МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 71B13ADF852F0D849D78875814FBEF47
Владелец: Баранов Юрий Александрович
Действителен: с 15.10.2025 до 08.01.2027

УТВЕРЖДЕНО

Заместитель директора,
совмещающий обязанности директора
филиала КузГТУ в г. Новокузнецке

_____Баранов Ю.А.

«29» мая 2026г.

Рабочая программа дисциплины

Безопасность систем баз данных

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация «Специалист по защите информации»

Формы обучения: очная

Год набора 2026

Новокузнецк 2026 г.

Рабочая программа обсуждена на заседании учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол № 6 от 29.05.2026

Зав. Кафедрой ИТиЭД _____ В. В. Шарлай
подпись

СОГЛАСОВАНО:

Заместитель директора по УР _____ Т. А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Безопасность систем баз данных", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-12 - Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Имеет представление о системе управления базами данных как об одной из основных составляющих эффективных систем автоматизированной обработки информации; о современных концепциях безопасности баз данных.

Результаты обучения по дисциплине:

Знать принципы построения, функционирования, архитектуру, примеры реализаций современных систем управления базами данных; последовательность и содержание этапов проектирования баз данных; средства обеспечения безопасности данных.

Уметь создавать объекты базы данных; выполнять запросы к базе данных; разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; применять средства обеспечения безопасности данных.

Владеть языковыми средствами взаимодействия с реляционными базами данных; навыками нормализовывать отношения при проектировании реляционной базы данных; навыками реализации политики безопасности баз данных.

2 Место дисциплины "Безопасность систем баз данных" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Языки программирования, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Технологии и методы программирования, Нормативные требования по защите информации, Основы информатики, организации ЭВМ, вычислительных и информационных систем, Информационные угрозы, Классификация защищаемой информации и информационных систем.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Безопасность систем баз данных" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Безопасность систем баз данных" составляет 4 зачетных единицы, 144 часа.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 3/Семестр 5			
Всего часов	144		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	16		
Лабораторные занятия	32		
Практические занятия	32		
Внеаудиторная работа			

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	16		
Самостоятельная работа	48		
Форма промежуточной аттестации	зачет		

4 Содержание дисциплины "Безопасность систем баз данных", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
1. Введение в теорию баз данных	
1.1. Основы систем баз данных. Назначение и основные компоненты системы баз данных	2
1.2. Этапы проектирования и создания баз данных	2
1.3. Язык запросов SQL	2
2. Основы информационной безопасности баз данных	
2.1. Основные определения и понятия безопасности информационных систем и баз данных	1
2.2. Угрозы безопасности автоматизированных систем	1
3. Организация и средства защиты информационных процессов в автоматизированных системах	
3.1. Организационные, технические и программно-аппаратные средства защиты информации	2
3.2. Защита информации базы данных средствами СУБД	2
3.3. Обеспечение доступности, целостности и конфиденциальности в автоматизированных системах и базах данных	2
3.4. Защита сервера баз данных	2
Итого	**16**

4.2. Лабораторные занятия

Наименование работы	Трудоемкость в часах
	ОФ
1. Проектирование защищенной базы данных	16
2. Защита базы данных от SQL-инъекций	8
3. Защита базы данных средствами СУБД	8

Итого	**32**

4.3 Практические (семинарские) занятия

Тема занятия	**Трудоемкость в часах**
	ОФ
1. Основы систем баз данных. Назначение и основные компоненты системы баз данных.	4
2. Этапы проектирования и создания баз данных.	4
3. Основные определения и понятия безопасности информационных систем и баз данных.	4
4. Угрозы безопасности автоматизированных систем.	4
5. Организационные, технические и программно- аппаратные средства защиты информации.	4
6. Защита информации базы данных средствами СУБД.	6
7. Обеспечение доступности, целостности и конфиденциальности в автоматизированных системах и базах данных.	6
Итого	**32**

4.4 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	20
Оформление отчетов по практическим и(или) лабораторным работам	22
Подготовка к промежуточной аттестации	6
Итого	**48**

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Безопасность систем баз данных"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)
Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения компетенции**	**Результаты обучения по дисциплине (модулю)**	**Уровень**

Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-12 - Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	Имеет представление о системе управления базами данных как об одной из основных составляющих эффективных систем автоматизированной обработки информации; о современных концепциях безопасности баз данных.	**Знать** принципы построения, функционирования, архитектуру, примеры реализаций современных систем управления базами данных; последовательность и содержание этапов проектирования баз данных; средства обеспечения безопасности данных. **Уметь** создавать объекты базы данных; выполнять запросы к базе данных; разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных; применять средства обеспечения безопасности данных. **Владеть** языковыми средствами взаимодействия с реляционными базами данных; навыками нормализовывать отношения при проектировании реляционной базы данных; навыками реализации политики безопасности баз данных.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции** - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции** - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

5.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины

Обучающийся отвечает на 2 вопроса, либо отвечает на 10 тестовых заданий.

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:
- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень контрольных вопросов:

1. Введение в теорию баз данных

1. Понятие базы данных, ее назначение
2. Определить понятия «запись», «атрибут», «поле», «ключ», «кортеж»
3. Понятие СУБД, ее назначение
4. Разновидности и классификация БД
5. Способы обращения к БД и работы с ней

2. Основы информационной безопасности баз данных

1. Задачи обеспечения информационной безопасности баз данных.
2. Источники угроз информации баз данных.
3. Принципы построения защищенных систем баз данных.
4. Сущность понятия безопасности баз данных.
5. Средства обнаружения уязвимостей баз данных

3. Организация и средства защиты информационных процессов в автоматизированных системах

1. Из каких трех основных элементов состоит комплексная защита информации в АС
2. Программно-аппаратные механизмы защиты информационных процессов в автоматизированных системах
3. Организационные мероприятия и процедуры, выполняемые на стадии предпроектного обследования объекта и АИС
4. На каких принципах основывается создание базовой системы зашиты информации в автоматизированных ИС?
5. Основные механизмы безопасности информационных процессов в АИС

Примерный перечень тестовых заданий:

1. Введение в теорию баз данных

1. Что такое база данных?

Совокупность структурированных данных о реальных объектах окружающего мира
Совокупность разнообразных для об объектах окружающей действительности
Информационная структура для хранения данных

2. В базе данных информация может быть структурирована в виде:

сети

файла
иерархической структуры
таблицы

3. Выберите наименьший элемент таблицы в реляционной базе данных

поле
запись
ячейка
шаблон

2. Основы информационной безопасности баз данных

1. Какие традиционные способы защиты имеет база данных?

установка пароля
защита на уровне пользователя
ограничение доступа
шифрование БД
рабочие группы

2. К внутренним угрозам информационной безопасности баз данных относится: выбрать все верные:

умышленные, деструктивные действия лиц с целью искажения, уничтожения или хищения программ, данных и документов системы, причиной которых являются нарушения информационной безопасности защищаемого объекта
изменения состава и конфигурации комплекса взаимодействующей аппаратуры системы за пределы, проверенные при тестировании или сертификации системы
недостаточная эффективность используемых методов и средств обеспечения информационной безопасности в штатных или особых условиях эксплуатации системы

3. Право доступа открытия Базы данных в монопольном режиме имеет… .

База данных
программа Access
формы
модули
макросы

3. Организация и средства защиты информационных процессов в автоматизированных системах

1. На какой стадии создания системы защиты информации АС создается частное техническое задание на СЗИ?

стадия классификации АС
предпроектная стадия
стадия проектирования
стадия ввода в действие

2. В случае обеспечения безопасности в локальных вычислительных сетях, входящих в состав АИС, средства защиты должны использоваться:

во всех узлах сети, где обрабатывается конфиденциальная информация
во всех узлах сети, независимо от того, обрабатывают они конфиденциальную информацию или нет
на серверах сети
на пользовательских ЭВМ

3. Какое средство защиты позволяет выявлять несанкционированный доступ (или попытки несанкционированного доступа) к ресурсам автоматизированной системы?

межсетевой экран
IDS
антивирус

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1.Тема работы.

2. Задачи работы.

3. Краткое описание хода выполнения работы.

