодня алгоритмы шифрования, в которых сам алгоритм преобразований широко известен и доступен каждому.
В современной криптографии размер ключа составляет от 56 до 4096 бит!!!

Все криптоалгоритмы с ключом делятся на
симметричные и ***асимметричные***.

Применяют термин ***тайный ключ***, а сами системы называют ***шифрами на тайном ключе.***

Общая схема процесса передачи сообщения

В асимметричном шифровании для шифрования сообщения используется один ключ, а для дешифрования – другой:



Асимметричное шифрование

Ключ шифрования может быть известен всем пользователям сети и называться ***открытым ключом***,

а ключ дешифрования называют ***закрытым***.

Сами же асимметричные системы получили название ***шифра на открытом ключе***.

Симметричные криптоалгоритмы делятся на

поточные и *блочные шифры*.

Принципы криптографических преобразований, носящих название блочных шифров.

Основным законом блочного шифрования является "или блок или ничего", то есть, преобразования могут осуществляться только над информацией строго определенного объема.

Частичное шифрование (например, попытка обработать 177 бит) невозможно. Блочное шифрование получило значительно более широкое распространение.

Таким образом, если поточные шифры одинаково часто реализуются как программно, так и аппаратно, то блочные шифры по большей части имеют программную реализацию.

Теоретически возможно создание поточных асимметричных систем, однако практической ценности такие системы иметь не будут.

Общая схема классификации

Абсолютная стойкость шифра может быть достигнута только в случае, когда размер ключа равен или превышает размер исходного сообщения. Если же размер ключа меньше объема исходного сообщения, тогда теряется непредвиденность.

Ключ считается подобранным, если в результате дешифрования в сообщении определилась часть, имеющая смысл.

Таким образом, любой шифр, длина которого меньше длины передаваемого сообщения, не является абсолютно стойким.

Практически стойким называют шифр, к которому нельзя применить какие-нибудь результативные методы атаки, кроме полного перебора всех возможных ключей.

основные виды атак

Атака на основе шифротекста — это попытка злоумышленника выявить или исходный текст, или ключ шифрования с помощью достаточно большого объема зашифрованных данных.

Атака на основе известного открытого текста – ситуация, когда злоумышленник знает и исходный, и преобразованный в процессе шифрования текст и желает узнать о ключе шифрования.

Атака на основе выбранного открытого текста является модификацией предыдущей атаки в том случае, когда злоумышленник находится среди обслуживающего персонала системы и может навязать службе шифрования, какую информацию необходимо передать по криптоканалу.

Например, после доказательства Дж. Месси и Э. Берлекампом теоремы о том, что при перехвате *2*N* бит шифрующей последовательности линейного регистра сдвига всегда можно восстановить его внутреннюю структуру, линейные регистры сдвига покинули класс надежных шифров и применяются только как составные элементы более сложных криптоалгоритмов.

До сих пор не существует теории, позволяющей генерировать надежные на 100% практически стойкие шифры.

Итак, какой угодно шифр можно открыть простым перебором ключей. Все зависит от размера ключа, определяющего количество времени на перебор всех вариантов.

Так, если длина ключа составляет 32 бита (4 млрд. вариантов), то требуется несколько дней (или недель) для его открытия. Ключи длиной 128 бит в современных надежных шифрах невозможно открыть полным перебором на современных ЭВМ.

СИММЕТРИЧНАЯ КРИПТОГРАФИЯ. ПОТОЧНЫЕ ШИФРЫ

Характерной особенностью поточных шифров является побитовая обработка информации.

Обработка информации может быть представлена в виде автомата, который на каждом своем такте:

-генерирует по некоторому закону один бит шифрующей последовательности;

-каким-либо обратным преобразованием накладывает на один бит открытого потока этот шифрующий бит и получает зашифрованный бит.

Шифрующую последовательность достаточно ограничить только одним битом на бит исходного текста.

две обратимые операции: исключающее ИЛИ (оно же сложение по модулю 2) и отрицание.

Таким образом, как бы много ни было создано шифрующих битов на один бит исходного текста, все они будут накладываться на данный бит путем комбинации из операций *XOR* и "Отрицание".

