Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.78:681.17

ДУДКИНА
Екатерина Алексеевна

АЛГОРИТМЫ И СРЕДСТВА АВТОМАТИЗАЦИИ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

АВТОРЕФЕРАТ

диссертации на соискание степени магистра
по специальности 7-06-0611-07 Бизнес-аналитика и цифровой маркетинг
(профилизация «Бизнес-аналитика»)

Научный руководитель
канд.техн.наук, доцент
ПАРАМОНОВ Антон Иванович

Минск 2026

Работа выполнена на кафедре экономической информатики инженерно-экономического факультета учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель:	**ПАРАМОНОВ Антон Иванович**, заведующий кафедрой информационных систем и технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент
Рецензент:	**ЛЕВЧЕНЯ Жанна Брониславовна**, доцент кафедры проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент

Защита диссертации состоится «22» июня 2026 г. года в $9^{\underline{00}}$ часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. Платонова, 39 (5 корпус БГУИР), ауд. 806, тел. +375 (17) 293-22-88, E-mail: o.lavrova@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

Современные организации, включая образовательные учреждения, сталкиваются с возрастающими требованиями к обеспечению безопасности и эффективности процессов управления доступом. Традиционные методы контроля, такие как бумажные журналы посещений, ручная идентификация по документам или пропускам, обладают рядом существенных недостатков: низкая пропускная способность, высокая вероятность ошибок, обусловленных человеческим фактором, недостаточная защита персональных данных, отсутствие интеграции с информационными системами учёта рабочего времени и электронными журналами.

Наиболее часто встречающимися способами идентификации в системах контроля доступа являются использование электронных карт, QR-кодов, а также биометрических данных (отпечатки пальцев, сетчатка глаза, лицо). QR-коды получили широкое распространение благодаря низкой стоимости внедрения, простоте генерации и возможности использования на мобильных устройствах. Однако системы, основанные только на QR-кодах, остаются уязвимыми для компрометации идентификатора (фотографирование кода, его копирование). Биометрическая верификация по лицу, напротив, обеспечивает высокую степень достоверности, но требует вычислительных ресурсов и может давать сбои при изменении внешности.

Рассмотрение вопроса адаптивного обучения биометрических систем в процессе эксплуатации (Human-in-the-Loop) началось сравнительно недавно, и точные методики накопления вариаций внешности без переобучения нейросетевой модели в литературе практически отсутствуют.

На основании анализа существующих подходов возможно обоснование архитектуры двухфакторной системы контроля доступа, сочетающей идентификацию по динамическому QR-коду и верификацию по лицу с возможностью обучения через ручное подтверждение охранником. Применение такой методики позволяет выявить и устранить недостатки однокомпонентных систем, а также адаптироваться к изменениям внешности пользователей.

На сегодняшний день существует большое число работ в области автоматизации контроля доступа. Наиболее значимые результаты были получены российскими и белорусскими учёными, которые проводили исследования по разработке систем контроля и управления доступом (Т.А. Умарова, Я.Ю. Головко), по интеллектуальной обработке фотографий в системах доступа (А.В. Балдин, Д.В. Елисеев, Г.А. Савченко), по биометрической верификации личности на основе нейронных сетей (В.И. Васильев, И.Е. Панфилова, А.Е. Сулавко). Среди зарубежных авторов особый интерес вызывают работы Ф. Шроффа (FaceNet), Цзянь Дэна (ArcFace), а также исследования в области векторных баз данных и инференса нейросетей (ONNX Runtime, pgvector).

Разработка научных и технических основ проектирования двухфакторных биометрических систем контроля доступа, их программная реализация, тестирование и оценка эффективности доказывают актуальность темы.

Автор выражает благодарность научному руководителю Парамонову А.И., кандидату технических наук, доценту, а также коллективу кафедры за квалифицированную помощь и консультации во время подготовки магистерской диссертации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Традиционные методы контроля доступа (бумажные журналы, ручная проверка документов) характеризуются низкой пропускной способностью, высокой вероятностью ошибок, недостаточной защитой персональных данных и отсутствием интеграции с современными информационными системами. В условиях цифровой трансформации и роста требований к безопасности разработка интеллектуальных автоматизированных решений, сочетающих идентификацию по QR-кодам и биометрическую верификацию лица, является востребованной задачей для образовательных учреждений, офисных центров и других организаций.

