

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Проректор по науке

и международным связям

А.В. Толстиков

2 марта 2020 г.



АДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ

Рабочая программа

для обучающихся по направлению подготовки: 10.06.01 Информационная безопасность

Профиль (направленность):

Методы и системы защиты информации, информационная безопасность
форма обучения (очная)

Захаров А.А. Администрирование баз данных Рабочая программа для обучающихся по направлению подготовки 10.06.01 Информационная безопасность, профиль (направленность): методы и системы защиты информации, информационная безопасность, форма обучения (очная). Тюмень, 2020.

Рабочая программа дисциплины (модуля) Администрирование баз данных опубликована на сайте ТюмГУ: [электронный ресурс] / Режим доступа: <https://www.utmn.ru/sveden/education/#>

1. Пояснительная записка

Администрирование баз данных формирует у аспирантов совокупность профессиональных качеств, обеспечивающих решение проблем, связанных с использованием и проектированием баз данных под управлением современных систем управления базами данных (СУБД), а также связанных с обеспечением безопасности информации в автоматизированных информационных системах (АИС), основу которых составляют базы данных (БД), навыкам работы со встроенными в системы управления базами данных (СУБД) средствами защиты.

Задачи курса - изучение:

- обучить принципам работы современных систем управления базами данных;
- привить навыки проектирования и реализации баз данных;
- приобретение системного подхода к проблеме защиты информации в СУБД;
- изучение моделей и механизмов защиты в СУБД;
- приобретение практических навыков организации защиты БД
- обучить проводить обоснование и выбор рационального решения по защите систем управления баз данных с учетом заданных требований;
- обучить формализовать поставленную задачу по обеспечению защиты БД;
- обучить применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- привить навыки разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в СУБД;

1.1. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина входит в блок Б1 Дисциплины (модули). Вариативная часть. Для освоения данной дисциплины необходимы знания и умения, приобретенные обучающимися в результате освоения следующих, предшествующих данной, дисциплин: «Разработка защищенных прикладных решений на базе современных систем управления базами данных», «Безопасность баз данных».

1.2. Компетенции обучающегося, формируемые в результате освоения данной дисциплины (модуля)

Код и наименование компетенции	Компонент (знаниевый/функциональный)
ПК-2 – способность к разработке и реализации принципов и решений (технических, математических, организационных и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования	Знает: основные информационные технологии, используемые в автоматизированных системах; – принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; – методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; Умеет: выявлять потенциальные уязвимости информационной безопасности автоматизированных систем; - разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.
ПК-7 – способность к анализу рисков нарушения информационной безопасности и уязвимости процессов переработки информации в	Знает: основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); - о развитии аппаратных технологий защиты данных;

информационных системах любого вида и области применения	Умеет: проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; - проводить технико-экономическое обоснование проектных решений; работать с технической документацией на компоненты автоматизированных систем; - самостоятельно восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях.
ПК-10 – способность к созданию новых и совершенствованию существующих технологий идентификации и аутентификации пользователей и субъектов информационных процессов.	Знает: историю развития программных средств защиты данных; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; основные способы обработки исключительных ситуаций; Умеет: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем.

2. Структура и объем дисциплины

Таблица 1

Вид учебной работы	Всего часов (академические часы)	Часов в семестре (академические часы)
		3
Общий объем зач. ед. час.	5	5
	180	180
Из них:		
Часы аудиторной работы (всего):	54	54
Лекции	36	36
Практические занятия	18	18
Лабораторные/практические занятия по подгруппам	0	0
Часы внеаудиторной работы, включая самостоятельную работу обучающегося	126	126
Вид промежуточной аттестации (зачет, диф.зачет, экзамен)		зачет

3. Система оценивания

3.1. Для текущего контроля применяется 100-балльная система оценивания. Баллы проставляются за посещение практических занятий и активную работу на них, а также за выполненные лабораторные работы по каждой теме дисциплины. Результаты текущего контроля учитываются при промежуточной аттестации. Для зачета надо набрать не менее 61 балла. Обучающиеся, не набравшие достаточного количества баллов для оценки, сдают зачет в период зачетной сессии. Форма проведения зачета – контрольная работа. Продолжительность выполнения контрольной работы – 2 астрономических часа.

4. Содержание дисциплины

4.1. Тематический план дисциплины

Таблица 2

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.				
		Всего	Виды аудиторной работы (академические часы)			Иные виды контак тной работы
			Лекции	Практические занятия	Лабораторные/пр активные занятия по подгруппам	
1	2	3	4	5	6	7
1.	Основы теории баз данных. Реляционные базы данных	34	8	4	0	0
2.	Проектирование баз данных. Язык SQL	30	6	4	0	0
3.	Физическая организация баз данных. Средства поддержания интерфейса с различными категориями пользователей	30	6	4	0	0
4.	Концепция безопасности баз данных. Средства обеспечения целостности баз данных	30	8	2	0	0
5.	Аудит систем баз данных. Криптографические средства защиты информации, применяемые при защите баз данных	26	4	2	0	0
6.	Средства поддержки высокой готовности систем баз данных	28	4	2	0	0
7.	Зачет	2	0	0	0	2
	Итого (часов)	180	36	18	0	2

4.2. Содержание дисциплины (модуля) по темам

Тема 1. Основы теории баз данных. Реляционные базы данных. История развития, назначение и роль баз данных. Информация и данные. Базы данных и файловые системы. Понятие базы данных. Основы построения реляционных БД. История реляционной модели. Реляционная модель. Терминология. Структура реляционных данных. Реляционные ключи. Реляционная целостность. Реляционная алгебра. Реляционное исчисление. Представления.

