Аннотация

Криптография

Рабочая программа учебной дисциплины «Криптография» разработана для студентов 4 курса, обучающихся по направлению 09.03.03 «Прикладная информатика».

Общая трудоемкость освоения дисциплины составляет 180 часов.Дисциплина реализуется на 4 курсе в 8-м семестре.

При изучении дисциплины охватывается следующий круг вопросов: докомпьютерная криптография, блочно-итеративные криптосистемы, криптосистемы с открытым ключом, современные подходы к защите информации.

В процессе изучения данного курса студенты должны овладеть базовыми знаниями в области криптологии и усовершенствовать свои навыки в решении прикладных математических задач, в разработке алгоритмов и реализации их в виде программ, а также в анализе текстов с описанием алгоритмов и документации к программным системам и утилитам. В результате изучения данного курса студенты должны приобрести навыки и умения, расширить эрудицию в области современных информационных технологий, но также познакомиться с некоторыми социальными функциями информатики.

Данный УМКД содержит некоторые материалы, которые представлены на странице курса, размещенной в Интернет и предназначенной для использования студентами в процессе обучения. Приведен перечень основных тем, излагаемых на лекциях, а также тексты задач, в процессе решения которых студенты вырабатывают и совершенствуют навыки и умения, необходимые для будущей профессиональной деятельности в сфере информационных технологий.

Курс включает в себя следующие основные темы

- Классическая криптография.
- Основы теории информации Шеннона.

- Блочные симметричные итеративные шифры.
- Элементы теории сложности.
- Системы с открытым ключом.
- Первообразные корни и их свойства.
- Протокол взаимной аутентификации.
- Современные криптографические протоколы для обеспечения секретности и идентификации.
- Квантовая криптография.

В рамках этого курса демонстрируется применение математических методов к формированию алгоритмов и протоколов, связанных с защитой информации. В курсе используются навыки и умения, полученные на предыдущих стадиях подготовки в рамках таких предметов, как дискретная математика, алгебра, теория вероятностей, языки программирования.

Цель изучения курса является освоение математических основ криптологии и принципов защиты информации при ее хранении, обработке и передаче, а также совершенствование навыков решения задач с использованием компьютера.

Задачи:

1. Изучение математических основ криптологии.
2. Выработка умений для анализа и реализации в виде программного обеспечения алгоритмов и протоколов, используемых при защите информации.
3. Формирование представлений о роли информационных технологий в жизни общества.

ПК-12 Способностью эксплуатировать и сопровождать информационные системы и сервисы	знает	методологии и технологии криптографической защиты при эксплуатации и сопровождения информационных систем и сервисов; типовые модели бизнес-процессов эксплуатации и сопровождения информационных систем и сервисов; методы управления сервисами информационных технологий; инструментальные средства автоматизации бизнес-процессов эксплуатации и сопровождения информационных систем и сервисов.

	умеет	выполнять эксплуатацию и сопровождение информационных систем и сервисов; совершенствовать процессы эксплуатации и сопровождения информационных систем и сервисов; применять инструментальные средства автоматизации бизнес-процессов эксплуатации и сопровождения информационных систем и сервисов.
	владеет	навыками эксплуатации и сопровождения информационных систем и сервисов; навыками управления процессом эксплуатации и сопровождения информационных систем и сервисов; навыками применения инструментальные средства автоматизации бизнес-процессов эксплуатации и сопровождения информационных систем и сервисов.

ОПК-3 Способностью использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности	знает	принципы теорий, связанных с прикладной математикой и информатикой
	умеет	использовать базовые знания естественных наук, математики и информатики
	владеет	навыками использования базовых знаний естественных наук, математики и информатики
ОПК-4 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной	знает	современные информационно-коммуникационные технологии
	умеет	использовать современные информационно-коммуникационные технологии
	владеет	навыками использования современных информационно-коммуникационные технологий

безопасности		