

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.



**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ
БАЗАМИ 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. Информационная безопасность систем управления базами 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) Информационная безопасность систем управления базами данных опубликована на сайте ТюмГУ: [электронный ресурс] / Режим доступа: <https://www.utmn.ru/sveden/education/#>

1. Пояснительная записка.

Целью изучения дисциплины «Информационная безопасность систем управления базами данных» является теоретическая и практическая подготовка специалистов к деятельности, связанной с защитой данных в информационной системе; обучение базовым принципам информационной безопасности, в автоматизированных информационных системах (АИС), основу которых составляют базы данных (БД) навыкам работы со встроенными в системы управления базами данных (СУБД) средствами защиты.

В **задачи** дисциплины «Информационная безопасность систем управления базами данных» входит формирование необходимого минимума специальных теоретических знаний и практических навыков по следующим аспектам:

- принципам работы современных систем управления базами данных;
- навыкам проектирования и реализации баз данных;
- системному подходу к проблеме защиты информации в СУБД;
- существующим моделям и механизмам защиты в СУБД;
- практическим навыкам организации защиты БД.
- технологиям выбора рационального решения по защите систем управления баз данных с учетом заданных требований;
- формализации задач обеспечения защиты БД.

1.1. Место дисциплины в структуре образовательной программы (ОП):

Данная дисциплина входит в блок ФТД Факультативы.

Для успешного усвоения данной дисциплины необходимо, чтобы аспирант владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Защита сетей», «Защита информационных систем персональных данных».

Компетенции обучающегося, формируемые в результате освоения данной дисциплины

Код и наименование компетенции	Компонент (знаниевый/функциональный)
ПК-6 - способность к созданию новых и совершенствованию существующих моделей и методов формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования	Знает: -принципы работы современных систем управления базами данных; -основные угрозы информационной безопасности современных систем управления базами данных. Умеет: -проектировать и реализовывать базы данных; -применять существующие средства защиты современных систем управления базами данных.
ПК-9 - способность к созданию новых и совершенствованию существующих моделей и методов оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты вне зависимости от области их функционирования	Знает: -основные средства защиты информации в системах управления базами данных; Умеет: -выбирать необходимый и достаточный комплекс средств защиты информации для решения конкретной задачи обеспечения безопасности современной системы управления базами данных.
ПК-11 - способность к реализации мероприятий и механизмов формирования политики обеспечения информационной	Знает: -основные средства аудита и обеспечения целостности базы данных.

Таблица 1

Текущий контроль не предполагает формализованной оценки работы обучающегося. В период проведения занятий по дисциплине преподаватель консультирует аспирантов по вопросам, возникающим у них в ходе самостоятельного изучения теоретического материала и выполнения контрольных работ. Проверка усвоения теоретического материала осуществляется во время проведения зачета.

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 актические занятия по подгруппам	
1	2	3	4	5	6	7
1.	Безопасность БД, угрозы, защита	24	6	4	0	0
2.	Модели безопасности в СУБД	24	4	2	0	0
3.	Целостность БД и способы ее обеспечения	22	4	2	0	0
4.	Зачет	2	0	0	0	2
	Итого (часов)	72	14	8	0	2

4.2. Содержание дисциплины (модуля) по темам

Тема 1. Безопасность БД, угрозы, защита.

Классификация угроз конфиденциальности СУБД. Критерии защищенности БД. Шифрование данных. Обезличивание данных.

Тема 2. Модели безопасности в СУБД.

Средства идентификации и аутентификации. Средства управления доступом.

Тема 3. Целостность БД и способы ее обеспечения.

Аудит и подотчетность. Транзакции и блокировки.

5. Учебно-методическое обеспечение и планирование самостоятельной работы обучающихся

Таблица 3

№ темы	Темы	Формы СРС, включая требования к подготовке к занятиям
1.	Безопасность БД, угрозы, защита	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к сдаче зачета.
2.	Модели безопасности в СУБД	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к сдаче зачета.
3.	Целостность БД и способы ее обеспечения	Конспектирование материала на лекционных занятиях. Работа с учебной литературой. Подготовка к сдаче зачета.

6. Промежуточная аттестация по дисциплине

6.1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

Вопросы к зачету:

1. Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные.
2. Способы шифрования данных. Виды шифрования. Примеры реализации в СУБД.
3. Обезличивание данных. Назначение обезличивания. Виды обезличивания.

