МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Направление подготовки: 10.03.01 Информационная безопасность
Образовательная программа: "Информационная безопасность / Information security"

Дисциплина:
«*Информационная безопасность баз данных*»

КУРСОВАЯ РАБОТА

на тему *«Информационная система магазина техники Apple»*

Выполнил студент:
N3346 / ИББД_ТЗИ_N3 1.4
Бардышев Артём Антонович /_____
ФИО *Подпись*

Проверил:
Салихов Максим Русланович, преподаватель ФБИТ /_____
ФИО *Подпись*

_____
Отметка о выполнении (один из вариантов: отлично, хорошо, удовлетворительно)

_____
Дата

Санкт-Петербург
2025г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

ЗАДАНИЕ НА КУРСОВОЙ ПРОЕКТ

Студент Бардышев А.А.
(Фамилия, И., О.)

Факультет Безопастности информационных технологий

Группа N3346

Направление (специальность) 10.03.01 Информационная безопасность

Руководитель Салихов Максим Русланович, преподаватель ФБИТ
(Фамилия, И.О., должность, ученое звание, степень)

Дисциплина Информационная безопасность баз данных

Наименование темы ***Проектирование и реализация информационной системы магазина техники «Apple»***

Задание *Разработать защищенную базу данных и API-сервис для ИС «Магазин техники Apple» с механизмами аутентификации.*

Краткие методические указания Выполнить проектирование, реализацию и защиту БД в PostgreSQL (мониторинг, RBAC, шифрование). Разработать API-сервис с использованием ORM и настроить систему резервного копирования.

Содержание пояснительной записки Инфологическое моделирование; реализация БД в PostgreSQL; защита данных (мониторинг, RBAC, шифрование); реализация API-сервиса; резервное копирование и восстановление; анализ реализованных мер защиты.

Рекомендуемая литература Основы технологий баз данных: учебное пособие / Б. А. Новиков, Е. А. Горшкова, Н. Г. Графеева; под ред. Е. В. Рогова. — 2-е изд. — М.: ДМК Пресс, 2020. — 582 с.

Руководитель _____
Подпись, дата

Студент _____
Подпись, дата

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

ГРАФИК ВЫПОЛНЕНИЯ КУРСОВОГО ПРОЕКТА (РАБОТЫ)

Студент Бардышев Артём Антонович
(Фамилия, И.О.)
Факультет Безопасности информационных технологий
Группа N3346
Направление (специальность) 10.03.01 Информационная безопасность
Руководитель Салихов Максим Русланович, преподаватель ФБИТ
(Фамилия, И.О., место работы, должность, ученое звание, степень)
Дисциплина Информационная безопасность баз данных

Наименование темы Проектирование и реализация защищенной базы данных для информационной системы «Проката электросамокатов»

№ п/п	Наименование этапа	Дата завершения		Оценка и подпись руководителя
		Планируемая	Фактическая	
1	*Инфологическое моделирование баз данных по методу «сущность-связь»*	10.10.2025	10.10.2025	
2	Реализация БД в рамках СУБД	11.10.2025	10.10.2025	
3	Защита баз данных	15.10.2025	13.10.2025	
4	Реализация сервиса для взаимодействия с разработанной базой данных	17.10.2025	16.10.2025	
5	Резервирование БД и восстановление по контрольным точкам	20.10.2025	21.10.2025	

Руководитель _____
подпись, дата

Студент _____
подпись, дата

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

АННОТАЦИЯ НА КУРСОВОЙ ПРОЕКТ (РАБОТУ)

Студент Бардышев Артём Антонович
(Фамилия, И.О.)

Факультет Безопасности информационных технологий

Группа N3346

Направление (специальность) 10.03.01 Информационная безопасность

Руководитель Салихов Максим Русланович, преподаватель ФБИТ
(Фамилия, И.О., место работы, должность, ученое звание, степень)

Дисциплина Информационная безопасность баз данных

Наименование темы Проектирование и реализация защищенной базы данных для информационной системы «Магазин техники Apple»

ХАРАКТЕРИСТИКА КУРСОВОГО ПРОЕКТА (РАБОТЫ)

1. Цель и задачи работы

☒ Предложены студентом

☐ Сформулированы при участии студента

☐ Определены руководителем

2. Характер работы

☐ Расчет ☐ Конструирование

☒ Моделирование ☐ Другое,

4. Содержание работы

Выполнен полный цикл разработки: спроектирована и реализована в PostgreSQL база данных для ИС «Магазин техники Apple». Внедрены механизмы защиты (аудит, шифрование, RBAC) и отказоустойчивости (резервное копирование). Разработан API-сервис на Python/Flask с аутентификацией на основе JWT.

