МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
"Курский государственный университет"

Кафедра программного обеспечения и администрирования информационных систем

УТВЕРЖДЕНО

протокол заседания
Ученого совета от 24.04.2017 г., №10

Рабочая программа дисциплины
Криптографические методы защиты информации

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 3 ЗЕТ

Виды контроля в семестрах:

зачет(ы) с оценкой 7

курсовой проект 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Лабораторные	36	36	36	36
Итого ауд.	54	54	54	54
Контактная работа	54	54	54	54
Сам. работа	54	54	54	54
Итого	108	108	108	108

Курск 2017

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Ознакомление с основами математической теории методов криптозащиты и криптоанализа. Приобретение навыков в практическом использовании современных алгоритмов криптопреобразования и криптоанализа.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.Б

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-1: Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
Знать:
понятие составляющие и проблемы информационной безопасности;
объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные и аппаратные средства
нормативно-правовые, экономические и технологические методы обеспечения информационной безопасности.
Уметь:
обосновать и сформулировать решения по применению технологических и нормативно-правовых средств и методов обеспечения информационной безопасноти
Применять криптогргфические и информационно-аналитические системы, информационные ресурсы и информационные технологии
Сформулировать основные криптографические методы и методы стеганографии
Владеть:
Методом дискретного логарифмирования в конечных циклических группах
Методом применения основных криптосистем и систем стеганографирования
Методом применения алгоритмов проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах

ПК-2: Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
Знать:
программные средства системного, прикладного и специального назначения
инструментальные средства, язык и системы программирования
основные проблемы применения программных средств, системного прикладного и специального назначения
Уметь:
применять программные средства системного, прикладного и специального назначения
применять инструментальные средства, язык и системы программирования
применять методы решения основных проблем при применении программных средств, системного прикладного и специального назначения
Владеть:
Навыками применения программных средств системного, прикладного и специального назначения
Навыками применения инструментальных средств, языка и системы программирования
Навыками применения методов решения основных проблем при применении программных средств, системного прикладного и специального назначения

ПК-7: Способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
Знать:
методы и способы получения хранения и переработки информации, структуру локальных и глобальных компьютерных сетей
основные понятия математической логики и теории алгоритмов;
основные понятия и методы дискретной математики, включая дискретные функции, конечные автоматы, комбинаторный анализ;
Уметь:
Сформулировать основные методы и способы получения хранения и переработки информации, структуру локальных и глобальных компьютерных сетей
Применять основные дискретные структуры, используемые в компьютерных системах, структуру локальных и глобальных компьютерных сетей;

Применять технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми
Владеть:
Навыками использования основных методов и способов получения хранения и переработки информации, структуру локальных и глобальных компьютерных сетей
Навыками сбора и анализа исходных данных для проектирования систем защиты информации, а так же определением требований и сравнительным анализом подсистем по показателям информационной безопасности.
Методом проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;