

«УТВЕРЖДАЮ»
Директор института цифровых
технологий и математики
С.А. Рощупкин



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.01.08 Безопасность систем управления базами данных

Направление подготовки: 10.03.01 Информационная безопасность

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

Квалификация (степень): бакалавр

Форма обучения: очная

Институт: цифровых технологий и математики

Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	очно-заочная форма	заочная форма
Курс	3		
Семестр	6		

Лекции	18		
Лабораторные занятия	36		
Практические (семинарские) занятия	18		
в т.ч. практическая подготовка			
Форма(ы) промежуточной аттестации	Экзамен-0,3		
Контроль	9		
Иные формы работы			
Самостоятельная работа	26,7		

Всего часов: 108

Трудоемкость: 3 зачетных единиц.

Разработчики рабочей программы:

к.п.н., доцент Щучка Т.А., ассистент Андропова О.Ю.

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины: формирование компетенций обучающегося в области администрирования подсистем информационной безопасности систем управления базами данных. Изучение особенностей применения, функционирования систем управления базами данных (СУБД) и встроенных в них средств защиты информации; эффективно разрабатывать и внедрять стратегии защиты информации в современных СУБД, учитывающих актуальные угрозы и риски в области информационной безопасности. Изучение теоретических основ и практических аспектов обеспечения безопасности данных, включая методы предотвращения несанкционированного доступа, обеспечения целостности и конфиденциальности информации, а также управление транзакциями и восстановление данных.

Задачи изучения дисциплины:

- рассмотреть современные концепции безопасности баз данных, критерии и методы оценивания надежности механизмов защиты систем баз данных;
- формирование навыков практической работы с базами данных, системами управления базами данных, моделями и механизмами защиты данных в базах данных;
- уметь устанавливать и настраивать системы управления базами данных с учетом требований по обеспечению защиты информации.

Место дисциплины в структуре ОПОП: реализуется в рамках части, формируемой участниками образовательных отношений, блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
УК-10	Знать: – действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности, а также способы профилактики коррупции и формирования нетерпимого отношения к ней.	Знает: – технологии выявления компьютерных атак и их возможности; – основные уязвимости и распространенные типы атак на СУБД; – основные законодательные акты и стандарты, регулирующие безопасность данных.
	Уметь: – планировать, организовать и проводить мероприятия, обеспечивающие формирование гражданской позиции и предотвращение коррупции в обществе.	Умеет: – разрабатывать и внедрять средства безопасности для управления доступом и защиты данных; – применять полученные знания на практике, включая использование специализированных инструментов для обеспечения безопасности баз данных.
	Владеть: – правилами общественного взаимодействия на основе нетерпимого отношения к коррупции.	Владеет: – методами и средствами защиты баз данных, включая шифрование, аутентификацию и авторизацию пользователей.
ПКС-1	Знать: – сущность и понятие информа-	Знает: – основы информационной безопасности,

	<p>ционной безопасности, характеристику ее составляющих, источники угроз и меры по их предотвращению;</p> <p>– методы и средства управления информационной безопасностью, а также основные подходы к разработке, реализации, эксплуатации, диагностике, анализу, сопровождению и совершенствованию систем защиты информации.</p>	<p>ее значимость для защиты данных и информации в организациях;</p> <p>– методы и стратегии для предотвращения угроз, включая использование технологий защиты, обучение персонала и внедрение политик безопасности;</p> <p>– особенности реализации методов защиты информации современными программно-аппаратными средствами.</p>
	<p>Уметь:</p> <p>– оценивать защищенность, классифицировать основные угрозы, обеспечивать информационную безопасность компьютерных систем, применяя необходимые программно-аппаратные средства и системы защиты информации;</p> <p>– принимать управленческие и административные решения в сфере защиты информации.</p>	<p>Умеет:</p> <p>– применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных баз данных;</p> <p>– проводить диагностику и анализ систем безопасности для выявления уязвимостей и оценки их эффективности.</p>
	<p>Владеть:</p> <p>– категориальным аппаратом в области обеспечения комплекса мер по администрированию и диагностике систем защиты информации;</p> <p>– правилами, методами, средствами, процедурами управления и администрирования информационной безопасностью объекта.</p>	<p>Владеет:</p> <p>– навыками мониторинга систем на предмет подозрительной активности и проведения аудита безопасности для оценки соблюдения политик и стандартов;</p> <p>– специализированными инструментами и технологиями для обеспечения безопасности, такими как шифрование данных и антивирусные решения.</p>

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№	Наименование разделов и тем	Всего часов	Ауд. занятия			Сам. раб.
			ЛК	ПЗ	ЛБ	
	Раздел 1. Проектирование защищенных систем баз данных	30	6	6	10	8
1	Тема 1. Понятие защищенной системы баз данных.	6	2		2	2
2	Тема 2. Анализ существующих подходов к проектированию защищенных систем баз данных	9	1	2	4	2

