

Документ подписан простой электронной подписью
Информация о владельце:

ФИО: Худин Александр Николаевич

Должность: Ректор

Дата подписания: 22.02.2018 12:58:09

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

Защита СУБД

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) 5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	5 (3.1)		Итого	
	18			
Неделя	уп	рпд	уп	рпд
Лекции	18	18	18	18
Практические	18	18	18	18
В том числе инт.	8	8	8	8
Итого ауд.	36	36	36	36
Контактная работа	36	36	36	36
Сам. работа	72	72	72	72
Итого	108	108	108	108

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Дисциплина "Защита СУБД" имеет целью приобретение студентами знаний по организационному обеспечению защиты информации и формирование основных практических навыков работы в данной области.
-----	---

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.В.ДВ.3
--------------------	-----------

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:

сущность и понятие информации, информационной безопасности и характеристику ее составляющих
место и роль информационной безопасности в системе национальной безопасности Российской Федерации
сновные средства и способы обеспечения информационной безопасности, принципы построения систем

Уметь:

анализировать и оценивать угрозы информационной безопасности объекта
разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем
выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить

Владеть:

профессиональной терминологией в области информационной безопасности
методами формирования требований по защите информации
навыками в выборе, разработке и применении эффективных методов защиты компьютерных систем