Аннотация к рабочей программе дисциплины
«Криптографические методы защиты информации»

Рабочая программа по курсу «Криптографические методы защиты информации» разработана для студентов, обучающихся по направлению 10.03.01 «Информационная безопасность».

В настоящем учебном пособии представлен учебно-методический материал по организации аудиторных занятий и самостоятельной работы студентов, а также различные виды тестовых заданий в полном соответствии с программой этого курса для студентов данной специальности.

Цели: ознакомление студентов с основными принципами и методами, применяемыми при синтезе и анализе криптосистем.

Задачи:

- дать студентам представление о наиболее известных криптоалгоритмах с симметричным и асимметричным ключом, о функциях хэширования;

- ознакомление студентов с универсальными методами криптоанализа и условиями их применения;

- обучить студентов методам криптографических алгоритмов и криптографических параметров, обеспечивающих необходимую стойкость.

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные.

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ПК-1) способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств	Знает	основные криптопротоколы
	Умеет	применять полученные знания к исследованию простых шифров
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем

защиты информации		
(ПК-12) способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знает	основные методы анализа и синтеза криптоалгоритмов
	Умеет	решать основные задачи на применение криптографических алгоритмов в области защиты информации
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем
(ПК-15) способностью разрабатывать планы и программы проведения научных исследований и технических разработок	Знает	основные факты о системах с открытым ключом
	Умеет	строить и изучать математические модели криптоалгоритмов
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем
(ОПК-7) способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает	угрозы безопасности информации и возможные пути их реализации
	Умеет	определять информационные ресурсы, подлежащие защите
	Владеет	основным криптографическим инструментарием, необходимым для построение защищенных информационных систем
	Умеет	проводить выбор необходимых технологий и технических средств, организовать их внедрение
	Владеет	методами формирования требований по защите информации
(ПСК-3.3) способностью разрабатывать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, проводить выбор необходимых технологий и технических средств, организовать внедрение и последующее сопровождение	Знает	комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации
	Умеет	проводить выбор необходимых технологий и технических средств, организовать их внедрение
	Владеет	методами формирования требований по защите информации