Однако отрицание можно вносить внутрь операции *XOR,* то есть, для любых *a* и *b:*

$$NOT(a\ XOR\ b) = a\ XOR\ (NOT\ b) = (NOT\ a)\ XOR\ b$$

Итак, какой бы ни была сложной композиция из шифрующих битов и исходного, ее всегда можно разделить, то есть, представить в виде:

$$p\ XOR\ F(gl,g2,g3)$$

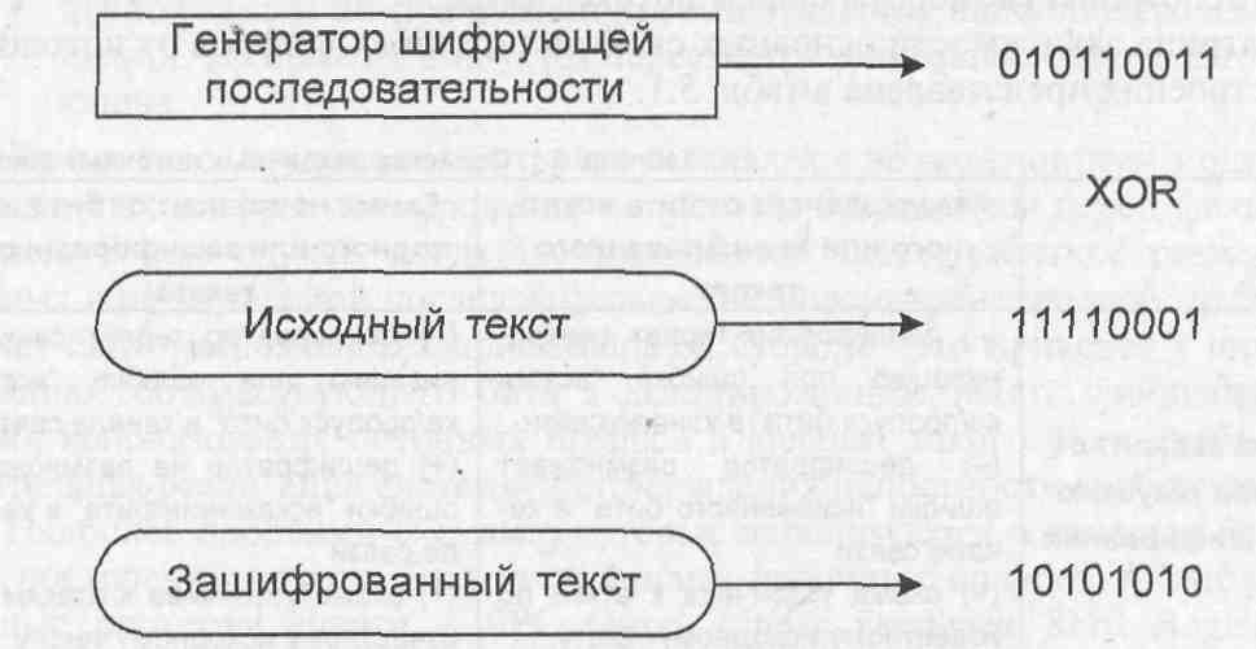
где *p* – исходный бит (от англ. "plain“ – “открытий"), *g* – шифрующие биты, *F* – некоторая функция, содержащая в себе операции исключающее ИЛИ и отрицание.

вся формула шифрования будет иметь универсальный вид:

$$c = p\ XOR\ g$$

где *c* – зашифрованный бит (от англ. "ciphered“ – “зашифрованный").

Общая схема шифрования поточным шифром:



Бит шифрования, который появляется на каждом новом шаге автомата, или целый набор таких битов, принято обозначать символом *y* (гамма), а сами поточные шифры получили за это второе название – ***шифры гаммирования***.

Тремя основными компонентами, над которыми вычисляется функция, порождающая гамму, являются:

-ключ;
-номер текущего шага шифрования;
-ближайшие от текущей позиции биты исходного и/или зашифрованного текста.

Ключ является необходимой частью гаммирующего шифра. Если ключ и схема порождения гаммы не являются тайными, то поточный шифр превращается в обычный преобразователь – кодер – скремблер (от англ. «scramble» – «перемешивать»).

