МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
математического моделирования
_____ Костин В.А.
подпись
03.07.2018

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.Б.28 Безопасность систем баз данных

Код и наименование дисциплины в соответствии с Учебным планом

1. Шифр и наименование специальности:
10.05.04 Информационно-аналитические системы безопасности

2. Специализация:

Информационная безопасность финансовых и экономических структур

3. Квалификация (степень) выпускника: специалист

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины: математического моделирования математического факультета

6. Составитель программы: Костин Алексей Владимирович, к. ф.-м н,
ФИО, ученая степень, ученое звание

7. Рекомендована: научно-методическим советом математического факультета, протокол от 03.07.2018, № 0500-07
наименование рекомендующей структуры, дата, номер протокола

_____
отметки о продлении

8. Учебный год: 2018/2019 **Семестр(-ы):** 4,5

9. Цели и задачи учебной дисциплины: Основной целью изучения дисциплины является: формирование у студента личностных и профессиональных качеств, позволяющих осуществлять профессиональную деятельность, связанную с анализом, разработкой и внедрением информационно- аналитических систем; изучение программы, проблематики и областей использования методов автоматизации анализа информационной подготовки принятия управленческих решений с употреблением современных инструментальных средств широкого применения и специализированных пакетов прикладных программ; освоение основ разработки и сопровождения систем загрузки данных, информационных хранилищ, технологий оперативного и интеллектуального анализа данных, отражающих деятельность в различных предметных областях; познание основ проблематики и областей использования искусственного интеллекта, экспертных и основанных на знаниях систем

10. Место учебной дисциплины в структуре ООП:

Учебная дисциплина «Безопасность систем баз данных» относится к циклу «Дисциплины» Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.05.04 Информационно-аналитические системы безопасности (специалитет) и входит в базовую часть этого цикла.

Теоретической и практической основой для освоения учебной дисциплины «Безопасность систем баз данных» являются знания, умения и навыки студентов, приобретенные ими в процессе освоения курсов «Математическая логика и теория алгоритмов», «Языки программирования», «Операционные системы»,

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ОПК-7	способность применять методы и средства обеспечения информационной безопасности специальных ИАС	***знать:*** как применять методы и средства обеспечения информационной безопасности специальных ИАС ***уметь:*** применять методы и средства обеспечения информационной безопасности специальных ИАС ***владеть:*** навыками применять методы и средства обеспечения информационной безопасности специальных ИАС
ПК-9	способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах	***знать:*** как выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах ***уметь:*** выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах ***владеть:*** навыками выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах

12 Объем дисциплины в зачетных единицах/часах (в соответствии с учебным планом) — **5 / 180.**

Форма промежуточной аттестации (зачет/экзамен) – зачет, экзамен.

13. Виды учебной работы:

Вид учебной работы	Трудоемкость (часы)			
	Всего	По семестрам		
		4 сем.	5 сем.	
Аудиторные занятия	86	32	54	
в том числе: лекции	48	16	36	
практические	0	0	0	
лабораторные	34	16	18	
Самостоятельная работа	58	40	18	
Форма промежуточной аттестации *зачет – 0 час. / экзамен – __час.)*	36	0	36	
Итого:	**180**	**72**	**108**	

13.1. Содержание дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Постановка задачи обеспечения информационной безопасности баз данных	1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных 2. Критерии качества баз данных 3. Сущность понятия безопасности баз данных 4. Основные подходы к методам построения защищенных информационных систем 5. Архитектура систем управления базами данных 6. Структура свойства информационной безопасности баз данных
2	Угрозы информационной безопасности баз данных	1. Источники угроз информации баз данных 2. Классификация угроз информационной безопасности баз данных 3. Угрозы, специфичные для систем управления базами данных 4. Объекты и субъекты моделей информационной безопасности баз данных на примере СУБД Oracle
3	Политика безопасности	1. Сущность политики безопасности 2. Цель формализации политики безопасности 3. Принципы построения защищенных систем баз данных 4. Стратегия применения средств обеспечения информационной безопасности
4	Атаки, специфические для баз данных	1. Подбор и манипуляция с паролями как метод реализации несанкционированных прав 2. Нецелевое расходование вычислительных ресурсов сервера 3. Использование триггеров для выполнения незапланированных функций 4. Использование SQL-инъекции для нештатного использования процедур и функций
5	Анализ методов	1. Аутентификация, основанная на знании и защита

