



АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Криптография»

по направлению/специальности 09.03.02 Информационные системы и технологии

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 «Криптография» относится к числу дисциплин блока Б1.В.1.ДВ.07, предназначенного для студентов, обучающихся по направлению: 09.03.02 Информационные системы и технологии.

Для успешного изучения дисциплины необходимы знания и умения, приобретённые в результате освоения курсов Аппаратные средства ЭВМ и полностью или частично сформированные компетенции ПК-10.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Инфокоммуникационные системы и сети, Операционные системы, Информационные технологии, Преддипломная практика, Проектная деятельность, Технологии дополненной реальности, Управление программно-аппаратными средствами информационных систем, Выполнение и защита выпускной квалификационной работы.

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

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- Способен управлять программно-аппаратными средствами информационных систем (ПК-10)

В результате изучения дисциплины студент должен:

знать:

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 шифрования и программно-аппаратными средствами защиты информации.

4. Общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 3 ЗЕТ зачетных единицы (108 часов).

5. Образовательные технологии

При реализации учебного процесса по курсу применяются классические и современные образовательные технологии: лекции для изложения теоретического материала и практические лабораторные занятия для изучения методов разработки, тестирования и оценивания программного обеспечения.

Самостоятельная работа студентов осуществляется в виде изучения теоретического материала, основной и дополнительной литературы, рекомендованной по дисциплине, выполнения лабораторных работ по практической части дисциплины.

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

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: Тесты .
Промежуточная аттестация проводится в форме: Зачет.