Свойства различных поточных шифров

	Гамма зависит от бита исходного или зашифрованного текста	**Гамма не зависит от бита исходного или зашифрованного текста**
Гамма зависит от номера текущего такта шифрования	(-) дешифратор теряет синхронизацию при ошибке "вставка/пропуск бита" в канале связи. (-) дешифратор размножает ошибки "искаженного бита" в ка нале связи (+) схема устойчива к атаке по известному исходному тексту	(-) дешифратор теряет синхронизацию при ошибке "вставка/пропуск бита" в канале связи (+) дешифратор не размножает ошибки "искажения бита" в канале связи (+) схема устойчива к атакам по известному исходному тексту
Гамма не зависит от номера текущего такта шифрования	(+) дешифратор не теряет синхронизацию при ошибке "вставка/пропуск бита" в канале связи (-) дешифратор размножает ошибки "искажение бита" в канале связи (-) схема неустойчива к атаке по известному исходному тексту	

Таким образом, шифры, которые зависят только от ключа и номера такта шифрования (правый столбец, верхняя строка в таблице) получили наибольшее распространение в современной практике.

Лекция

Тема лекции: «СТАНДАРТНЫЕ ЛОКАЛЬНЫЕ СЕТИ»

За время, прошедшее с появления первых локальных сетей, было разработано несколько сотен самых разных сетевых технологий.

Далеко не всегда стандартные сети имеют рекордные характеристики, обеспечивают наиболее оптимальные режимы обмена.

Немаловажно и то, что производители программных средств также в первую очередь ориентируются на самые распространенные сети.

В настоящее время тенденция уменьшения количества типов используемых сетей все усиливается. Дело в том, что увеличение скорости передачи в локальных сетях до 100 и даже до 1000 Мбит/с требует применения самых передовых технологий, проведения серьезных и дорогих научных исследований.

В ближайшем будущем вряд ли стоит ожидать принятия принципиально новых стандартов.

На рынке имеются стандартные локальные сети всех возможных топологий, так что выбор у пользователей имеется.

Стандартные сети обеспечивают большой диапазон допустимых размеров сети, допустимого количества абонентов сети и, что не менее важно, большой диапазон цен на аппаратуру.

Ошибки в выборе аппаратуры гораздо дороже ошибок в выборе программных средств.

Сети Ethernet и Fast Ethernet

Наибольшее распространение среди стандартных сетей получила сеть **Ethernet**. Впервые она появилась в 1972 году (разработчиком выступила известная фирма Xerox).

Сеть оказалась довольно удачной, и вследствие этого ее в 1980 году поддержали такие крупнейшие фирмы, как DEC и Intel (объединение этих фирм, поддерживающих Ethernet, назвали DIX по первым буквам их названий).

Стандарт получил название IEEE 802.3. Он определяет множественный доступ к моноканалу типа «шина» с обнаружением конфликтов и контролем передачи.

Основные характеристики стандарта IEEE 802.3 следующие: топология – шина, среда передачи – коаксиальный кабель, скорость передачи – 10 Мбит/с, максимальная длина ~ 5 км, максимальное количество абонентов – до 1024, длина сегмента сети – до 500 м, количество абонентов на одном сегменте – до 100, метод доступа –CSMA/CD, передача узкополосная, то есть без модуляции (моноканал).

