МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»**

Кафедра теории функции и стохастического анализа

# РАЗРАБОТКА СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студента 2 курса 248 группы

направления 09.04.03 – Прикладная информатика

механико-математического факультета
Есипова Сергея Владимировича

Научный руководитель
доцент, к.ф-м.н., доцент _____ М.Г.Плешаков

Заведующий кафедрой
д.ф.м.н., доцент _____ С.П. Сидоров

Саратов 2025

**Введение.** В современном мире обеспечение безопасности становится все более актуальной задачей в различных сферах деятельности. Среди ключевых аспектов обеспечения безопасности выделяется контроль и управление доступом к физическим и информационным ресурсам. Создание эффективной системы контроля и управления доступом становится важной составляющей в защите активов, обеспечении безопасности персонала и ограничении несанкционированного доступа.

**Цель работы** состоит в изучении и анализе основных аспектов создания СКУД, их роли в обеспечении безопасности, а также в рассмотрении методов, технологий и компонентов, необходимых для разработки и внедрения подобных систем.

В рамках исследования будут рассмотрены основные принципы функционирования систем контроля и управления доступом, ключевые компоненты таких систем, технологии и методы их применения. Также будет проанализировано влияние СКУД на обеспечение безопасности в различных сферах, включая бизнес, государственные учреждения, промышленные объекты и другие.

**Задачи работы** включают в себя:

1. Изучение основных принципов систем контроля и управления доступом:
   - Анализ основных концепций и принципов, лежащих в основе функционирования систем контроля доступа.
2. Рассмотрение ключевых компонентов и технологий СКУД:
   - Исследование различных типов идентификации и аутентификации пользователей, включая биометрические методы и электронные ключи.
   - Анализ компонентов СКУД, таких как чтецы, контроллеры доступа, базы данных и программное обеспечение управления.
3. Изучение влияния систем контроля доступа на безопасность:
   - Оценка влияния внедрения СКУД на обеспечение безопасности в различных сферах, включая предприятия, образовательные учреждения, здравоохранение и другие.
4. Анализ современных тенденций и подходов к созданию СКУД:

   - Рассмотрение новейших технологий и инноваций в области систем контроля и управления доступом.
   - Выявление преимуществ и ограничений существующих подходов к реализации СКУД.
5. Формирование выводов и рекомендаций:
   - Обобщение полученных результатов и выработка рекомендаций по созданию, внедрению и оптимизации систем контроля и управления доступом.
6. Разработка собственного программного продукта.

Работа прошла апробацию на различных конференциях, в частности, на ежегодной студенческой конференции «Актуальные проблемы математики и механики», которую проводил механико-математический факультет СГУ в апреле 2025 года, в секции «Анализ данных», в XIII Международной молодежной научно-практической конференции «Математическое и компьютерное моделирование в экономике, страховании и управлении рисками», ноябрь 2024 года.

**Структура** данной работы состоит из следующих разделов.

- Поставлены цели и задачи работы, а также описываются возможные способы реализации.
- Спроектирована система контроля и управления доступом.
- Производится анализ существующих СКУД.
- Программная реализация СКУД на языке программирования Python и dart всех необходимых функций для полной работоспособности системы.

Работа прошла апробацию на различных конференциях, в частности, на ежегодной студенческой конференции "Актуальные проблемы математики и механики которую проводил механико-математический факультет СГУ в апреле 2025 года, в секции "Анализ данных в XIII Международной молодежной научно-практической конференции «Математическое и компьютерное моделирование в экономике, страховании и управлении рисками», ноябрь 2024 года.

**Основное содержание работы.**

**Основные принципы функционирования СКУД** включают в себя

идентификацию, аутентификацию и авторизацию. Идентификация представляет собой процесс определения личности или объекта, требующего доступа. Аутентификация подтверждает подлинность предъявленной идентификационной информации. Авторизация определяет разрешения на доступ в зависимости от идентифицированного и аутентифицированного пользователя или объекта.

СКУД базируются на концепциях идентификации, аутентификации и авторизации. Идентификация представляет собой процесс определения и подтверждения личности или объекта, требующего доступа к определенным ресурсам. Это может быть пользователь, сотрудник, посетитель или объект, чья идентификация необходима для определения разрешенного уровня доступа.

**Идентификация** осуществляется с помощью различных методов, включая использование карточных систем, биометрических данных например, отпечатки пальцев, сканы сетчатки глаза или распознавание лиц, или электронных ключей. Каждый из этих методов имеет свои преимущества и ограничения, но их цель состоит в том, чтобы достоверно установить личность или объект, запрашивающий доступ.

**Аутентификация** - это процесс проверки подлинности предъявленных идентификационных данных. СКУД используют различные методы подтверждения подлинности, такие как пароли, PIN-коды, биометрические сканы или двухфакторная аутентификация, чтобы обеспечить дополнительный уровень защиты и предотвратить несанкционированный доступ.