Степень разработанности проблемы

Анализ существующих систем (QRPassport, QR-Gate, QR-Access) показал, что каждое из решений имеет ограничения: QRPassport требует замены инфраструктуры и может повлечь кадровые изменения, QR-Gate избыточен для малых учреждений, QR-Access не обеспечивает должной безопасности. Теоретические основы автоматизации СКУД рассмотрены в работах Умаровой, Балдина, Головко, Васильева и др. Однако вопросы адаптивного обучения биометрической системы в процессе эксплуатации (Human-in-the-Loop) остаются недостаточно проработанными, что определяет направление настоящего исследования.

Цель и задачи исследования

Целью работы является исследование алгоритмов и средств автоматизации контроля и управления доступом.

Поставленная цель работы определяет следующие задачи исследования:

– изучить современные технологии и методы автоматизации контроля доступа, выявить их преимущества и ограничения;

– провести сравнительный анализ существующих отраслевых решений, определить их сильные и слабые стороны;

– выявить текущие проблемы и ограничения, характерные для систем контроля доступа в различных сферах деятельности;

– определить функциональные и нефункциональные требования к разрабатываемой системе;

– разработать архитектуру системы, обеспечивающую взаимодействие между пользователем, устройствами идентификации и базой данных;

– построить модели объекта доступа и бизнес-процессов с использованием UML и IDEF0;

– разработать алгоритмы управления доступом, охватывающие регистрацию пользователей, генерацию QR-кодов и управление биометрическими шаблонами;

– реализовать алгоритмы контроля доступа, включающие детекцию лица, извлечение признаков, сравнение с эталонными шаблонами и принятие решения на основе пороговых значений с возможностью ручного подтверждения.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) ОСВО 7-06-0231-01-2023 специальности 7-06-0611-07 Бизнес-аналитика и цифровой маркетинг (профилизация «Бизнес-аналитика»).

Теоретическая и методологическая основа исследования

В основу диссертации легли методы системного анализа, функционального моделирования (IDEF0), объектно-ориентированного моделирования (UML), алгоритмизации процессов управления и контроля, а также современные подходы к распознаванию лиц с использованием нейросетевых моделей (ArcFace) и библиотек инференса (ONNX Runtime). Информационную базу составили научные публикации, технические нормативные правовые акты (Федеральный закон № 152-ФЗ «О персональных данных»), документация облачных сервисов (Firebase, Cloudinary) и векторного расширения PostgreSQL (pgvector).

Научная новизна, теоретическая и практическая значимость

Научная новизна заключается в разработке гибридной двухфакторной схемы контроля доступа, объединяющей идентификацию по QR-коду и биометрическую верификацию лица с возможностью дообучения через механизм Human-in-the-Loop. В отличие от статических систем, предложенный подход адаптируется к изменениям внешности пользователя (очки, причёска, мимика) без переобучения нейросетевой модели, накапливая вариации биометрических шаблонов в векторной базы данных. Теоретическая значимость состоит в формализации моделей объекта доступа и бизнес-процессов (UML, IDEF0), а также в разработке алгоритмов управления и контроля доступа для двухфакторной верификации. Практическая значимость заключается в создании готового прототипа, который может быть внедрён в школах, офисах и других учреждениях. Система не требует дорогостоящего оборудования (работает на стандартных ноутбуках с веб-камерами), а использование облачных сервисов (Firebase, Cloudinary) упрощает масштабирование и администрирование.

Основные положения, выносимые на защиту:

1 Разработанная двухфакторная схема контроля доступа, объединяющая идентификацию по QR-коду и биометрическую верификацию лица, позволяет

повысить безопасность по сравнению с системами, использующими только один из этих факторов.

2 Предложенный механизм обучения системы с участием охранника (Human-in-the-Loop) обеспечивает накопление вариаций лица (изменение причёски, очки, мимика) и повышение точности распознавания в процессе эксплуатации без переобучения нейросетевой модели.

3 Экспериментально подтверждено, что после трёх последовательных подтверждений охранником косинусное сходство для одного и того же пользователя возрастает с 14 % до 82 %, что позволяет системе перейти от режима ручного подтверждения к автоматическому распознаванию.

