Криптографическое преобразование информации – это метод защиты информации, основанный на использовании методов сокрытия смысла защищаемой информации, т.е. преобразовании информации к виду, бесполезному для нарушителя. Сущность криптографического преобразования заключается в том, что лицо, владеющее некоторой секретной информацией, может очень быстро восстановить смысл информации, подвергнутой криптографическому преобразованию. В то же время лицу, не владеющему такой секретной информацией, для восстановления смысла информации потребуется время, значительно большее, чем время жизни информации. В отличие от других методов защиты, криптографическое преобразование информации на носителе обеспечивает ее защиту в случае перехвата или хищения носителя. Защита информации при помощи криптографических методов составляет предмет ***криптологии***.

Сообщение, текст которого необходимо сделать непонятным для посторонних лиц, будем называть открытым сообщением.

Сообщение, смысл которого непонятен для посторонних лиц, называется закрытым сообщением.

Шифрование данных – процесс преобразования открытого сообщения в закрытое сообщение (шифротекст, криптограмму) при помощи шифра и шифратора. Иногда этот процесс называют закрытием данных.

Дешифрование данных – процесс преобразования закрытого сообщения в открытое сообщение при помощи шифра и дешифратора.

Процесс преобразования закрытых данных в открытые данные без применения шифра и дешифратора называют раскрытием данных. Раскрытие данных составляет предмет ***криптоанализа***.

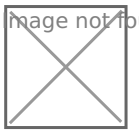
Шифр – совокупность множества обратимых преобразований множества открытых данных во множество закрытых данных, заданных алгоритмом криптографического преобразования.

Ключ – конкретное состояние некоторых параметров алгоритмов криптографических преобразований, обеспечивающее выбор одного конкретного

преобразования из совокупности возможных для данного алгоритма при известном алгоритме шифрования.

Канал связи, в который сообщение поступает в том же виде, в котором оно была сформировано отправителем, называется открытым каналом связи. Если до передаче в канал связи сообщение шифруется, такой канал связи называется закрытым.

Криптографическое преобразование информации можно представить в виде схемы (рисунок 1). Шифратор и дешифратор могут быть реализованы как программно, так и аппаратно.



Криптографическое преобразование информации является наиболее эффективным средством защиты информации от НСД при соблюдении следующих условий:

– криптографический алгоритм достаточно эффективен, т.е. не позволяет раскрыть закрытые данные без знания ключа за разумное время;

– нарушителю не доступен ключ и исходный текст.

Криптографической системой (криптосистемой) называется совокупность криптографических алгоритмов и правил формирования и распространения ключей.

Важнейшей характеристикой криптографической системы является ***криптостойкость*** – стойкость шифра к раскрытию (взлому) нарушителем без знания ключа. Криптостойкость характеризует количество возможных вариантов сообщения, которые нужно получить из зашифрованного сообщения, чтобы раскрыть *смысл* зашифрованного сообщения.

Известные криптосистемы можно разделить на три типа:

– симметричные криптосистемы;

– несимметричные криптосистемы;

– гибридные криптосистемы.

В симметричных криптосистемах для шифрования и дешифрования используется один и тот же секретный ключ. В несимметричных криптосистемах для шифрования и дешифрования используются различные ключи, один из которых не может быть получен из другого.

В гибридных криптосистемах шифрование и дешифрование сообщений осуществляется при помощи симметричных криптосистем, а шифрование ключей для симметричных криптосистем осуществляется при помощи несимметричных криптосистем или криптопротоколов, не использующих общего секретного ключа.