	аутентификации участников взаимодействия в процессе обработки баз данных	от компрометации паролей 2. Аутентификация, основанная на наличии, и защита от компрометации 3. Аутентификация, основанная на биометрических характеристиках 4. Аутентификация пользователей в Oracle 5. Внешняя аутентификация пользователей Oracle 6. Аутентификация на основе инфраструктуры сертификатов
6	Методы дискреционного разграничения доступа	1. Реализация модели дискреционного управления доступом в Oracle 2. Базовое понятие системы разграничения доступа — привилегии 3. Предоставление системных привилегий 4. Отмена привилегий
7	Роли и разграничение доступа на основе ролей	1. Базовая ролевая модель разграничения доступа 2. Расширенные ролевые модели 3. Управление привилегиями с помощью ролей в СУБД Oracle 4. Управление допустимостью использования ролей 5. Технология обеспечения конфиденциальности системы распределенных баз данных на основе ролевой модели доступа

13.2 Темы (разделы) дисциплины и виды занятий:

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные занятия	Самостоятельная работа	Всего
1	Постановка задачи обеспечения информационной безопасности баз данных	6	4	10	20
2	Угрозы информационной безопасности баз данных	7	5	12	24
3	Политика безопасности	7	5	12	24
4	Атаки, специфические для баз данных	7	5	12	24
5	Анализ методов аутентификации участников взаимодействия в процессе обработки баз данных	7	5	12	24
6	Методы дискреционного разграничения доступа	7	5	12	24
7	Роли и разграничение доступа на основе ролей	7	5	12	24
	Итого:	**48**	**34**	**58**	**144**

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

При прохождении дисциплины используются активные и интерактивные формы проведения лекций и практических занятий и осуществляется контроль посещаемости и выполнения всех видов самостоятельной работы. В течение семестра студенты выполняют задания, указанные преподавателем, к каждому занятию. Кроме того, предусмотрена работа с текстом конспекта лекции, изучение рекомендованной литературы, систематическая подготовка к лабораторным занятиям, выполнение домашних заданий.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список оформляется в соответствии с требованиями ГОСТ, используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	*Девянин П. И. Модели безопасности компьютерных систем: Учеб. пособие для вузов — М.: Академия, 2005.*
2	*Гайдамакин Н. А. Автоматизированные информационные системы, базы и банки данных. — М.: Гелиос АРВ, 2002.*
3	Саймон А. Безопасность баз данных//СУБД. — № 1.— 1997.

б) дополнительная литература:

№ п/п	Источник
4	*ЗегждаД. П., Ивашко А. М. Как построить защищенную информационную систему. Технология создания безопасных систем / Под ред. П. Д. Зегжды, В. В. Платонова — СПб.: НПО Мир и Семья-95, 1998.*

в)информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
5	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru)

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы.

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

а) основная литература:	
б) дополнительная литература:	
в) информационные электронно-образовательные ресурсы**:**	

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости).

Стандартное современное программное обеспечение персонального компьютера, позволяющее, в том числе, писать и компилировать программы, эффективно использовать поисковые ресурсы глобальных сетей.

18. Материально-техническое обеспечение дисциплины:

1. Типовое оборудование компьютерного класса.
2. Программное обеспечение учебного процесса.

19. Фонд оценочных средств:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения:

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОК-7 способность применять методы и средства обеспечения информационной безопасности специальных ИАС способность применять методы и средства обеспечения информационной безопасности специальных ИАС	***знать:*** как применять методы и средства обеспечения информационной безопасности специальных ИАС		
	уметь: применять методы и средства обеспечения информационной безопасности специальных ИАС		
	владеть: навыками применять методы и средства обеспечения информационной безопасности специальных ИАС		
ПК-9 способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах	***знать:*** как выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах		
	уметь: выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в		

	компьютерных системах		
	владеть: навыками выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах		
			КИМ № 1

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения на зачете используются следующие ***показатели:***

1) знание основных возможностей проектирования баз данных
2) знание основных возможностей защиты информации в базах данных
3) умение работать с прикладными программами и информационными ресурсами;
4) успешное прохождение текущей аттестации.

