Технологии сети Интернет: прикладные протоколы и сервисы.
Экзаменационные вопросы за весенний семестр 2019 года.

1. Основные виды уязвимостей информационной безопасности в Интернет.

2. Симметричные шифры. Основные понятия. Принципы использования.

3. Криптографические контрольные суммы и хэш-функции. Определения. Примеры использования.

4. Асимметричные криптографические алгоритмы. Основные понятия. Принципы использования. Электронная цифровая подпись.

5. Аутентификация сторон при сетевых соединениях.

6. Распределение открытых ключей. Инфраструктура открытых ключей X.509, основные понятия.

7. Протокол SSL/TLS. Назначение. Архитектура, внутренние протоколы, Record Layer.

8. Протокол SSL/TLS. Установление защищенного соединения. Внутренний протокол Handshake.

9. Протокол SSL/TLS. Обзор уязвимостей. Атака Renegotiation.

10. Протокол SSL/TLS. Обзор уязвимостей. Атаки BEAST, POODLE.

11. Протокол Kerberos.

12. Протоколы защищенной передачи данных в интернет (обзор).