2.4. Современные приложения криптографии

Значение криптографии выходит далеко за рамки обеспечения секретности данных. По мере все большей автоматизации процессов передачи и обработки информации и интенсификации информационных потоков криптографические методы приобретают уникальное значение. Новые информационные технологии в своей основе имеют двухключевую криптографию, которая позволяет реализовать протоколы, предполагающие, что секретный ключ известен только одному пользователю, т. е. протоколы, ориентированные на взаимное недоверие взаимодействующих сторон. Отметим основные приложения современной криптографии.

- Защита от несанкционированного чтения (или обеспечение конфндециальности информации).
- Защита от навязывания ложных сообщений (умышленных и непреднамеренных).
- Аутентификация законных пользователей.
- Контроль целостности информации.
- Аутентификация информации.
- Электронная цифровая подпись.
- Системы тайного электронного голосования.
- Электронные деньги.
- Электронная жеребьевка.
- Защита от отказа факта приема сообщения.