Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

УТВЕРЖДАЮ
Директор УрТИСИ СибГУТИ
Минина Е.А.
«28» 11 2025 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ПО ДИСЦИПЛИНЕ
Б1.В.21 Методы и средства защиты баз данных

Направление подготовки / специальность: **09.03.01 «Информатика и вычислительная техника»**

Направленность (профиль) /специализация: **Инженерия программного обеспечения и искусственного интеллекта**

Форма обучения: **очная**

Год набора: 2026

Разработчик (-и):
ст.преподаватель _____ / М.Ю. Казанцев /
подпись

к.т.н., доцент _____ / Т.А. Черных /
подпись

Оценочные средства обсуждены и утверждены на заседании информационных систем и технологий (ИСТ)
Протокол от 27.11.2025 г. № 3
Заведующий кафедрой _____ / Д.И. Бурумбаев /
подпись

Екатеринбург, 2025

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

УТВЕРЖДАЮ
Директор УрТИСИ СибГУТИ
_____Минина Е.А.
«____» _____2025 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ПО ДИСЦИПЛИНЕ
Б1.В.21 Методы и средства защиты баз данных

Направление подготовки / специальность: **09.03.01 «Информатика и вычислительная техника»**

Направленность (профиль) /специализация: **Инженерия программного обеспечения и искусственного интеллекта**

Форма обучения: **очная**

Год набора: 2026

Разработчик (-и):
ст.преподаватель _____ / М.Ю. Казанцев /
подпись
к.т.н., доцент _____ / Т.А. Черных /
подпись

Оценочные средства обсуждены и утверждены на заседании информационных систем и технологий (ИСТ)
Протокол от 27.11.2025 г. № 3
Заведующий кафедрой _____ / Д.И. Бурумбаев /
подпись

Екатеринбург, 2025

1. Перечень компетенций и индикаторов их достижения

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенций	Этап	Предшествующие этапы (с указанием дисциплин/практик)
ПК 1 Способен проектировать и разрабатывать программное обеспечение	ПК 1.4 - Знает методы, средства и стандарты проектирования баз данных ПК 1.5 - Умеет применять методы и средства проектирования баз данных ПК 1.6 - Владеет навыками использования методов и средств проектирования баз данных	3	1 этап Б1.О.07 Программирование на языке Python Б1.О.17 Программирование на языке C# Б1.В.01 Web-технологии Б1.О.18 Программирование на языке C/C++ 2 этап Б1.О.11 Технологии баз данных Б1.В.15 Разработка интерактивных приложений Б1.В.22 Разработка на платформе JVM Б1.В.11 Разработка мобильных приложений Б2.О.02(П) Производственная технологическая практика
ПК 2 Способен выполнять работы и управлять работами по проектированию, созданию и модификации ИС	ПК 2.1 - Знает технологии, стандарты, применяемые для проектирования, создания и модификации информационных систем и баз данных ПК 2.2 - Умеет выполнять работы по проектированию, созданию и модификации информационных систем и баз данных ПК 2.3 - Владеет навыками проектирования, создания и модификации ИС и баз данных	2	1 этап Б1.О.11 Технологии баз данных

Форма итоговой аттестации по дисциплине – зачет

2. Показатели, критерии и шкалы оценивания компетенций

2.1 Показателем оценивания компетенций на этапе их формирования при изучении дисциплины является уровень их освоения.

Индикатор освоения компетенции	**Показатель оценивания**	**Критерий оценивания**
ПК 1.4 - Знает методы, средства и стандарты проектирования баз данных	Тест/опрос по темам защиты БД при проектировании: модели угроз, принципы CIA, RBAC/ABAC/DAC/MAC (на уровне понимания), политики доступа, классификация данных, методы защиты на уровне схемы (ограничения, представления), криптографические основы (хэширование/шифрование), стандарты и регламенты (152-ФЗ, локальные политики), журналирование и аудит	не менее 70% верных ответов; корректно объясняет основные методы защиты БД и их назначение; различает аутентификацию/авторизацию, роли/права, шифрование/хэширование; понимает связь требований закона/политик с проектными решениями
ПК 1.5 - Умеет применять методы и средства	Практические занятия: проектирование схемы с учетом безопасности (разделение данных, минимизация доступа), разработка ролей и прав (GRANT/REVOKE), применение представлений для ограничения доступа, настройка ограничений целостности, параметризация запросов (защита от SQL-инъекций), базовая настройка аудита	выбранные меры соответствуют модели угроз и требованиям; права настроены по принципу минимальных привилегий; запросы параметризованы; реализованы корректные ограничения/представления; решения воспроизводимы (скрипты/инструкции)
ПК 1.6 - Владеет навыками использования методов и средств проектирования баз данных	Мини-проект в рамках практических занятий: разработка «безопасной» БД (схема, роли, аудит), демонстрация сценариев доступа разных ролей, настройка резервного копирования/восстановления (при наличии темы), оформление документации (модель угроз, матрица доступа)	БД развернута и работает; реализована матрица доступа и роли; доступы проверены на тестовых сценариях (разрешено/запрещено); включено журналирование/аудит (в рамках курса); подготовлены скрипты и краткая документация
ПК 2.1 - Знает технологии, стандарты, применяемые для проектирования,	Экзаменационные вопросы/тест по технологиям защиты: механизмы СУБД (роли, схемы, привилегии, RLS), транзакции и изоляция как	не менее 70%; студент корректно описывает механизмы защиты в СУБД и типовые угрозы; знает, какие технологии применяются для обеспечения конфиденциальности/целостности/доступности

