


Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Криптография»

по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи»

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 базовой части цикла Блока 1 образовательной программы и читается в 7-м семестре студентам по направлению подготовки «Инфокоммуникационные технологии и системы связи» 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. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

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
ПК-13	Знать: основные виды симметричных и асимметричных

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

	криптографических алгоритмов; математические модели шифров; Уметь: проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; Владеть: криптографической терминологией;
Готовность к организационно-управленческой работе с малыми коллективами исполнителей на техническую поддержку инфокоммуникационных систем и/или их составляющих	Знать: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; Уметь: проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; Владеть: криптографической терминологией;

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 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: контрольные работы, проверка решения задач.

Промежуточная аттестация проводится в форме зачета.