АННОТАЦИЯ

Рабочая программа учебной дисциплины **Технологии защиты информации** разработан для студентов 3 курса, обучающихся по направлению подготовки— **09.03.03 Прикладная информатика**, в соответствие с требованиями ОС ВО ДВФУ по данному направлению и входит в блок вариативных дисциплин цикла Б1.В.03.01

Общая трудоемкость освоения дисциплины составляет 144 часов, 4 зачётных единицы. Учебным планом предусмотрены лекции (18 часов), Лабораторные занятия (36 часов), самостоятельная работа (90 час.). Дисциплина реализуется на 3 курсе в 5-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-3 способностью использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной	знает	современные информационно-коммуникационные технологии
	умеет	использовать современные информационно-коммуникационные технологии
	владеет	навыками использования современных информационно-коммуникационные технологий

деятельности		
ПК-1 способностью проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе	знает	основные принципы математического моделирования в современном естествознании, технике и социальных науках;
	умеет	формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций
	владеет	навыками использования современных программных средств визуализации результатов с учетом представлений о последствиях своей профессиональной деятельности

ПК-7 способностью проводить описание прикладных процессов и информационного обеспечения решения прикладных задач	знает	базовые методы и математические модели в выбранной предметной области;
	умеет	использовать современные информационно-коммуникационные технологии
	владеет	навыками использования современных программных средств решения математических задач

Для формирования вышеуказанных компетенций в рамках дисциплины «Технологии 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).