Аннотация рабочей программы дисциплины
«Криптографические методы защиты информации»
для направления подготовки 09.03.02 Информационные системы и технологии, направленность (профиль) образовательной программы – Безопасность информационных систем

1. **Цели и задачи освоения дисциплины:**

Цель дисциплины (модуля):

Цель преподавания дисциплины «Криптографические методы защиты информации» изложить основные положения и понятия криптографии и изучить криптографические методы защиты информации, а также и примеры реализации криптографических методов защиты информации на практике.

Задачи дисциплины (модуля):

- дать основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов, принципов синтеза и анализа криптосистем, математических методов, используемых для оценки стойкости криптосистем;
- изучение основных понятий и определений криптографии;
- освоение криптографических методов защиты информации;
- формирование устойчивых навыков практического использования криптографических методов защиты информации.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций: ОПК-4; ПК-25; ДПК-3.

В результате изучения дисциплины студент должен:

В процессе освоения данной дисциплины студент формирует и демонстрирует следующие компетенции:

- пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4);
- способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований (ПК-25);
- способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ДПК-3).

3. **Содержание дисциплины**

Докомпьютерная и компьютерная криптография. Обзор криптографических методов защиты информации. Основные понятия и задачи криптографии. Математическая формализация криптографии. Алгоритмы криптографических систем. Основные понятия и задачи криптографии. Криптографическая стойкость шифра. Практическая стойкость шифров. Шифры замены, перестановки, гаммирования. Понятие и примеры криптографических протоколов. Методы шифрования. Шифры перестановки. Шифры замены. Методы шифрования. Блочные шифры. Криптосистема DES и ее свойства. Криптосистема IDEA. Криптосистема RSA и ее анализ. Криптосистема Эль-Гамаля, Мак-Эллиса, Меркля- Хеллмана. ГОСТы в криптографии зарубежной и отечественной. Схемы цифровой подписи. ГОСТы ЭЦП. Основные задачи защиты информации современными криптографическими методами.