АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»

по направлению подготовки 02.03.03 «Математическое обеспечение и администрирование информационных систем»

1. Цели и задачи освоения дисциплины

Цели освоения дисциплины:

- приобретение общих представлений о криптографических методах и средствах обеспечения информационной безопасности;
- знакомство с важнейшими криптоалгоритмами, принципами их построения.

Задачи освоения дисциплины:

- освоение основных методов выбора алгоритмов для различных применений и оценки их качества;
- дать основы системного подхода к организации защиты информации; принципов синтеза и анализа шифров;
- дать основы математических методов, используемых в криптоанализе.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к вариативной части Блока 1 образовательной программы и читается в 7-м семестре студентам по направлению подготовки «Математическое обеспечение и администрирование информационных систем» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра и геометрия», «Дискретная математика», «Теория вероятностей и математическая статистика», «Информатика и программирование». Предполагается также знакомство с одним из языков программирования высокого уровня (например, C/C++).

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: вычислительные методы в алгебре и теории чисел.

Результаты освоения дисциплины будут необходимы для дальнейшего процесса обучения в рамках поэтапного формирования компетенций при изучении следующих специальных дисциплин: «Обнаружение вторжений и защита информации», а также для прохождения преддипломной практики и государственной итоговой аттестации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины «Криптографические методы защиты информации» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-2 – способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности	Знать: основные задачи и понятия криптографии; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки; алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и

	многочленов на множители, дискретного логарифмирования в конечных циклических группах; Уметь: проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; Владеть: навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.
ПК-2 – способен использовать основные методы и средства автоматизации проектирования, реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта и программных комплексов, а также способен использовать методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов	Знать: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров и математические методы их исследования Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах Владеть: навыками применения криптографических методов
ПК-3 – способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств; операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности	Знать: требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования; Уметь: корректно применять симметричные и асимметричные криптографические алгоритмы в программных системах и комплексах в профессиональной деятельности; Владеть: навыками применения криптографических методов
ПК-4 – способен использовать основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования, методы, способы и средства разработки программ в рамках этих направлений	Знать: требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования; Уметь: корректно применять симметричные и асимметричные криптографические алгоритмы в программных системах и комплексах в профессиональной деятельности; Владеть: навыками применения криптографических методов
ПК-5 – способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов	Знать: требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования; Уметь:

прикладных программ моделирования	корректно применять симметричные и асимметричные криптографические алгоритмы в программных системах и комплексах в профессиональной деятельности; Владеть: навыками применения криптографических методов

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов)

5. Образовательные технологии

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии:

- чтение лекций;
- проведение практических и лабораторных занятий;
- организация самостоятельной образовательной деятельности;
- организация и проведение консультаций;
- проведение зачета.

При организации самостоятельной работы занятий используются следующие образовательные технологии:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- подготовка к практическим занятиям, решение задач.

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: проверка лабораторных работ, проверка решения задач.

Промежуточная аттестация проводится в форме зачета.