Для оценивания результатов обучения на зачете используется ***шкала:*** «зачтено», «незачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Полное соответствие ответа обучающегося всем перечисленным показателям по каждому из вопросов контрольно-измерительного материала.	Повышенный уровень	зачтено
Несоответствие ответа обучающегося одному из перечисленных показателей (к одному из вопросов контрольно-измерительного материала) и правильный ответ на дополнительный вопрос в пределах программы. ИЛИ Несоответствие ответа обучающегося любым двум из перечисленных показателей (либо двум к одному вопросу, либо по одному к каждому вопросу контрольно-измерительного материала) и правильные ответы на два дополнительных вопроса в пределах программы.	Базовый уровень	зачтено
Несоответствие ответа обучающегося любым двум из перечисленных показателей и неправильный ответ на дополнительный вопрос в пределах программы. ИЛИ Несоответствие ответа обучающегося любым трем из перечисленных показателей (в различных комбинациях по отношению к вопросам контрольно-измерительного материала).	Пороговый уровень	зачтено
Несоответствие ответа обучающегося любым четырем из перечисленных показателей (в различных комбинациях по отношению к вопросам контрольно-измерительного материала).	–	незачтено

Для оценивания результатов обучения на зачете используется ***шкала:*** «зачтено», «незачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Полное соответствие ответа обучающегося всем перечисленным показателям по каждому из вопросов контрольно-измерительного материала.	Повышенный уровень	отлично
Несоответствие ответа обучающегося одному из перечисленных показателей (к одному из вопросов контрольно-измерительного материала) и правильный ответ на дополнительный вопрос в пределах программы. ИЛИ Несоответствие ответа обучающегося любым двум из перечисленных показателей (либо двум к одному вопросу, либо по одному к каждому вопросу контрольно-измерительного материала) и правильные ответы на два дополнительных вопроса в пределах программы.	Базовый уровень	хорошо
Несоответствие ответа обучающегося любым двум из перечисленных показателей и неправильный ответ на дополнительный вопрос в пределах программы. ИЛИ Несоответствие ответа обучающегося любым трем из перечисленных показателей (в различных комбинациях по отношению к вопросам контрольно-измерительного материала).	Пороговый уровень	удовлетворительно
Несоответствие ответа обучающегося любым четырем из перечисленных показателей (в различных комбинациях по отношению к вопросам контрольно-измерительного материала).	–	неудовлетворительно

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Перечень вопросов к промежуточной аттестации – зачету, экзамену:

1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных
2. Критерии качества баз данных
3. Сущность понятия безопасности баз данных
4. Основные подходы к методам построения защищенных информационных систем
5. Архитектура систем управления базами данных
6. Структура свойства информационной безопасности баз данных
7. Источники угроз информации баз данных
8. Классификация угроз информационной безопасности баз данных
9. Угрозы, специфичные для систем управления базами данных
10. Объекты и субъекты моделей информационной безопасности баз данных на примере СУБД Oracle
11. Сущность политики безопасности
12. Цель формализации политики безопасности
13. Принципы построения защищенных систем баз данных
14. Стратегия применения средств обеспечения информационной безопасности

15. Подбор и манипуляция с паролями как метод реализации несанкционированных прав
16. Нецелевое расходование вычислительных ресурсов сервера
17. Использование триггеров для выполнения незапланированных функций
18. Использование SQL-инъекции для нештатного использования процедур и функций
19. Аутентификация, основанная на знании и защита от компрометации паролей
20. Аутентификация, основанная на наличии, и защита от компрометации
21. Аутентификация, основанная на биометрических характеристиках
22. Аутентификация пользователей в Oracle
23. Внешняя аутентификация пользователей Oracle
24. Аутентификация на основе инфраструктуры сертификатов
25. Реализация модели дискреционного управления доступом в Oracle
26. Базовое понятие системы разграничения доступа — привилегии
27. Предоставление системных привилегий
28. Отмена привилегий
29. Базовая ролевая модель разграничения доступа
30. Расширенные ролевые модели
31. Управление привилегиями с помощью ролей в СУБД Oracle
32. Управление допустимостью использования ролей
33. Технология обеспечения конфиденциальности системы распределенных баз данных на основе ролевой модели доступа

19.3.2 Перечень практических заданий для текущей аттестации: не предусмотрен

19.3.3 Перечень тем рефератов для текущей аттестации: не предусмотрены.