**Авторизация** определяет разрешения на доступ в зависимости от идентифицированного и аутентифицированного пользователя или объекта. Системы контроля доступа управляют правами доступа, определяя, какие пользователи имеют доступ к определенным зонам или ресурсам и на каких условиях.

СКУД часто интегрируются с другими системами безопасности, такими как системы видеонаблюдения или сигнализации. Это обеспечивает комплексный уровень защиты, позволяя системам взаимодействовать и реагировать на события безопасности более эффективно.

СКУД регистрируют события доступа, сохраняя журналы, которые содержат информацию о времени, местоположении и личности или объекте,

запрашивающем доступ.

СКУД находят широкое применение в различных сферах, включая бизнес, здравоохранение, образование и государственные учреждения.

**Анализ современных тенденций и подходов к созданию систем контроля доступа.** СКУД включает в себя использование искусственного интеллекта для анализа поведения пользователей, распознавание образов с помощью машинного зрения, а также разработку более точных и надежных биометрических систем.

Возникает все больший интерес к гибридным и облачным решениям. Это позволяет управлять доступом из удаленных точек, обеспечивает гибкость, масштабируемость и возможность интеграции с другими системами безопасности.

Современные системы контроля доступа стремятся к повышению адаптивности и удобства использования. Это включает в себя разработку более интуитивных интерфейсов, автоматизацию процессов, а также создание систем, способных адаптироваться к изменяющимся потребностям и условиям безопасности.

**Проектирование системы контроля и управления доступом.** Первоначальным этапом проектирования системы контроля и управления доступом является идентификация основных потребностей, которые требуется удовлетворить.

Этот этап проекта направлен на полное понимание основных потребностей, которые необходимо удовлетворить при создании системы контроля и управления доступом.

— Анализ безопасности объекта:
— Определение пользователей и их требований:
— Оценка функциональности системы:
— Документирование потребностей:

**Анализ функциональных требований.** Определение функциональных требований включает в себя выявление конкретных функций, которые система контроля доступа должна выполнять. Это может включать в себя:

— Идентификацию и аутентификацию.
— Управление доступом.

— Мониторинг и журналирование.

**Учет требований законодательства и приватности данных.** При анализе потребностей важно учитывать соответствие системы контроля доступа законодательству и нормативным актам, касающимся защиты данных. Это включает в себя требования GDPR, правила хранения и защиты личной информации, а также прочие местные и международные нормы в области безопасности данных.

**Проектирование системы контроля доступа.** Этот этап включает в себя разработку структуры системы СКУД, начиная с определения количества и расположения чтецов и считывателей. Определяются места, где будет осуществляться контроль доступа, учитывая потребности безопасности объекта. Также важным аспектом является выбор и настройка оборудования, архитектура сети передачи данных для обеспечения надежной и быстрой передачи информации.

**Интеграция с другими системами безопасности** предполагает совместную работу различных систем для создания единой системы обеспечения безопасности. Например, информация о доступе может использоваться совместно с данными систем видеонаблюдения для подтверждения личности пользователей при входе в защищенные зоны или для более точного мониторинга. Это также включает разработку интерфейсов для взаимодействия различных систем и синхронизацию данных для более эффективного контроля за безопасностью объекта.

**Анализ существующих систем контроля и управления доступом.** Современные системы контроля и управления доступом играют ключевую роль в обеспечении безопасности и защиты информации в различных организациях и учреждениях. С их помощью осуществляется контроль за перемещением сотрудников и посетителей, предотвращаются несанкционированные доступы, а также ведется учет рабочего времени. В условиях повышенного внимания к вопросам безопасности, особенно на фоне развития технологий и роста числа киберугроз, важность надежных и эффективных СКУД становится очевидной.

**Результат анализа** показывает, что каждая из компаний имеет свои сильные и слабые стороны. Основные направления для улучшения включают:

1. Снижение стоимости: Разработка экономически эффективных решений без ущерба для безопасности и функциональности может сделать системы более доступными для малого и среднего бизнеса.
2. Упрощение установки и настройки: Внедрение интуитивных инструментов для установки и настройки систем позволит снизить затраты на техническую поддержку и упростит процесс интеграции.
3. Улучшение интеграции: Разработка стандартных интерфейсов для более легкой интеграции с оборудованием и системами других производителей.
4. Расширение функциональных возможностей: Увеличение функциональности программного обеспечения, в том числе за счет внедрения аналитики и искусственного интеллекта.
5. Повышение надежности и безопасности: Регулярные обновления безопасности и внедрение резервных механизмов для обеспечения непрерывной работы системы.

