

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Худин Александр Николаевич

Должность: Ректор

Дата подписания: 22.02.2018 12:58:18

Уникальный программный ключ:

08303ad8de1c60b761561de7088acdb09ac3da14314155621a10ee37e75a15

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 Технологии обнаружения сетевых атак

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 4 ЗЕТ

Виды контроля в семестрах:
экзамен(ы) 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
	18			
Неделя	уп	рпд	уп	рпд
Лекции	36	36	36	36
Лабораторные	36	36	36	36
В том числе инт.	16	16	16	16
Итого ауд.	72	72	72	72
Контактная работа	72	72	72	72
Сам. работа	36	36	36	36
Часы на контроль	36	36	36	36
Итого	144	144	144	144

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности систем и их информационной инфраструктуры; развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления; привитие стремления к поиску оптимальных, простых и надежных решений.
-----	--

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.В.ОД
--------------------	---------

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:

основные принципы построения защищенных распределенных компьютерных систем

Уметь:

формализовать задачу управления безопасностью информационных систем

Владеть:

навыками выявления и устранения уязвимостей компьютерной сети

ПК-1: Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

Знать:

основные принципы построения систем обнаружения компьютерных атак

Уметь:

анализировать защищенность систем

Владеть:

навыками организации защищенного удаленного доступа к информационным ресурсам и способами настройки стандартных систем обнаружения компьютерных атак

ПК-2: Способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

Знать:

способы обнаружения и нейтрализации последствий вторжений в компьютерные системы

Уметь:

администрировать системы обнаружения компьютерных атак

Владеть:

навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем

