

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**ФИЗИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ  
Кафедра «Информационные системы и технологии»**

**СОГЛАСОВАНО**

Руководитель образовательной программы

\_\_\_\_\_/ М.Х. Мальсагов  
от «3» марта 2025г.

**УТВЕРЖДАЮ**

И.о. декана физико-математического  
факультета

\_\_\_\_\_/ Б.С.Кульбужев  
от«14» марта 2025г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б1.В.05. Управление доступом и технологии  
обеспечения безопасности БД**

**Направление подготовки**

**09.03.02 Информационные системы и технологии**

**Направленность (профиль подготовки)**

**Безопасность информационных систем**

**Квалификация выпускника**

Бакалавр

**Форма обучения**

Очная, очно-заочная

## ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

### Цели освоения дисциплины:

– формирование у студентов теоретических знаний и практических навыков в области управления доступом к базам данных (БД) и применения современных технологий обеспечения их безопасности, направленных на решение профессиональных задач в области информационной безопасности, включая анализ рисков, разработку политик безопасности и коллективную работу в проектных группах.

### Задачи освоения дисциплины:

- Изучить принципы и модели управления доступом (RBAC, ABAC, DAC, MAC) и их реализацию в СУБД.
- Освоить технологии аутентификации, авторизации и криптографической защиты данных.
- Развить навыки настройки систем управления идентификацией и доступом (IAM, IdM).
- Научиться анализировать угрозы безопасности БД и разрабатывать меры их нейтрализации.
- Сформировать умения коллективной работы при проектировании и реализации политик безопасности в СУБД.

## 2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Управление доступом и технологии обеспечения безопасности БД» относится к блоку профессиональных дисциплин и изучается на 7–8 семестрах бакалавриата по направлению 09.03.02 «Информационные системы и технологии», профиль «Безопасность информационных систем».

### Предшествующие дисциплины (из перечня):

- «Алгоритмизация и программирование»
- «Управление данными»
- «Криптографические методы защиты информации»
- «Основы и стандарты информационной безопасности»

### Последующие дисциплины:

- «Угрозы информационной безопасности, анализ и обнаружение атак»
- «Методы и средства защиты информации»

Знания и навыки, полученные в рамках дисциплины, необходимы для проектирования защищенных информационных систем, администрирования БД и выполнения выпускной квалификационной работы.

## 3. КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с

**планируемыми результатами освоения образовательной программы**

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	Компетенция реализуется полностью	УК-9.1. Понимает базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике.	УК-9.2. Применяет методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые рынки.	
ОПК-7. Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем.	Компетенция реализуется полностью	ОПК-7.1. Знать: основные платформы, технологии и инструментальные программно-аппаратные средства для реализации информационных систем.	ОПК-7.2. Уметь: осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем, применять современные технологии реализации информационных систем.	ОПК-7.3. Иметь навыки: владения технологиями и инструментальными программно-аппаратными средствами для реализации информационных систем.
ПК-6. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию в программного обеспечения.		ПК-6.1. Знать: возможности существующей программно-технической архитектуры; возможности современных и перспективных средств разработки программных продуктов, технических средств; методологии разработки программного обеспечения и технологии программирования; методологии	ПК-6.2. Уметь: проводить анализ исполнения требований; вырабатывать варианты реализации требований; проводить оценку и обоснование рекомендуемых решений; осуществлять коммуникации с заинтересованными сторонами;	ПК-6.3. Иметь навыки: анализа возможностей реализации требований к программному обеспечению; оценки времени и трудоемкости реализации требований к программному обеспечению; согласования требований к программному обеспечению с заинтересованными сторонами; оценки и согласование

		и технологии проектирования и использования баз данных;		сроков выполнения поставленных задач.
--	--	---	--	---------------------------------------

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

	Всего	Семестр	
		1	2
Общая трудоемкость дисциплины всего (в з.е.), в том числе:	<b>252/63.ед</b>	<b>108</b>	<b>144</b>
Аудиторные занятия всего (в акад. часах), в том числе:			
Лекции	<b>42</b>	<b>18</b>	<b>24</b>
Практические занятия, семинары	<b>32</b>	<b>32</b>	
Лабораторные работы	<b>32</b>		<b>32</b>
Контроль самостоятельной работы (КСР)			
Самостоятельная работа всего (в акад. часах), в том числе:	<b>119</b>	<b>58</b>	<b>61</b>
Вид итоговой аттестации:			
Экзамен/зачет*	<b>27</b>	<b>*</b>	<b>27</b>

