Аннотация рабочей программы дисциплины «Методы и средства криптографической защиты информации» для 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 изучения дисциплины:

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 изучения дисциплины:

1. Дать представление о криптографических методах защиты информации;
2. изучить математические основы современной криптографии;
3. изучить современные стандарты симметричного шифрования;
4. изучить основные криптографические алгоритмы с открытым ключом;
5. изучить криптографические функции хеширования;
6. сформировать умение применять полученные знания для компьютерной реализации криптографических алгоритмов.

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

2.1 Профессиональные компетенции и индикаторы их достижения

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД-1ОПК-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 ин формации и сферы их применения ИД-2ОПК-9-уметь: использовать СКЗИ для решения задач профессиональной деятельности ИД-3ОПК-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-	ИД-1ОПК-4.3знать: основные меры по защите информации в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы ИД-2ОПК-4.3уметь: устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности

аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств ИД-3ОПК-4.3владеть: навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы

3. Содержание дисциплины

Основные цели и задачи криптографии. Историческая криптография. Симметричное шифрование. Криптография с открытым ключом. Электронная подпись. Протоколы.