3	Тема 3. Алгоритмы анализа структур функциональных зависимостей при проектировании баз данных. Синтез схемы базы данных.	8	2	2	2	2
4	Тема 4. Критерии защищенности баз данных. Многоуровневая модель безопасности баз данных.	7	1	2	2	2
	Раздел 2. Методы обеспечения целостности в СУБД	20	4	2	8	6
5	Тема 5. Понятие целостности. Ограничения целостности в реляционной модели баз данных.	6	2		2	2
6	Тема 6. Декларативная поддержка ограничений целостности. Ссылочная целостность.	5	1		2	2
7	Тема 7. Процедурная поддержка ограничений целостности. Хранимые процедуры и триггеры.	9	1	2	4	2
	Раздел 3. Методы обеспечения конфиденциальности в СУБД	23,5	3	4	10	6,5
8	Тема 8. Основные методы и средства обеспечения конфиденциальности в современных СУБД	5	1		2	2
9	Тема 9. Средства разграничения доступа в языке SQL	9,5	1	2	4	2,5
10	Тема 10. Использование представлений для обеспечения конфиденциальности информации в базе данных	9	1	2	4	2
	Раздел 4. Методы обеспечения готовности в СУБД	10	2	2	4	2
11	Тема 11. Методы и средства восстановления баз данных	10	2	2	4	2
	Раздел 5. Методы оценки безопасности компьютерных систем	15,2	3	4	4	4,2
12	Тема 12. Методы оценки безопасности компьютерных систем на основе стандартов информационной безопасности	8,2	2	2	2	2,2
13	Тема 13. Средства обеспечения безопасности данных и баз данных.	7	1	2	2	2
	<i>Форма отчетности: экзамен</i>	0,3				
	<i>Контроль</i>	9				
	<i>Итого за 6 семестр</i>					
	в т.ч. практическая подготовка					
	ИТОГО	108	18	18	36	26,7

**Очно-заочная форма обучения
не реализуется**

Заочная форма обучения
не реализуется

**III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

Текущая аттестация проводится в форме реферата.

Примерная тематика рефератов

1. Основы информационной безопасности в системах управления базами данных. Понятия, принципы и важность защиты данных.
2. Анализ угроз и уязвимостей в системах управления базами данных. Основные типы угроз и методы их выявления.
3. Шифрование данных в системах управления базами данных.
4. Принципы и технологии шифрования для защиты конфиденциальной информации.
5. Аутентификация и авторизация пользователей в СУБД. Методы и подходы к управлению доступом.
6. Политики безопасности для управления базами данных.
7. Методы резервного копирования и восстановления данных.
8. Использование систем мониторинга и аудита в СУБД.
9. Законодательство и стандарты в области безопасности данных.
10. Технологии защиты от несанкционированного доступа к базам данных.
11. Безопасность облачных баз данных.
12. Современные инструменты и технологии для обеспечения безопасности СУБД. Обзор популярных решений и их применения.
13. Методы управления транзакциями.
14. Декларативная поддержка ограничений целостности.
15. Роль резервного копирования и восстановления данных в обеспечении безопасности СУБД.
16. Аутентификация и авторизация пользователей в СУБД: Сравнительный анализ методов управления доступом и их эффективность.

Промежуточная аттестация обучающихся осуществляется в форме экзамена с использованием следующих оценочных материалов: перечень вопросов к экзамену.

Вопросы к экзамену
(6 семестр, очная форма обучения)

1. Система управления базами данных.
2. Виды систем баз данных.
3. Назначение баз данных. Преимущества подхода, предусматривающего использование базы данных.
4. Архитектура системы баз данных. Три уровня архитектуры.
5. Понятие защищенной системы баз данных.
6. Методы создания безопасных систем баз данных.
7. Критерии защищенности баз данных. Многоуровневая модель безопасности баз данных.
8. Алгоритмы анализа структур функциональных зависимостей при проектировании баз данных.
9. Защищенная система баз данных.
10. Критерии защищенности баз данных для оценки их безопасности.

11. Структура многоуровневой модели безопасности баз данных.
12. Алгоритмы анализа структур функциональных зависимостей при проектировании баз данных.
13. Целостность данных.
14. Ссылочная целостность.
15. Основные методы и средства обеспечения конфиденциальности данных в современных системах управления базами данных.
16. Методы управления транзакциями.
17. Методы и средства восстановления баз данных.
18. Методы оценки безопасности компьютерных систем на основе стандартов информационной безопасности.
19. Требования безопасности баз данных.
20. Угрозы безопасности баз данных: общие и специфичные.
21. Стандарты программного доступа к базам данных.
22. Угрозы конфиденциальности информации.
23. Средства идентификации и аутентификации в СУБД.
24. Использование представлений для обеспечения конфиденциальности информации.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Советов, Б. Я. Базы данных : учебник для вузов / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 403 с. — (Высшее образование). — ISBN 978-5-534-18479-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/535113> (дата обращения: 18.04.2025).
2. Гудов А. М. Администрирование систем управления базами данных : учебное пособие : [16+] / А. М. Гудов, И. Ю. Степанов ; Кемеровский государственный университет. — Кемерово : Кемеровский государственный университет, 2022. — 167 с. : ил. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=700656> (дата обращения: 18.04.2025). — ISBN 978-5-8353-2893-2. — Текст : электронный.

4.2. Дополнительная литература

1. Основы построения баз данных : учебное пособие : [16+] / А. В. Аверченков, Р. А. Филиппов, Ю. А. Леонов [и др.]. — Москва ; Берлин : Директ-Медиа, 2021. — 124 с. : ил., табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=602227> (дата обращения: 18.04.2025). — Библиогр. в кн. — ISBN 978-5-4499-2428-5. — Текст : электронный.
2. Илюшечкин В. М. Основы использования и проектирования баз данных : учебник для вузов / В. М. Илюшечкин. — Москва : Издательство Юрайт, 2024. — 213 с. — (Высшее образование). — ISBN 978-5-534-03617-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/535450> (дата обращения: 18.04.2025).

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
---------	------------------------------------	--	-------------

1.	http://edu.ru/	Российское образование: Федеральный портал. Включает ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- Libre Office;
- реляционная система управления базами данных с открытым исходным кодом – MySQL.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных классах, оснащенных автоматизированными рабочими местами с компьютерами.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.