4 Система демонстрирует высокую устойчивость к посторонним объектам: при предъявлении лица другого человека сходство не превышает 3,3 %, изображения кошки и сгенерированного нейросетью лица блокируются, а при отсутствии лица детектор OpenCV возвращает ошибку «No face detected». Ни одного ложного положительного срабатывания на тестовой выборке не зафиксировано.

5 Разработанный прототип, включающий Android-приложение на Java и Kotlin-сервер на Ktor с интеграцией Firebase Realtime Database, Cloudinary, PostgreSQL + pgvector и ONNX Runtime, может быть внедрён в школах, офисах и других учреждениях без дорогостоящего оборудования.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на 61-й научной конференции аспирантов, магистрантов и студентов БГУИР (Минск, 2025), XIII Международной научно-практической конференции «Экономика устойчивого развития региона: инновации, финансовые аспекты, технологические драйверы развития в сфере туризма и гостеприимства» (Ялта, 2026), а также на XVII Всероссийской научно-технической конференции с международным участием «Информатика, управляющие системы, математическое и компьютерное моделирование» (Донецк, 2026). Отдельные положения диссертации могут быть использованы при преподавании курсов по проектированию информационных систем и бизнес-аналитике.

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 4 печатных работах: 2 статьи в сборниках материалов конференций, 2 публикации в материалах международных конференций. Общий объем публикаций по теме диссертации составляет 6 страниц.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, четырех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе приведен обзор современного состояния проблемы автоматизации контроля и управления доступом, а также рассмотрена

возможность разработки двухфакторных систем на основе QR-кодов и биометрической верификации лица.

Во второй главе представлены формализация модели объекта доступа для частной школы, моделирование бизнес-процессов в нотации IDEF0, а также разработка алгоритмов управления и контроля доступом.

В третьей главе представлены обоснование выбора технологического стека (Kotlin, Ktor, Firebase, PostgreSQL+pgvector, ONNX Runtime), инфологическая модель, архитектура программной реализации, а также алгоритмы управления и контроля доступа с механизмом обучения Human-in-the-Loop.

В четвертой главе приведены методика экспериментального тестирования, оценка эффективности распознавания и механизма накопления биометрических вариаций, анализ устойчивости к посторонним объектам и обработке ошибок.

В приложении представлены публикации автора.

Общий объем диссертационной работы составляет 63 страниц. Из них 50 страниц основного текста, 15 иллюстраций, 2 таблицы, библиографический список из 31 наименования, список собственных публикаций соискателя из 5 наименований, 2 приложения.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе приведен обзор современного состояния проблемы автоматизации контроля и управления доступом, а также рассмотрена возможность построения двухфакторных систем на основе QR-кодов и биометрической верификации лица.

Из анализа следует, что традиционные методы (бумажные журналы, ручная проверка документов) характеризуются низкой скоростью обработки, высокой вероятностью ошибок, недостаточной защитой персональных данных и отсутствием интеграции с современными информационными системами. Существующие отраслевые решения (QRPassport, QR-Gate, QR-Access) имеют ограничения, делающие их неоптимальными для использования в образовательных учреждениях. Выявлено, что системы, использующие только QR-коды, остаются уязвимыми для компрометации идентификатора, а биометрические системы без механизма адаптации требуют повторной регистрации при изменении внешности. Это обуславливает актуальность разработки двухфакторной системы с возможностью обучения.

Проанализированы особенности построения систем контроля доступа на основе QR-кодов и распознавания лиц. Рассмотрены модели электростатического разряда (HBM, MM, CDM) применительно к защите биометрических устройств, однако основное внимание уделено алгоритмическим и программным аспектам. Выявлено, что ключевой проблемой является отсутствие методик накопления вариаций внешности пользователя без переобучения нейросетевой модели.

Во второй главе представлена формализация модели объекта доступа для частной школы «Ломоносовский лицей», а также моделирование бизнес-процессов и разработка алгоритмов управления и контроля доступом.

Сущность предложенного подхода состоит в выделении категорий субъектов доступа (ученики, сотрудники, родители, охрана, администратор, разработчик) с указанием их ролевых характеристик и численности. Объектом доступа является центральный вход, оборудованный турникетом со считывателем QR-кодов и камерой биометрической верификации. На UML-диаграмме классов (рис. 1) отражены основные сущности: «Пользователь», «Биометрический шаблон», «QR-код», «Событие доступа», «Точка доступа», а также связи между ними (наследование, композиция, ассоциация).