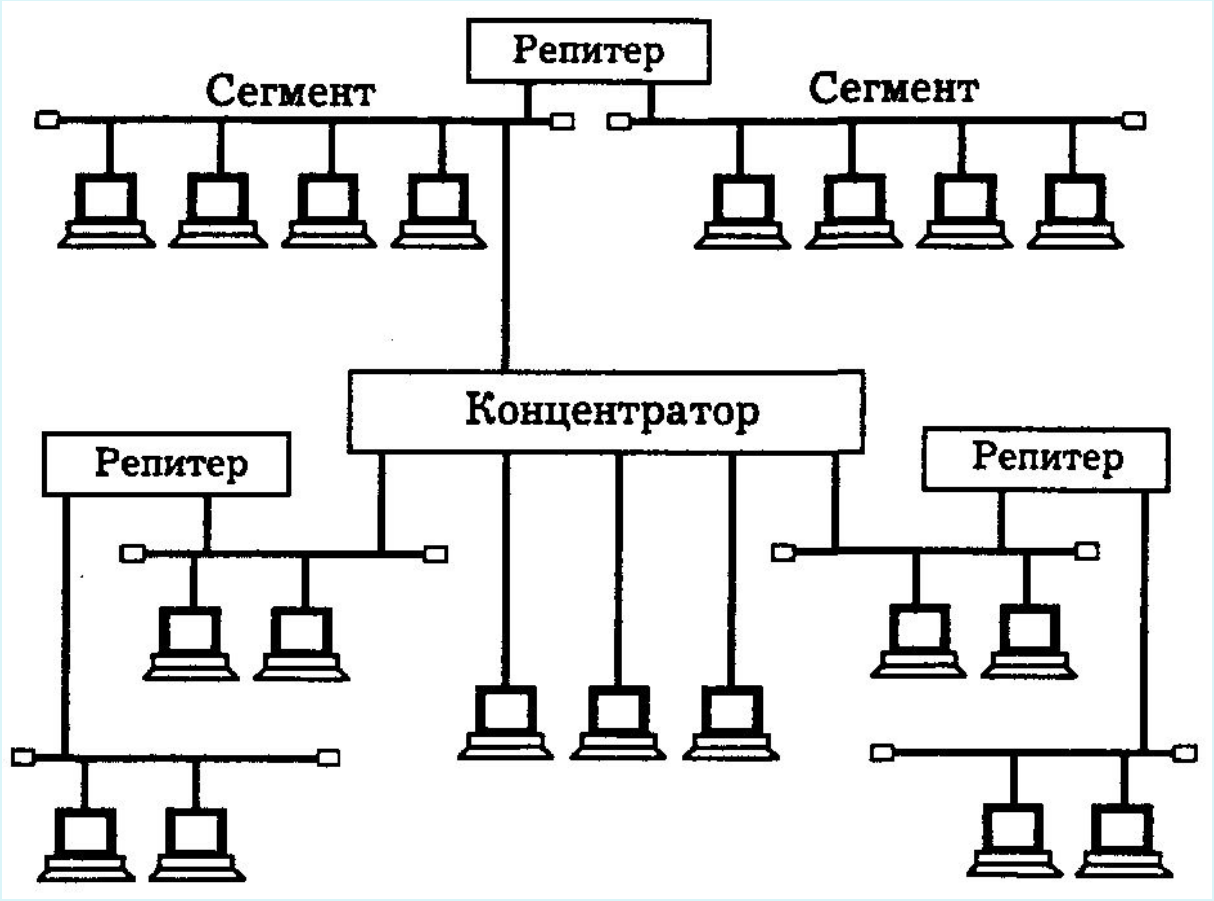
Между стандартами IEEE 802.3 и Ethernet существуют небольшие отличия, но о них обычно предпочитают не вспоминать.

Сеть Ethernet стала наиболее популярна в мире с середины 90-х (более 70 миллионов абонентов сети в 1996 году, свыше 100 миллионов абонентов в 1997 году, или более 80% рынка), и нет сомнения, что таковой она и останется в ближайшие годы.

В классической сети Ethernet применяется 50-омный коаксиальный кабель двух видов (толстый и тонкий).

Определен также стандарт для применения в сети оптоволоконного кабеля.

В 1995 году появился стандарт на более быструю версию Ethernet, работающую на скорости 100 Мбит/с (так называемый Fast Ethernet, стандарт IEEE 802.3u) и появилась и версия на скорость 1000 Мбит/с (Gigabit Ethernet, стандарт IEEE 802.3z).



Топология сети Ethernet

В качестве сегмента может также выступать единичный абонент.

Коаксиальный кабель используется для шинных сегментов, а витая пара и оптоволоконный кабель – для лучей пассивной звезды.

Фактически получается, что абоненты соединены в физическую шину.