5. Выводы

*Разработана защищенная база данных и API-сервис для ИС «*Магазин техники Apple*». Практически подтверждена эффективность реализованных механизмов безопасности и процедур обеспечения отказоустойчивости.*

Студент_____
(подпись)

Руководитель_____
(подпись)

«___» _____2025г.

Содержание

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ACID (Atomicity, Consistency, Isolation, Durability) — свойства транзакций СУБД

API (Application Programming Interface) — программный интерфейс приложения

ACL (Access Control List) — матрица/список контроля доступа

AES (Advanced Encryption Standard) — симметричный алгоритм шифрования

Bcrypt — алгоритм хеширования паролей

БД — база данных

DDL (Data Definition Language) — язык определения данных

DML (Data Manipulation Language) — язык манипулирования данными

ER (Entity–Relationship) — модель «сущность–связь»

FK (Foreign Key) — внешний ключ

HTML — HyperText Markup Language

HTTP — HyperText Transfer Protocol

JSON / JSONB — форматы хранения структурированных данных

JWT (JSON Web Token) — токен для аутентификации

ORM (Object–Relational Mapping) — технология объектно-реляционного отображения

PK (Primary Key) — первичный ключ

PITR (Point-in-Time Recovery) — восстановление на определённый момент времени

RBAC (Role-Based Access Control) — ролевая модель разграничения доступа

REST — архитектурный стиль построения API

SQL (Structured Query Language) — язык структурированных запросов

TLS/SSL — протоколы защиты сетевого взаимодействия

UI (User Interface) — пользовательский интерфейс

WAL (Write-Ahead Logging) — журнал предзаписи в PostgreSQL

СУБД — система управления базами данных

ИБ — информационная безопасность

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аутентификация — процесс проверки подлинности пользователя путем сопоставления введённых учётных данных с сохранёнными в системе.

Авторизация — предоставление аутентифицированному пользователю прав на выполнение определённых операций в системе.

Инфологическая модель — концептуальное описание предметной области, включающее сущности, атрибуты и связи между ними, независимое от конкретной СУБД.

Физическая модель данных — модель, описывающая структуру данных в конкретной СУБД, включая таблицы, типы данных, индексы, связи и ограничения.

Нормализация — процесс устранения избыточности данных и логических аномалий путём приведения схемы данных к нормальным формам.

Резервное копирование — создание копии данных для их восстановления после сбоев, повреждения или удаления.

Контрольная точка восстановления (restore point) — именованная точка в журнале WAL PostgreSQL, позволяющая выполнить PITR.

Журнал WAL — последовательный лог изменений в PostgreSQL, гарантирующий надёжность транзакций и позволяющий выполнять восстановление.

Триггер — объект БД, автоматически выполняющий заданную логику при вставке, обновлении или удалении данных.

Триггерная функция — хранимая функция PL/pgSQL, вызываемая триггером и обрабатывающая событие изменения данных.

Шифрование — преобразование данных в недоступный для чтения формат с использованием ключа.

Хэширование — необратимое преобразование данных в фиксированный хеш, используемое для проверки подлинности паролей.

JWT-токен — компактный объект в формате JSON, содержащий закодированные сведения о пользователе и применяемый для аутентификации.

ORM-модель — класс языка программирования, соответствующий таблице в БД, обеспечивающий объектно-ориентированную работу с данными.

Роль СУБД — сущность PostgreSQL, определяющая набор привилегий и уровней доступа для учетных записей.

Представление (View) — виртуальная таблица, содержащая результаты выполнения SQL-запроса и применяемая для разграничения доступа.

Система логирования — механизм фиксации операций в БД, обеспечивающий контроль изменений и аудит безопасности.

Веб-сервис — серверная часть приложения, обрабатывающая запросы клиентов и предоставляющая данные по API.

