**1. Чем отличаются подходы к обеспечению безопасности информации в криптографии и в стеганографии?**

В криптографии информация обычно защищается путем преобразования данных с использованием математических алгоритмов и ключей с целью обеспечения конфиденциальности и аутентификации, тогда как в стеганографии информация скрывается внутри других данных с целью сохранения тайны самого факта наличия скрытого сообщения.

**2. Что общего и в чем отличие криптографического преобразования информации от кодирования ее при защите от случайных угроз безопасности?**

Криптографическое преобразование обеспечивает конфиденциальность и аутентификацию данных с использованием секретных ключей, в то время как кодирование преобразует данные для представления в другой форме или системе без обязательной цели обеспечения конфиденциальности.

**3. Какими методами обеспечивается конфиденциальность информации?**

Конфиденциальность информации обеспечивается шифрованием данных

**4. Что такое целостность информации?**

Под целостностью информации понимается гарантия поступления информации из достоверного источника и в неискаженном виде

**5. Дайте определение имитостойкости шифра.**

Имитостойкость шифра – способность самого шифра противостоять активным атакам со стороны противника.

**6. Что такое имитовставка? Для каких целей она используется?**

Имитовставка – это проверочная комбинация, которая добавляется к сообщению для проверки целостности

**7. Для каких аспектов информационного взаимодействия необходима аутентификация?**

Аутентификация необходима для сеанса связи, сторон взаимодействия, самой информации и источника данных.

**8. Два основных требования к ключевым хэш-функциям. Против каких атак они направлены?**

Два основных требования к ключевым хэш-функциям:

-  невозможность вычисления значения **hk(М) = S**  для заданного сообщения **М** без знания ключа **k**

- невозможность подбора для заданного сообщения **М** с известным значением **hk (М) = S** другого сообщения **M1**, с известным значением **hk (M1) = S1**  без знания ключа **k**.

Первое требование направлено против создания под­дельных (сфабрикованных) сообщений при атаках типа ими­тация; второе — против модификации передаваемых сооб­щений при атаках типа подмена.

**9. Какие средства используются для обеспечения невозможности отказа от авторства?**

Для обеспечения невозможности отказа от авторства используются цифровая подпись

**10. Что означает свойство односторонности криптографической хэш-функции?**

Свойство односторонности криптографической хэш-функции означает, что по значению хеша никто не должен иметь возможность подоб­рать соответствующее сообщение

**11. В чем суть предварительного распределения ключей?**

Суть предварительного распределения ключей в том, чтобы хранить не сами ключи, а некоторую меньшую по объёму информацию, на основе которой каждая сторона может вычислить ключ для взаимодействия с другой стороной.

**12. Что такое сертификат открытого ключа?**

Сертификат – это набор данных, заверенных цифровой подписью центра сертификации, и включающий открытый ключ, и список дополнительных атрибутов, принадлежащих абоненту.

**13. Для чего используется схема разделения секрета?**

Схема разделения секрета используется для того, чтобы обезопасить процедуру принятия ре­шения и не отдавать все на волю одного человека, являюще­гося обладателем ключа