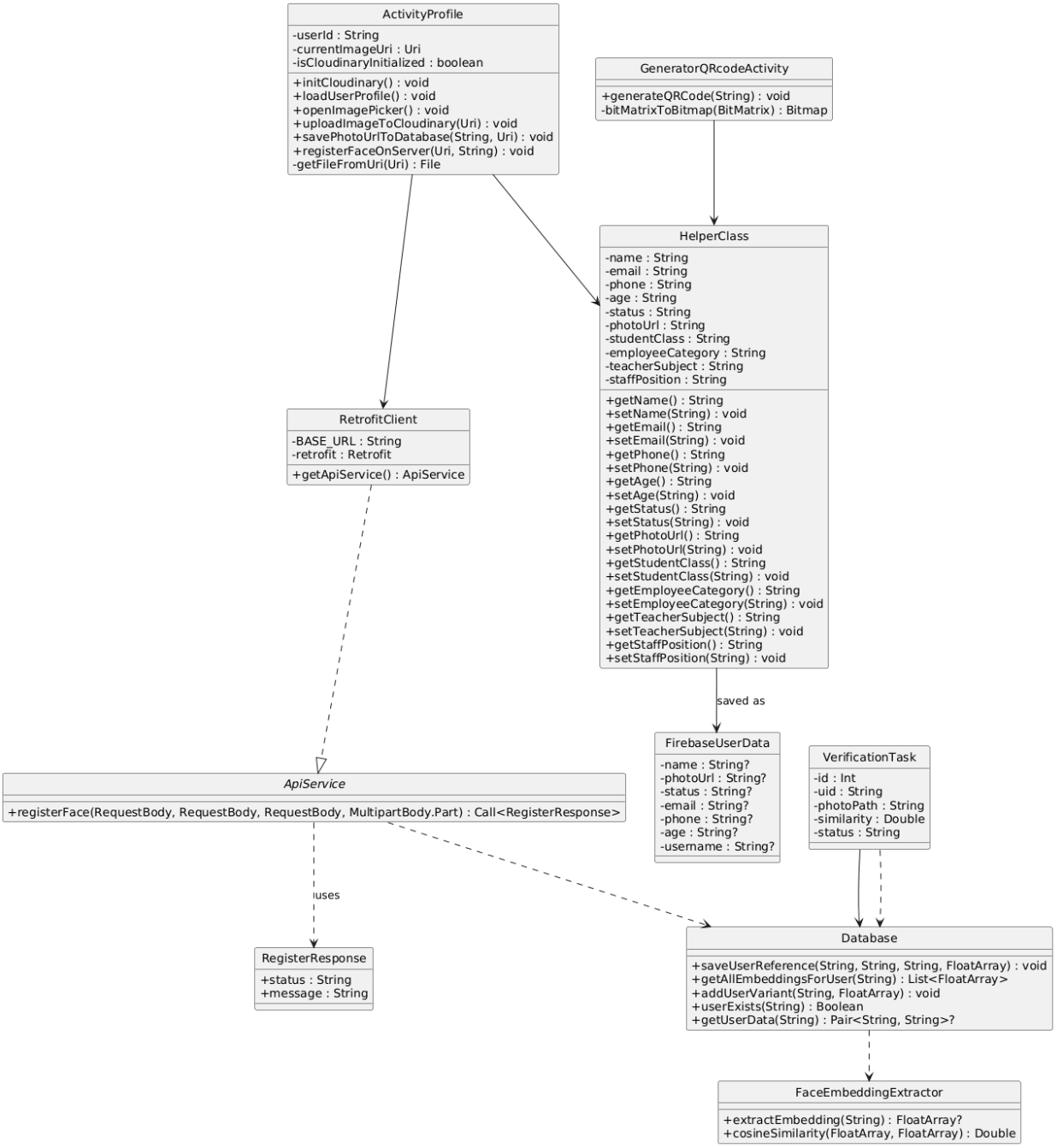


Рисунок 1 - UML - классов

Для формализации процедур контроля доступа применена методология IDEF0. Построена контекстная диаграмма A-0, определяющая границы системы и её взаимодействие с внешней средой: на вход поступают данные о пользователе, QR-код и текущее изображение лица; управление осуществляется Федеральным законом № 152-ФЗ и правилами лицея; выходами являются решение о допуске и запись в журнале событий. Декомпозиция контекстной диаграммы раскрывает последовательность четырёх взаимосвязанных функциональных блоков: регистрация пользователя, генерация QR-кода, идентификация по QR-коду и верификация по лицу. Такое моделирование позволило выявить узкие места существующей ручной процедуры и обосновать ожидаемые улучшения.

