Криптография

Преподаватель: Белов Сергей

Цели курса:

В курсе изучаются вопросы, связанные как с криптографией, так и вопросы, связанные с информационной безопасностью в целом. На паре слушатели узнают, что криптография включает в себя не только шифрование сообщений, но и широкий класс задач, таких как, например, обеспечение механизма безопасной работы с электронными деньгами, исследование вопросов, связанных с использованием электронно-цифровой подписи и другие механизмы и протоколы, без которых невозможно представить современное общество.

День 1

Исторический экскурс. Криптология, криптография и криптоанализ. Цели и задачи криптографии. Основные понятия. Примеры простейших шифров: шифр Цезаря, шифр замены, одноразовый блокнот.

День 2

Симметричная криптография. Основные определения. Область применения. Блочные и потоковые шифры. Сеть Фейстеля. DES, AES, ГОСТ 28147-89. Криптоанализ блочных и потоковых шифров.

День 3

Криптография с открытым ключом. Основные определения. Отличия от симметричной криптографии. Область применения. Проблема распределения ключей. Классы P и NP. Дискретное логарифмирование и факторизация чисел. RSA, протокол Диффи-Хеллмана, протокол Эль Гамаля.

День 4

Целостность сообщений. MAC. Хеш-функции, основные свойства. MD5, семейство SHA, ГОСТ 34.11-94. Поиск коллизий, первого и второго прообраза хеш-функций. Парадокс дней рождения. Схемы ЭЦП. Подпись RSA, подпись Эль Гамаля.

День 5

Криптографические протоколы. Понятие криптографического протокола. Атаки на криптографические протоколы. Протоколы распределению ключей.

Протоколы выработки случайного бита. Доказательства с нулевым разглашением. Электронные деньги.