#### 5. Структура и содержание дисциплины

##### 5.1 Структура дисциплины

Раздел, тема программы учебной дисциплины	Трудоемкость (час)				
	Всего	В том числе по видам учебных занятий			
		Лекции	Семинары, практические занятия	Лабораторные работы	Проверочные тесты
<b>7 СЕМЕСТР</b>					
<b>Управление доступом и технологии обеспечения безопасности БД.</b>					
Основы управления доступом и безопасности БД	8	4	4		
Модели управления доступом	10	4	6		
Аутентификация и авторизация в СУБД	12	4	8		
Криптографические методы защиты данных	9	3	6		
Мониторинг и аудит доступа	11	3	8		

<b>Итого</b>	<b>50</b>	<b>18</b>	<b>32</b>		
<b>8 СЕМЕСТР</b>					
<b>Управление доступом и технологии обеспечения безопасности БД.</b>	14	6		8	
Системы управления доступом (IAM, IdM)	14	6		8	
Защита от несанкционированного доступа	14	6		8	
Современные киберугрозы и методы их нейтрализации	14	6		8	
<b>Разработка политик безопасности БД</b>	14	6		8	
<b>Итого</b>	<b>56</b>	<b>24</b>		32	
<b>Итого часов</b>	<b>106</b>	<b>42</b>	<b>32</b>	32	
Самостоятельная работа студента, в том числе: - в аудитории под контролем преподавателя - курсовое проектирование (выполнение курсовой работы) - внеаудиторная работа	119	Формы текущего и рубежного контроля подготовленности обучающегося:			
Экзамен/зачет*	27				
Всего часов на освоение учебного материала	252				

## 5.2 Содержание дисциплины

### 7 семестр

#### Тема 1: Основы управления доступом и безопасности БД

Понятие управления доступом. Принципы CIA (конфиденциальность, целостность, доступность). Угрозы безопасности БД (SQL-инъекции, утечки данных). Нормативные документы (ФЗ-152, ГОСТ Р 57580).

#### Тема 2: Модели управления доступом

Ролевая (RBAC), атрибутная (ABAC), дискреционная (DAC), мандатная (MAC) модели. Реализация в PostgreSQL, Oracle, SQL Server. Сравнение моделей.

#### Тема 3: Аутентификация и авторизация в СУБД

Методы аутентификации: пароли, сертификаты, SSO, MFA. Управление ролями и привилегиями. Практическая настройка в PostgreSQL и SQL Server.

#### **Тема 4: Криптографические методы защиты данных**

Шифрование данных: TDE, шифрование столбцов. Российские стандарты (ГОСТ 34.12-2015). Управление ключами в СУБД.

#### **Тема 5: Мониторинг и аудит доступа**

Инструменты мониторинга (SIEM-системы). Настройка аудита в СУБД. Анализ логов для выявления угроз.

### **8 семестр**

#### **Тема 6: Системы управления доступом (IAM, IdM)**

Архитектура и настройка IAM-систем (Microsoft Entra, Solar InRights). Интеграция с СУБД.

#### **Тема 7: Защита от несанкционированного доступа**

Методы защиты от SQL-инъекций, DDoS, утечек данных. Организационные меры безопасности.

#### **Тема 8: Современные киберугрозы и методы их нейтрализации**

Анализ угроз: фишинг, вредоносное ПО, атаки на API. Практические кейсы и меры противодействия.

#### **Тема 9: Разработка политик безопасности БД**

Этапы разработки политик безопасности. Автоматизация управления доступом. Анализ реальных инцидентов в команде.

