СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Аннотация рабочей программы дисциплины (модуля)

дисциплина ***Б1.О.26 Основы безопасности систем баз данных***

обязательная часть

Направление

10.03.01 ***Информационная безопасность***
код наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очно-заочная

Для поступивших на обучение в
2023 г.

Стерлитамак 2023

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)
ОПК-1.3. Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям;	ОПК-1.3.1. Знания:	Обучающийся должен: знать методы защиты информации при работе с базами данных, при передаче информации по компьютерным сетям.
	ОПК-1.3.2. Умения:	Обучающийся должен: уметь применять методы защиты информации при работе с базами данных, при передаче информации по компьютерным сетям.
	ОПК-1.3.3. Владение:	Обучающийся должен: владеть навыками практического применения методов защиты информации при работе с базами данных, при передаче информации по компьютерным сетям.

2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:
Формирование у студентов знаний в области информационной безопасности систем баз данных для последующего практического использования.
- изучение методов проектирования баз данных;
- изучение принципов работы с СУБД;
- определение критериев защищенности баз данных;
- изучение механизмов контроля целостности в базах данных;
- формирование правильного подхода к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

Дисциплина изучается на 2 курсе в 3 семестре

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 5 зач. ед., 180 акад. ч.

Объем дисциплины	Всего часов
	Очно-заочная обучения
Общая трудоемкость дисциплины	180
Учебных часов на контактную работу с преподавателем:	
лекций	20
практических (семинарских)	22
лабораторных	22
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	34,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	80

Формы контроля	Семестры
экзамен	3

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	Наименование раздела / темы дисциплины	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
		Контактная работа с преподавателем			СР
		Лек	Пр/Сем	Лаб	
1	**Первый раздел**	**10**	**8**	**10**	**40**
1.1	Информационная модель безопасности автоматизированной информационной системы (АИС).	2	2	2	10
1.2	Политика безопасности сервера АИС и ее компоненты.	2	2	2	10
1.3	Системные привилегии. Роли.	2	2	4	10
1.4	Средства аудита.	4	2	2	10
2	**Второй раздел**	**10**	**14**	**12**	**40**
2.1	Иллюстрация решения комплексной задачи обеспечения безопасности.	2	4	4	10
2.2	Восстановление базы данных.	2	2	4	10
2.3	Развитые средства обеспечения безопасности в СУБД Oracle 9i.	2	4	2	10
2.4	Безопасные роли приложений.	4	4	2	10
	Итого	**20**	**22**	**22**	**80**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Первый раздел**	
1.1	Информационная модель	Информационная модель - на примере АИС,

	безопасности автоматизированной информационной системы (АИС).	реализованной на базе СУБД Oracle. Создание базы данных Oracle (ОС Windows 2000) и решение начальных задач обеспечения ее безопасности. Компоненты модели безопасности АИС. Политика безопасности сервера АИС и ее компоненты.
1.2	Политика безопасности сервера АИС и ее компоненты.	Политика безопасности данных, пользователя, управления паролем и т.д. – для СУБД Oracle. Краткое руководство по обеспечению безопасности. План обеспечения безопасности. Доступность базы данных. Идентификация пользователей.
1.3	Системные привилегии. Роли.	Использование параметра WITH ADMIN OPTION. Предоставление привилегий доступа к объекту. Управление привилегиями с помощью ролей. Системные привилегии, определяющие права по работе с ролями. Предопределенные роли. Создание ролей и предоставление им привилегий. Управление допустимостью использования ролей. Отмена привилегий. Отмена системных привилегий и ролей. Отмена привилегий доступа к объекту. Использование представлений, процедур и триггеров для повышения защищенности системы.
1.4	Средства аудита.	Использование представлений для разграничения доступа. Использование представлений администратора базы данных для выяснения вопросов обеспечения безопасности АИС. Использование хранимых процедур и триггеров для повышения защищенности системы. Средства аудита. Аудит системных событий. Аудит событий, связанных с доступом к системе. Прекращение регистрации событий. Обработка данных аудита.
2	**Второй раздел**	
2.1	Иллюстрация решения комплексной задачи обеспечения безопасности.	Профили пользователя, работа с паролями. Профили пользователя, как средство повышения защищенности системы. Работа с паролями. Предотвращение возможности повторного использования паролей. Задание сложности пароля. Безопасность паролей при регистрации - шифрование паролей. Возможности несанкционированного доступа к базе данных. Изменение пароля администратора базы.
2.2	Восстановление базы данных.	Физическое копирование и восстановление – принципы реализации. Примеры восстановления базы данных для различных сценариев:база данных находится в режиме archivelog (архивируется) или noarchivelog (не архивируется); имеется "холодная" или "горячая" резервные копии базы данных; в ходе работы с БД "утеряны" файлы данных; база данных находится в режиме archivelog (архивируется); утрачивается файл

		rbs1orcl.ora именно тогда, когда выполнение транзакции связано с использование rollback segments из табличного пространства ROLLBAC_DATA;база данных находится в режиме archivelog (архивируется); теряются незаархивированные оперативные файлы журнала.
2.3	Развитые средства обеспечения безопасности в СУБД Oracle 9i.	Гранулированный (fine grained access) доступ к базе данных, гранулированный (fine grained audit) аудит базы данных. Виртуальные частные базы данных. Шифрование содержимого базы данных. Написание процедур с правами пользователя (invoker).
2.4	Безопасные роли приложений.	Обеспечение безопасности с метками грифа секретности средствами Oracle Label Security.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Первый раздел**	
1.1	Информационная модель безопасности автоматизированной информационной системы (АИС).	Информационная модель - на примере АИС, реализованной на базе СУБД Oracle. Создание базы данных Oracle (ОС Windows 2000) и решение начальных задач обеспечения ее безопасности. Компоненты модели безопасности АИС. Политика безопасности сервера АИС и ее компоненты.
1.2	Политика безопасности сервера АИС и ее компоненты.	Политика безопасности данных, пользователя, управления паролем и т.д. – для СУБД Oracle. Краткое руководство по обеспечению безопасности. План обеспечения безопасности. Доступность базы данных. Идентификация пользователей.
1.3	Системные привилегии. Роли.	Использование параметра WITH ADMIN OPTION. Предоставление привилегий доступа к объекту. Управление привилегиями с помощью ролей. Системные привилегии, определяющие права по работе с ролями. Предопределенные роли. Создание ролей и предоставление им привилегий. Управление допустимостью использования ролей. Отмена привилегий. Отмена системных привилегий и ролей. Отмена привилегий доступа к объекту. Использование представлений, процедур и триггеров для повышения защищенности системы.
1.4	Средства аудита.	Использование представлений для разграничения доступа. Использование представлений администратора базы данных для выяснения вопросов обеспечения безопасности АИС. Использование хранимых процедур и триггеров для повышения защищенности системы. Средства аудита. Аудит системных событий. Аудит событий, связанных с доступом к системе. Прекращение регистрации

		событий. Обработка данных аудита.
2	**Второй раздел**	
2.1	Иллюстрация решения комплексной задачи обеспечения безопасности.	Профили пользователя, работа с паролями. Профили пользователя, как средство повышения защищенности системы. Работа с паролями. Предотвращение возможности повторного использования паролей. Задание сложности пароля. Безопасность паролей при регистрации - шифрование паролей. Возможности несанкционированного доступа к базе данных. Изменение пароля администратора базы.
2.2	Восстановление базы данных.	Физическое копирование и восстановление – принципы реализации. Примеры восстановления базы данных для различных сценариев:база данных находится в режиме archivelog (архивируется) или noarchivelog (не архивируется); имеется "холодная" или "горячая" резервные копии базы данных; в ходе работы с БД "утеряны" файлы данных; база данных находится в режиме archivelog (архивируется); утрачивается файл rbs1orcl.ora именно тогда, когда выполнение транзакции связано с использование rollback segments из табличного пространства ROLLBAC_DATA;база данных находится в режиме archivelog (архивируется); теряются незаархивированные оперативные файлы журнала.
2.3	Развитые средства обеспечения безопасности в СУБД Oracle 9i.	Гранулированный (fine grained access) доступ к базе данных, гранулированный (fine grained audit) аудит базы данных. Виртуальные частные базы данных. Шифрование содержимого базы данных. Написание процедур с правами пользователя (invoker).
2.4	Безопасные роли приложений.	Обеспечение безопасности с метками грифа секретности средствами Oracle Label Security.

Курс лабораторных занятий

№	**Наименование раздела / темы дисциплины**	**Содержание**
1	**Первый раздел**	
1.1	Информационная модель безопасности автоматизированной информационной системы (АИС).	Информационная модель - на примере АИС, реализованной на базе СУБД Oracle. Создание базы данных Oracle (ОС Windows 2000) и решение начальных задач обеспечения ее безопасности. Компоненты модели безопасности АИС. Политика безопасности сервера АИС и ее компоненты.
1.2	Политика безопасности сервера АИС и ее	Политика безопасности данных, пользователя, управления паролем и т.д. – для СУБД Oracle. Краткое

	компоненты.	руководство по обеспечению безопасности. План обеспечения безопасности. Доступность базы данных. Идентификация пользователей.
1.3	Системные привилегии. Роли.	Использование параметра WITH ADMIN OPTION. Предоставление привилегий доступа к объекту. Управление привилегиями с помощью ролей. Системные привилегии, определяющие права по работе с ролями. Предопределенные роли. Создание ролей и предоставление им привилегий. Управление допустимостью использования ролей. Отмена привилегий. Отмена системных привилегий и ролей. Отмена привилегий доступа к объекту. Использование представлений, процедур и триггеров для повышения защищенности системы.
1.4	Средства аудита.	Использование представлений для разграничения доступа. Использование представлений администратора базы данных для выяснения вопросов обеспечения безопасности АИС. Использование хранимых процедур и триггеров для повышения защищенности системы. Средства аудита. Аудит системных событий. Аудит событий, связанных с доступом к системе. Прекращение регистрации событий. Обработка данных аудита.
2	**Второй раздел**	
2.1	Иллюстрация решения комплексной задачи обеспечения безопасности.	Профили пользователя, работа с паролями. Профили пользователя, как средство повышения защищенности системы. Работа с паролями. Предотвращение возможности повторного использования паролей. Задание сложности пароля. Безопасность паролей при регистрации - шифрование паролей. Возможности несанкционированного доступа к базе данных. Изменение пароля администратора базы.
2.2	Восстановление базы данных.	Физическое копирование и восстановление – принципы реализации. Примеры восстановления базы данных для различных сценариев:база данных находится в режиме archivelog (архивируется) или noarchivelog (не архивируется); имеется "холодная" или "горячая" резервные копии базы данных; в ходе работы с БД "утеряны" файлы данных; база данных находится в режиме archivelog (архивируется); утрачивается файл rbs1orcl.ora именно тогда, когда выполнение транзакции связано с использование rollback segments из табличного пространства ROLLBAC_DATA;база данных находится в режиме archivelog (архивируется); теряются незаархивированные оперативные файлы журнала.
2.3	Развитые средства обеспечения безопасности в	Гранулированный (fine grained access) доступ к базе данных, гранулированный (fine grained audit) аудит

	СУБД Oracle 9i.	базы данных. Виртуальные частные базы данных. Шифрование содержимого базы данных. Написание процедур с правами пользователя (invoker).
2.4	Безопасные роли приложений.	Обеспечение безопасности с метками грифа секретности средствами Oracle Label Security.