Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)
Кафедра «Программное обеспечение автоматизированных систем»

УТВЕРЖДАЮ:
Ректор

_____ Н. В. Дубив

«____»_____ 2025 г.

Рабочая программа учебной дисциплины

АДМИНИСТРИРОВАНИЕ ПРОГРАММНЫХ СИСТЕМ

образовательных программ высшего образования:

программы бакалавриата
09.03.03 Прикладная информатика
направленность
Интеллектуальные информационные системы и технологии
форма обучения – очная

09.03.04 Программная инженерия
Направленность
Программное обеспечение автоматизированных систем
формы обучения – очная и заочная

Курган 2025

Рабочая программа дисциплины «Администрирование программных систем» составлена в соответствии с учебными планами программ бакалавриата «Прикладная информатика» (*Интеллектуальные информационные системы и технологии*) очной формы обучения и «Программная инженерия» (*Программное обеспечение автоматизированных систем*) очной и заочной форм обучения, утвержденными 27.06.2025г.

Рабочая программа дисциплины одобрена на заседании кафедры Программного обеспечения автоматизированных систем 30.06.2025 года, протокол № 12.

Рабочую программу разработал
доцент кафедры ПОАС _____ В.К. Волк

Заведующий
кафедрой ПОАС _____ С.В. Косовских

Согласовано:

Начальник
Управления
образовательной деятельности _____ Е.В. Григоренко

Специалист
по учебно-методической работе
Учебно-методического отдела _____ Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

09.03.03 Прикладная информатика	Распределение трудоемкости по семестрам и видам учебных занятий	
	Всего	6-й семестр
Трудоемкость освоения дисциплины, зач. ед.	**3**	**3**
Объем учебных занятий, акад. часов	**108**	**108**
Аудиторные занятия:	***48***	***48***
Лекции	16	16
Лабораторные работы	32	32
Самостоятельная работа:	***60***	***60***
Подготовка к зачету	18	18
Выполнение контрольной работы	18	18
Другие виды самостоятельной работы	24	24
Формы промежуточной аттестации	Зачет	Зачет

09.03.04 Программная инженерия	Распределение трудоемкости по семестрам и видам учебных занятий			
	Очная форма обучения		Заочная форма обучения	
	Всего	6-й семестр	Всего	6-й семестр
Трудоемкость освоения дисциплины, зач. ед.	**4**	**4**	**4**	**4**
Объем учебных занятий, акад. часов	**144**	**144**	**144**	**144**
Аудиторные занятия:	***48***	***48***	***10***	***10***
Лекции	16	16	4	4
Лабораторные работы	32	32	6	6
Самостоятельная работа:	***96***	***96***	***134***	***134***
Подготовка к экзамену	27	27	18	18
Выполнение контрольной работы	18	18	18	18
Другие виды самостоятельной работы	51	51	98	98
Формы промежуточной аттестации	Экзамен	Экзамен	Экзамен	Экзамен

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ

09.03.03 – Прикладная информатика.

Дисциплина «Администрирование программных систем» включена в состав элективного модуля «Технологии разработки и администрирование высокопроизводительных вычислительных систем» блока Б1 (часть, формируемая участниками образовательных отношений) учебного плана образовательных программы. Для освоения дисциплины необходимы компетенции, формируемые дисциплинами «Операционные системы», «Основы информационной безопасности» и «Базы данных».

09.03.04 – Программная инженерия.

Дисциплина «Администрирование программных систем» включена в состав элективного модуля «Промышленные технологии разработки и сопровождения программного обеспечения» блока Б1 (часть, формируемая участниками образовательных отношений) учебного плана образовательных программы. Для освоения дисциплины необходимы компетенции, формируемые дисциплинами «Операционные системы», «Основы информационной безопасности» и «Базы данных».

Компетенции, формируемые дисциплиной «Администрирование программных систем», могут быть применены в процессе выполнения выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

3.1 Цели и задачи изучения дисциплины

Основная цель изучения дисциплины – ознакомление с типовыми трудовыми функциями специалистов по сопровождению программных систем, определенными соответствующими профессиональными стандартами, и освоение технологий администрирования информационных систем.

Задачами дисциплины является практическое освоение технологий и инструментальных средств администрирования программных систем в процессе их эксплуатации.