Стратегия обезличивания данных.

4. Дискреционные модели безопасности СУБД. Пример реализации.
5. Рольевые модели безопасности СУБД. Пример реализации.
6. Мандатная модель безопасности СУБД. Пример реализации.
7. Многопользовательский режим доступа к СУБД. Управление доступом.
8. Понятие транзакции. Фиксация транзакции. Прокрутки вперед и назад.

Контрольная точка. Откат.

9. Транзакции как средство изолированности пользователей. Сериализация транзакций.

10. Журнал транзакций. Назначение. Пример реализации в СУБД.

11. Блокировки. Режимы блокирования. Правила согласования блокировок.

12. Целостность кода приложения. SQL-инъекции. Динамическое выполнение кода SQL.

13. Категории атак SQL-инъекцией. Методы SQL-инъекций. Противодействие атакам типа SQL-инъекции.

14. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.

6.2. Критерии оценивания компетенций

Карта критериев оценивания компетенций

№ п/п	Код и наименование компетенции	Компонент (знаниевый/функциональный)	Оценочные материалы	Критерии оценивания
1.	ПК-6 - способность к созданию новых и совершенствованию существующих моделей и методов формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования	Знает: -принципы работы современных систем управления базами данных; -основные угрозы информационной безопасности современных систем управления базами данных. Умеет: -проектировать и реализовывать базы данных; -применять существующие средства защиты современных систем управления базами данных.	опрос на занятии, зачет	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
2.	ПК-9 - способность к созданию новых и совершенствованию существующих моделей и методов оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты вне зависимости от области их функционирования	Знает: -основные средства защиты информации в системах управления базами данных; Умеет: -выбирать необходимый и достаточный комплекс средств защиты информации для решения конкретной задачи обеспечения безопасности современной системы управления базами данных.	опрос на занятии, зачет	текущем контроле успеваемости и промежуточной аттестации обучающихся ФГАОУ ВО ТюмГУ»

3.	ПК-11 - способность к реализации мероприятий и механизмов формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления	Знает: -основные средства аудита и обеспечения целостности базы данных. Умеет: -эффективно применять средства аудита и обеспечения целостности базы данных.	опрос на занятии, зачет	
----	---	---	-------------------------	--

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.

7.2. Дополнительная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш 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: 22.03.2020). – 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.

7.3. Интернет-ресурсы

1. Интернет ресурсы документация MS SQL Server <https://learn.microsoft.com/ru-ru/sql/sql-server/>

7.4 Современные профессиональные базы данных и информационные справочные системы:

Базы данных

- Institute of Electrical and Electronics Engineers, Inc (IEEE) <https://ieeexplore.ieee.org/Xplore/home.jsp?reload=true>

- МЕЖВУЗОВСКАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА (МЭБ) <https://icdlib.nspu.ru/>

- НАЦИОНАЛЬНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА <https://rusneb.ru/>

- Справочная правовая система КонсультантПлюс <http://www.consultant.ru/>

Наименование ПО

- Microsoft Office 365
- "Microsoft Imagine Academy (панель Dreamspark):MS Visual Studio, MS SQL Server, ОС семейства MS Windows, MS Visio, MS Project"

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

- гипервизор Oracle Virtual Box 5.*
- платформа для электронного обучения Microsoft Teams

Интернет, доступ в информационно-образовательную среду ТюмГУ, включающую в себя доступ к учебным планам и рабочим программам, к изданиям электронной библиотечной системы.

7.6. Источники Интернет:

1. ФСБ России [Электронный ресурс]. – Режим доступа: <http://fsb.ru> (дата обращения 01.02.2020);
2. ФСТЭК России [Электронный ресурс]. – Режим доступа: <http://fstec.ru> (дата обращения 01.02.2020).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

- Свободно распространяемая система виртуализации Virtual Box;
- Операционная система Linux;
- Программное обеспечение реляционной системы управления базами данных MS SQL Server или аналогичное

9. Технические средства и материально-техническое обеспечение дисциплины.

Для практических занятий необходимо наличие компьютерного класса, объединенного в локальную вычислительную сеть. На компьютерах должны быть установлены серверные версии операционной системы (ОС) Linux (в качестве альтернативы предусматривается развертывание ОС в рамках виртуальных машин).