ТЕМА 2. Криптографическая защита информации

2.1 Основные понятия и определения

Проблемой защиты информации путем ее преобразования занимается криптология (κρυπτος - тайный, λογος - наука (слово) (греч.)). Криптология разделяется на два направления – *криптографию* и *криптоанализ*. *Криптография* представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника.

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

Ключ — некоторый неизвестный параметр шифра, позволяющий выбрать для шифрования и расшифрования конкретное преобразование из всего множества преобразований, составляющих шифр.

Незашифрованное сообщение будем обозначать *P* или *M*, от слов plaintext и message. Зашифрованное сообщение будем называть шифртекстом или криптограммой и обозначать *C*, от слова ciphertext.

Шифрование ($C = E_к [P]$) – процесс создания шифрованного текста при наличии ключа.

Дешифрование ($P = D_K [C]$) – восстановление открытого текста или ключа из шифрованного текста.

Противник – субъект (или физическое лицо), который не знает и не должен знать ключа или открытого текста, но стремящийся получить его.

При этом шифртекст может содержать как новые знаки, так и уже имеющиеся в исходном сообщении. Количество знаков в криптограмме и в исходном тексте в общем случае может различаться. Непременным требованием является возможность однозначного и в полном объеме восстановления исходного текста, используя лишь некоторые логические действия с символами шифртекста.

Криптографическая атака – попытка криптоаналитика вызвать отклонения в атакуемой защищенной системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытие.

Примитивные с позиции сегодняшнего дня криптографические методы известны с древнейших времен и некоторое время рассматривались скорее как некоторые ухищрения, чем строгая научная дисциплина. По утверждению ряда специалистов криптография по возрасту - ровесник египетских пирамид. В документах древних цивилизаций – Индии, Египта, Месопотамии – есть сведения о системах и способах составления шифрованных писем.

Пробуждение значительного интереса к криптографии и ее последующее развитие началось в XIX веке, что связано с зарождением электросвязи. В XX столетии секретные службы большинства развитых

стран стали относиться к этой дисциплине как к обязательному инструменту своей деятельности.

Говоря об исторических аспектах научных исследований в области криптографии, необходимо отметить тот факт, что весь период с древних времен до 1949 года можно назвать донаучным периодом, поскольку средства закрытия письменной информации не имели строгого математического обоснования. Поворотным моментом, придавшим криптографии научность и выделившим ее в отдельное направление математики, явилась публикация в 1949 году статьи К. Э. Шеннона "Теория связи в секретных системах. Указанная работа послужила основой развития *одноключевых симметричных криптосистем***,** в которых предполагается обмен секретными ключами между корреспондентами. Впоследствии с учетом особенностей построения симметричные шифры были разделены на две криптосистемы: *поточные* и *блочные шифры***.** Отличительная особенность первых состоит в преобразовании каждого символа в потоке исходных данных, тогда как вторые осуществляют последовательное преобразование целых блоков данных.

Фундаментальным выводом из работы Шеннона стало определение зависимости *надежности* алгоритма от размера и качества секретного ключа, а также от *информационной избыточности* исходного текста. Шеннон ввел формальное определение информации и функции ненадежности ключа как его неопределенности при заданном количестве известных битов закрытого текста. Кроме того, им было введено важное понятие *расстояния единственности* как минимального размера текста, для которого еще возможно однозначное раскрытие исходного текста. Было показано, что расстояние единственности прямо пропорционально длине ключа и обратно пропорционально избыточности исходного текста.

Другим фундаментальным толчком развития криптографии явилась публикация и 1976 году статьи У. Диффи и М. Е. Хеллмана "Новые направления в криптографии". В этой работе впервые было показано, что секретность передачи информации может обеспечиваться без обмена секретными ключами. Тем самым была открыта эпоха *двухключевых (асимметричных) криптосистем***,** разновидностями которых являются системы электронной цифровой подписи, тайного электронного голосования, защиты от навязывания ложных сообщений, электронной жеребьевки, идентификации и аутентификации удаленных пользователей и ряд других систем.