**Атака** - это реализация угрозы безопасности для криптосистемы.

**Аутентификация** - процесс проверки соответствия полученной информации заявленной. Различают аутентификацию данных, источника данных и опознавание участника протокола.

**Гаммирование** – процесс наложения по определенному закону гаммы шифра на открытые данные. Под гаммой шифра понимается псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму и предназначенная как для зашифрования открытых данных, так и для расшифрования.

**Дешифрование –** это нарушение конфиденциальности шифртекста, достигнутое методами криптоанализа.

**Достоверность** – свойство информации, выражающееся в строгой принадлежности объекту, который является её источником, либо тому объекту, от которого эта информация принята.

**Зашифрование** – процесс маскировки сообщения способом позволяющим скрыть его суть.

**Имитозащита** является частным случаем аутентификации. Если криптоалгоритм обеспечивает защиту получателя от навязывания ложной информации, то говорят, что криптоалгоритм реализует имитозащиту данных.

**Ключ** – это сменный элемент шифра, применяемый для зашифрования отдельного сообщения, обеспечивающий выбор одного варианта преобразования из совокупности возможных. Ключом определяется в первую очередь криптостойкость защищаемой информации. Множество возможных ключей называют пространством ключей.

**Коллизией** называется пара аргументов М и М, которым соответствует одно и то же значение хэш-функции: h(M) = h(М’). Если число таких аргументов равно n, то говорят о коллизии кратности n. Если хэш-функция не имеет коллизий при заданных ограничениях на длину аргумента, то она называется свободной от коллизий.

**Конфиденциальность** – свойство информации быть доступной только ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.

**Криптоанализ** – это раздел прикладной математики изучающий методы, алгоритмы, программные и аппараты средства анализа криптосистем с целью извлечения конфиденциальных данных.

**Криптографический протокол** – алгоритм, выполняемый не менее чем двумя сторонами, задаваемый последовательностью операций, выполняемых каждой из сторон.

**Криптография** – это раздел прикладной математики изучающий методы преобразования информации в целях сокрытия ее содержания.

**Криптосистема** – это система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации. Она состоит из пространства ключей, открытых текстов, шифртекстов и алгоритмов зашифрования и расшифрования.

**Оперативность** – способность информации или некоторого информационного ресурса быть доступным для конечного пользователя в соответствии с его временными потребностями.

**Открытый текст** – исходное сообщение.

**Отправитель** – это субъект, посылающий сообщение.

**Получатель** – это субъект, получающий данное сообщение.

**Расшифрование –**  процесс преобразования шифртекста в открытый текст.

**Синхропосылка** – исходные открытые параметры алгоритма криптографического преобразования.

**Стеганография** применяется для скрытия факта передачи секретных сообщений в другие сообщения, при этом скрывается даже само существование секрета.

**Стойкость криптоалгоритма** (криптостойкость) заключается в способности шифра противостоять попыткам его расшифрования. Криптостойкость зависит от сложности алгоритма преобразования, длины ключа и объема ключевого пространства.

**Текст** – упорядоченный набор из элементов выбранного алфавита.

**Хэш-функция** – это функция, отображающая аргумент произвольной конечной длины в образ фиксированной длины. Функция, для которой по данному аргументу вычислить её значение легко, а по данному значению функции аргумент найти сложно, называется хэш-функцией, вычислимой в одну сторону. Все хэш-функции считаются **вычислимыми в одну сторону**. Если хэш-функция зависит от секретного ключа, она называется **ключевой**, в противном случае – **бесключевой.**

**Целостность** – свойство информации или программного обеспечения сохранять свою структуру и содержание в процессе передачи и хранения.

**Шифр** – совокупность обратимых преобразований множеств открытых данных на множество зашифрованных данных, заданны алгоритмом криптографического преобразования.

**Шифртекстом (криптограммой)** называется зашифрованное сообщение.