## **6. Учебно-методическое и информационное обеспечение дисциплины**

### **Рекомендуемая литература**

#### **Основная литература:**

1. Милославская Н.Г., Толстой А.И. Информационная безопасность: учебник для вузов / Н.Г. Милославская, А.И. Толстой. — М.: Юрайт, 2023. — 480 с. — (Высшее образование). — ISBN 978-5-534-15022-3. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/520123>
2. Афанасьев А.А., Веденьев Л.Т., Воронцов А.А. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие для вузов / под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. — 2-е изд., стер. — М.: Горячая линия-Телеком, 2012. — 550 с. — ISBN 978-5-9912-0257-2. — Текст: электронный // ЭБС Znanium [сайт]. — URL: <https://znanium.ru/catalog/product/436855> (дата обращения: 16.04.2025).
3. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учебное пособие / А.В. Васильков, И.А. Васильков. — М.: ИНФРА-М, 2022. — 320 с. — ISBN 978-5-16-017345-0. — Текст: электронный // ЭБС Znanium [сайт]. — URL: <https://znanium.ru/catalog/product/1901234>

#### **Дополнительная литература:**

1. Белов Е.Б., Лось В.П., Мещеряков Р.В. Основы информационной безопасности: учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков. — М.: Горячая линия-Телеком, 2020. — 256 с. — ISBN 978-5-9912-0789-8. — Текст: электронный // ЭБС Znanium [сайт]. — URL: <https://znanium.ru/catalog/product/1234567>

2. Полтавцева М.А. Информационная безопасность баз данных: учебное пособие / М.А. Полтавцева. — СПб.: Лань, 2021. — 208 с. — ISBN 978-5-8114-7890-3. — Текст: электронный // Издательство Лань [сайт]. — URL: <https://lanbook.com/book/245678>
3. Новиков Б.А., Горшкова Е.А., Графеева Н.Г. Основы технологий баз данных: учебное пособие / под ред. Е.В. Рогова. — 2-е изд. — М.: ДМК Пресс, 2020. — 582 с. — ISBN 978-5-97060-841-8. — Текст: электронный // Postgres Professional [сайт]. — URL: <https://edu.postgrespro.ru/bases.pdf>

## **7. Материально-техническое обеспечение дисциплины**

Лекции читаются в аудитории, приспособленной для работы с проектором. Лабораторные занятия проводятся в компьютерном классе с доступом в Интернет, из расчета: один компьютер на одного обучающегося. Минимальные требования к компьютерам — ОЗУ 1ГБ, рекомендуемые — ОЗУ 2ГБ и более. Операционная система — семейства MS Windows или семейства GNU/Linux.

Самостоятельная работа выполняется в компьютерных классах и читальном зале университета.

**Электронная информационно-образовательная среда** университета обеспечивает:

- доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программам практик;
- формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося и оценок за эти работы.

В случае реализации программы магистратуры с применением электронного обучения, дистанционных образовательных технологий электронная информационно-образовательная среда дополнительно обеспечивает:

- фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы;
- проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;
- взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет».

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих.

Функционирование электронной информационно-образовательной среды соответствует законодательству Российской Федерации.

Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и подлежит обновлению (при необходимости) в соответствии с требованиями ФГОС ВО и ПООП.

## **Информационно-библиотечное обеспечение образовательной программы**

Информационно-библиотечное обслуживание студентов и профессорско-преподавательского состава осуществляется Научной библиотекой (НБ) ИнГУ и играет ключевую роль в учебно-методическом обеспечении образовательных программ.

В Научной библиотеке созданы и действуют в настоящее время: отделы обслуживания читателей, отделы хранения фондов, отдел справочно-библиографической, информационной и методической работы, отдел комплектования, учёта и научной обработки литературы, отдел автоматизации и ИТ службы, 4 читальных зала, электронный

читальный зал, а также электронная библиотека. В читальных залах НБ 454 посадочных места.

Электронный читальный зал НБ предоставляет доступ к следующим ЭБС: IPR-books <http://www.iprbookshop.ru>

Президентская библиотека им. Б.Н. Ельцина Национальная библиотека (НЭБ)

АИБС МегаПро

Единое окно доступа к образовательным ресурсам <http://window.edu.ru/> E-library.ru (научные статьи)

Русская виртуальная библиотека <http://rvb.ru> (классика русской литературы)

Ресурсный объем библиотечной деятельности, динамика пополнения и обновления фондов, их состав по качественным и временным параметрам позволяют Университету обеспечить образовательный процесс на качественном уровне.