3.2. Формируемые компетенции и индикаторы их достижения

3.2.1. Направление подготовки 09.03.03 – Прикладная информатика

Компетенции	Индикаторы достижения компетенций		Планируемые результаты обучения		Оценочные средства
	Код	Наименование	Код	Наименование	
ПК-5 Способность разрабатывать и проводить установку, настройку, оптимизацию функционирования сетевого и прикладного программного обеспечения	ИД-1$_{ПК-5}$	*Должен знать* методы управления надежностью хранения данных в автоматизированных информационных системах, методы управления информационной безопасностью в автоматизированных информационных системах	З (ИД-1 $_{ПК-5}$)	*Знает* базовые понятия целостности данных (ограничения типов, явные ограничения целостности, ссылочная целостность), проблемы сохранения целостности в условиях «мягких» и «жестких» сбоев и методы обеспечения целостности в реляционных базах данных (нормализация баз данных, резервное копирование и восстановление данных, использование журнала транзакций для выполнения их отката или повторного выполнения), базовые понятия и специфику дискреционной и мандатной защиты данных, модель ролевого управления доступом к объектам баз данных.	Результаты тестирования (рубежный контроль №1).
	ИД-2$_{ПК-5}$	*Должен уметь* использовать базовые конструкции языка SQL для управления разрешениями доступа к объектам реляционных баз данных.	У (ИД-3$_{ПК-5}$)	*Умеет* настраивать систему разграничения доступа субъектов к объектам баз данных СУБД MS SQL Server.	Отчеты о выполнении лабораторных работ №2.1 и №2.2.
	ИД-3$_{ПК-5}$	*Должен владеть* средствами управления доступа к объектам баз данных одного из промышленных серверов баз данных.	В (ИД-4$_{ПК-5}$)	*Владеет* инструментальными средствами управления доступа к объектам баз данных.	Отчеты о выполнении лабораторных работ №2.2 и №2.3.
ПК-8 Владение навыками использования операционных систем, сетевых технологий, систем управления базами данных	ИД-1$_{ПК-8}$	*Должен знать* методы защиты и разграничения доступа к элементам данных, реализованные в одном из промышленных серверов баз данных.	З (ИД-2 $_{ПК-8}$)	*Знает* технологию использования мета-данных о пользователях для разграничения их доступа к различным строкам таблиц (RLS), средства маскирования и шифрования данных, применяемы в СУБД MS SQL Server.	Результаты тестирования (рубежный контроль №2). Отчеты о выполнении лабораторной работы №2.4.
	ИД-2 $_{ПК-8}$	*Должен уметь* использовать средства сокрытия от непривилегированных пользователей реальных значений конфиденциальных данных без их шифрования	У (ИД-3$_{ПК-8}$)	*Умеет* использовать встроенные функции динамического маскирования данных столбцов таблиц баз данных СУБД MS SQL Server.	Результаты тестирования (рубежный контроль №2). Отчеты о выполнении лабораторной работы №2.5.

Компетенции	Индикаторы достижения компетенций		Планируемые результаты обучения		Оценочные средства
	Код	Наименование	Код	Наименование	
	ИД-3 $_{ПК-8}$	*Должен владеть* техникой шифрования конфиденциальной информации, реализованной в одном из промышленных серверов баз данных.	В (ИД-4$_{ПК-8}$)	*Владеет* навыками использования встроенных функций шифрования данных, реализованных в СУБД MS SQL Server.	Результаты тестирования (рубежный контроль №2). Отчеты о выполнении лабораторной работы №2.6.
ПК-15 Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью .	ИД-1$_{ПК-15}$	*Должен знать* требования к уровню защищенности автоматизированных систем различных классов, требования профессиональных стандартов к составу трудовых функций и компетентности специалистов по администрированию баз данных и информационных систем, типовую архитектуру системы защиты данных одного из промышленных серверов баз данных.	З (ИД-1$_{ПК-15}$)	*Знает* классы защищенности автоматизированных систем, установленные соответствующими регламентирующими документами, и требования к трудовым функциям специалистов по администрированию подсистем защиты информации автоматизированных систем, определенные российскими и зарубежными профессиональными стандартами, архитектуру системы информационной безопасности СУБД MS SQL Server: типовые задачи защиты данных, решаемые на уровне сервера и уровне баз данных, компоненты системного каталога базы данных и средства разграничения доступа, маскирования и шифрования данных.	Результаты тестирования (рубежный контроль №1). Отчеты о выполнении лабораторных работ №2.2 и №2.3.
	ИД-2 $_{ПК-15}$	*Должен уметь* выполнять настройки серверов баз данных для обеспечения требуемого уровня защищенности данных	У (ИД-3$_{ПК-15}$)	*Умеет* разграничивать доступ пользователей к объектам баз данных MS SQL Server и проводить тестирование системы разграничения доступа.	Отчеты о выполнении лабораторных работ №2.2 и №2.3.
	ИД-3 $_{ПК-15}$	*Должен владеть* навыками использования средств управления защитой данных, предоставляемых одним из промышленных серверов баз данных.	В (ИД-4$_{ПК-15}$)	*Владеет* навыками управления компонентами подсистемы защиты данных с использованием инструментальных средств, предоставляемых использование мета-данных о пользователях для разграничения их доступа к различным строкам таблиц .	Отчеты о выполнении лабораторных работ №2.2 и №2.3.