создания и модификации информационных систем и баз данных	фактор целостности, бэкапы и WAL/журналы (на уровне принципов), контроль изменений (миграции), стандарты безопасной разработки (OWASP Top 10 — на уровне SQL-injection), требования к хранению ПДн	
ПК 2.2 - Умеет выполнять работы по проектированию, созданию и модификации информационных систем и баз данных	Выполнение практических заданий: создание защищенной структуры БД (DDL), настройка ролей/политик, реализация миграций без потери прав/целостности, настройка бэкапов и восстановление на стенде, анализ инцидента (например, утечка через неверные права)	DDL/миграции применяются без ошибок; изменения не нарушают целостность и безопасность; права и политики сохраняются/обновляются корректно; бэкап/restore выполняется успешно; студент объясняет внесенные изменения и риски
ПК 2.3 - Владеет навыками проектирования, создания и модификации ИС и баз данных	Итоговый мини-проект: защищенная подсистема хранения данных (БД + правила доступа) для кейса (например, CRM/заказы): схема, роли, политики доступа, аудит, резервное копирование; демонстрация и защита	решение работоспособно и воспроизводимо; безопасность реализована комплексно (минимальные привилегии, разграничение доступа, защита типовых уязвимостей, аудит); продемонстрированы сценарии доступа и журналирование; есть документация (модель угроз, матрица прав, инструкции развертывания)

Шкала оценивания.

Зачет

Зачтено	Критерии оценки
«зачтено»	Студент демонстрирует сформированность компетенций ПК 1.4–ПК 1.6, ПК 2.1–ПК 2.3 на пороговом уровне и выше: знает типовые угрозы для БД и основные меры защиты (аутентификация/авторизация, роли и привилегии, принцип минимальных привилегий, ограничения целостности, представления/ограничение доступа к данным, базовые принципы криптографической защиты и хранения секретов, журналирование/аудит, резервное копирование и восстановление — в рамках курса). Умеет применять средства СУБД для разграничения доступа (GRANT/REVOKE, роли, политики доступа), корректно проектирует/модифицирует схему с учетом безопасности и целостности, выполняет практические задания без критических ошибок, оформляет скрипты/инструкции воспроизводимо и обосновывает принятые решения.

«не зачтено»	Компетенции ПК 1.4–ПК 1.6, ПК 2.1–ПК 2.3 не сформированы на пороговом уровне: студент не владеет базовыми понятиями и мерами защиты БД, не может объяснить типовые угрозы (например, SQL-инъекции, неверные права, утечки), допускает критические ошибки при настройке доступа (нет ролей/прав, избыточные привилегии, отсутствует разграничение), не обеспечивает целостность данных, не способен выполнить или воспроизвести практическое задание (скрипты не работают/отсутствуют), не может обосновать решения. Практические работы не выполнены или выполнены с критическими недочетами.

3. Методические материалы, определяющие процедуры оценивания по дисциплине

3.1. В ходе реализации дисциплины используются следующие формы и методы текущего контроля

Тема и/или раздел	**Формы/методы текущего контроля успеваемости**
ПК 1 Способен проектировать и разрабатывать программное обеспечение	
Криптографическая защита данных в БД и при передаче (TLS)	Самостоятельная работа, конспект лекции
Безопасная разработка и защита от SQL инъекций	Самостоятельная работа, конспект лекции
Применение pgcrypto для шифрования и хеширования полей, тестирование сценариев доступа	Практическая работа
ПК 2 Способен выполнять работы и управлять работами по проектированию, созданию и модификации ИС	
Угрозы и модель безопасности баз данных	Самостоятельная работа, конспект лекции
Архитектура защиты в PostgreSQL и основы hardening	Самостоятельная работа, конспект лекции
Разграничение доступа RBAC и принцип наименьших привилегий	Самостоятельная работа, конспект лекции
Контроль доступа на уровне строк и данных	Самостоятельная работа, конспект лекции
Аудит журналирование и мониторинг безопасности	Самостоятельная работа, конспект лекции
Резервное копирование восстановление и отказоустойчивость как часть защиты	Самостоятельная работа, конспект лекции
Построение модели угроз для БД сервиса и выбор приоритетных мер защиты	Практическая работа
Настройка безопасной аутентификации и сетевого доступа в PostgreSQL через pg_hba.conf и параметры сервера	Практическая работа
Реализация RBAC, создание ролей и выдача минимально необходимых прав для приложения и администраторов	Практическая работа
Настройка Row Level Security и проверка корректности политик на тестовых пользователях	Практическая работа
Защита чувствительных данных через представления и ограничение доступа к столбцам	Практическая работа

