АННОТАЦИЯ
рабочей программы дисциплины «Криптографические методы защиты информации» по направлению подготовки 10.03.01 Информационная безопасность

1. Цели освоения дисциплины.

- Представить основные методы исследования и решения задач защиты информации теоретического и практического характера.
- Выработать умение самостоятельно расширять знания и проводить анализ данных.
- Способствовать развитию навыков в применении методологии и методов количественного и качественного анализа с использованием математического аппарата и ЭВМ.

2. Требования к уровню освоения содержания дисциплины.

Процесс изучения дисциплины «Криптографические методы защиты информации» направлен на формирование следующих общекультурных и профессиональных компетенций:

- способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления (ОК-8);
- способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1);
- способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5);
- способность применять программные средства системного, прикладного и специального назначения (ПК-15);
- способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-21);
- способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-27)

3. Требования к результатам освоения дисциплины.

В результате изучения дисциплины обучающиеся должны:

знать:

– основы криптографии;
– основные криптографические системы

уметь:

– применять методы криптографического анализа;

владеть:

– Навыками применения методов дисциплины.

4. Содержание дисциплины.

В структуру учебной дисциплины «Криптографические методы защиты информации» входят следующие составные части: Классические шифры. Системы шифрования с открытыми ключами. Криптографическая стойкость шифров. Основные требования к шифрам. Имитостойкость и помехоустойчивость шифров. Методы получения случайных и псевдослучайных последовательностей. Программные реализации шифров. Особенности использования вычислительной техники в криптографии. Вопросы

организации сетей засекреченной связи. Ключевые системы. Криптографические хеш-функции. Электронная подпись. Криптографические протоколы

Разработчик: Погосян С.Л.

Кафедра информационной, техносферной безопасности и правовой защиты информации — **О.В. Воробьева**

Председатель Межкафедрального координационного учебно-методического совета — **И.В. Анциферова**