Аннотация к рабочей программе дисциплины
Автор: Боровский А.С.
Наименование дисциплины: Б1.В.ДВ.03.02 Математические основы криптографии
Цель освоения дисциплины:
- формирование теоретических знаний основных криптографических алгоритмов и практических навыков их применения для защиты информации;
- изучение основных положений криптографии, ознакомление с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами, электронной подписью.

1. Требования к результатам освоения дисциплины:

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ПК-2 - способностью создавать и исследовать модели автоматизированных систем	Этап 1: базовые понятия основ моделирования	Этап 1: использовать методы моделирования для создания моделей	Этап 1: использования методов моделирования для создания моделей
ПК-2 - способностью создавать и исследовать модели автоматизированных систем	Этап 2: модели автоматизированных систем	Этап 2: использовать структурные модели	Этап 2: использования структурных моделей

2. Содержание дисциплины:
Раздел 1 Введение. Стойкость криптографических систем и алгоритмов.
Тема 1 Основные понятия и определения. История развития криптографии. Законодательные и правовые основы защиты компьютерной информации и информационных технологий.
Тема 2 Энтропия, теоретическая и практическая стойкость, вычислительная стойкость.
Раздел 2 Современные симметричные криптосистемы. Распределение ключей.
Тема 3 Блочные и поточные шифры. Шифры DES, режимы работы DES, AES, ГОСТ 28147-89.
Тема 4 Поточные шифры: РСЛОС, RC4, шифр Рона.
Раздел 3 Асимметричные криптосистемы.
Тема 5 Общая схема функционирования систем с открытыми ключами.
Тема 6 Криптосистема RSA и ее модификации. Криптосистема Эль Гамаля. Криптосистема Рабина. Электронная цифровая подпись.
Раздел 4 Криптографические протоколы.
Тема 7 Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля. Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний. Схемы обязательств. Системы электронного голосования. Цифровые сертификаты: системы перераспределения доверия, неявные сертификаты.
Тема 8 Тесты на простоту и факторизация. Надежность криптосистем. Элементы криптоанализа.

3. Общая трудоёмкость дисциплины: 2 ЗЕ