Разработаны детализированные алгоритмы управления доступом: регистрация пользователя (ввод персональных данных, выбор статуса, загрузка эталонного фото, создание биометрического шаблона), генерация динамического QR-кода (с синхронизацией времени, шифрованием и автоматическим обновлением каждые 60 секунд), проверка актуальности и прав доступа при сканировании, а также алгоритм управления биометрическими шаблонами (накопление векторов признаков при успешных проходах).

Алгоритмы контроля доступа реализуют двухфакторную верификацию: считывание и расшифровка QR-кода, извлечение UID и временной метки, поиск пользователя в Firebase, загрузка всех принадлежащих ему биометрических шаблонов (эталонного и накопленных вариаций), захват текущего изображения лица с камеры турникета, детекция лица с использованием каскадов Хаара OpenCV, предобработка (масштабирование до 112×112, нормализация), извлечение 512-мерного эмбеддинга через ONNX Runtime с моделью ArcFace, вычисление косинусного сходства с каждым шаблоном, принятие решения на основе двух пороговых значений (верхний порог 0,95, нижний 0,70). При попадании оценки в «серую зону» инициируется процедура ручного подтверждения охранником, и в случае положительного решения вектор признаков добавляется в коллекцию накопленных шаблонов.

В третьей главе представлены обоснование выбора технологического стека, инфологическая модель, архитектура программной реализации, а также детальная реализация алгоритмов управления и контроля доступа с механизмом обучения Human-in-the-Loop.

На основании анализа требований к производительности, безопасности и масштабируемости выбраны следующие технологии: язык Kotlin и фреймворк Ktor для серверной части (асинхронная неблокирующая модель на корутинах), Firebase Realtime Database для хранения профилей пользователей, PostgreSQL с расширением pgvector для векторного хранения эмбеддингов лиц, ONNX Runtime для инференса модели ArcFace на CPU, Cloudinary для хранения фотографий профиля. Клиентская часть реализована на Java (Android) с использованием библиотек ZXing (генерация QR-кодов), Retrofit (HTTP-клиент) и Firebase SDK.

Инфологическая модель включает сущности «Пользователь», «Фотография профиля», «QR-код», «Эмбеддинг лица» (эталонный и дополнительные вариации), «Задача на подтверждение», «Модель ONNX». Данные распределены между Firebase Realtime Database (профили пользователей в узле user_profiles/{uid}), Cloudinary (бинарные файлы фотографий), PostgreSQL (таблицы users и user_embeddings) и оперативной памятью сервера (список задач). Показано, что один пользователь может иметь один эталонный эмбеддинг и множество дополнительных вариаций (связь «один-ко-многим»). Задачи на подтверждение существуют только в оперативной памяти и теряются при перезапуске сервера, что допустимо из-за короткого жизненного цикла (несколько секунд).

Архитектура системы (компонентная диаграмма UML, рис. 3.1) включает Android-клиент (пользовательский интерфейс, Cloudinary Uploader, QR-генератор, HTTP-клиент) и Kotlin-сервер (REST API, FaceEmbeddingExtractor, Database Manager, Task Manager). Взаимодействие с внешними системами осуществляется через HTTPS (Firebase, Cloudinary), JDBC (PostgreSQL) и нативные вызовы (ONNX Runtime). Предложенная модульная организация обеспечивает независимость компонентов и упрощает их модернизацию.

Реализация алгоритмов управления доступом охватывает полный жизненный цикл пользователя: динамическую регистрацию с выбором роли («Ученик» или «Сотрудник») и дополнительных полей (класс, предмет, должность), валидацию ввода, генерацию уникального UID через Firebase Authentication, сохранение профиля в Firebase, загрузку эталонной фотографии в Cloudinary с регистрацией лица через эндпоинт /register-face, а также генерацию QR-кода на основе UID. Итоговое решение о доступе принимается только после биометрической верификации, что делает QR-код первым, но не единственным фактором.