3.2.3. Направление подготовки 09.03.04 – Программная инженерия

Компетенции	Индикаторы достижения компетенций		Планируемые результаты обучения		Оценочные средства
	Код	Наименование	Код	Наименование	
ПК-6 Владение навыками использования операционных систем, сетевых технологий, систем управления базами данных	ИД-1$_{ПК-6}$	*Должен знать* методы защиты и разграничения доступа к элементам данных, реализованные в одном из промышленных серверов баз данных.	З (ИД-2 $_{ПК-6}$)	*Знает* технологию использования мета-данных о пользователях для разграничения их доступа к различным строкам таблиц (RLS), средства маскирования и шифрования данных, применяемы в СУБД MS SQL Server.	Результаты тестирования (рубежный контроль №2). Отчеты о выполнении лабораторной работы №2.4.
	ИД-2 $_{ПК-6}$	*Должен уметь* использовать средства сокрытия от непривилегированных пользователей реальных значений конфиденциальных данных без их шифрования	У (ИД-3$_{ПК-6}$)	*Умеет* использовать встроенные функции динамического маскирования данных столбцов таблиц баз данных СУБД MS SQL Server.	Результаты тестирования (рубежный контроль №2). Отчеты о выполнении лабораторной работы №2.5.
	ИД-3 $_{ПК-6}$	*Должен владеть* техникой шифрования конфиденциальной информации, реализованной в одном из промышленных серверов баз данных.	В (ИД-4$_{ПК-6}$)	*Владеет* навыками использования встроенных функций шифрования данных, реализованных в СУБД MS SQL Server.	Результаты тестирования (рубежный контроль №2). Отчеты о выполнении лабораторной работы №2.6.
ПК-11 Способность проводить установку, настройку и оптимизацию функционирования прикладного программного обеспечения	ИД-1$_{ПК-11}$	*Должен знать* методы управления надежностью хранения данных в автоматизированных информационных системах, методы управления информационной безопасностью в автоматизированных информационных системах	З (ИД-1 $_{ПК-11}$)	*Знает* базовые понятия целостности данных, проблемы сохранения целостности в условиях «мягких» и «жестких» сбоев и методы обеспечения целостности в реляционных базах данных, базовые понятия и специфику дискреционной и мандатной защиты данных, модель ролевого управления доступом к объектам баз данных.	Результаты тестирования (рубежный контроль №1).
	ИД-2$_{ПК-11}$	*Должен уметь* использовать базовые конструкции языка SQL для управления разрешениями доступа к объектам реляционных баз данных.	У (ИД-3$_{ПК-11}$)	*Умеет* настраивать систему разграничения доступа субъектов к объектам баз данных СУБД MS SQL Server.	Отчеты о выполнении лабораторных работ №2.1 и №2.2.
	ИД-3$_{ПК-11}$	*Должен владеть* средствами управления доступа к объектам баз данных одного из промышленных серверов баз данных.	В (ИД-4$_{ПК-11}$)	*Владеет* инструментальными средствами управления доступа к объектам баз данных.	Отчеты о выполнении лабораторных работ №2.2 и №2.3.

Компетенции	Индикаторы достижения компетенций		Планируемые результаты обучения		Оценочные средства
	Код	Наименование	Код	Наименование	
ПК-12 Способность проводить конфигурирование и настройку сетевых устройств и программного обеспечения	ИД-1$_{ПК-12}$	*Должен знать* методы защиты и разграничения доступа к элементам данных, реализованные в одном из промышленных серверов баз данных.	З (ИД-2 $_{ПК-12}$)	*Знает* технологию использования мета-данных о пользователях для разграничения их доступа к различным строкам таблиц (RLS), средства маскирования и шифрования данных, применяемы в СУБД MS SQL Server.	Результаты тестирования (рубежный контроль №2). Отчеты о выполнении лабораторной работы №2.4.
	ИД-2 $_{ПК-12}$	*Должен уметь* использовать средства сокрытия от непривилегированных пользователей реальных значений конфиденциальных данных без их шифрования	У (ИД-3$_{ПК-12}$)	*Умеет* использовать встроенные функции динамического маскирования данных столбцов таблиц баз данных СУБД MS SQL Server.	Результаты тестирования (рубежный контроль №2). Отчеты о выполнении лабораторной работы №2.5.
	ИД-3 $_{ПК-12}$	*Должен владеть* техникой шифрования конфиденциальной информации, реализованной в одном из промышленных серверов баз данных.	В (ИД-4$_{ПК-12}$)	*Владеет* навыками использования встроенных функций шифрования данных, реализованных в СУБД MS SQL Server.	Результаты тестирования (рубежный контроль №2). Отчеты о выполнении лабораторной работы №2.6.
ПК-13 Способность выполнять администрирование средств обеспечения информационной безопасности .	ИД-1$_{ПК-13}$	*Должен знать* методы управления надежностью хранения данных в автоматизированных информационных системах, методы управления информационной безопасностью в автоматизированных информационных системах	З (ИД-1 $_{ПК-13}$)	*Знает* базовые понятия целостности данных (ограничения типов, явные ограничения целостности, ссылочная целостность), проблемы сохранения целостности в условиях «мягких» и «жестких» сбоев и методы обеспечения целостности в реляционных базах данных (нормализация баз данных, резервное копирование и восстановление данных, использование журнала транзакций для выполнения их отката или повторного выполнения), базовые понятия и специфику дискреционной и мандатной защиты данных, модель ролевого управления доступом к объектам баз данных	Результаты тестирования (рубежный контроль №1).
	ИД-2$_{ПК-13}$	*Должен уметь* использовать базовые конструкции языка SQL для управления разрешениями доступа к объектам реляционных баз данных.	У (ИД-3$_{ПК-13}$)	*Умеет* настраивать систему разграничения доступа субъектов к объектам баз данных СУБД MS SQL Server.	Отчеты о выполнении лабораторных работ №2.1 и №2.2.
	ИД-3$_{ПК-13}$	*Должен владеть* средствами управления доступа к объектам баз данных одного из промышленных серверов баз данных.	В (ИД-4$_{ПК-13}$)	*Владеет* инструментальными средствами управления доступа к объектам баз данных.	Отчеты о выполнении лабораторных работ №2.2 и №2.3.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Учебно-тематический план

