Аннотация рабочей программы дисциплины
«Методы и средства криптографической защиты информации»
направления подготовки 10.03.01 «Информационная безопасность»,
направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отраслям или в сфере профессиональной деятельности)»

1. Цели и задачи освоения дисциплины

Цель дисциплины (модуля): формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

Задачи дисциплины

- дать представление о криптографических методах защиты информации;
- изучить математические основы современной криптографии;
- изучить современные стандарты симметричного шифрования;
- изучить основные криптографические алгоритмы с открытым ключом;
- изучить криптографические функции хеширования;
- сформировать умение применять полученные знания для компьютерной реализации криптографических алгоритмов.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины и индикаторы их достижения

Общепрофессиональные компетенции и индикаторы их достижения

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД-1$_{ОПК-9}$-знать: основные понятия и задачи криптографии, математические модели криптографических систем, основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы, национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения ИД-2$_{ОПК-9}$-уметь: использовать СКЗИ для решения задач профессиональной деятельности ИД-3$_{ОПК-9}$- владеть навыками: применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности
ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ИД-1$_{ОПК-4.3}$знать: основные меры по защите информации в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы ИД-2$_{ОПК-4.3}$уметь: устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств ИД-3$_{ОПК-4.3}$владеет: навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы

3. Содержание дисциплины

Основные цели и задачи криптографии. Триада и гексада Паркера. Основные понятия криптографических методов защиты информации: шифрование, расшифрование, дешифрование, криптография, криптоанализ, хеширование, электронная подпись. Классификация криптосистем. Математическая модель шифра. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования. DES. ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. Режимы шифрования, иммитовставка, AES. Принципы поточного шифрования. Типы поточного шифрования. Синхронные и самосинхронизирующиеся шифры. Атаки на симметричные шифры. Слайдовая атака. Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема ЭльГамаля. Криптосистема Рабина. Генерация случайных чисел. Псевдослучайные числа и их отличия от истинно случайных чисел. Подходы к получению псевдослучайных чисел. Криптографические хеш-функции. ГОСТ Р 34.11- 2012. SHA-3. Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. Инфраструктура открытого ключа. Протокол раздельного вручения бита. Протоколы доказательства знания с нулевым разглашением. Протоколы простановки "слепых" подписей. Протоколы голосования. Протоколы безопасных вычислений.