Алгоритмы контроля доступа реализуют полный конвейер: захват изображения через веб-камеру, детекцию лица каскадами Хаара OpenCV, предобработку (вырезание области лица, масштабирование до 112×112, нормализация пикселей в диапазон [-1,1]), извлечение 512-мерного эмбеддинга через ONNX Runtime с моделью ArcFace, сравнение полученного вектора со всеми эмбеддингами пользователя (эталонным и ранее подтверждёнными вариациями) по косинусному сходству, выбор максимального значения. При превышении порога 0,65 доступ автоматически разрешается, в противном случае создаётся задача, и охранник может вручную подтвердить или отклонить доступ, а при подтверждении эмбеддинг текущего снимка добавляется в таблицу user_embeddings (механизм обучения Human-in-the-Loop). Отказоустойчивость обеспечивается блокировкой доступа при любых ошибках (отсутствие лица, сбои ONNX, проблемы с БД).

Функциональное тестирование подтвердило корректную работу всех сценариев: регистрация с динамическими полями, загрузка фото профиля, генерация QR-кода, сканирование и верификация через веб-интерфейс

охранника. Показано, что при низком сходстве (14 %) система требует подтверждения, при достижении порога 65 % выдает «ДОСТУП РАЗРЕШЁН», после обучения сходство возрастает до 78 % и 82 %. Время обработки одного запроса /verify составило 0,8–1,2 секунды на тестовой конфигурации (Intel Core i5, 16 ГБ RAM), что приемлемо для оперативного контроля доступа.

В четвертой главе представлены методика экспериментального тестирования, оценка эффективности распознавания и механизма накопления биометрических вариаций, а также анализ устойчивости к посторонним объектам и обработке ошибок.

Эксперимент проводился на одном добровольце (сотрудник). Эталонное изображение было загружено через Android-приложение. Тестовый набор состоял из четырёх снимков того же человека в различных условиях (изменённая причёска, очки, улыбка), а также изображений другого человека, кошки и сгенерированного нейросетью несуществующего лица.

Первый тестовый снимок дал косинусное сходство 14,0 %, система вернула статус need_verification (рис. 2).

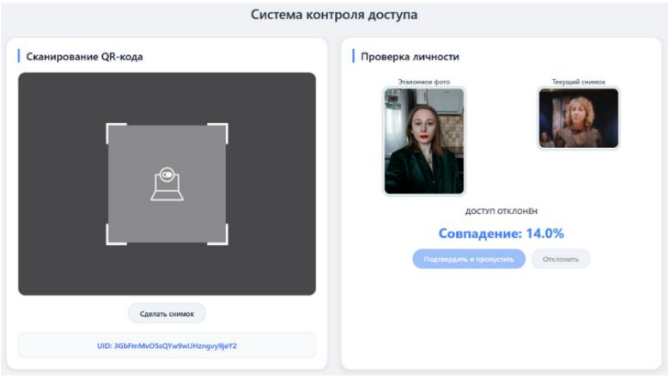


Рисунок 2 - Результат первичной верификации: низкое косинусное сходство (14,0 %)

После подтверждения охранником эмбеддинг был добавлен в user_embeddings. При следующем снимке сходство достигло 65,0 % (порог автоматического распознавания), доступ разрешён (рис. 3).

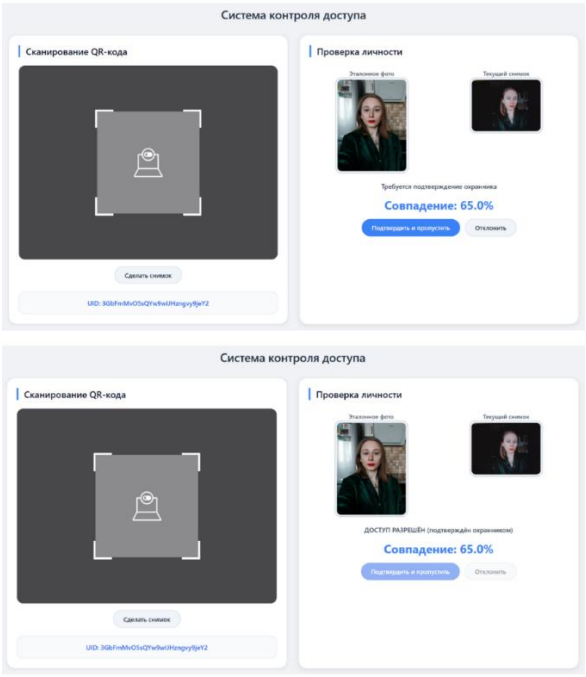


Рисунок 3 - Достижение порога автоматического распознавания (65,0 %): верхний фрагмент – требуется подтверждение охранника; нижний фрагмент – доступ разрешён после подтверждения

Последующие подтверждения повысили сходство до 78,4 % и 82,1 % (рис. 4).

