08303ad8de1c60b987361de7085acb509ac3da143f415362ffaf0ee37e73fa19

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 протоколы

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 5 ЗЕТ

Виды контроля в семестрах:
экзамен(ы) 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	9			
Вид занятий	УП	РПД	УП	РПД
Лекции	36	36	36	36
Лабораторные	36	36	36	36
В том числе инт.	8	8	8	8
Итого ауд.	72	72	72	72
Контактная работа	72	72	72	72
Сам. работа	72	72	72	72
Часы на контроль	36	36	36	36
Итого	180	180	180	180

Курск 2017

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Ознакомление студентов с основными понятиями теории криптографических протоколов; овладение основными идеями и методами современной теории криптографических протоколов; ознакомление студентов с основными криптографическими протокола распределения ключей, протоколами аутентификации, различными промежуточными и более развитыми протоколами; развитие навыка построения криптографического протокола из элементарных протоколов, и развития логического мышления в рамках этой задачи; овладение навыком разложения любого криптографического протокола на промежуточные с целью создания программного обеспечения, обслуживающего исполнение протокола. Овладение основными идеями и методами классической и современной криптографии, зна- комство со средствами криптографической защиты информации, знание основополагающих документов в области защиты информации.

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

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОПК-7: Способностью определять информационные ресурсы , подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты
Знать:
профессиональные функции в соответствии с направлением и профилем подготовки
теоретические основы исследования информационных процессов предприятий, организаций, их классификацию
Правила установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы информационной безопасности по установленным требованиям
Уметь:
Производить сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности
администрирование подсистем информационной безопасности объекта;
выполнять вычислительные эксперименты с использованием стандартных программных средств для реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты
Владеть:
Методикой сбора и анализа исходных данных для проектирования систем защиты информации и определение требований, а так же сравнительный анализ подсистем по показателям информационной безопасности
Методом проведения администрирования подсистем информационной безопасности объекта
Навыками позволяющими выполнять вычислительные эксперименты с использованием стандартных программных средств для реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты

ПСК-1.4: Способностью проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей
Знать:
Основные угрозы компьютерных систем систем
основные понятия и базовые содержательные положения информационной безопасности и защиты информации
современную доктрину информационной безопасности её цели и принципы защиты информации.
Уметь:
Проводить сбор и анализ исходных данных для проектирования систем защиты информации.
Проводить сравнительный анализ подсистем по показателям информационной безопасности
Проведить вычислительные эксперименты с использованием стандартных программных средств;
Владеть:
Навыками проведение экспериментов по заданной методике, а так же способом обработка и анализа результатов
Навыками проведение предварительного технико-экономического обоснования проектных расчётов
Методикой проведение вычислительных экспериментов с использованием стандартных программных средств;