АННОТАЦИЯ

Рабочая программа учебной дисциплины «Математические методы защиты информации» разработан для студентов 1 курса, обучающихся по направлению подготовки 02.03.01 Математика и компьютерные науки, Профиль: «Сквозные цифровые технологии» в соответствие с требованиями ОС ВО ДВФУ по данному направлению и положением об учебно-методических комплексах дисциплин образовательных программ высшего профессионального образования (утверждено приказом и.о. ректора ДВФУ от 07.07.2015 № 12-13-1282) и входит в блок дисциплин по выбору цикла Б1.В.01.04.

Общая трудоемкость освоения дисциплины составляет 108 часов, 3 зачётных единицы. Учебным планом предусмотрены лекционные занятия (18 часов), практические занятия (18 часов), самостоятельная работа (72 часов). Дисциплина реализуется на 1 курсе в 2-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.

Курс включает в себя следующие основные темы:

1 Классическая криптография.
2 Основы теории информации Шеннона.
3 Блочные симметричные итеративные шифры.
4 Элементы теории сложности.
5 Системы с открытым ключом.
6 Первообразные корни и их свойства.
7 Протокол взаимной аутентификации.
8 Современные криптографические протоколы для обеспечения секретности и идентификации.

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.

Для успешного изучения дисциплины «Математические методы защиты информации» у обучающихся должны быть сформированы следующие предварительные компетенции*:*

-способность приобретать и использовать организационно управленческие навыки в профессиональной и социальной деятельности (ПК-8);

-готовность использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в будущей профессиональной деятельности(ОПк 1)

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные/ общепрофессиональные/ профессиональные компетенции (элементы компетенций).

Код и	**Этапы формирования компетенции**

формулировка компетенции		
ОПК 4 способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	Знает	Методы самостоятельного анализа научной литературы и применения изученной информации для расчетов
	Умеет	Выбирать необходимые для расчетов алгоритмы и модифицировать их для решения поставленной задачи
	Владеет	Навыком самостоятельного подбора лучшего алгоритма и последующего его программирования с применением различных программных комплексов
ОПК 2 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной	Знает	Основные криптологические методы
	Умеет	Применять алгоритмы шифрования на практике
	Владеет	Навыком реализации нужных алгоритмов на нужных платформах

безопасности		
ПК-8 способность к обоснованному выбору, проектированию и внедрению специальных технических и программно-математических средств в избранной профессиональной области	Знает	основы работы в составе научно-исследовательского и производственного коллектива
	Умеет	использовать организационно-управленческие навыки в профессиональной и социальной деятельности
	Владеет	организационно-управленческими навыками работы в составе научно-исследовательского и производственного коллектива

Для формирования вышеуказанных компетенций в рамках дисциплины «Математические методы защиты информации» применяются следующие методы активного/ интерактивного обучения:

• мини-лекции с актуализацией изучаемого содержания,

• презентации с использованием доски, книг, видео, слайдов, компьютеров и т.п., с последующим обсуждением материалов,

• обратная связь с формированием общего представления об уровне владения знаниями студентов, актуальными для занятия,