Настройка TLS для подключений и проверка шифрования канала между клиентом и PostgreSQL	Практическая работа
Включение логирования и аудита, настройка pgaudit и анализ журнала событий безопасности	Практическая работа
Резервное копирование и восстановление, pg_dump pg_restore, проверка восстановления и целостности данных	Практическая работа

3.2. Типовые материалы текущего контроля успеваемости обучающихся

ПК 1 Способен проектировать и разрабатывать программное обеспечение;
ПК 2 Способен выполнять работы и управлять работами по проектированию, созданию и модификации ИС

Пример задания на практическое занятие

Цель: Освоить настройку комплексной защиты базы данных PostgreSQL: разграничение доступа, защита чувствительных данных, шифрование канала, аудит и проверка сценариев нарушения доступа.

Задание: Настройка защиты БД сервиса «Заказы» в PostgreSQL

Задачи: Определение требований:

- Опишите функциональные требования к безопасности: роли (администратор, приложение, аналитик), ограничения доступа к заказам, доступ к чувствительным полям (телефон/адрес).

- Опишите нефункциональные требования: принцип минимальных привилегий, журналирование действий, шифрование соединения, воспроизводимость настройки (скрипты).

Проектирование:

- Опишите модель данных (таблицы users/orders) и определите, какие поля являются чувствительными.

- Составьте матрицу доступа (роль → разрешенные операции/объекты).

- Определите модель угроз (2–3 ключевые угрозы) и меры защиты под них.

Выбор технологий и средств:

- Определите средства PostgreSQL, которые будут использоваться: роли и привилегии (RBAC), RLS, VIEW, TLS, logging/pgaudit, pg_hba.conf.

- Определите формат поставки результата: SQL-скрипты + инструкция запуска.

Реализация:

- Создайте таблицы и тестовые данные.

- Создайте роли и настройте права (GRANT/REVOKE) по принципу минимальных привилегий.

- Настройте Row Level Security для таблицы заказов: пользователь видит только свои записи.

- Реализуйте ограничение доступа к чувствительным данным через VIEW для аналитика.

- Настройте TLS для подключений и убедитесь, что соединение шифруется.

- Включите логирование и аудит (logging и/или pgaudit) для ключевых событий.

Тестирование и проверка:

- Проверьте сценарии:
  - пользователь не видит чужие заказы;
  - аналитик не может читать телефон/адрес напрямую;
  - попытка запретной операции фиксируется в логах.

- Зафиксируйте результаты (вывод команд/скриншоты/фрагменты логов).

Документация:

- Подготовьте краткую документацию: как развернуть БД, применить скрипты, создать роли, проверить доступ и TLS.

Отчет:
Подготовьте отчет о выполненной работе, который включает:
- Описание требований и выбранных мер защиты.
- Матрицу доступа (роль → права).
- SQL-скрипты (или ссылку на репозиторий) и примеры команд проверки.
- Примеры логов/аудита при успешных и запрещенных действиях.
- Выводы о проделанной работе.

Типовые вопросы и задания к экзамену
1. Что такое модель угроз для БД? Примеры угроз (утечка, подмена, отказ, эскалация прав).
2. Принцип наименьших привилегий: как реализуется в PostgreSQL.
3. RBAC в PostgreSQL: роли, привилегии, схемы, права на таблицы/функции/представления.
4. Зачем нужны pg_hba.conf и методы аутентификации? Какие риски у «слишком открытого» доступа.
5. Row Level Security: назначение, что такое policy, типовые ошибки настройки.
6. Как ограничить доступ к отдельным столбцам (VIEW, отдельные таблицы, функции, маскирование).
7. TLS для PostgreSQL: зачем нужен, что защищает и как проверить, что соединение шифруется.
8. pgcrypto: для чего применяют шифрование и хеширование в БД; где нельзя хранить ключи.
9. Аудит и журналирование: зачем нужны, что фиксировать, базовая идея pgaudit.
10. Резервное копирование: pg_dump/pg_restore, что важно проверять при восстановлении.
11. SQL-инъекции: причины, примеры, защита (параметризация, права приложения, валидация).
12. Практическое задание: по описанию кейса настроить роли/права и показать, что «лишние» операции запрещены (скрипт + проверка).

Банк контрольных вопросов, заданий и иных материалов, используемых в процессе процедур текущего контроля и промежуточной аттестации находится в учебно-методическом комплексе дисциплины и/или представлен в электронной информационно-образовательной среде по URI: http://www.aup.uisi.ru.

3.3. Методические материалы проведения текущего контроля и промежуточной аттестации обучающихся

Перечень методических материалов для подготовки к текущему контролю и промежуточной аттестации:

1. Методические указания по выполнению практических занятий по дисциплине «Технологии командной разработки программного обеспечения». –URL: http://aup.uisi.ru/4629963/

2 Образовательная среда УрТИСИ СибГУТИ – URL: https://moodle.uisi.ru