В настоящее время фонд Научной библиотеки университета состоит из учебной, учебно- методической, научной, научно-популярной, общественно-политической и художественной литературы. Комплектование библиотечного фонда осуществляется в соответствии с заявками заведующих кафедрами и начальника научно-исследовательского сектора.

Фонд библиотеки насчитывает 235908 единиц хранения, в том числе:

## **8. Методические указания для обучающихся по освоению дисциплины**

На лекциях преподаватель знакомит слушателей с основными понятиями и положениями по текущей теме. На лекциях слушатель получает только основной объем информации по теме. Только посещение лекций является недостаточным для подготовки к лабораторным занятиям и экзамену. Требуется также самостоятельная работа по изучению основной и дополнительной литературы и закрепление полученных на лабораторных занятиях навыков.

Практические задания по темам выполняются на лабораторных занятиях в компьютерном классе. Если лабораторные занятия пропущены (по уважительной или неуважительной причине), то соответствующие задания необходимо выполнить самостоятельно и представить результаты преподавателю на очередном занятии, консультации или через образовательный портал.

Самостоятельная работа студентов – способ активного, целенаправленного приобретения студентом новых для него знаний, умений и навыков без непосредственного участия в этом процесса преподавателя.

Качество получаемых студентом знаний напрямую зависит от качества и количества необходимого доступного материала, а также от желания (мотивации) студента их получить. При обучении осуществляется целенаправленный процесс взаимодействия студента и преподавателя для формирования знаний, умений и навыков.



Рабочая программа дисциплины «Управление доступом и технологии обеспечения безопасности БД» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02. «Информационные системы и технологии», профиль «Безопасность информационных систем» утвержденного приказом Министерства науки и высшего образования Российской Федерации от « 19 » сентября 2017 г. № 926 (ред.08.02.2021)

Программу составили: старший преподаватель кафедры «Информационные системы и технологии» Алтемиров А.С.

Программа одобрена на заседании кафедры «Информационные системы и технологии» Протокол № 6 от « 3 » марта 2025 года

Программа одобрена Учебно-методической комиссией физико-математического факультета Протокол № 7 от « 13 » марта 2025 года

**Сведения о переутверждении программы на очередной учебный год и регистрации изменений**

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой

Приложение

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б1.В.05 Управление доступом и технологии обеспечения безопасности БД**

**Направление подготовки**

**09.03.02 Информационные системы технологии**

**Направленность (профиль подготовки)**

**Безопасность информационных систем**

**Квалификация выпускника**

**бакалавр**

**Форма обучения**

**Очная, очно-заочная**

Магас, 2025г.

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	Компетенция реализуется полностью	УК-9.1. Понимает базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике.	УК-9.2. Применяет методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые рынки.	
ОПК-7. Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем.	Компетенция реализуется полностью	ОПК-7.1. Знать: основные платформы, технологии и инструментальные программно-аппаратные средства для реализации информационных систем.	ОПК-7.2. Уметь: осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем, применять современные технологии реализации информационных систем.	ОПК-7.3. Иметь навыки: владения технологиями и инструментальными программно-аппаратными средствами для реализации информационных систем.
ПК-6. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию в программного обеспечения.		ПК-6.1. Знать: возможности существующей программно-технической архитектуры; возможности современных и перспективных средств разработки программных продуктов, технических средств; методологии разработки программного обеспечения и технологии программирования; методологии	ПК-6.2. Уметь: проводить анализ исполнения требований; вырабатывать варианты реализации требований; проводить оценку и обоснование рекомендуемых решений; осуществлять коммуникации с заинтересованными сторонами;	ПК-6.3. Иметь навыки: анализа возможностей реализации требований к программному обеспечению; оценки времени и трудоемкости реализации требований к программному обеспечению; согласования требований к программному обеспечению с заинтересованными сторонами; оценки и согласование

		и технологии проектирования и использования баз данных;	сроков выполнения поставленных задач.
--	--	---	---------------------------------------

# ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

## Шкала и критерии оценки промежуточной аттестации в форме зачета

Оценка (баллы)	Уровень сформированности компетенций	Общие требования к результатам аттестации в форме зачета	Планируемые результаты обучения
«Зачтено»	Высокий уровень	Теоретическое содержание курса освоено полностью без пробелов или в целом, или большей частью, необходимые практические навыки работы с освоенным материалом сформированы или в основном сформированы, все или большинство предусмотренных рабочей программой учебных заданий выполнены, от- дельные из выполненных заданий содержат ошибки	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы;</li> <li>- точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы;</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин;</li> <li>- творческая самостоятельная работа на практических/ семинарских/лабораторных занятиях, активное участие в групповых обсуждениях, высокий уровень культуры исполнения заданий;</li> </ul> <p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>- безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач;</li> <li>- выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине;</li> </ul>

	Базовый уровень	Теоретическое содержание курса освоено в целом без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, предусмотренные рабочей учебной программой учебные задания выполнены с отдельными неточностями, качество выполнения большинства заданий оценено числом баллов, близким к максимуму.	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- достаточно полные и систематизированные знания по дисциплине;</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- ориентироваться в основных теориях, концепциях и направлениях дисциплины и давать им критическую оценку;</li> <li>- использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;</li> </ul> <p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>- владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач;</li> <li>- усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине;</li> <li>- самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий;</li> <li>- средний уровень сформированности заявленных в рабочей программе компетенций.</li> </ul>
	Минимальный уровень	Теоретическое содержание курса освоено большей частью, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных рабочей учебной программой учебных заданий выполнены, отдельные из выполненных заданий содержат ошибки.	<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>- Достаточный минимальный объем знаний по дисциплине;</li> <li>- усвоение основной литературы, рекомендованной учебной программой;</li> </ul> <p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>- умение ориентироваться в основных теориях, концепциях и Направлениях по дисциплине и давать им оценку;</li> <li>- использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать</li> </ul>

			<p>выводы без существенных ошибок;</p> <p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>- владение инструментарием учебной дисциплины, умение его использовать в решении типовых задач;</li> <li>- умение под руководством преподавателя решать стандартные задачи;</li> <li>- работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий;</li> <li>- достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций.</li> </ul>
«Не зачтено»	компетенции, закрепленные за дисциплиной, <b>не сформированы</b>	Теоретическое содержание курса освоено частично, необходимые навыки работы не сформированы или сформированы отдельные из них, большинство предусмотренных рабочей учебной программой заданий не выполнено либо выполнено с грубыми ошибками, качество их выполнения оценено числом баллов, близким к минимуму.	Планируемые результаты обучения не достигнуты

## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ

Типовые контрольные задания или иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

### Вопросы к экзамену

**по дисциплине Управление доступом и технологии обеспечения безопасности БД.**

1. Что такое управление доступом к базам данных? Опишите основные принципы CIA (конфиденциальность, целостность, доступность).
2. Какие нормативные документы регулируют безопасность БД в России? Опишите их основные требования.
3. Какие типы угроз безопасности БД существуют? Приведите примеры и способы их минимизации.
4. Как принцип минимальных привилегий применяется в управлении доступом к БД? Примеры реализации.