ВВЕДЕНИЕ

Актуальность данной работы обусловлена необходимостью комплексного подхода к разработке и защите баз данных в современных ИС розничной торговли. Магазины бренда Apple предъявляют повышенные требования к качеству обслуживания и безопасности данных клиентов, а значит, инфраструктура должна включать надежные механизмы разграничения прав доступа, мониторинга операций, криптографической защиты и восстановления после сбоев.

Целью данной курсовой работы является проектирование, реализация и обеспечение безопасности базы данных для информационной системы розничной торговли техникой Apple, а также разработка сервиса для безопасного взаимодействия с БД.

Для достижения поставленной **цели** в работе решаются следующие задачи:

− Выполнить анализ предметной области и построить инфологическую модель данных по методу «сущность–связь».

− На основе инфологической модели разработать физическую структуру реляционной базы данных в СУБД PostgreSQL.

− Реализовать требования безопасности: мониторинг операций на основе триггеров, криптографическую защиту данных, ролевую модель управления доступом (RBAC)

− Разработать серверное приложение на базе Flask и SQLAlchemy для интерактивной работы с БД, реализовав безопасную аутентификацию и распределение прав ролей.

− Настроить механизмы резервного копирования и восстановление по контрольным точкам (PITR), обеспечивающие отказоустойчивость системы.

− Выполнить итоговый анализ безопасности и оценить эффективность внедрённых решений.

1 СИСТЕМНЫЙ АНАЛИЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ «APPLE STORE»

Разрабатываемая информационная система ориентирована на автоматизацию процессов розничной торговли фирменной техникой Apple. Предметная область включает продажу iPhone, iPad, MacBook, аксессуаров и сопутствующих устройств, а также управление заказами, оплатами и взаимодействием с клиентами. В отличие от классических розничных точек, Apple Store предполагает расширенный сервис, включающий предзаказы, оформленные онлайн, полный цикл покупки, а также обслуживание постоянных клиентов.

1.1 Описание процессов и задач

В ходе анализа были выделены основные бизнес-процессы:

1. Управление каталогом товаров:

- ведение списка моделей устройств и их характеристик;
- хранение актуальных цен;
- учёт остатка товара на складе.

2. Работа с клиентами:

- регистрация новых клиентов;
- ведение контактной информации;
- отображение истории заказов.

3. Оформление заказов:

- формирование заказа;
- расчёт итоговой суммы;
- присвоение статуса заказа (создан, оплачен, отправлен, отменён).

4. Финансовые операции:

- привязка платежей к заказам;
- контроль статуса платежа (pending, success, refunded).

5. Администрирование:

- управление учётными записями персонала (manager, admin);
- контроль доступа к таблицам.

Эти процессы формируют структуру будущей базы данных и определяют перечень сущностей.

1.2 Выделение сущностей и построение ER-диаграммы

На основе предметной области были выделены следующие сущности (лабораторная №1):

- Customer — информация о клиентах
- Product — товары магазина Apple
- Order — заказ пользователя
- OrderItem — состав заказа

– Payment — платежи по заказу

Связи между сущностями:

– Customer 1:M Order

– Order 1:M OrderItem

– Product 1:M OrderItem

– Order 1:M Payment

Связи полностью соответствуют принципам ER-моделирования и отражены в лабораторной работе №1 (инфологическая модель).

1.3 Приведение схемы отношений к третьей нормальной форме

Анализ лабораторной работы №1 показал:

– Все атрибуты атомарны → 1НФ выполнена.

– Во всех таблицах PK — простой → частичных зависимостей нет → 2НФ выполнена.

– Неключевые атрибуты не зависят друг от друга → 3НФ выполнена.

– Таким образом, схема логически корректна и пригодна для физической реализации.

1.4 Моделирование уровня представлений

В соответствии с потребителями информации (клиент, менеджер, администратор) спроектированы представления:

– Каталог товаров (для менеджера)

Содержит productid, название, цену, остаток.

– Заказы (для менеджера и администратора)

Содержит OrderID, дату, статус, сумму, клиента.

– Мои заказы (для клиента)

Фильтр по e-mail текущего авторизованного пользователя.

– Платежи (для менеджера/админа)

Содержит paymentid, сумму, статус и дату.

Эти представления были реализованы в ЛР №4.

