Аннотация к рабочей программе дисциплины
Автор: Н.П. Мошуров
Наименование дисциплины: Б1.Б.1.26 Криптографические методы защиты информации
Цель освоения дисциплины:

- формирование у студентов знаний теории и методов защиты информации путем криптографической защиты сообщений, осуществления секретной связи на основе симметричных и асимметричных криптосистем, а также методов реализации электронной (цифровой) подписи;

- раскрытие возможностей и особенностей криптографии и криптоанализа применительно к задачам проектирования защищенных систем и сетей связи и передачи данных.

1. **Требования к результатам освоения дисциплины:**

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 1: Цели, задачи, принципы и основные направления обеспечения криптографической информационной безопасности государства	Этап 1: Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня защиты с учетом криптографических средств защиты информации	Этап 1: Профессиональной терминологией и методами теоретического обоснования в выборе криптографических средств обеспечения информационной безопасности
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 2: Современные подходы к построению криптографических систем защиты информации	Этап 2: Применять отечественные и зарубежные стандарты в области компьютерной безопасности с использованием криптографических средств обеспечения информационной безопасности.	Этап 2: Владеть методологическим и принципами оценки защищенности объектов информатизации и обеспечения требуемого уровня защиты с использованием криптографических средств обеспечения информационной безопасности

ПК-14 – способностью проводить контрольные проверки работоспособности применяемых программно аппаратных, криптографических и технических средств защиты информации	Этап 1: основные этапы контрольных проверок технических средств защиты информации	Этап 1: разрабатывать методику контрольных проверок технических средств защиты информации	Этап 1: навыки применения контрольных проверок;
ПК-14 – способностью проводить контрольные проверки работоспособности применяемых программно аппаратных, криптографических и технических средств защиты информации	Этап 2: основные принципы работы технических средств защиты информации	Этап 2: разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации	Этап 2: навыки оценки эффективности применении аппаратно - программных комплексов

2. Содержание дисциплины:

Раздел 1 Введение. Стойкость криптографических систем и алгоритмов

Тема 1 Классификация криптографических систем

Тема 2 Простые шифры и их свойства

Раздел 2 Современные симметричные криптосистемы. Распределение ключей

Тема 3 Симметричные системы шифрования (системы шифрования с секретным ключом)

Тема 4 Системы шифрования с открытым ключом

Раздел 3 Асимметричные криптосистемы

Тема 5 Общая схема функционирования систем с открытыми ключами

Тема 6 Криптосистема RSA и ее модификации

Раздел 4 Криптографические протоколы

Тема 7 Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля

Тема 8 Тесты на простоту и факторизация

3. Общая трудоёмкость дисциплины: 5 ЗЕ