АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
«Методы и средства криптографической защиты информации»

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

Направленность (профиль): Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)
Общий объем дисциплины – 4 з.е. (144 часов)
Форма промежуточной аттестации – Экзамен.
В результате освоения дисциплины у обучающихся должны быть сформированы компетенции с соответствующими индикаторами их достижения:
- ОПК-9.2: Способен применять средства криптографической защиты при решении профессиональных задач;

Содержание дисциплины:
Дисциплина «Методы и средства криптографической защиты информации» включает в себя следующие разделы:
Форма обучения очная. Семестр 5.
1. Введение в криптографию. Традиционные криптосистемы. Основные понятия и определения. Цели и задачи криптографии. Классификация шифров и их характеристики. Классические шифры: шифры перестановки, шифры простой замены, шифры сложной замены. Шифрование телеграфных сообщений. Шифрование в аналоговой телефонии. Роторные машины. Методы взлома классических шифров и способы защиты от них. Особенности применения средств криптографической защиты при решении профессиональных задач защиты информации при ее хранении и передаче..
2. Современные симметричные шифры. Современные симметричные криптосистемы. Требования к шифрам. Принципы построения современных шифров. Американский стандарт шифрования данных DES. Алгоритм шифрования данных IDEA. Алгоритм шифрования AES. Отечественные стандарты шифрования ГОСТ: описание и режимы работы. Атаки на блочные шифры и способы защиты от них. Понятие дифференциального и линейного криптоанализа. Отечественные средства криптографической защиты КрипоПРО и КриптоАРМ..
3. Поточные шифры. Понятие поточных шифров и сфера их применения. Абсолютно стойкий шифр. Шифрование методом гаммирования. Методы генерации псевдослучайных последовательностей. Требования к поточным шифрам. Современные поточные шифры. Регистры сдвига с линейной обратной связью. Криптографические алгоритмы защиты данных в сетях мобильной связи..
4. Асимметричная криптография. Концепция криптосистем с открытым ключом и требования к алгоритмам. Решаемые задачи. Однонаправленные (односторонние) функции: понятие и примеры. Открытое распределение ключей Диффи-Хеллмана. Элементы теории чисел. Современные алгоритмы ассиметричного шифрования, их безопасность и быстродействие. Гибридные криптосистемы. Атаки на алгоритмы и способы защиты..
5. Цифровая (электронная) подпись. Основные понятия и концепции. Понятие и классификация хэш-функций. Современные отечественные и зарубежные хэш-функции. Обеспечение целостности данных. Задачи цифровой (электронной) подписи. Современные отечественные и зарубежные алгоритмы и средства электронной подписи..
6. Управление ключами. Классификация ключей, используемых в алгоритмах. Понятие управления ключами. Методы генерации и распределения криптографических ключей. Сертификация открытых ключей. Инфраструктура открытых ключей. Центры сертификации. Протокол OCSP. Носители ключевой информации и особенности их хранения и использования..
7. Криптографические протоколы. Понятие и классификация протоколов. Примитивные протоколы. Прикладные протоколы. Идентификация и аутентификация. Протоколы аутентификации. Применение криптографических протоколов при защите информации в компьютерных системах и сетях. Программно-аппаратные средства криптографической защиты информации..

8. Практика применения средств криптографической защиты информации. Законодательное регулирование использования средств криптографической защиты информации. Сертификация средств защиты. Лицензирование в области защиты информации. Особенности режима безопасности при использовании средств криптографической защиты информации..
9. Перспективы развития криптографических методов защиты информации. Современное состояние криптографии и предстоящие вызовы. Стеганография. Цифровой водяной знак, защита авторских прав. Платежные системы. Технология блокчейн. Электронные деньги. Криптовалюты. Квантовая криптография..

Разработал:
доцент
кафедры ИВТиИБ А.В. Санников

Проверил:
Декан ФИТ А.С. Авдеев