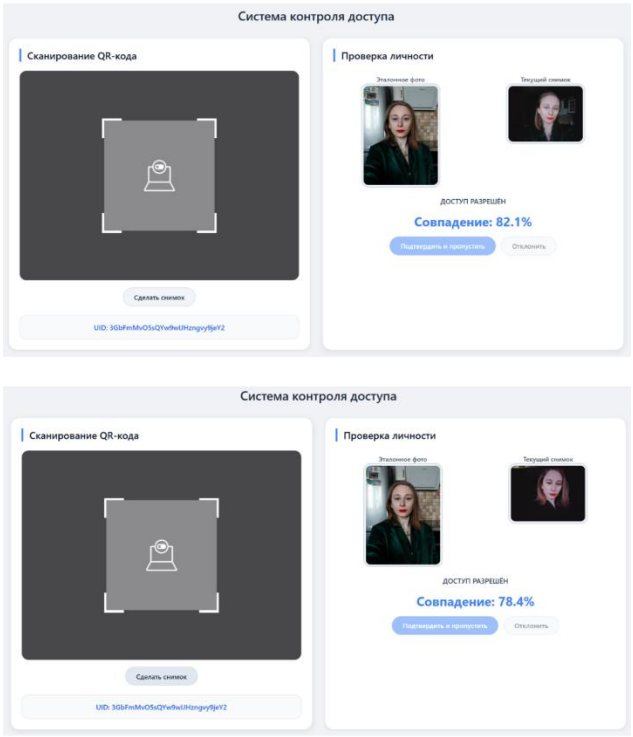


Рисунок 4 - Автоматическое распознавание после обучения: сходство 78,4 % и 82,1 %, доступ разрешён без участия охранника

Динамика роста максимального косинусного сходства в зависимости от количества подтверждений представлена на рисунке 5: уже после первого

подтверждения сходство увеличилось с 14 % до 65 %, а после третьего — до 82 %. Таким образом, механизм Human-in-the-Loop полностью реализован и эффективен.

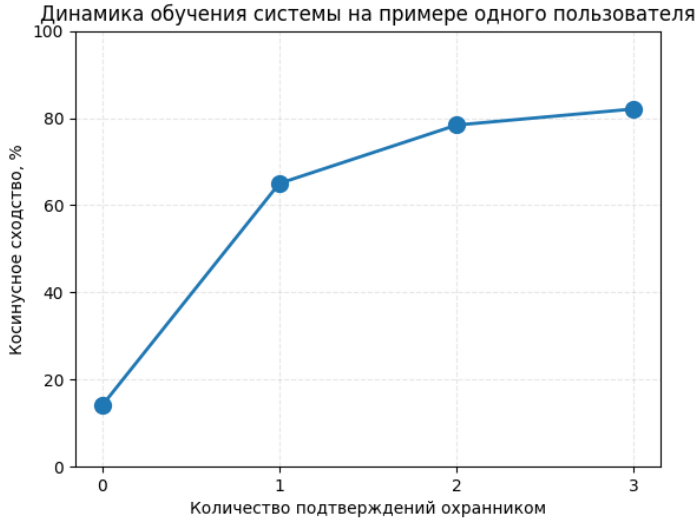


Рисунок 5 - Динамика роста максимального косинусного сходства в зависимости от количества подтверждений охранником

Проверка устойчивости к посторонним объектам показала: чужое лицо дало сходство 3,3 %, доступ отклонён; изображение кошки вызвало ошибку «No face detected». Ни одного ложного положительного срабатывания на тестовой выборке не зафиксировано.