Тема 2. Проектирование баз данных. Язык SQL. Языковые средства СУБД для различных моделей данных. Язык SQL Языковые средства манипулирования данными в реляционных СУБД. Язык SQL. Оператор SELECT. Запросы с использованием данных одной таблицы. Реализация операций селекции и проекции. Вычисляемые поля, именование столбцов. Сортировка и группировка результатов запроса. Агрегатные функции. Операции соединения: внутреннее соединение, внешние соединения. Подзапросы. Использование предикатов в подзапросах.

Тема 3. Физическая организация баз данных. Средства поддержания интерфейса с различными категориями пользователей. Структуры данных и базы данных. Способы хранения информации в базах данных. Способы повышения эффективности обработки данных за счет их организации. Планирование, проектирование и администрирование БД Жизненный цикл приложения баз данных. Этапы жизненного цикла приложения БД. Обзор процедуры проектирования БД. Проектирование приложений. Выбор СУБД. Особенности средств управления в реализациях реляционных СУБД. Администрирование.

Тема 4. Концепция безопасности баз данных. Средства обеспечения целостности баз данных. Нормализация баз данных. Аномалии при эксплуатации баз данных. Нормальные формы БД. Денормализация. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Виды привилегий: привилегии безопасности и доступа. Использование ролей и привилегий пользователей. Соотношение прав доступа, определяемых ОС и СУБД. Использование представлений для обеспечения конфиденциальности информации в СУБД. Средства реализации мандатной политики безопасности в СУБД.

Тема 5. Аудит систем баз данных. Криптографические средства защиты информации, применяемые при защите баз данных. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия. Особенности применения криптографических методов.

Тема 6. Средства поддержки высокой готовности систем баз данных. Технология и модели архитектуры клиент/сервер Серверы баз данных. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Использование средств прямого ввода-вывода, управления памятью, поддержания целостности, защиты от сбоев. Технология оперативной обработки транзакции (OLTP-технология). Поддержка Internet-технологий. Оценка эффективности и адаптации функционирования сервера баз данных. Проблемы оптимизации доступа к базе данных. Перспективы развития СУБД.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Основы теории баз данных. Реляционные базы данных	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
2.	Проектирование баз данных. Язык SQL	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
3.	Физическая организация баз данных. Средства поддержания интерфейса с различными категориями пользователей	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
4.	Концепция безопасности баз данных. Средства	Конспектирование материала на лекционных занятиях. Работа с учебной литературой.

	обеспечения целостности баз данных	Подготовка к выполнению лабораторной работы
5.	Аудит систем баз данных. Криптографические средства защиты информации, применяемые при защите баз данных	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы
6.	Средства поддержки высокой готовности систем баз данных	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к выполнению лабораторной работы

Порядок выполнения каждого вида самостоятельной работы:

1. Изучение лекционного материала по теме.
2. Изучение рекомендованной основной и дополнительной литературы.
3. Разбор примеров контрольных работ.

Контроль за самостоятельной работой осуществляется при выполнении обучающимся теста, контрольной работы.

6. Промежуточная аттестация по дисциплине (модулю)

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине (модулю)

Вопросы к зачету

1. Информация, данные, информационная система.
2. Распределение обязанностей в системах с базами данных.
3. Модели данных. Сущности и связи.
4. Инфологическая модель данных. Элементы. Способ построения.
5. Дatalogическая модель данных.
6. Трехуровневая архитектура ANSI-SPARC.
7. Сетевая и иерархическая модели данных.
8. Реляционная модель.
9. Реляционные ключи. Реляционная целостность.
10. Реляционная алгебра. Реляционное исчисление. Представления.
11. Способы хранения информации в базах данных.
12. Процедура проектирования БД.
13. Метаданные. Ссылочная целостность. Механизм транзакций.
14. Архитектура СУБД
15. Технологии доступа к данным.
16. Серверы баз данных.
17. SQL. Операторы определения данных.
18. SQL. Операторы манипулирования данными: выборка, сортировка, группирование, обновление данных.
19. SQL. Создание баз данных. Операторы создания и удаления таблиц.
20. Задачи и этапы проектирования баз данных.
21. Нормализация. Избыточность и аномалии. Функциональные зависимости.
22. Нормальные формы 1НФ, 2НФ, 3НФ, НФБК, нормальные формы более высокого порядка.
23. Методология концептуального проектирования БД.
24. Методология логического проектирования БД.
25. Методология физического проектирования БД.
26. Защита данных. Управление транзакциями.
27. Объектно-ориентированное программирование в СУБД.