Разделы дисциплины		Часов контактной работы с преподавателем	
№	Наименование	Лекции	Лабораторные работы
1	Администрирование программных систем как вид профессиональной деятельности.	2	0
2	Управление надежностью и информационной безопасностью	14	28
	Рубежный контроль №1	-	2
	Рубежный контроль №2	-	2
Всего по дисциплине:		**16**	**32**

4.2 Содержание лекций

Наименование и содержание лекции	Часов контактной работы с преподавателем
РАЗДЕЛ №1. АДМИНИСТРИРОВАНИЕ ПРОГРАММНЫХ СИСТЕМ КАК ВИД ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ	
Лекция 1.1. ***Задачи администрирования программных систем*** Цели и задачи изучения дисциплины; взаимосвязи с другими дисциплинами; обзор рабочей программы и учебно-методических материалов. Задачи администрирования программных систем и трудовые функции администраторов. Обзор профессиональных стандартов РФ: 06.011 – Администратор баз данных; 06.026 – Системный администратор ИКС; 06.030 – Специалист по защите информации в ТКС и сетях; 06.033 – Специалист по защите информации в АС.	**2**
РАЗДЕЛ №2. УПРАВЛЕНИЕ НАДЕЖНОСТЬЮ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ	
Лекция 2.1 ***Триада CIA и стратегия глубокой многоуровневой защиты*** Компоненты информационной безопасности – триада CIA: конфиденциальность, целостность и доступность данных. Стратегия глубокой многоуровневой защиты. Уровень данных: обзор защитных мер, реализуемых на уровнях баз данных и серверов баз данных. Группы и классы защищенности автоматизированных систем. Требования к системе защиты информации: подсистема управления доступом, подсистема регистрации и учета, криптографическая подсистема, подсистема обеспечения целостности данных.	**2**
Лекция 2.2 ***Обеспечение целостности данных*** Понятие и аспекты целостности данных: явные (*checked*) ограничения целостности; нормализация базы данных; ссылочная целостность. Проблема модификации взаимозависимых значений в таблицах базы данных – использование триггеров и транзакций. Резервное копирование и восстановление базы данных после «жесткого» сбоя: разностные копии, использование BCM- и DCM-страниц файлов базы данных. Использование журнала транзакций для восстановления базы данных после «мягкого» сбоя: протокол WAL, откат (UnDo) и повторное выполнение (ReDo) транзакции. Точки сохранения (save points) и точки физической согласованности (TPC – Time of Physical Consistency).	**2**

Наименование и содержание лекции	Часов контактной работы с преподавателем
Лекция 2.3 ***Управление доступом к данным*** Терминология: объекты и субъекты доступа; разрешения и правила; идентификация, аутентификация и авторизация; уровень полномочий; дискреционная («логическая») и мандатная («физическая») защита. Дискреционная модель управления доступом: категории разрешений, SQL-команды управления разрешениями, преимущества и недостатки дискреционной защиты. Мандатная модель управления доступом: метки безопасности объектов и субъектов доступа; уровни ценности (WAL-уровни) и уровни конфиденциальности (RAL-уровни) объектов и субъектов доступа; модель Белла – Лападулы; преимущества и недостатки мандатной защиты.	**2**
Лекция 2.4 ***Двухуровневая архитектура системы дискреционного управления доступом СУБД MS SQL Server*** Уровень сервера: объекты и субъекты доступа, идентификация и аутентификация учетных записей, фиксированные серверные роли, хранение информации об учетных записях в системном каталоге. Уровень базы данных: объекты и субъекты доступа, фиксированные роли, пользователи и пользовательские роли, хранение информации о субъектах доступа в системном каталоге базы данных. Примеры DCL-команд управления доступом. Иерархия (приоритетность) разрешений доступа.	**2**
Лекция 2.5 ***Безопасность уровня строк таблиц в СУБД MS SQL Server*** Технология RLS (Row Level Security) – использование мета-данных о пользователях для разграничения их доступа к различным строкам таблиц. Предикаты и политики безопасности. Этапы подготовки RLS. Примеры.	**2**
Лекция 2.6 ***Динамическое маскирование данных в СУБД MS SQL Server*** Dynamic Data Masking (DDM) как средство сокрытия от непривилегированных пользователей реальных значений конфиденциальных данных (столбцов таблиц) без их шифрования. Обзор функций маскирования данных. Примеры создания, использования и отмены маскирования данных.	**2**
Лекция 2.7 ***Шифрование данных в СУБД MS SQL Server*** Иерархическая инфраструктура управления шифрованием: симметричные и асимметричные ключи различных уровней, сертификаты, подписи, хеширование. Функции шифрования / дешифрования данных. Ключи шифрования: *главный ключ службы* (Service Master Key, SMK), *главный ключ базы данных* (Database Master Key, DMK). *Ключ шифрования базы данных* (Database Encryption Key, DEK), используемый для *прозрачного шифрования* (Transparent Data Encryption, TDE). Примеры.	**2**
Всего часов лекционных занятий по дисциплине	**16**

4.3 Лабораторные работы

Наименование и содержание лабораторной работы	Часов контактной работы с преподавателем
РАЗДЕЛ №2. УПРАВЛЕНИЕ НАДЕЖНОСТЬЮ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ	
Лабораторная работа №2.1 ***Анализ архитектуры подсистемы информационной безопасности СУБД MS SQL Server*** Анализ свойств учетных записей, пользователей и ролей уровня сервера и уровня базы данных (доступом к соответствующим компонентам системного каталога БД). Выполнение и защита практических заданий.	**4**
Лабораторная работа №2.2 ***Анализ средств управления доступом к объектам БД*** Освоение SQL-средств управления доступом, членством в пользовательских ролях БД. Выполнение и защита практических заданий.	**4**
Лабораторная работа №2.3 ***Анализ иерархии прав доступа к объектам БД*** Практическое изучение системы приоритетов разрешений доступа. Экспериментальная проверка гипотез о приоритетности разрешений, выданных на различных уровнях или полученных различными способами. Выполнение и защита практических заданий.	**6**
Рубежный контроль №1	**2**
Лабораторная работа №2.4 ***Безопасность уровня строк таблиц (RLS)*** Создание предикатов и политик безопасности, подготовка и проверка реализации RLS. Выполнение и защита практических заданий.	**4**
Лабораторная работа №2.5 ***Динамическое маскирование данных (DDM)*** Изучение встроенных DDM-функций, их применение и проверка реализации защиты данных. Выполнение и защита практических заданий	**4**
Лабораторная работа №2.6 ***Шифрование данных*** Изучение схемы иерархической инфраструктуры управления шифрованием, реализованную в MS SQL Server: включение/отключение режима TDE, шифрование / дешифрование данных столбцов таблиц. Выполнение и защита практических заданий	**6**
Рубежный контроль №2	**2**
Всего часов лабораторных занятий по дисциплине	**32**

4.4. Контрольная работа

Контрольная работа выполняется согласно методических рекомендаций.

5 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

5.1 Курс лекций

Детальное содержание лекционного материала представлено в учебном пособи [2], структура и содержание которого соответствует тематическому плану

изучения дисциплины. Учебное пособие содержит контрольные вопросы, ответы на которые должны быть получены обучающимся в процессе самостоятельной проработки материала соответствующей лекции.

5.2 Лабораторный практикум

Лабораторный практикум включает практические задания по второму тематическому разделу «Управление надежностью и информационной безопасностью» и имеет целью практическое освоение обучающимися соответствующих технологий и инструментальных средств. Все работы выполняются в соответствии с индивидуальными заданиями, выданными преподавателем. Состав заданий, методические указания по их выполнению и требования к содержанию и оформлению отчетов приведены в соответствующих разделах учебного пособия [12].

5.3 Самостоятельная работа

Самостоятельная работа обучающихся по освоению дисциплины включает проработку материала лекционного курса, подготовку и выполнение лабораторных работ, а также подготовку к рубежному контролю и промежуточной аттестации по дисциплине, проводимой в форме зачета.

Таблица 5.1 – Рекомендуемая трудоемкость самостоятельной работы

Виды самостоятельной работы	Трудоемкость, акад. часов		
	09.03.03 (очная форма)	09.03.04	
		Очная форма обучения	Заочная форма обучения
Изучение материала лекционного курса	**10**	**20**	**40**
Задачи администрирования программных систем, требования стандартов	2	4	8
Триада CIA, дискреционная (логическая) и мандатная (физическая) защита данных	2	4	8
Обеспечение целостности данных	2	4	8
Управление доступом к данным	2	4	8
Динамическое маскирование и шифрование данных	2	4	8
Подготовка к выполнению лабораторных работ	**10**	**27**	**58**
Архитектура системы защиты данных СУБД MS SQL Server	2	4	12
Иерархия системы разграничения доступа	2	4	12
Безопасность уровня строк таблиц	2	8	12
Динамическое маскирование данных	2	4	10
Шифрование данных	2	7	12
Выполнение контрольной работы	**18**	**18**	**18**
Подготовка к рубежному контролю	**4**	**4**	**-**
Рубежный контроль №1: Управление доступом к данным (тестирование)	2	2	-
Рубежный контроль №2: RLS, DDM, шифрование данных	2	2	-

(тестирование)			
Подготовка к промежуточной аттестации	**18**	**27**	**18**
Всего:	**60**	**96**	**134**

6 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1 Перечень оценочных средств

Фонд оценочных средств по дисциплине содержит следующие компоненты, включенные в состав учебно-методического комплекса дисциплины:

1. Балльно-рейтинговая система контроля о оценки академической активности обучающихся КГУ.
2. Вопросы и задания для тестирования при проведении мероприятий рубежного контроля, в том числе – задания для пробного самотестирования обучающихся.
3. Вопросы для подготовки к зачету и экзамену по дисциплине.
4. Примерные задания для проведения зачета по дисциплине.
5. Экзаменационные билеты.
6. Образцы отчетов по лабораторным и контрольным работам.
7. 7. Контрольная работа.

Банк заданий для проведения мероприятий рубежных контроля и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, а также методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

6.2 Система балльно-рейтинговой оценки работы обучающихся

№	Наименование	Содержание					
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения обучающихся на первом учебном занятии)*	Распределение баллов за 5 семестр					
		Вид учебной работы:	Выполнение лабораторной работы	Рубежный контроль №1	Рубежный контроль №2	Контрольная работа	Зачет, экзамен
		Балльная оценка:	до 8	до 5	до 5	12	до 30
		Примечания:	$8_б$ х 6=$48_б$				

2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – не зачтено; 61…100 – зачтено	
3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации по дисциплине за семестр обучающийся должен набрать по итогам текущего и рубежного контролей не менее 51 балла. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается. Для получения зачета и экзамена без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежных контролей. При этом, на усмотрение преподавателя, балльная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность. Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог балльной оценки по дисциплине не снижается. За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30. Основанием для получения дополнительных баллов являются: - выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем; - участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.	
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (экзамену, зачету) набрана сумма менее 51 балла, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.	

6.4 Процедура оценивания результатов освоения дисциплины

Программой изучения дисциплины предусмотрены мероприятия текущего и рубежного контроля и промежуточная аттестация в форме зачета (экзамена).

Текущий контроль проводится в форме защиты отчетов по выполненным лабораторным работам на аудиторных занятиях в соответствии с расписанием. В процессе защиты отчета оценивается уровень понимания обучающимся методики проведения работы, полнота и качество выполнения заданий, степень освоения инструментальных средств и качество написанного обучающимся программного кода, а также качество ответов на вопросы, заданные преподавателем, и обоснованность выводов, сделанных студентом по результатам проведенной работы.

Рубежный контроль проводится в форме фронтального тестирования по соответствующим тематическим разделам дисциплины. Каждый из тестов содержит 30 вопросов, расчетное время проведения тестирования – 60 минут. Оценивается количество правильных ответов на задания теста: обучающийся, ответивший правильно менее, чем на 15 заданий теста, считается не прошедшим тестирование и обязан повторно пройти этот тест.

Промежуточная аттестация по дисциплине

Промежуточная аттестация проводится в традиционной форме собеседования: обучающийся выполняет задания билета, включающего два вопроса и одну задачу, и отвечает преподавателю. Оцениваются полнота и правильность ответов студента, а также его эрудиция в смежных вопросах.

Результаты текущего контроля успеваемости и экзамена (зачета) заносятся преподавателем в экзаменационную (зачетную) ведомость, которая сдается в организационный отдел института в день экзамена (зачета), а также выставляются в зачетную книжку обучающегося.

6.5 **Примеры оценочных средств для рубежных контролей, экзамена и зачета**

6.5.1 Задания тестов для рубежного контроля

Рубежный контроль №1. Задачи администрирования и управление доступом

Вопрос	*№*	*Варианты ответов*
Верно ли утверждение о том, что при дискреционном («логическом») управлении доступом информация о защите данных хранится в базе данных отдельно от самих защищаемых данных?	1	Да
	2	Нет
	3	Такая информация хранится вне базы данных
Какие из перечисленных способов обеспечения целостности БД реализуются на стадии ее проектирования?	1	Использование проверяемых ограничений целостности (CHECK CONSTRAINT).
	2	Нормализация БД.
	3	Объединение нескольких операций доступа к данным в единую транзакцию.

Вопрос	*№*	*Варианты ответов*
	4	Использование хранимых процедур-триггеров.
Какие из перечисленных структур данных используются в процессе восстановления БД после «мягкого сбоя»?	1	Резервная копия БД
	2	Файловые страницы типа «Free Space».
	3	Журнал транзакций (LOG-файл).
	4	Таблица SysLogins системного каталога сервера БД.
Следующий SQL-оператор: **GRANT** <тип разрешения> **ON** <объект> **TO** <субъект> [**WITH GRANT OPTION**] используется для	1	Запрета доступа субъекта к объекту БД
	2	Отмены ранее выданных субъекту разрешений доступа к объекту БД
	3	Выдачи субъекту разрешений доступа к объекту БД
	4	Создания субъекта доступа к БД
Верно ли утверждение о том, что при мандатном («физическом») управлении доступом информация о защите данных хранится в базе данных отдельно от самих защищаемых данных?	1	Да
	2	Нет
	3	Информация о защите данных хранится вне базы данных
Позволяет ли классическая модель мандатного управления доступом (модель Белла – Лападулы) субъекту доступа ***читать*** объект, уровень конфиденциальности которого ***выше*** его собственного уровня?	1	Да, позволяет
	2	Нет, не позволяет
Позволяет ли классическая модель мандатного управления доступом (модель Белла – Лападулы) субъекту доступа ***модифицировать*** объект, уровень конфиденциальности которого ***ниже*** его собственного уровня?	1	Да, позволяет
	2	Нет, не позволяет
Сохранение высокого уровня конфиденциальности объекта БД в системах с мандатной защитой информации обеспечивается	1	Применением SQL-оператора REVOKE
	2	Применением SQL-оператора DENY
	3	Запретом субъекту доступа права чтения объекта доступа, *RAL*-уровень которого выше его собственного *RAL*-уровня
	4	Запретом субъекту доступа, имеющему права чтения объекта, права модификации (изменения, удаления или вставки) этого объекта, если *RAL*-уровень этого объекта выше *WAL*-уровня самого субъекта.
К какому классу защищенности следует отнести автоматизированную систему регистрации результатов приема пациентов врачами поликлиники (согласно Руководящему документу ФСТЭК «Автоматизированные	1	Класс «1Д»
	2	Класс «2Б»
	3	Класс «3А»