4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

5. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации являютя экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

ответы на вопросы во время опроса по разделам дисциплины или пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает на 2 вопроса, либо отвечает на 20 тестовых заданий

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
	не зачтено		зачтено		

Критерии оценивания при тестировании:

- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85…94 баллов – при правильном ответе на 16-18 вопросов;
- 75…84 баллов – при правильном ответе на 13-15 вопросов;
- 65…74 баллов – правильном ответе на 10-12 вопросов
- 25…64 – при правильном ответе только на 1-9 вопрос(ов);
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень вопросов на экзамен:

1. Условия осуществления несанкционированного доступа к базам данных. Каналы несанкционированного доступа к базам данных.
2. Методы добычи злоумышленником информации.
3. Критерии качества баз данных. Сущность понятия безопасности баз данных

4. Основные подходы к методам построения защищенных информационных систем.
5. Структура, свойства информационной безопасности баз данных
6. Источники угроз информации баз данных. Классификация угроз информационной безопасности баз данных
7. Угрозы, специфичные для систем управления базами данных. Объекты и субъекты моделей информационной безопасности баз данных
8. Подбор и манипуляция с паролями как метод реализации несанкционированных прав.
9. Нецелевое расходование вычислительных ресурсов сервера. Использование триггеров для выполнения незапланированных функций
10. Сущность политики безопасности.
11. Цель формализации политики безопасности.
12. Принципы построения защищенных систем баз данных
13. Стратегия применения средств обеспечения информационной безопасности. Методы обеспечения безопасности
14. Дискреционные модели безопасности СУБД. Реализация ролевой модели политики безопасности в СУБД Oracle.
15. Мандатная модель политики безопасности. БД с многоуровневой секретностью (MLS). Многозначность.
16. Авторизация меток пользователя. Специальные привилегии доступа. Меточные функции. Опции ограничения.
17. Целостность кода приложения. SQL-инъекции. Динамическое выполнение кода SQL и PL/SQL.
18. Категории атак SQL-инъекцией. Методы SQL-инъекций.
19. Противодействие атакам типа SQL-инъекции.
20. Подотчетность действий пользователя и аудит связанных с безопасностью событий.
21. Регистрация действий пользователя. Управление набором регистрируемых событий.
22. Причины возникновения уязвимостей баз данных.
23. Средства обнаружения уязвимостей баз данных.
24. Методы и утилиты для оценки критичности уязвимостей баз данных.
25. Классификация и порядок реализации угроз информационной безопасности баз данных.
26. Основные принципы обеспечения безопасности баз данных.
27. Управление доступом к базам данных.
28. Идентификация, авторизация и аутентификация пользователей баз данных.
29. Дискреционное, мандатное и ролевое разграничение доступа к базам данных.
30. Модели систем безопасности баз данных.
31. Системы безопасности уровня сервера.
32. Системы безопасности уровня баз данных
33. Методы обеспечения безопасности базы данных.
34. Методика резервного копирования и восстановления базы данных.
35. Понятие защиты баз данных.
36. Основные типы угроз безопасности баз данных.
37. Аппаратные средства защиты баз данных.
38. Программные средства защиты баз данных.

Примерный перечень тестовых заданий на экзамен:

1. Что такое база данных?

Совокупность структурированных данных о реальных объектах окружающего мира
Совокупность разнообразных для об объектах окружающей действительности
Информационная структура для хранения данных

2. В базе данных информация может быть структурирована в виде:

сети
файла
иерархической структуры
таблицы

3. Выберите наименьший элемент таблицы в реляционной базе данных

поле


1774206217

запись
ячейка
шаблон

4. Какие традиционные способы защиты имеет база данных?

установка пароля
защита на уровне пользователя
ограничение доступа
шифрование БД
рабочие группы

5. К внутренним угрозам информационной безопасности баз данных относится: выбрать все верные:

умышленные, деструктивные действия лиц с целью искажения, уничтожения или хищения программ, данных и документов системы, причиной которых являются нарушения информационной безопасности защищаемого объекта
изменения состава и конфигурации комплекса взаимодействующей аппаратуры системы за пределы, проверенные при тестировании или сертификации системы
недостаточная эффективность используемых методов и средств обеспечения информационной безопасности в штатных или особых условиях эксплуатации системы

6. Право доступа открытия Базы данных в монопольном режиме имеет… .

