МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и автоматизации производственных процессов

Кафедра интеллектуальных систем и информационной безопасности

УТВЕРЖДАЮ
И.о. проректора по учебной работе
Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность систем баз данных
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Безопасность систем баз данных» является предоставление студентам теоретических знаний и практических навыков в области современных средств и методов защиты и администрирования баз данных и систем данных.

Задачи изучения дисциплины:

– ознакомить студентов с теоретическими положениями безопасности систем баз данных и систем данных в современных информационных системах;

– изучить основные принципы администрирования и резервирования систем баз данных;

– научиться использовать полученные знания в прикладных исследованиях, проектировании и эксплуатации информационных систем и технологий.

Дисциплина направлена на формирование общепрофессиональной (ОПК-12) компетенции выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит обязательную часть БЛОКА 1 «Дисциплины (модули)», подготовки студентов по специальности 10.05.03 «Информационная безопасность автоматизированных систем» (10.05.03-05 «Безопасность открытых информационных систем»).

Дисциплина реализуется кафедрой охраны специализированных компьютерных систем. Основывается на базе дисциплин: «Математический анализ», «Информатика», «Основы программирования», «Математическая логика и теория алгоритмов», «Базы данных»..

Является основой для изучения следующих дисциплин: «Программно-аппаратные средства защиты информации», «Разработка и эксплуатация защищённых автоматизированных систем»..

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с разработкой программного обеспечения.

Курс является фундаментом для ориентации студентов в сфере разработки программного обеспечения информационных систем.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 ак.ч. Программой дисциплины предусмотрены лекционные (36 ак.ч.), лабораторные (36 ак.ч.) занятия и самостоятельная работа студента (72 ак.ч.).

Дисциплина изучается на 3 курсе в 6 семестре. Форма промежуточной аттестации – экзамен.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Безопасность систем баз данных» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 –Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12	ОПК-12.3. Применяет знания в области безопасности баз данных при разработке автоматизированных систем

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 4 зачётных единицы, 144 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к экзамену.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		6
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	72	72
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	18	18
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	-	-
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	15	15
Работа в библиотеке	15	15
Подготовка к экзамену	15	15
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоемкость дисциплины		
ак.ч.	144	144
з.е.	4	4

5 Содержание дисциплины

С целью освоения компетенции, приведенной в п.3 дисциплина разбита на 3 темы:

– тема 1 (Средства обеспечения безопасности данных и баз данных);

– тема 2 (Администрирование систем баз данных);

– тема 3 (Аудит безопасности баз данных).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Средства обеспечения безопасности данных и баз данных	Теоретические основы безопасности БД и СУБД: понятие безопасности БД, угрозы безопасности БД, меры защиты БД и СУБД Атаки, специфические для баз данных. Методы дискреционного обеспечения доступа	4	-	-	Анализ угроз и уязвимостей для клиент-серверной СУБД	6
		Обеспечение целостности БД: принципы. Обработка транзакций. Управление параллельностью работы транзакций. Реализация ограничений в базах данных.	4	-	-	Управление транзакциями	6
		Защита от несанкциони-рованного доступа пользователей к объектам баз данных и сервисам СУБД. Использование криптографических методов защиты информации в системах баз данных. Защита баз данных от «внедрения в SQL».	10	-	-	Разграничение прав доступа и аудит пользователей в СУБД	6

Продолжение таблицы 3

1	2	3	4	5	6	7	8
1	Средства обеспечения безопасности данных и баз данных	Понятие целостности данных. Модели проверки целостности. Доменная целостность, трехзначная логика, ссылочная и сущностная целостность. Стратегии и средства обеспечения целостности. Ограничения и правила.	2	-	-	–	-
2	Администрирование систем баз данных	Основные понятия. Администратор данных и баз данных. Основные функции администрирования	2	-	-	Задачи администрирования баз данных	6
		Методы и механизмы обеспечения доступности баз данных и СУБД. Резервное копирование и восстановление баз данных. Резервирование серверов СУБД.	2	-	-	Резервное копирование и восстановление баз данных	6
		Понятие об однопользовательских и многопользовательских системах баз данных. Преимущества и недостатки их использования. Централизованное управление данными на предприятии. Преимущества и недостатки централизованного подхода к управлению данными.	6	-	-	Обеспечение доступа к базе данных в многопользовательском режиме	6

Завершение таблицы 3

1	2	3	4	5	6	7	8
3	Аудит безопасности баз данных	Верификация баз данных и проведение аудита в СБД. Методы и средства верификации баз данных. Активный аудит систем баз данных. Программа ISS Database Scanner. Мониторинг активности пользователей на уровне СУБД. Организация местного аудита в базах данных с использованием триггеров.	6	-	-	-	-
Всего аудиторных часов			36	-		36	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 5.

Таблица 5 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-12	Экзамен	Комплект контролирующих материалов для экзамена

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

– лабораторные работы – всего 90 баллов;

– за выполнение реферата – всего 10 баллов.

