**План**

1. HTTPS
2. Симметричное шифрование
3. Ассиметричное шифрование (шифрование с открытым ключом)
4. Расчёт ключа шифрования, по алгоритму Диффи - Хеллмана (Pre-master Secret)
5. Проблемы безопасности ассиметричного шифрования
6. Протокол TLS/SSL
7. Уровни модели TCPIP
8. Установка соединения в TLS 1.2
9. Установка соединения в TLS 1.3
10. Проверка целостности сообщений. Хеширование сообщений в TLS. Для открытого ключа
11. Инфраструктура открытых ключей
12. SSL-сертификат
13. Электронная подпись
14. **HTTPS**
15. Что такое HTTPS
16. Как HTTPS обозначается в адресной строке
17. Чем отличается от HTTP
18. Почти тоже что и HTTP? Только + TLS
19. Чем обеспечивается безопасность
20. Просмотр подробностей о сертификате
21. От каких атак защищает
22. Когда был определён. Стандарт
23. Следующий слайд «Уровни модели TCP/IP»
24. TLS/SSL – это устаревший стандарт
25. Немного о модели TCP/IP
26. Но, вернёмся немного назад и посмотри с чего вообще всё начиналось

**2. Симметричное шифрование**

1. Изначально для шифрования данных использовалось симметричное шифрование
2. Шифр Цезаря
3. Симметричное шифрование
4. Достоинства
5. Недостатки
6. Не смотря на достоинства, данный тип шифрования не обеспечивает достаточный уровень безопасности, поэтому в TLS используется комбинация из симметричного и ассиметричного шифрования

**Ассиметричное шифрование**

**(шифрование с открытым ключом)**

1. Принципы
2. Как это работает
3. Как совместно работают открытый и закрытый ключи
4. Нюансы передачи зависят от выбранного протокол - RSA или Диффи Хелмана

**Диффи – Хеллман**

1. Как это работает

**Проблемы безопасности ассиметричного шифрования**

**Протокол TLS/SSL**

**Установка соединения в TLS 1.2**