2 РЕАЛИЗАЦИЯ БАЗЫ ДАННЫХ В РАМКАХ СУБД POSTRESQL

2.1 Обоснование выбора СУБД

Выбор PostgreSQL обусловлен следующими характеристиками:

- поддержка ACID-транзакций;
- развитые типы данных (Numeric, JSONB);
- высокая стабильность и отказоустойчивость;
- поддержка механизмов шифрования (pgcrypto);
- бесплатность и открытый код;
- встроенная модель ролей и привилегий (RBAC).

2.2 Создание и наполнение таблиц

Таблицы созданы на основе модели из ЛР №1 и полностью реализованы в ЛР №2. В БД apple_store созданы таблицы:

- product
- customer
- orders
- order_items
- payments

Эти таблицы наполнялись тестовыми данными для последующего тестирования CRUD-операций и формирования сервисов.

2.3 Реализация индексов и внешних ключей

Для оптимизации операций:

- Созданы FK между всеми связанными таблицами.
- Созданы индексы по ключевым полям: customerid, productid, orderid, paymentid.

Это обеспечило эффективные операции JOIN и быстрый доступ к данным.

2.4 Создание представлений

Представления реализованы на уровне веб-сервиса (ЛР №4):

- products
- orders
- payments
- my_orders

Они обеспечивают ограничение доступа в соответствии с ролью.

2.5 Создание представлений

Проводилось:

- через сервис в Flask;

- через прямые SQL-операции;
- через REST-эндпоинты.

Проверялись:

- корректность CRUD;
- валидация FK;
- отображение данных в HTML-шаблонах.

3 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БАЗЫ ДАННЫХ

3.1 Мониторинг операций в БД на основе триггеров

На основании ЛР №3 разработана полноценная система аудита:

- создана таблица action_log;
- реализована универсальная функция логирования old/new данных;
- созданы триггеры для всех таблиц: product, customer, orders, order_items, payments.

Фиксируются:

- тип операции;
- пользователь;
- время;
- старые данные;
- новые данные.

3.2 Шифрование конфиденциальных данных

Использовано:

- расширение pgcrypto;
- шифрование методом pgp_sym_encrypt;
- симметричный ключ хранится вне БД (по примеру ЛР №3 и ЛР №5).

Шифровались:

- API-ключи (для сервисов);
- чувствительная информация пользователей.

3.3 Ролевое разграничение доступа (RBAC)

Созданы роли:

- customer
- manager
- admin

На уровне сервиса (ЛР №4):

- customer видит только свои заказы
- manager видит товары, заказы, платежи
- admin может управлять каталогом (CRUD)

На уровне СУБД:

- каждая роль имеет строго ограниченный набор прав
- запрет прямого доступа к базовым таблицам
- разрешён доступ только к представлениям

4 РЕАЛИЗАЦИЯ СЕРВИСА ДЛЯ ВЗАИМОДЕЙСТВИЯ С БАЗОЙ ДАННЫХ

4.1 Обоснование выбора стека технологий

Стек подобран в ЛР №4:

- Flask — веб-фреймворк
- SQLAlchemy — ORM
- psycopg2-binary — драйвер PostgreSQL
- Flask-Login — аутентификация
- Jinja2 — шаблонизатор
- Bcrypt — безопасное хранение паролей

Этот стек обеспечивает высокую безопасность, модульность и расширяемость.

4.2 Архитектура сервиса и описание маршрутов

Архитектура:

- models_apple.py — ORM-модели
- auth.py — регистрация/логин/выход
- crud.py — операции с товарами
- app.py — маршруты, ACL, привязка ролей
- templates — HTML-интерфейс
- errors — страницы ошибок

Маршруты:

- /login, /register
- /products
- /orders
- /payments
- /my_orders

ACL реализован через декоратор **role_required**.

5 РЕЗЕРВИРОВАНИЕ БАЗЫ ДАННЫХ И ВОССТАНОВЛЕНИЕ

5.1 Создание резервной копии

В ЛР №5 реализовано:

– включение WAL:

wal_level = replica

archive_mode = on

archive_command

– создание ночного резервного копирования через PowerShell-скрипты

– использование pg_basebackup

5.2 Демонстрация восстановления

Проведено:

– создание restore point

– намеренное внесение ошибок: INSERT/UPDATE/DELETE

– восстановление на момент restore point

– проверка отката данных

Использован PITR и архив WAL-логов.

