1.                       Правила безопасности при работе с компьютером.

2.                       Перечислить и охарактеризуйте меры защиты информации в компьютере?

3.                       Что такое вирус? Дать классификацию вирусов.

4.           Что такое антивирусная программа? Дать классификацию антивирусных программ. Привести примеры.

5. Перечислите услуги, обеспеченные SSL или TLS.

1. Объясните, как в SSL создается из *предварительного главного секретного кода* *главный секретный код*.
2. Объясните, как в TLS создается из *предварительного главного секретного кода* *главный секретный код*.
3. Объясните, как в SSL создается из *главного секретного кода* *материал для ключей*.
4. Объясните, как в TLS создается из *главного секретного кода* *материал для ключей*.
5. Покажите различия между сеансом и соединением.
6. Перечислите цель четырех протоколов, определенных в SSL или TLS.
7. Определите цель каждой фазы в *протоколе установления соединения*.
8. Сравните и противопоставьте *протоколы установления соединения* в SSL и TLS.
9. Сравните и противопоставьте *протоколы передачи записей* в SSL и TLS.
10. Покажите, как SSL или TLS реагируют на атаку воспроизведения. То есть покажите, как SSL или TLS отвечает нападавшему, который пытается имитировать одно или более сообщений установления соединения (предварительно записав сообщение).
11. Покажите, как SSL или TLS реагируют на атаку грубой силы. Может ли злоумышленник использовать исчерпывающий компьютерный поиск и найти ключ шифрования в SSL или TLS? Какой протокол более безопасен в этом отношении - SSL или TLS?
12. Каков риск использования ключей короткой длины в SSL или TLS? Какую атаку злоумышленник может применить, если ключи коротки?
13. Действительно ли SSL или TLS относительно безопасны к атаке "посредника"? Может ли злоумышленник создать *материал для ключей* между клиентом и самим собой и между собой и сервером?
14. SSL-архитектура и роль
15. Построение системы защиты персональных данных
16. Рассмотри каждый *класс* ИСПД в отдельности, и перечисли все категории
17. Уязвимость информационной системы персональных данных
18. Что такое информационная безопасность, принципы защиты информации
19. Целостность информационной безопасности
20. Хэш для сообщения Finished в TLS