Вопрос	№	Варианты ответов
системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»)?		
К какому классу защищенности следует отнести автоматизированную систему регистрации результатов сдачи экзаменов студентами университета (согласно Руководящему документу ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»)?	1	Класс «1Д»
	2	Класс «2Б»
	3	Класс «3А»
К какому классу защищенности следует отнести автоматизированную систему регистрации адресов, паролей и явок агентов государственной службы внешней разведки (согласно Руководящему документу ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»)?	1	Класс «1Б»
	2	Класс «2А»
	3	Класс «3Б»
Какие из перечисленных ***объектов доступа*** определены на уровне ***сервера*** баз данных (MS SQL Server)	1	База данных
	2	Таблица базы данных
	3	Строка таблицы базы данных
Какие из перечисленных ***субъектов доступа*** определены на уровне ***базы данных*** (MS SQL Server)	1	Учетная запись
	2	Хранимая процедура
	3	Таблица базы данных

Рубежный контроль №2. RLS, DDM, шифрование данных

Вопрос	№	Варианты ответов
Какие задачи защиты данных решаются средствами DDM (динамическое маскирование данных)?	1	Блокировка чтения конфиденциальной информации
	2	Блокировка модификации ценной информации
	3	Затруднение интерпретации прочитанных данных
Какие методы шифрования данных применяются в технологии динамического маскирования данных (DDM)?	1	Симметричное шифрование
	2	Асимметричное шифрование
	3	DDM не использует шифрования данных

Какие задачи решаются средствами прозрачного шифрования (Transparent Data Encryption, TDE)?	1	Шифрация / дешифрация отдельных столбцов таблиц базы данных
	2	Шифрация / дешифрация ввода-вывода
	3	Маскирование данных
Какие задачи защиты данных решаются средствами RLS?	1	Маскирование данных всей строки таблицы
	2	Разграничение доступа к отдельным строкам таблицы со стороны различных пользователей
	3	Шифрование данных отдельных строк таблицы
	4	Затруднение интерпретации прочитанных данных

6.5.2 Вопросы для подготовки к промежуточной аттестации

1. *Типовые задачи и стандарты администрирования программных систем.*

▪ Трудовые функции и квалификационные уровни специалистов, определенные профессиональным стандартом 06.011 − «Администратор баз данных».
▪ Трудовые функции и квалификационные уровни специалистов, определенные профессиональным стандартом 06.026 − «Системный администратор информационно-коммуникационных систем».
▪ Трудовые функции и квалификационные уровни специалистов, определенные профессиональным стандартом 06.033 − «Специалист по защите информации в автоматизированных системах».
▪ Группы и классы защищенности автоматизированных систем. Требования к системе защиты информации: подсистема управления доступом, подсистема регистрации и учета, криптографическая подсистема, подсистема обеспечения целостности данных.

2. Обеспечение целостности и восстановление БД

▪ Журнализация изменений БД как метод обеспечения согласованности данных.
▪ Методы восстановления БД после мягкого сбоя.
▪ Методы восстановления БД после жесткого сбоя.

5. Информационная безопасность

▪ Логическая (дискреционная) защита.
▪ Физическая (мандатная) защита.
▪ Архитектура подсистемы информационной безопасности сервера баз данных.
▪ Объекты и субъекты доступа к данным.
▪ Средства разграничения доступа к объектам базы данных.
▪ Иерархия прав доступа к объектам базы данных.

7 ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная литература

1. Волк В.К. Базы данных. Часть 2. Администрирование: учебное пособие. – Курган: Изд-во Курганского гос. ун-та, 2018, – 127 с.

2. Волк В.К. Базы данных. Проектирование, программирование, управление и администрирование: учебник для вузов / В.К. Волк – 3-е изд. – Санкт-Петербург: Лань, 2022. – 244 с.