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в форме устного опроса (индивидуального опроса, фронтальных бесед по вопросам семинарских занятий); оценки результатов практической деятельности (лабораторной работы). Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и умений.

При оценивании используются количественные шкалы оценок. Критерии оценивания приведены выше.

Форма контрольно-измерительного материала

УТВЕРЖДАЮ
Зав. кафедрой математического моделирования

_____ В.А. Костин
__.__.20__

Направление подготовки: 10.05.04 Информационно-аналитические системы безопасности
Дисциплина: *Б1.Б.28* Безопасность систем баз данных .
Курс: 2,3
Форма обучения: очная
Вид аттестации: промежуточная
Вид контроля: зачет, экзамен

Контрольно-измерительный материал № 10

1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных
2. Критерии качества баз данных
3. Сущность понятия безопасности баз данных
4. Основные подходы к методам построения защищенных информационных систем
5. Архитектура систем управления базами данных
6. Структура свойства информационной безопасности баз данных
7. Источники угроз информации баз данных
8. Классификация угроз информационной безопасности баз данных
9. Угрозы, специфичные для систем управления базами данных
10. Объекты и субъекты моделей информационной безопасности баз данных на примере СУБД Oracle
11. Сущность политики безопасности
12. Цель формализации политики безопасности
13. Принципы построения защищенных систем баз данных
14. Стратегия применения средств обеспечения информационной безопасности
15. Подбор и манипуляция с паролями как метод реализации несанкционированных прав
16. Нецелевое расходование вычислительных ресурсов сервера
17. Использование триггеров для выполнения незапланированных функций
18. Использование SQL-инъекции для нештатного использования процедур и функций
19. Аутентификация, основанная на знании и защита от компрометации паролей
20. Аутентификация, основанная на наличии, и защита от компрометации
21. Аутентификация, основанная на биометрических характеристиках
22. Аутентификация пользователей в Oracle
23. Внешняя аутентификация пользователей Oracle
24. Аутентификация на основе инфраструктуры сертификатов
25. Реализация модели дискреционного управления доступом в Oracle
26. Базовое понятие системы разграничения доступа — привилегии
27. Предоставление системных привилегий
28. Отмена привилегий
29. Базовая ролевая модель разграничения доступа
30. Расширенные ролевые модели
31. Управление привилегиями с помощью ролей в СУБД Oracle
32. Управление допустимостью использования ролей

33. Технология обеспечения конфиденциальности системы распределенных баз данных на основе ролевой модели доступа

Преподаватель _____ Костин А.В

ЛИСТ СОГЛАСОВАНИЙ

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальность 10.05.04 *Информационно-аналитические системы безопасности*
шифр и наименование направления/специальности

Дисциплина *Б1.Б.28* Безопасность систем баз данных
код и наименование дисциплины

Специализация *Информационная безопасность финансовых и экономических структур*
в соответствии с учебным планом

Форма обучения очная

Учебный год 2018/2019

Ответственный исполнитель

Доцент кафедры математического моделирования _____ Костин А.В____ 03.07.2018

должность, подразделение *подпись* *расшифровка подписи*

СОГЛАСОВАНО

Куратор ООП ВО
по направлению/ специальности _____ Костин В.А.._____ 03.07.2018

подпись *расшифровка подписи*

Начальник отдела
обслуживания ЗНБ _____ Васильченко Л.В._ 03.07.2018

подпись *расшифровка подписи*

Программа рекомендована НМС математического факультета

наименование факультета, структурного подразделения

протокол № 0500-07 от 03.07.2018 г.