5. Какие роли играют субъект и объект в моделях управления доступом? Опишите их взаимодействие.
6. Сравните модели управления доступом (RBAC, ABAC, DAC, MAC) по критериям гибкости и сложности реализации.
7. Как реализуется ролевая модель (RBAC) в PostgreSQL? Приведите пример настройки.
8. В чем преимущества атрибутной модели (ABAC) перед дискреционной (DAC)? Примеры сценариев применения.
9. Опишите мандатную модель (MAC) и её применение в высокозащищённых системах.
10. Какой подход к управлению доступом лучше использовать в корпоративной БД? Обоснуйте.
11. Какие методы аутентификации применяются в современных СУБД? Опишите их преимущества и недостатки.
12. Что такое многофакторная аутентификация (MFA)? Как её настроить в Microsoft SQL Server?
13. Как работает технология единого входа (SSO) в контексте СУБД? Примеры реализации.
14. Как осуществляется управление ролями и привилегиями в Oracle Database? Приведите пример SQL-запроса.
15. Какие риски связаны с использованием слабых паролей в СУБД? Меры их минимизации.
16. Что такое прозрачное шифрование данных (TDE)? Как оно реализуется в Oracle и SQL Server?
17. Опишите процесс шифрования столбцов в PostgreSQL. Какие стандарты шифрования используются?
18. Как российский стандарт ГОСТ 34.12-2015 применяется в защите БД? Сравните с AES.
19. Какие методы управления криптографическими ключами применяются в СУБД? Примеры.
20. Как криптографические методы помогают минимизировать риски утечек данных?
21. Какие функции выполняют SIEM-системы в мониторинге безопасности БД? Примеры (Splunk, Solar Security).
22. Как настроить аудит доступа в PostgreSQL? Приведите пример SQL-запроса для анализа логов.
23. Какие типы событий необходимо отслеживать при аудите БД? Обоснуйте.
24. Как анализ логов помогает выявить несанкционированный доступ? Приведите пример кейса.
25. Какие инструменты используются для автоматизации мониторинга БД? Сравните их возможности.
26. Опишите архитектуру систем IAM (на примере Microsoft Entra). Как они интегрируются с СУБД?
27. Какие функции выполняет Solar InRights в управлении доступом? Примеры сценариев.
28. Как системы IdM повышают безопасность БД? Приведите пример настройки.
29. Какие методы защиты от SQL-инъекций применяются в СУБД? Примеры реализации.
30. Как организовать защиту БД от DDoS-атак? Роль IAM-систем в этом процессе.
31. Какие современные киберугрозы наиболее опасны для БД (фишинг, вредоносное ПО, API-атаки)?
32. Проанализируйте кейс реальной утечки данных и предложите меры предотвращения.
33. Как защитить БД от атак на API? Примеры инструментов и методов.
34. Какие организационные меры помогают минимизировать риски киберугроз?
35. Как использовать результаты анализа угроз в коллективной разработке политики безопасности?
36. Опишите этапы разработки политики безопасности БД. Какие аспекты учитываются?

37. Как автоматизировать управление доступом в СУБД? Примеры инструментов.
38. Как организовать коллективную работу при разработке политики безопасности?.
39. Проанализируйте реальный инцидент безопасности БД и предложите улучшения политики.
40. Как нормативные требования влияют на разработку политики безопасности БД?

**Практические задания к экзамену  
по дисциплине Управление доступом и технологии обеспечения безопасности БД.**

1. Составьте перечень потенциальных угроз безопасности для базы данных интернет-магазина (например, SQL-инъекции, утечки данных). Разработайте рекомендации по их минимизации.
2. Изучите положения ФЗ-152 «О персональных данных» и составьте список требований к защите БД, содержащей персональные данные клиентов.
3. Проведите анализ принципов CIA (конфиденциальность, целостность, доступность) на примере реальной БД. Определите, какие меры защиты соответствуют каждому принципу.
4. Подготовьте отчет о роли нормативных документов (ГОСТ Р 57580) в обеспечении безопасности БД. Приведите примеры их применения.
5. Настройте ролевую модель доступа (RBAC) в PostgreSQL для трех пользователей: администратор, аналитик, гость. Определите привилегии для каждого.
6. Реализуйте атрибутную модель доступа (ABAC) в SQL Server, используя атрибуты (например, время доступа, IP-адрес). Проверьте работу модели.
7. Сравните дискреционную (DAC) и мандатную (MAC) модели управления доступом. Настройте DAC в PostgreSQL для таблицы с конфиденциальными данными.
8. Разработайте сценарий применения RBAC и ABAC для базы данных предприятия. Опишите, как модели дополняют друг друга.
9. Создайте SQL-скрипт для реализации ролей в Oracle Database с ограничением доступа к таблице сотрудников по отделам.
10. Настройте многофакторную аутентификацию (MFA) для доступа к Microsoft SQL Server с использованием пароля и сертификата.
11. Реализуйте механизм единого входа (SSO) для PostgreSQL, интегрированного с LDAP. Проверьте доступ для тестового пользователя.
12. Создайте SQL-скрипт для управления привилегиями в Oracle: назначьте пользователю права на чтение и запись в таблицу, затем отзовите права на запись.
13. Настройте аутентификацию на основе сертификатов в PostgreSQL. Проверьте доступ для пользователя с сертификатом.
14. Разработайте сценарий для ограничения доступа к БД по времени суток (например, доступ только с 9:00 до 18:00) в SQL Server.
15. Настройте прозрачное шифрование данных (TDE) в Microsoft SQL Server для базы данных. Проверьте защиту данных при экспорте.
16. Реализуйте шифрование столбца с конфиденциальными данными (например, номера кредитных карт) в PostgreSQL. Проверьте доступ к зашифрованным данным.
17. Создайте систему управления ключами шифрования в Oracle Database. Опишите процесс ротации ключей.
18. На основе ГОСТ 34.12-2015 реализуйте шифрование тестового набора данных в PostgreSQL с использованием внешнего криптографического модуля.
19. Проведите сравнительный анализ производительности БД с включенным и отключенным TDE в SQL Server. Подготовьте отчет.
20. Настройте аудит доступа к таблице в PostgreSQL. Создайте отчет о попытках несанкционированного доступа.
21. Реализуйте мониторинг активности пользователей в SQL Server с использованием встроенных инструментов аудита. Проанализируйте логи.
22. Настройте интеграцию PostgreSQL с SIEM-системой (например, Splunk) для анализа логов. Выявите подозрительные действия.
23. Напишите SQL-запрос для анализа логов аудита в Oracle Database, выявляющий попытки изменения данных.