28. Многоплатформные СУБД.
29. Концепции и разработка распределенных БД.
30. Объектные, объектно-ориентированные и объектно-реляционные СУБД.
31. Web-технологии и СУБД.
32. Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные.
33. Понятие политики безопасности. Сущность политики безопасности. Цели формализации политики безопасности. Принципы построения защищенных систем.
34. Дискреционные модели безопасности СУБД. Реализация ролевой модели политики безопасности в СУБД Oracle.
35. Мандатная модель политики безопасности.
36. БД с многоуровневой секретностью (MLS). Многозначность. Реализация модели MLS. Авторизация меток пользователя. Специальные привилегии доступа. Меточные функции. Опции ограничения.
37. Блокировки. Режимы блокирования. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Взаимоблокировки, их распознавание и разрушение.
38. Целостность кода приложения. SQL-инъекции. Динамическое выполнение кода SQL и PL/SQL. Категории атак SQL-инъекцией. Методы SQL-инъекций. Противодействие атакам типа SQL-инъекции.
39. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.

6.2. Критерии оценивания компетенций:

Таблица 4

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ПК-2 – способность к разработке и реализации принципов и решений (технических, математических, организационных и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования	Знает: основные информационные технологии, используемые в автоматизированных системах; – принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных; – методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; Умеет: выявлять потенциальные уязвимости информационной безопасности автоматизированных систем; - разрабатывать предложения по совершенствованию системы управления информационной	Собеседование, лабораторные работы, вопросы для зачета	Компетенция сформирована при правильности и полноте ответов на теоретические вопросы, при глубине понимания вопроса и правильности выполнения предложенных заданий. Шкала критериев применена согласно требованиям п. 4.29 «Положения о текущем контроле

		безопасностью автоматизированных систем;		успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»
2.	ПК-7 – способность к анализу рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения	Знает: основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); - о развитии аппаратных технологий защиты данных; Умеет: проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; - проводить технико-экономическое обоснование проектных решений; работать с технической документацией на компоненты автоматизированных систем; - самостоятельно восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;	Собеседование, лабораторные работы, вопросы для зачета	
3.	ПК-10 – способность к созданию новых и совершенствованию существующих технологий идентификации и аутентификации пользователей и субъектов информационных процессов	Знает: историю развития программных средств защиты данных; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; основные способы обработки исключительных ситуаций; Умеет: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем;	Собеседование, лабораторные работы, вопросы для зачета	

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература:

1. Дадян, Э. Г. Методы, модели, средства хранения и обработки данных : учебник / Э.Г. Дадян, Ю.А. Зеленков. — Москва : Вузовский учебник : ИНФРА-М, 2017. — 168 с. - ISBN 978-5-9558-0490-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/543943> (дата обращения: 01.03.2020). — Режим доступа: по подписке.
2. Култыгин, О. П. Администрирование баз данных. СУБД MS SQL Server [Электронный ресурс] : учеб. пособие / О. П. Култыгин. - Москва : МФПА, 2012. - 232 с. - (Университетская серия). - ISBN 978-5-4257-0026-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/451114> (дата обращения: 01.03.2020). — Режим доступа: по подписке.

7.2. Дополнительная литература:

3. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаев А.В. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2017. — 322 с. — (Высшее образование). — www.dx.doi.org/10.12737/11380. - ISBN 978-5-369-01450-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/763644> (дата обращения: 01.03.2020). — Режим доступа: по подписке.
4. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2020. — 327 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1035570> (дата обращения: 01.03.2020). — Режим доступа: по подписке.

7.3. Интернет-ресурсы

1. вузовские электронно-библиотечные системы учебной литературы.
2. <http://www.infosecurity.Report.ru> (портал по информационной безопасности).
3. база научно-технической информации ВИНТИ РАН.
4. среды разработки на языках C#, C++, Delphi.
5. Порталы разработчиков систем управления базами данных: MS SQL Server, InterBase/FireBird, MySQL, Oracle, SQL Postgre.

7.4. Современные профессиональные базы данных и информационные справочные системы

Базы данных научно-технической информации, научных трудов, статей, материалов, доступных в Тюменском государственном университете <https://www.utmn.ru/upload/medialibrary/fc5/Perechen-podpisnykh-litsenzionnykh-baz-dannykh-i-baz-dannykh-dostupnykh-v-ramkakh-natsionalnoy-podpiski.doc>

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- Для организации самостоятельной работы аспирантов необходим компьютерный класс с пакетом прикладных программ, в том числе с установленной средой разработки на языке C#, C++, Pascal, Java, с системами управления базами данных: MS SQL Server, со средством моделирования MS Office Visio.
- платформа для электронного обучения Microsoft Teams.

9. Технические средства и материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения лекций и практических занятий;

Лаборатории, оснащенные лабораторным оборудованием в соответствии с ФГОС ВО 3+ по данному направлению.

Для организации самостоятельной работы аспирантов необходим компьютерный класс с пакетом прикладных программ, в том числе с установленной средой разработки на языке C#, C++, Pascal, Java, с системами управления базами данных: MS SQL Server, со средством моделирования MS Office Visio.