АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Криптографические методы защиты информации»

по основной профессиональной образовательной программе по направлению подготовки 10.03.01 «Информационная безопасность» (уровень бакалавриата)

Направленность (профиль): Организация и технология защиты информации
Общий объем дисциплины – 3 з.е. (108 часов)
Форма промежуточной аттестации – Экзамен.
В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

- ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач;
- ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;
- ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

Содержание дисциплины:
Дисциплина «Криптографические методы защиты информации» включает в себя следующие разделы:
Форма обучения очная. Семестр 5.
1. Введение. Традиционные криптосистемы.. Значение информации в развитии современного общества. Применение информационных технологий для поиска и обработки информации, а также для ее защиты. Основные понятия и определения. Шифры перестановки: шифр перестановки «скитала», шифрующие таблицы, применение магических квадратов. Шифры простой замены: полибианский квадрат, система шифрования Цезаря, аффинная система подстановок Цезаря, система Цезаря с ключевым словом, шифрующие таблицы Трисемуса, биграммный шифр Плейфера, криптосистема Хилла, система омофонов. Шифры сложной замены: шифр Гронсфельда, система шифрования Вижинера, шифр «двойной квадрат» Уитсона, одноразовая система шифрования, шифрование методом Вернама, роторные машины. Методы взлома классических шифров..
2. Современные симметричные шифры.. Применение информационных технологий для криптографического преобразования информации. Современные симметричные криптосистемы. Принцип итерирования. Конструкция Фейстеля. Американский стандарт шифрования данных DES. Область применения алгоритма DES. Основные режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Отечественный стандарт шифрования данных: режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки. Атаки на блочные шифры. Дифференциальный криптоанализ. Линейный криптоанализ. Современный стандарт шифрования США..
3. Потоковые шифры.. Блочные и поточные шифры. Шифрование методом гаммирования: методы генерации псевдослучайных последовательностей чисел. Современные потоковые шифры. Регистры сдвига с линейной обратной связью. Генераторы истинно случайных последовательностей..
4. Асимметричное шифрование.. Концепция криптосистемы с открытым ключом. Однонаправленные функции. Применение математического аппарата для решения профессиональных задач защиты информации. Алгоритмы на основы задачи об укладке рюкзака. Криптосистема шифрования данных RSA: процедуры шифрования и расшифрования в криптосистеме RSA, безопасность и быстродействие криптосистемы RSA. Схема шифрования Полига-Хеллмана. Схема шифрования Эль-Гамаля. Комбинированный метод шифрования. Генерация простых чисел. Построение больших простых чисел. Тесты проверки на простоту. Криптосистемы с открытым ключом на основе конечных автоматов..
5. Цифровая (электронная) подпись.. Идентификация и проверка подлинности. Основные понятия и концепции. Взаимная проверка подлинности пользователей. Протоколы идентификации

с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Параллельная схема идентификации с нулевой передачей знаний. Схема идентификации Гиллоу-Куискоутера. Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Алгоритм безопасного хэширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции. Алгоритмы электронной цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи. Порядок выполнения работ по установке, настройке и обслуживанию современных криптографических средств защиты информации..

6. Криптографические протоколы.. Введение в протоколы. Протоколы с посредником. Атаки на протоколы. Обмен ключами. Атака «человек посередине». Аутентификация. Разделение секрета. Групповые подписи. Подписи по доверенности. Подбрасывание монеты и игра в карты по телефону. Эзотерические протоколы. Применение криптографических протоколов..

Разработал:
доцент
кафедры ИВТиИБ А.В. Санников
Проверил:
Декан ФИТ А.С. Авдеев