При реализации программного прототипа использовались: среда разработки Android Studio, сервер на Kotlin/Ktor, база данных PostgreSQL 16 с pgvector, облачные сервисы Firebase и Cloudinary. Результаты моделирования и экспериментов подтверждают работоспособность и практическую пригодность разработанной системы.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1 Выполнен анализ существующих методов и технологий автоматизации контроля и управления доступом, включая системы на основе QR-кодов, биометрической верификации лица и облачных сервисов. Выявлено, что традиционные ручные методы (бумажные журналы, проверка документов) характеризуются низкой скоростью, высокой вероятностью ошибок и недостаточной защитой данных, а существующие отраслевые решения (QRPassport, QR-Gate, QR-Access) имеют ограничения, не позволяющие использовать их в образовательных учреждениях без доработок.

2 Разработана двухфакторная схема контроля доступа, объединяющая идентификацию по динамическому QR-коду и биометрическую верификацию лица с механизмом обучения Human-in-the-Loop. Предложены алгоритмы

управления доступом (регистрация пользователя, генерация QR-кода, проверка актуальности кода, управление биометрическими шаблонами) и контроля доступа (детекция лица, извлечение эмбеддинга через ONNX Runtime, сравнение по косинусному сходству, принятие решения на основе порога 0,65).

3 В результате реализации программного прототипа (Android-приложение на Java, Kotlin-сервер на Ktor, Firebase Realtime Database, PostgreSQL с расширением pgvector, ONNX Runtime, Cloudinary) экспериментально подтверждена эффективность механизма обучения: после трёх последовательных подтверждений охранником косинусное сходство для одного и того же пользователя возросло с 14 % до 82 %, что позволило системе перейти от ручного подтверждения к автоматическому распознаванию. Система продемонстрировала высокую устойчивость к посторонним объектам: чужое лицо дало сходство 3,3 %, изображения кошки и сгенерированного нейросетью лица были заблокированы, ложных положительных срабатываний не зафиксировано.

Рекомендации по практическому использованию результатов

1 Представленные в работе алгоритмы и программный прототип могут быть использованы для построения автоматизированных систем контроля доступа в образовательных учреждениях, офисных центрах и других организациях. Система не требует дорогостоящего оборудования и может функционировать на стандартных ноутбуках с веб-камерами, а использование облачных сервисов Firebase и Cloudinary обеспечивает простоту масштабирования и централизованного администрирования.

2 Результаты диссертации могут быть внедрены в учебный процесс на кафедрах, связанных с проектированием информационных систем, бизнес-аналитикой и цифровым маркетингом, в качестве материала для курсов по автоматизации бизнес-процессов, проектированию систем контроля доступа и применению технологий машинного обучения в задачах биометрической верификации.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в сборниках научных трудов

1 Dudkina, E. A. Innovative approaches to automating access control systems using QR technologies / E. A. Dudkina // Актуальные вопросы экономики и информационных технологий : сборник материалов докладов 61-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 20–25 апреля 2025 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2025. – С. 665–668.

2 Дудкина, Е. А. Философия цифровой эпохи: онтология, эпистемология и этика / Е. А. Дудкина // Компьютерные системы и сети : материалы 61-й научной конференции аспирантов, магистрантов и студентов, Минск, 22–26 апреля 2025

г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2025. – С. 521–522.

Тезисы конференций

3 Дудкина, Е.А. Интеллектуальные системы управления доступом для безопасности и устойчивого развития в сфере гостеприимства / Е.А. Дудкина // XIII Междунар. науч.-практ. конф. «Экономика устойчивого развития региона: инновации, финансовые аспекты, технологические драйверы развития в сфере туризма и гостеприимства», Ялта, 24–27 марта 2026 г.

4 Дудкина Е.А., Парамонов А.И. Автоматизация контроля и управления доступом на основе биометрической верификации по лицу., XVII Всерос. науч.-техн. конф. с междунар. участием «Информатика, управляющие системы, математическое и компьютерное моделирование-2026» (ИУСМКМ-2026), Донецк, 2026 г. : ДонНТУ, 2026.

5 Дудкина, Е. А. Интеллектуальные системы управления доступом для безопасности и устойчивого развития в сфере гостеприимства / Е. А. Дудкина, А. И. Парамонов // Экономика устойчивого развития региона: инновации, финансовые аспекты, технологические драйверы развития в сфере туризма и гостеприимства : Материалы XIII Международной научно-практической конференции, Симферополь, 24–27 марта 2026 года. – Симферополь: ООО "Издательство Типография "Ариал", 2026. – С. 156-159.