АННОТАЦИЯ

дисциплины «Математические методы защиты информации»

Рабочая программа учебной дисциплины «Математические методы защиты информации» разработан для студентов 4 курса, обучающихся по направлению подготовки— 01.03.02 Прикладная математика и информатика, профили «Математическое и информационное обеспечение производственной деятельности» и «Системное программирование», в соответствие с требованиями ОС ВО ДВФУ по данному направлению и входит в вариативную часть профессиональных дисциплин (Б1.В.0.3).

Общая трудоемкость освоения дисциплины составляет 108 часов, 3 зачётных единицы. Учебным планом предусмотрены лекции (18 ч.), лабораторные работы (18 ч.), самостоятельная работа (72 час.). Дисциплина реализуется на 1 курсе во 2-м семестре.

При изучении дисциплины охватывается следующий круг вопросов: классические математические проблемы и построение на их базе алгоритмов шифрования, эллиптические кривые, электронной цифровая подпись, хеширование файлов для сохранения целостности данных, алгоритмы с открытым и закрытым ключами.

Курс включает в себя следующие основные темы:

1. Классическая криптография.
2. Системы шифрования с открытым ключом
3. Алгоритмы факторизации
4. Криптографические алгоритмы, основанные на задаче дискретного логарифмирования в конечном поле
5. Эллиптические кривые и их приложения в криптографии
6. Отображения Вейля и Тейта

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);

способность к самостоятельной научно-исследовательской работе (ОПК-3).

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

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОПК-4 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-	знает	современные информационно-коммуникационные технологии
	умеет	использовать современные информационно-коммуникационные технологии
	владеет	навыками использования современных информационно-коммуникационные

коммуникационных технологий и с учетом основных требований информационной безопасности		технологий
ПК-9 способность к обоснованному выбору, проектированию и внедрению специальных технических и программно-математических средств в избранной профессиональной области	знает	специальные технические и программно-математические средства
	умеет	выбирать, проектировать и внедрять специальные технические и программно-математические средств
	владеет	навыками выбора, проектирования и внедрения специальных технических и программно-математических средств

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,
- разминка с вопросами, ориентированными на выстраивание логической цепочки из полученных знаний (конструирование нового знания),
- коллективные решения творческих задач, которые требуют от студентов не простого воспроизводства информации, а творчества, поскольку задания содержат больший или меньший элемент неизвестности и имеют, как правило, несколько подходов,
- работа в малых группах (дает всем студентам возможность участвовать в работе, практиковать навыки сотрудничества, межличностного общения).