24. Разработайте сценарий автоматического оповещения при обнаружении несанкционированного доступа в PostgreSQL.
25. Настройте интеграцию Microsoft Entra с SQL Server для управления доступом пользователей. Проверьте авторизацию.
26. Реализуйте управление идентификацией (IdM) в Solar InRights для базы данных PostgreSQL. Настройте роли для пользователей.
27. Разработайте сценарий интеграции IAM-системы с Oracle Database для автоматического управления учетными записями.
28. Проведите тестирование производительности БД при использовании IAM-системы (Solar InRights) для управления доступом.
29. Создайте документацию для настройки Microsoft Entra в контексте управления доступом к БД. Опишите этапы интеграции.
30. Реализуйте защиту от SQL-инъекций в PostgreSQL, используя параметризованные запросы. Проверьте устойчивость к тестовым атакам.
31. Настройте защиту БД от DDoS-атак с использованием фильтрации на уровне IAM-системы (Microsoft Entra).
32. Разработайте сценарий защиты от утечек данных в SQL Server с использованием маскирования данных.
33. Проведите анализ уязвимостей БД с помощью инструмента Kali Linux (например, sqlmap). Составьте отчет с рекомендациями.
34. Настройте ограничение доступа к БД по IP-адресам в PostgreSQL. Проверьте работу ограничений.
35. Проанализируйте кейс реальной утечки данных (например, из открытых источников). Разработайте план предотвращения.
36. Реализуйте защиту от фишинговых атак, направленных на кражу учетных данных для доступа к БД. Настройте MFA в Oracle.
37. Проведите симуляцию атаки вредоносного ПО на БД с использованием Kali Linux. Разработайте меры реагирования.
38. Настройте мониторинг API-запросов к БД для выявления подозрительной активности. Используйте SIEM-систему.
39. Разработайте сценарий реагирования на инцидент, связанный с компрометацией БД (например, ransomware).
40. Разработайте политику безопасности для базы данных предприятия, включающую RBAC, шифрование и аудит. Проверьте ее реализацию в PostgreSQL.
41. Создайте автоматизированный скрипт для проверки соответствия БД требованиям Ф3-152 (например, наличие шифрования, аудита).
42. Проведите аудит существующей политики безопасности БД. Предложите улучшения на основе анализа рисков.
43. Разработайте план резервного копирования и восстановления БД с учетом требований безопасности (Ф3-152).
44. Создайте UML-диаграмму для системы управления доступом к БД, включающую роли, привилегии и аудит.
45. Реализуйте программный код на C++ для проверки целостности данных в БД (например, вычисление хэша).
46. Разработайте сценарий автоматизации управления доступом в PostgreSQL с использованием скриптов на Python.
47. Проведите командный анализ кейса инцидента безопасности (например, утечка данных) и разработайте рекомендации.
48. Настройте политику ротации паролей для пользователей БД в SQL Server. Проверьте ее выполнение.
49. Реализуйте тестовую среду для проверки политики безопасности БД в VirtualBox. Опишите результаты.
50. Разработайте программу на C++ для мониторинга активности пользователей в БД, интегрированную с логами PostgreSQL.