**Разработка и создание собственной СКУД** на основе модулей Arduino является доступным и экономичным решением, которое позволяет реализовать широкий спектр функций безопасности. Arduino предоставляет гибкую платформу для разработки, что делает ее идеальным выбором для создания индивидуальных систем, адаптированных под конкретные требования.

**Необходимые модули и компоненты** для создания СКУД на основе Arduino:

1. Arduino Uno – микроконтроллер, который будет служить основой для управления всеми подключенными устройствами.
2. Модуль RFID RC522 – для считывания RFID-карт и меток, которые будут использоваться для идентификации пользователей.
3. Сервопривод – для управления замками и другими механическими устройствами.
4. Клавиатура 4x4 – для ввода паролей или PIN-кодов.
5. Дисплей LCD 16x2 с I2C интерфейсом – для отображения информации, такой как приветственные сообщения или статусы системы.
6. Реле модуль – для управления электроцепями, такими как включение

и выключение дверных замков.

7. Блок питания 5V – для питания всех компонентов системы.
8. Провода, разъемы и монтажная плата – для соединения всех компонентов между собой.

**Серверная часть** системы контроля управления доступом реализована с использованием языка Python и микрофреймворка Flask, который является легким, гибким и идеально подходящим для построения RESTful API. В качестве базы данных используется PostgreSQL, а подключение к ней осуществляется через модуль psycopg2. Также применено контейнеризованное окружение с использованием Docker. Такой подход был обусловлен рядом причин:

— Flask — это минималистичный и гибкий фреймворк для Python, который идеально подходит для построения RESTful API. Благодаря простоте интеграции с внешними модулями и высоким уровнем контроля, Flask позволяет точно реализовать логику обработки доступа, генерации QR-кодов и ведения логов.

— PostgreSQL — одна из самых надёжных и производительных СУБД с поддержкой транзакций, хранимых процедур и продвинутой работы с типами данных. Она подходит для хранения как регистрационных данных пользователей, так и метаданных QR-кодов и логов доступа.

— Docker позволяет создать изолированную среду для сервера и базы данных, что упрощает развертывание на любом Linux-сервере, обеспечивает повторяемость и надёжность в продакшн-среде.

Функциональность серверной части позволяет пользователям:

— Регистрацию и авторизацию пользователей.
  – POST /api/register — регистрация нового пользователя с хэшированием пароля по алгоритму SHA-256.
  – POST /api/login — аутентификация пользователя и генерация mock-токена в формате mock-token-<user_id> в реальной системе может быть JWT.

— Проверку доступа на основе сканируемого QR-кода.
  – POST /api/verify_qr — точка входа для мобильного приложения при сканировании QR-кода. Происходит разбор QR-строки, прове-

ряется срок действия кода, с опоставляется код с сохраненными в БД, сравнивается уровень доступа пользователя с требуемым и результат сохраняется в журнал access_logs.

— Генерацию QR-кодов с метаданными: организация, подразделение, уровень доступа, временная метка и подтверждающий код.
  – POST /api/generate_qr — создаёт QR-код по следующему шаблону: organization/department/timestamp/access-lvl/access_level/confirm_code

    Генерация сопровождается записью в таблицу qr_codes, чтобы позже обеспечить возможность сверки.
— Ведение журналов доступа access_logs с привязкой к пользователю и считанному QR-коду.
  – GET /api/access_logs — возвращает 100 последних записей из таблицы логов доступа с привязкой к пользователю и использованному QR-коду.
— Получение профиля пользователя и проверка его уровня доступа, отображение панели администратора в мобильном приложении.
  – GET /api/profile — получение профиля пользователя по токену из заголовка Authorization. Проверка токена реализована вручную и декодируется user_id.
  – POST /api/change_password — смена пароля с валидацией текущего пароля и обновлением его хэшированной версии в базе данных.

Каждый запрос, требующий авторизации, сопровождается токеном Bearer mock-token-<user_id> в заголовке. Хотя это не полноценная система токенов, она имитирует JWT и показывает принцип работы.

Обращение к базе изолировано функцией get_db_connection(), что улучшает читаемость кода и упростит переход на пул соединений в будущем например, через psycopg2.pool или SQLAlchemy.

Вся логика разнесена по маршрутам и снабжена проверками корректности входных данных, что исключает SQL-инъекции и снижает вероятность ошибок.

Разработанное серверное приложение выполняет все ключевые функции для работы СКУД, включая управление пользователями, верификацию

QR-кодов, хранение логов и базовую авторизацию. Простота архитектуры делает систему легко расширяемой, а выбранные технологии — проверенными и масштабируемыми.

**Мобильное приложение.** Основная функция данного приложения авторизация пользователя и сканирование QR-кода для доступа.

Входными данными является логин и пароль пользователя, QR-код.

