**Методы преобразования информации с целью её защиты**

Проблемой защиты информации путем ее преобразования занимает-ся **криптология** (kryptos - тайный, logos - наука). Криптология разделяется на два направления - **криптографию** и **криптоанализ**. Цели этих направлений прямо противоположны.

**Криптография** занимается поиском и исследованием математических методов преобразования информации.

Сфера интересов **криптоанализа** - исследование возможности расшифровывания информации без знания ключей.

**Терминология**

Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите. Под этими терминами понимается следующее.

*Алфавит* - конечное множество используемых для кодирования информации знаков.

*Текст* - упорядоченный набор из элементов алфавита.

*Шифрование* - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

*Дешифрование*- обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

*Ключ* - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

*Криптографическая система* представляет собой семейство **T**преобразований открытого текста. Члены этого семейства индексируются, или обозначаются символом k; параметр k является ключом.
Пространство ключей K - это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на *симметричные* и *с открытым ключом*.

*В симметричных криптосистемах* и для шифрования, и для дешифрования используется один и тот же ключ.

*В системах с открытым ключом* используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины *распределение ключей* и *управление ключами* относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

*Электронной (цифровой) подписью* называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

*Криптостойкостью* называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

1. количество всех возможных ключей;
2. среднее время, необходимое для криптоанализа.

Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

**Криптографические методы защиты информации**

Совpеменная кpиптогpафия включает в себя четыpе кpупных pаздела:

Криптографическими средствами защиты называются специальные средства и методы преобразования информации, в результате которых маскируется ее содержание.

Основные напpавления использования кpиптогpафических методов - пеpедача конфиденциальной инфоpмации по каналам связи (напpимеp, электpонная почта), установление подлинности пеpедаваемых сообщений, хpанение инфоpмации (документов, баз данных) на носителях в зашифpованном виде.

*Криптографические методы* можно разбить на два класса:

1. обработка информации путем замены и перемещения букв, при котором объем данных не меняется (шифрование);
2. сжатие информации с помощью замены отдельных сочетаний букв, слов или фраз (кодирование).

По способу реализации криптографические методы возможны в аппаратном и программном исполнении.

Для защиты текстовой информации при передачах на удаленные станции телекоммуникационной сети используются аппаратные способы шифрования и кодирования. Для обмена информацией между ЭВМ по телекоммуникационной сети, а также для работы с локальными абонентами возможны как аппаратные, так и программные способы. Для хранения информации на магнитных носителях применяются программные способы шифрования и кодирования.

*Аппаратные способы шифрования информации*применяются для передачи защищенных данных по телекоммуникационной сети.
Для реализации шифрования с помощью смешанного алфавита используется перестановка отдельных разрядов в пределах одного или нескольких символов.

*Программные способы*применяются для шифрования информации, хранящейся на магнитных носителях (дисках, лентах). Это могут быть данные различных информационно-справочных систем АСУ, АСОД и др. программные способы шифрования сводятся к операциям перестановки, перекодирования и сложения по модулю 2 с ключевыми словами.

Особое место в программах обработки информации занимают операции кодирования. Преобразование информации, в результате которого обеспечивается изменение объема памяти, занимаемой данными, называется *кодированием.*На практике кодирование всегда используется для уменьшения объема памяти, так как экономия памяти ЭВМ имеет большое значение в информационных системах. Кроме того, кодирование можно рассматривать как криптографический метод обработки информации.