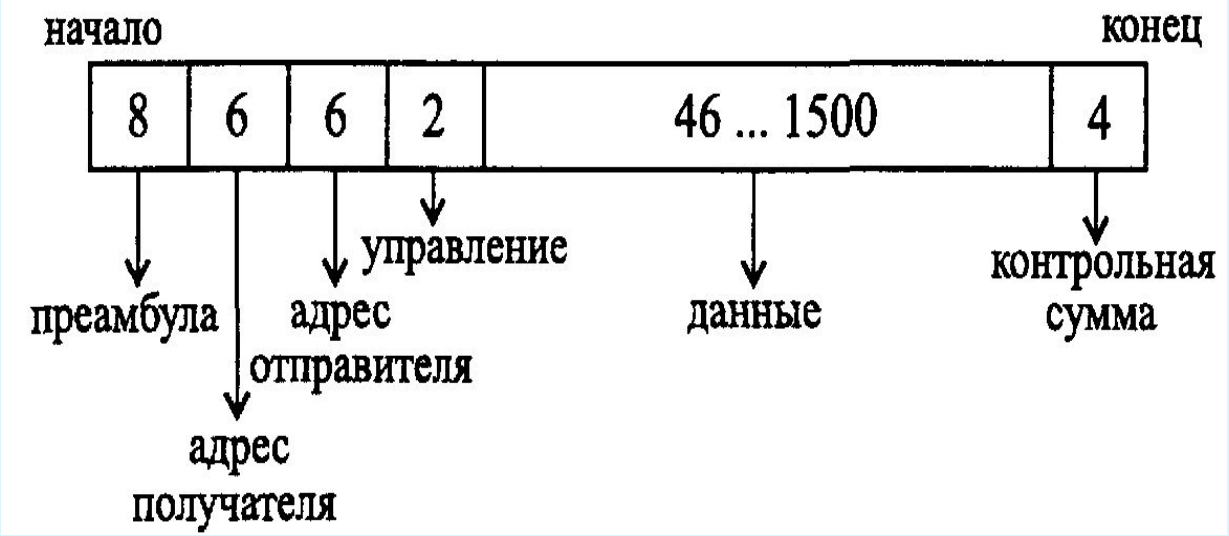
Максимальная длина кабеля всей сети в целом (максимальный путь сигнала) теоретически может достигать 6,5 км, но практически не превышает 2,5 км.

В сети Fast Ethernet не предусмотрена физическая топология «шина», используется только «пассивная звезда» или «пассивное дерево».

При увеличении в 10 раз скорости передачи и сохранении формата пакета его минимальная длина становится в десять раз короче (5,12 мкс против 51,2 мкс в Ethernet).

Для передачи информации в сети Ethernet применяется стандартный код Манчестер-II.

Гальваническая развязка осуществляется аппаратурой адаптеров, репитеров и концентраторов. При этом **приемопередатчик** сети гальванически развязан от остальной аппаратуры с помощью трансформаторов и изолированного источника питания, а *с кабелем сети соединен напрямую.*



Структура пакета сети Ethernet, (цифры показывают количество байт)

Длина кадра Ethernet должна быть не менее 512 битовых интервалов, или 51,2 мкс.

В пакет Ethernet входят следующие поля:

• **Преамбула** состоит из 8 байт, первые семь из которых представляют собой код 10101010, а последний восьмой – код 10101011.

• **Адрес получателя** (приемника) и адрес отправителя (передатчика) включают по 6 байт и строятся по стандарту.

• **Поле управления** (L/T - Length/Type) содержит информацию о длине поля данных. Оно может также определять тип используемого протокола.

В пакет Ethernet входят следующие поля:

• **Поле данных** должно включать в себя от 46 до 1500 байт данных. Если пакет должен содержать менее 46 байт данных, то поле данных дополняется байтами заполнения.

• **Поле контрольной суммы** (FCS – Frame Check Sequence) содержит 32-разрядную циклическую контрольную сумму пакета (CRC) и служит для проверки правильности передачи пакета.

Минимальная длина кадра составляет 64 байта (512 бит). Именно эта величина определяет максимально допустимую двойную задержку распространения сигнала по сети в 512 битовых интервалов (51,2 мкс для Ethernet, 5,12 мкс для Fast Ethernet).

Максимальная длина кадра равна 1518 байтам (12144 бита, то есть 1214,4 мкс для Ethernet, 121,44 мкс для Fast Ethernet).

Для сети Ethernet, работающей на скорости 10 Мбит/с, стандарт определяет четыре основных типа среды передачи информации:

- 10BASE5 (толстый коаксиальный кабель);
- 10BASE2 (тонкий коаксиальный кабель);
- 10BASE-T (витая пара);
- 10BASE-FL (оптоволоконный кабель).

Точно так же для сети Ethernet, работающей на скорости 100 Мбит/с (Fast Ethernet) стандарт определяет три типа среды передачи:

- 100BASE-T4 (счетверенная витая пара);
- 100BASE-TX (сдвоенная витая пара);
- 100BASE-FX (оптоволоконный кабель).

Благодаря мощной поддержке, высочайшему уровню стандартизации, огромным объемам выпуска технических средств, Ethernet резко выделяется среди других стандартных сетей, и поэтому любую другую сетевую технологию принято сравнивать именно с Ethernet.