Выходные данные: Авторизационные данные и результаты сканирования QR-кода.

Мобильное приложение было разработано на фреймворке Flutter, что позволило реализовать кроссплатформенное решение, работающее как на Android, так и на iOS. Основными причинами выбора Flutter стали:

— Быстрая разработка с возможностью "горячей перезагрузки";
— Богатая библиотека готовых UI-компонентов;
— Высокая производительность благодаря нативной компиляции;
— Возможность адаптации интерфейса под различные устройства.

Пользователи с уровнем доступа 9 и выше получают доступ к адмнпанели, где могут просматривать журнал сканирований. Запрос к API /api/access_logs возвращает список последних событий.

**Генератор QR-кодов.** Основной функцией является генерация уникальных кодов для посетителей и сохранение информации в базе данных.

Входными данными является информация о посетителе например, идентификатор посетителя, имя, время входа и выхода.

Выходные данные: Изображение QR-кода и запись в базе данных.

Данная программа создаёт каждые 5 минут создаёт новый QR-код, который содержит в себе следующую информацию:

1. Наименование организации
2. Подразделение
3. Время создания
4. Требуемый уровень доступа
5. Код подтверждения

В приложении были учтены все ранее разработанные требования к генерации QR-кодов, что обеспечивает безопасность, устойчивость к подделке и возможность последующего анализа сканирований.

При запуске приложение немедленно отправляет POST-запрос на серверный API /api/generate_qr, передавая следующую информацию:

— organization — имя организации

— department — название/номер отделения

— access_level — минимальный уровень доступа, требуемый для входа

В ответ сервер генерирует строку по шаблону, сохраняя её в базу данных и возвращает приложению, где она преобразуется в QR-изображение.

Экран максимально упрощён и содержит крупное изображение QR-кода, метку с датой и временем последнего обновления, автообновление без необходимости вручную перезапускать приложение.

Таким образом, генератор QR-кодов выполняет ключевую роль в системе доступа: он создаёт временные ключи с определённым уровнем допуска, которые валидируются при сканировании. Это позволяет системе контролировать потоки пользователей и вести журнал доступа в автоматическом режиме.

**Турникет с QR-код и RFID считывателем.** Данный турникет предполагает вывод QR-кода на дисплей для авторизации пользователей через мобильное приложение, также необходимо наличие RFID считывателя.

Данный раздел можно интегрировать не только с турникетом, но и другими методами реализации контроля доступа к примеру двери на электромагнитном замке.

Также для реализации данного функционала будут необходимы библиотеки – дополнительные программные модули для работы с RFID, дисплеем и другими компонентами. Например, библиотека MFRC522 для работы с RFID RC522 и библиотека LiquidCrystal_I2C для управления LCD дисплеем.

**Преимущества и недостатки создания собственной СКУД.**

**Преимущества:**

1. Экономичность: Создание системы на базе Arduino обходится значительно дешевле, чем покупка готовых решений.
2. Гибкость: Возможность адаптации системы под конкретные нужды и добавления новых функций.
3. Обучение: Процесс сборки и программирования системы способствует развитию навыков в области электроники и программирования.

**Недостатки:**

1. Время и усилия: Первичная сборка и настройка системы требуют значительного времени и усилий.
2. Поддержка: Отсутствие официальной технической поддержки, что может усложнить решение возникших проблем.

Создание собственной СКУД представляет собой полезный проект, который успешно реализован. Несмотря на некоторые ограничения, такая система может обеспечить необходимый уровень безопасности и контроля доступа при минимальных затратах. В дальнейшем, возможно расширение функциональности системы и ее интеграция с другими элементами безопасности, что позволит создать комплексное решение для различных объектов.

**Заключение.** В результате данной работы были изучены и проанализированны различные варианты СКУД, а также разработана собственная. Успешно достигнуты цели и реализованы поставленные задачи:

— изучены основные принципы систем контроля и управления доступом
— рассмотрены ключевые компоненты и технологии идентификации и аутентификации пользователей
— произвведён анализ потребностей и функциональных требований включая выбор методов идентификации, а также интеграции с другими системами безопасности
— Проведён анализ современных тенденций и подходов к созданию СКУД
— разработан сервер отвечающей за безопасность и логику всей системы, также реализующий функционал для корректной работы мобильных приложений
— разработано пользовательское мобильное приложение с дополнительным функционалом для администратора позволяющее удобное взаимодействие с пропускной системой и отслеживание времени входа и выхода пользователей
— разработано мобильное приложение создающее QR-коды с технологиями шифрования для повышения уровня безопасности

Дальнейшее развитие СКУД предполагает постоянное совершенствование, чтобы поддерживать эффективность и безопасность системы, соответствующей потребностям объекта, безопасности и удобства пользователей.