**6Лекция. Основы криптографии. СКЗИ с симметричными ключами.**

**Симметричное распределение  ключей**

[http://ru.wikipedia.org/wiki/Симметричные\_криптосистемы](http://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%8B%D0%B5_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B)

**Достоинства**

* высокая скорость шифрования
* простота реализации
* меньшая требуемая длина ключа для сопоставимой стойкости
* изученность (давно используется)

**Недостатки**

* сложность управления ключами в большой сети. Для сети в 100  абонентов требуется 4950 ключей, для 1000 — 499500 и т. д.
* сложность обмена ключами (защита каналов передачи).

При симметричном шифровании используются одинаковые ключи (симметричные).

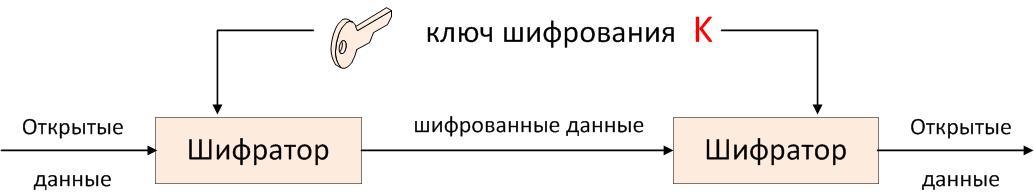


Рис. Симметричное шифрование

**K**  -  ключ шифрования. Секретный элемент схемы. Должен быть известен паре непосредственно взаимодействующих шифраторов.

В случае ГОСТ 28147-89 для разных криптосетей используются разные узлы замены УЗ (разные S-блоки).

[http://ru.wikipedia.org/wiki/ГОСТ\_28147-89](http://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_28147-89)

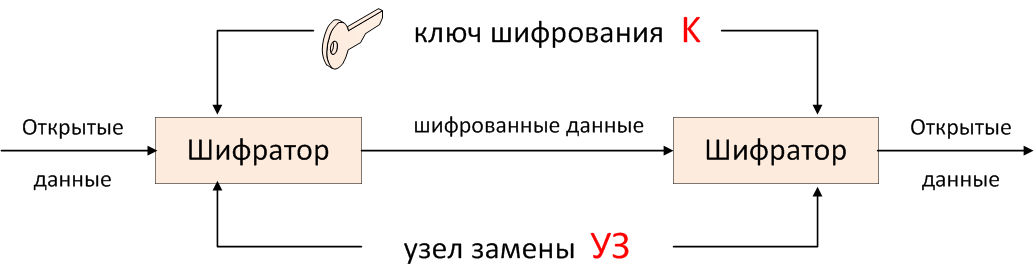


Рис. Симметричное шифрование по ГОСТ 28147-89

**УЗ** - узел замены длиной 512 бит (64 байта). Сменный несекретный элемент, определяющий настройку алгоритма шифрования (S-блоки). Должен быть известен всем участвующим в информационном обмене шифраторам.

**Криптографическая сеть**

Рассмотрим пример криптографической сети из 6-ти участников.

Рис. Криптографическая сети из 6-ти участников.

Для 6 участников криптосети необходимо сгенерировать симметричные ключи.

Рис. Матрица ключей криптографической сети из 6-ти участников.

Ключи парно-выборочной связи K21 и K12одинаковые.

Поэтому для криптосети из 6 участников необходимо 15 ключей.

Каждому участнику необходимо выделить сетевой набор ключей парно-выборочной связи.

Рис. Выбор сетевого набора для участника 4.

Каждому участнику необходимо доставить его сетевой набор (защищенным способом).

Рис. Сетевой набор для участника 4.

Представьте сеть на 1000 участников в одной криптосети, и представьте когда необходимо работать в нескольких криптосетях (у каждого участника должно быть несколько сетевых наборов).

**Сеансовые (рабочие) ключи**

Поскольку на одном ключе безопасно можно зашифровать только ограниченное количество данных, то при шифровании больших объемов данных необходимо часто менять ключи шифрования, из-за этого непосредственное использование ключей парно-выборочной связи для шифрования сетевых данных невозможно.

Поэтому для шифрования данных необходимо использовать рабочий ключ, который генериться периодически.

Рабочие ключи шифруются ключом связи из сетевого набора, и передаются по сети до передачи шифрованных данных.

Рис. Шифрование с использованием рабочего ключа.

**kij** - ключ связи узла i с узлом j .

**k**- рабочий ключ.

**Хранение ключевой информации**

Если вы участник нескольких криптосетей, то после перезагрузки вам необходимо каждый раз вставлять в компьютер все ключевые носители.

Что бы этого не делать их необходимо шифровать главным ключом - **ГК**.

Рис. Хранение шифрованных ключей на диске.

 Рис. Полная схема шифрования с использованием главного ключа.

**Применение симметричного шифрования**

 Примеры шифрование данных:

1. при передачи по каналам связи
2. хранимых на жестком диске или на внешних носителях (Flash, CD, DVD и т.д.)

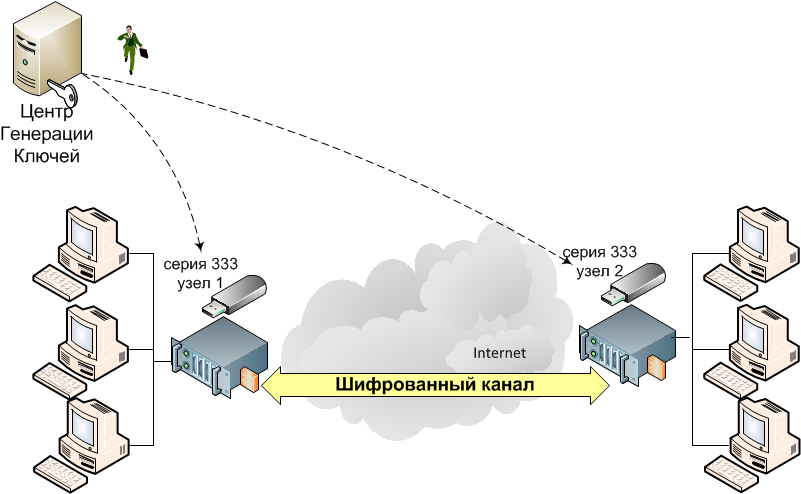


 Рис. Шифрование канала