6 АУДИТ БЕЗОПАСНОСТИ РЕАЛИЗОВАННОГО РЕШЕНИЯ

6.1 Анализ реализованных мер защиты

Система защиты включает:

- аудит операций (триггеры)
- шифрование ключей
- модель ролей
- защищённый сервис Flask

6.2 Преимущества и недостатки

Преимущества:

- работа ACL
- невозможность SQL-инъекций через ORM
- полная история изменений

Недостатки:

- внутренние логи удаляются после восстановления (если не вынесены наружу)
- требуется HTTPS для защиты трафика
- JWT-токен нельзя отозвать немедленно (stateless)

6.3 Рекомендации

- использовать внешнюю SIEM
- включить SSL/TLS
- хранить аудиты вне БД
- использовать PITR постоянно
- внедрить blacklist JWT

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы была разработана и реализована комплексная система управления данными для информационной системы розничной торговли техникой Apple. В рамках проекта последовательно выполнены проектирование, реализация, защита и тестирование базы данных, а также разработка безопасного сервиса для взаимодействия с ней.

В результате решения поставленных задач были достигнуты следующие результаты:

1. **Построена инфологическая модель предметной области**, включающая сущности Product, Customer, Order, OrderItem и Payment, а также связи между ними. Модель была нормализована и приведена к третьей нормальной форме, что исключает избыточность данных и минимизирует логические аномалии.
2. **Реализована физическая база данных в PostgreSQL**, включающая структуры таблиц, внешние ключи, индексы и тестовое наполнение. База данных полностью соответствует требованиям предметной области и обеспечивает корректное выполнение бизнес-процессов магазина Apple.
3. **Внедрены механизмы защиты данных**, разработанные на основе лабораторной работы №3:
   - система аудита на базе триггеров фиксирует операции INSERT, UPDATE и DELETE;
   - реализовано шифрование конфиденциальных данных с использованием pgcrypto;
   - настроено ролевое разграничение доступа (RBAC), обеспечивающее безопасное разделение пользовательских прав.
4. **Разработан веб-сервис на Flask**, обеспечивающий взаимодействие клиентов, менеджеров и администраторов с базой данных. В сервисе реализованы механизмы аутентификации, матрица доступа, ACL, а также функциональность просмотра и управления данными. Использование ORM SQLAlchemy позволило исключить риски SQL-инъекций и повысить безопасность приложения.
5. **Настроены процедуры резервного копирования и восстановления**, включая архивирование WAL, создание контрольных точек и восстановление на определённый момент времени (PITR). Практически продемонстрирована возможность отката состояния базы данных к restore-point, что подтверждает устойчивость системы к ошибкам и повреждениям.
6. **Проведён итоговый аудит безопасности**, выявивший как сильные стороны решения (защищённая архитектура, корректно настроенная модель доступа, криптографическая защита, аудит операций), так и направления дальнейшего совершенствования (необходимость вынесения логов за пределы основной БД, использование TLS/SSL, внедрение черного списка JWT-токенов).

В целом разработанная база данных и сервис взаимодействия демонстрируют соответствие требованиям безопасности, устойчивость к основным угрозам и корректную

реализацию бизнес-процессов. Полученные в ходе работы результаты подтверждают эффективность применения ролевой модели, механизмов триггерного аудита, шифрования и резервного копирования в современных информационных системах розничной торговли.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Основы технологий баз данных: учебное пособие / Б. А. Новиков, Е. А. Горшкова, Н. Г. Графеева; под ред. Е. В. Рогова. — 2-е изд. — М.: ДМК Пресс, 2020. — 582 с.

2. Базы данных: Учебник для высших учебных заведений / Под ред. проф. А. Д. Хомоненко. — 6-е изд., доп. - СПб.: КОРОНА-Век, 2009. – 736 с.

3. Psycopg – PostgreSQL database adapter for Python : официальная документация [Электронный ресурс] / The Psycopg Team. – URL: https://www.psycopg.org/docs/ (дата обращения: 28.09.2025)

4. PostgreSQL 16 Documentation. F.28. pgcrypto. [Электронный ресурс] – URL: https://www.postgresql.org/docs/current/pgcrypto.html (дата обращения: 29.09.2025).

5. Официальная документация Flask [Электронный ресурс] – URL: https://flask.palletsprojects.com/ (дата обращения: 10.10.2025).

6. Официальная документация SQLAlchemy [Электронный ресурс] – URL: https://www.sqlalchemy.org/ (дата обращения: 10.10.2025).