Экзамен проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Экзамен по дисциплине «Безопасность систем баз данных» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку либо в форме устного собеседования по приведенным ниже вопросам (п.п. 6.5), либо в результате тестирования.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 6.

Таблица 6 –Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашние задания не предусмотрены.

6.3Темы для рефератов (презентаций) – индивидуальное задание

Рефераты (индивидуальные задания) не предусмотрены

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1. Средства обеспечения безопасности данных и баз данных.

1) Основное содержание процедуры идентификации состоит в … идентификационного признака

а) предъявлении

б) предъявлении и проверке

в) назначении

2) Анализ безопасности архитектурных решений и их программных реализаций в СУБД должен включать исследование проблемы...

а) наличия вирусов

б) технологии реализации дискреционной, мандатной и ролевой моделей доступа к ресурсам системы

в) идентификации и аутентификации субъектов системы

г) действия по поиску опасных программ

3) При реализации оборонительной стратегии обеспечения информационной безопасности в первую очередь учитываются ... угрозы

а) все потенциальные

б) все идентифицированные

в) наиболее опасные

4) К внешним угрозам информационной безопасности баз данных относятся ...

а) искажения в каналах передачи информации, поступающей от внешних источников, циркулирующих в системе и передаваемой потребителям, а также недопустимые значения и изменения характеристик

потоков информации из внешней среды и внутри системы

б) ошибки при определении условий и параметров функционирования внешней среды., в которой предстоит использовать информационную систему и, в частности, программно-аппаратные средства защиты данных

в) системные ошибки при постановке целей и задач проектирования автоматизированных информационных систем и их компонент, допущенные при формулировке требований к функциям и характеристикам средств обеспечения безопасности системы

5) К внутренним угрозам информационной безопасности баз данных относится … *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

Тема 2. Администрирование систем баз данных.

1) При регистрации нового пользователя в системе администратор ... *выполняет поиск пользователя *изменяет привилегии пользователя *выполняет предоставление пользователю привилегий конкретной роли *выполняет учет пользователя

2) Реализация принципа наименьших привилегий предполагает, чтобы …

а) каждый пользователь (процесс) системы оперировал с данными, используя наименьший из возможных набор привилегий, необходимых для выполнения конкретной функции

б) минимальное количество пользователей (процессов) системы оперировало с данными, используя заданный набор привилегий, необходимых для выполнения конкретной функции

в) каждый пользователь (процесс) системы оперировал с данными, используя установленный набор привилегий, необходимых для выполнения минимального количества функций

3) Максимальный срок действия пароля целесообразно назначать в интервале ...

а) 10-15 рабочих дней

б) 30-60 дней

в) 50-100 рабочих дней

4) Расположите в порядке возрастания эффективности технологии подбора паролей

а) тотальный перебор, оптимизированный с помощью словарей

б) подбор пароля с использованием знаний о пользователе

в) тотальный перебор, оптимизированный по статистике встречаемости символов 4 тотальный перебор

5) Основная цель процедуры аутентификации состоит в ...

а) проверке дополнительных идентификационных признаков

б) предоставлении субъекту определенных полномочий

в) установлении валидности субъекта

Тема 3. Аудит безопасности баз данных.

1) Характеристики, входящие в состав многомерного вектора модели информационной безопасности, должны быть ...

а) независимы

б) попарно зависимы

в) взаимозависимы

2) Неверно, что при построении процедур аутентификации используется такой параметр, как ...

а) знание идентификационного признака

б) владение идентификационным признаком

в) модификация идентификационного признака

3) Формализация политики безопасности проводится для ...

а) представления информации в виде, наиболее пригодном для размещения на электронном носителе

б) ясного изложения взглядов руководства организации на сущность угроз информационной безопасности организации и технологии обеспечения безопасности ее информационных ресурсов

в) приведения терминологического аппарата в соответствие с требованиями нормативных документов по обеспечению информационной безопасности

4) Система защиты должна функционировать на …

а) уровне конфиденциальности, уровне целостности и уровне доступности

б) уровне доступности и физическом уровне

в) уровне конфиденциальности, физическом и аппаратном уровне физическом и аппаратном уровне

5) Право доступа к информации - это ...

а) лицо или процесс, осуществляющие несанкционированного доступа к информации нарушение установленных правил разграничения доступа

б) совокупность правил., регламентирующих порядок и условия доступа субъекта к информации и ее носителям

в) возможность доступа к информации, не нарушающая установленные правила разграничения доступа

в) совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации

6.5 Вопросы для подготовки к экзамену

1) Дайте определению понятию «системы баз данных». Какие рсновные составляющие системы баз данных Вы знаете?
2) Как обеспечить независимость от данных?
3) Какие виды систем баз данных Вы знаете?
4) Что такое архитектура системы баз данных?
5) Что такое «целостность данных»?
6) Что означают понятия «первичный ключ», «внешний ключ» таблицы?
7) Какие операторы объединения таблиц в языке SQL Вы знаете?
8) Как реализуется объединение результатов нескольких SQL-запросов?
9) Что такое вложенные подзапросы?
10) Какие Вы знаете стандарты программного доступа к базам данных?
11) Как осуществляется организация программного доступа к базе данных в .NET Framework?
12) Как осуществляется программный доступ к автономным данным?
13) Что такое представления?
14) Что такое хранимые процедуры?
15) Что такое триггеры и генераторы?
16) Что такое транзакции? Какие есть уровни изоляции транзакций?
17) Что такое безопасность базы данных?
18) Угрозы безопасности баз данных: общие и специфичные?
19) Какие есть требования безопасности баз данных?
20) Как осуществляется защита от несанкционированного доступа к БД?
21) Что такое целостность баз данных? Как она обеспечивается?
22) Какие Вы знаете угрозы конфиденциальности информации?
23) Какие есть средства идентификации и аутентификации в СУБД?
24) Какие есть средства управления доступом?

25) Какие есть виды привилегий для пользователей?

26) Как использовать представления для обеспечения конфиденциальности информации?

27) Что такое аудит связанных с безопасностью событий? Что такое аудит безопасности СУБД? Для чего он нужен?

29) Какие сведения содержит журнал аудита?

30) Что такое трассировка СУБД? Какие события протоколируются в СУБД?

31) Зачем нужно проводить анализ журнала транзакций?

32) Что такое «темпоральные данные»? Зачем они нужны?

33) Как создаются и как хранятся аудиторские следы в данных?

34) Как работает мониторинг сетевого трафика сервера БД?

35) Как работает мониторинг сервера БД?

6.6 Примерная тематика курсовых работ

Курсовая работа не предусмотрена.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Агафонов А. А. Безопасность систем баз данных: учебное пособие / А.А. Агафонов, А.С. Юмаганов. – Самара: Издательство Самарского университета, 2023 – 272 с. http://repo.ssau.ru/bitstream/Uchebnye-izdaniya/Bezopasnost-sistem-baz-dannyh-104397/1/978-5-7883-1916-2_2023.pdf. (Дата обращения 26.08.2024).

Дополнительная литература

1. Галатенко, В. А. Стандарты информационной безопасности : Курс лекций / В. А. Галатенко. - Москва : Интернет-Университет Информационных Технологий, 2004. - 326 с. - (Основы информационных технологий). https://reallib.org/reader?file=600131. (Дата обращения 26.08.2024).

Учебно-методическое обеспечение

1. Бизянов, Е.Е. Базы данных : лабораторный практикум / Е.Е. Бизянов, Н.Н. Кононенко ; ГОУ ВПО ДонГТУ, каф. специализированных компьютерных систем. Алчевск : ГОУ ВО ЛНР ДонГТИ, 2023. – 187 с. : ил. https://library.dstu.education/list.php?IDlist=Q_2

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. — URL: library.dstu.education.— Текст : электронный.
2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: http://ntb.bstu.ru/jirbis2/.— Текст : электронный.
3. Консультант студента : электронно-библиотечная система.— Москва. — URL: http://www.studentlibrary.ru/cgi-bin/mb4x.— Текст : электронный.
4. Университетская библиотека онлайн : электронно-библиотечная система.— URL: http://biblioclub.ru/index.php?page=main_ub_red.— Текст : электронный.

8 Материально-техническое обеспечение дисциплины

Материально-техническая база обеспечивает проведение всех видов деятельности в процессе обучения, соответствует требованиям ФГОС ВО.

Материально-техническое обеспечение представлено в таблице 9.

Таблица 9 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: *Мультимедийная лекционная аудитория. (60 посадочных мест)*, оборудованная специализированной (учебной) мебелью (скамья учебная –20 шт., стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. Аудитории для проведения лекций: *Компьютерный класс (22 посадочных места),* оборудованный учебной мебелью, компьютерами (12 шт.) с неограниченным доступом к сети Интернет, включая доступ к ЭБС	ауд. *207* корп. *4* ауд. *211* корп. *4*

Лист согласования рабочей программы дисциплины

Разработал
и.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности _____ Е.Е.Бизянов
(должность) (подпись Ф.И.О.)

_____ _____ _____
(должность) (подпись Ф.И.О.)

_____ _____ _____
(должность) (подпись Ф.И.О.)

и.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности _____ Е.Е. Бизянов
(подпись Ф.И.О.)

Протокол № 1 заседания кафедры СКС от 27.08.2024 г.

И.о. декана факультета _____ В.В. Дьячкова
(подпись Ф.И.О.)

Согласовано

Председатель методической
комиссии по специальности 10.05.03
«Информационная безопасность автоматизированных
систем» _____ Е.Е. Бизянов
(подпись Ф.И.О.)

Начальник учебно-методического центра _____ О.А.Коваленко
(подпись Ф.И.О.)

Лист изменений и дополнений

<table>
<tr><td colspan="2">Номер изменения, дата внесения изменения, номер страницы для внесения изменений</td></tr>
<tr><td>ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td><td>ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td></tr>
<tr><td colspan="2">Основание:</td></tr>
<tr><td colspan="2">Подпись лица, ответственного за внесение изменений</td></tr>
</table>