7.2. Дополнительные информационные источники:

3. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Руководящий документ ФСТЭК.
URL: https://fstec.ru/component/attachments/download/296.
4. Standard Occupational Classification [Electronic resource] / U.S. Bureau of Labor Statistics. – Electronic data (1 file: 974848 bytes). – Access mode: https://www.bls.gov/soc/2018/soc_structure_2018.pdf, free. – Title from screen.
5. Sys.database_permissions (Transact-SQL) *[*Электронный ресурс*]* − Режим доступа: https://docs.microsoft.com/en-us/sql/relational-databases/system-catalog-views/sys-database-permissions-transact-sql (Заголовок с экрана).
6. Sys.fn_builtin_permissions (Transact-SQL) *[*Электронный ресурс*]* − Режим доступа: https://docs.microsoft.com/en-us/sql/relational-databases/system-functions/sys-fn-builtin-permissions-transact-sql (Заголовок с экрана).
7. ГОСТ Р 56413-2015 Информационные технологии. Европейские профили профессий ИКТ-сектора /CWA 16458:2012 Information technologies. European ICT professional profiles [Текст]. – Введ. 01.06.2016 приказом Федерального агентства по техническому регулированию и метрологии от 29 мая 2015 г. № 465-ст.
8. Профессиональный стандарт 06.011 − «Администратор баз данных» [Текст]. Утвержден приказом Министерства труда и социальной защиты Российской федерации от 12 декабря 2016 г. №727н.
9. Профессиональный стандарт 06.015 − «Специалист по информационным системам» [Текст]. Утвержден приказом Министерства труда и социальной защиты Российской федерации от 12 декабря 2016 г. №727н.
10. Профессиональный стандарт 06.026 − «Системный администратор информационно-коммуникационных систем» [Текст]. Утвержден приказом Министерства труда и социальной защиты Российской федерации от 5 октября 2015 г. №684н.
11. Профессиональный стандарт 06.033 − «Специалист по защите информации в автоматизированных системах» [Текст]. Утвержден приказом Министерства труда и социальной защиты Российской федерации от 15 сентября 2016 г. №522н.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

12. Волк В.К. Базы данных. Сборник задач с комментариями и примерами решений: учебное пособие / В.К. Волк, В.Ю. Осеев, О.С. Черепанов. – Курган, Издательство Курганского государственного университета, 2024. – 265 с.

9. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- Сайт дистанционного обучения в НОУ «ИНТУИТ» (http://www.intuit.ru).
- Федеральный портал «Российское образование» http://www.edu.ru/
- Федеральный образовательный портал. Библиотека. Единое окно доступа к образовательным ресурсам: http://window.edu.ru/library.

10. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань»
2. ЭБС «Znanium.com»

Программное обеспечение

№	Наименование	Использование
1	StarUML™. The Open Source UML/MDA Platform.	Используются в качестве Case-средства поддержки программных проектов при выполнении контрольных работ и курсовых проектов.
2	MS SQL Server (Express)	Используется в качестве среды разработки и администрирования баз данных при выполнении лабораторных работ и курсовом проектировании.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины соответствует требованиям к образовательной программе, предъявляемым ФГОС ВО.

12 ИСПОЛЬЗОВАНИЕ ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

При использовании электронного обучения (ЭО) и дистанционных образовательных технологий (ДОТ) аудиторные занятия, а также текущий/рубежный контроль и промежуточная аттестация по дисциплине полностью или частично проводятся в режиме онлайн.

При использовании ЭО и ДОТ объем дисциплины, ее содержание и распределение по видам учебных занятий соответствуют п.4.1, п.4.2, п.4.3 и п.4.4.

Состав и формы проведения контрольно-аттестационных мероприятий и балльные оценки соответствуют п.6.1 и п.6.2 настоящей рабочей программы либо, в случае перехода на ЭО и ДОТ в процессе обучения, могут быть изменены соответствующим решением кафедры.

Решение об используемых ДОТ, системе оценивания достижений студентов и видах учебных занятий, проводимых в режиме онлайн, принимается кафедрой с

учетом мнения ведущего преподавателя и доводится до сведения студентов, изучающих дисциплину.

АННОТАЦИЯ

рабочей программы учебной дисциплины

АДМИНИСТРИРОВАНИЕ ПРОГРАММНЫХ СИСТЕМ

образовательных программы высшего образования

1. Программа бакалавриата **09.03.03 Прикладная информатика,** направленность

Интеллектуальные информационные системы и технологии, форма обучения – очная.

Трудоемкость – 3 зач. ед. (108 акад. часов)

Семестр: 6-й

Промежуточная аттестация: Зачет

Дисциплина «Администрирование программных систем» включена в состав элективного модуля «Технологии разработки и администрирование высокопроизводительных вычислительных систем» блока Б1 (часть, формируемая участниками образовательных отношений) учебного плана образовательных программы. Для освоения дисциплины необходимы компетенции, формируемые дисциплинами «Операционные системы», «Основы информационной безопасности» и «Базы данных».

2. Программа бакалавриата **09.03.04 Программная инженерия**, направленность

Программное обеспечение автоматизированных систем, формы обучения – очная и заочная.

Трудоемкость – 4 зач. ед. (144 акад. часа)

Семестр: 6-й

Промежуточная аттестация: Экзамен (очная форма), зачет (заочная форма)

Дисциплина «Администрирование программных систем» включена в состав элективного модуля «Промышленные технологии разработки и сопровождения программного обеспечения» блока Б1 (часть, формируемая участниками образовательных отношений) учебного плана образовательных программы. Для освоения дисциплины необходимы компетенции, формируемые дисциплинами «Операционные системы», «Основы информационной безопасности» и «Базы данных».

Компетенции, формируемые дисциплиной «Администрирование программных систем», могут быть применены в процессе выполнения выпускной квалификационной работы.