База данных
программа Access
формы
модули
макросы

7. На какой стадии создания системы защиты информации АС создается частное техническое задание на СЗИ?

стадия классификации АС
предпроектная стадия
стадия проектирования
стадия ввода в действие

8. В случае обеспечения безопасности в локальных вычислительных сетях, входящих в состав АИС, средства защиты должны использоваться:

во всех узлах сети, где обрабатывается конфиденциальная информация
во всех узлах сети, независимо от того, обрабатывают они конфиденциальную информацию или нет
на серверах сети
на пользовательских ЭВМ

9. Какое средство защиты позволяет выявлять несанкционированный доступ (или попытки несанкционированного доступа) к ресурсам автоматизированной системы?

межсетевой экран
IDS
антивирус
СКД

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

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Основы построения защищенных баз данных : лабораторный практикум : учебное пособие : [16+] / авт.-сост. Л. Л. Гусева ; Министерство науки и высшего образования Российской Федерации, Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 120 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=563264 (дата обращения: 09.04.2026). – Библиогр. в кн. – Текст : электронный.

2. Безопасность систем баз данных : учебное пособие / А. В. Скрыпников, С. В. Родин, Г. В. Перминов, Е. В. Чернышова. — Воронеж : ВГУИТ, 2015. — 139 с. — ISBN 978-5-00032-122-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/76236 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.2 Дополнительная литература

1. Основы построения защищенных баз данных : практикум : учебное пособие : [16+] / авт.-сост. Л. Л. Гусева. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 110 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=563266 (дата обращения: 09.04.2026). – Библиогр. в кн. – Текст : электронный.

2. Букатов, А. А. Методы и средства интеграции независимых баз данных в распределенных телекоммуникационных сетях / А. А. Букатов, А. В. Пыхалов ; Федеральное агентство по образованию, Южный федеральный университет, Южно-Российский региональный центр информатизации. – Ростов-на-Дону : Южный федеральный университет, 2013. – 160 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=241130 (дата обращения: 15.04.2026). – библиогр. с: С. 150-155 – ISBN 978-5-9275-1189-1. – Текст : электронный.

3. Аврунев, О. Е. Модели баз данных : учебное пособие : [16+] / О. Е. Аврунев, В. М. Стасышин. – Новосибирск : Новосибирский государственный технический университет, 2018. – 124 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575324 (дата обращения: 10.04.2026). – Библиогр. в кн. – ISBN 978-5-7782-3749-0. – Текст : электронный.

6.3 Методическая литература

1. Безопасность систем баз данных : методические указания к курсовой работе для обучающихся специальности 10.05.03 "Информационная безопасность автоматизированных систем" очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. безопасности ; сост. Е. В. Прокопенко. – Кемерово : КузГТУ, 2018. – 10 с. – URL: http://library.kuzstu.ru/meto.php?n=4610 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
2. Электронная библиотечная система «Лань» http://e.lanbook.com
3. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
4. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
5. Образовательная платформа «Юрайт» https://urait.ru/
6. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/projects/subscription/rus_titles_open.asp?
7. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

1. Вестник Кузбасского государственного технического университета : научно-технический журнал https://vestnik.kuzstu.ru/
2. Информационные системы и технологии : научно-технический журнал

https://eivis.ru/browse/publication/542286

3. Информационные технологии и вычислительные системы : журнал https://elibrary.ru/contents.asp?titleid=8746

4. Информация и безопасность : научный журнал

5. Открытые системы. СУБД : журнал https://eivis.ru/browse/publication/64072

6. Программные продукты и системы : международный научно-практический журнал

7. САПР и графика : журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Безопасность систем баз данных"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Безопасность систем баз данных", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Libre Office
2. Mozilla Firefox
3. Google Chrome
4. 7-zip
5. Microsoft Windows
6. ESET NOD32 Smart Security Business Edition
7. Kaspersky Endpoint Security

8. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Безопасность систем баз данных"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.