УДК 004.9:005.9;338.46

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ БЕЗОПАСНОСТИ И УСТОЙЧИВОГО РАЗВИТИЯ В СФЕРЕ ГОСТЕПРИИМСТВА

Дудкина Екатерина Алексеевна
магистрант,
Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Парамонов Антон Иванович
кандидат технических наук, доцент, Белорусский государственный университет информатики и радиоэлектроники, Институт информационных технологий, кафедра информационных систем и технологий,
г. Минск, Республика Беларусь

Аннотация. В данной статье рассматриваются вопросы разработки современной автоматизированной системы контроля и управления доступом с использованием двухфакторной аутентификации на основе динамических QR-кодов и биометрических данных. Предложены алгоритмы адаптивного распознавания лиц, предусматривающие накопление вариаций внешности и участие оператора в «серых» зонах для дообучения системы. Результаты исследования могут быть применены для создания надежных и масштабируемых пропускных систем в организациях различного типа.

Ключевые слова: контроль доступа, QR-код, биометрическая верификация, распознавание лиц, адаптивное обучение.

Развитие цифровых технологий оказывает кардинальное влияние на трансформацию многих сфер деятельности, включая обеспечение безопасности и управление доступом на различных объектах. Современные организации, сталкиваются с возрастающими требованиями к эффективности, надёжности и скорости идентификации лиц, которые имеют доступ на объект. Традиционные методы, основанные на бумажных журналах, ручной проверке документов или устаревших электронных пропусках характеризуются низкой пропускной способностью, высокой вероятностью ошибок, обусловленных человеческим фактором, недостаточной защитой персональных данных. Особую значимость приобретает разработка интеллектуальных автоматизированных решений, способных обеспечить не только надёжную идентификацию, но и адаптивность к изменяющимся условиям, масштабируемость и удобство для всех категорий пользователей. В современных условиях автоматизированные системы контроля и управления доступом (СКУД) становятся всё более распространёнными в образовательных учреждениях, офисах, корпоративных и частных организациях [1]. Внедрение современных технологий, таких как системы на основе QR-кодов для идентификации и контроля прохода, обеспечивают быструю обработку и передачу данных в информационную систему, что исключает проблемы ручного ввода и минимизирует риски утраты или подделки информации.

Анализ существующих отраслевых решений, таких как QRPassport [2], QR-Gate [3] и QR-Access, показал, что, несмотря на наличие функционала для прохода по QR-кодам, каждое из них имеет существенные ограничения. Глобально проблема автоматизации управления доступом связана с необходимостью разработки универсальных алгоритмов и средств, способных адаптироваться к различным условиям использования, учитывать специфику организации, масштабируемость системы, а также возможность интеграции с другими информационными платформами.

В работе поставлена цель – разработка СКУД на базе алгоритмов и современных средств автоматизации процессов управления доступом на объект. Достижение данной цели требует использования комплексного подхода.

Формирование требований к СКУД

Субъектами доступа являются физические лица, взаимодействующие с системой для получения разрешения на вход. Объектами доступа в рамках рассматриваемой задачи является вход в помещение, который предполагается оборудовать турникетной системой. Турникет оснащается считывателем QR-кодов и камерой для биометрической верификации. Пост охраны сохраняется для обработки нештатных ситуаций (сбой оборудования, отсутствие у пользователя мобильного устройства, визит родителей). Таким образом, физическая инфраструктура проектируемой системы предполагает одну точку доступа «центральный вход» и пост охраны как резервный канал подтверждения

личности; в перспективе возможно расширение набора объектов доступа (внутренние двери, кабинеты), однако в данной работе модель ограничивается контролем входа в здание.

Для обеспечения функционирования СКУД предполагается хранить следующие атрибуты субъектов доступа: идентификационные данные; контактные данные, используемые для уведомлений и восстановления доступа; ролевая принадлежность: статус (например, сотрудник), и детализации (например, должность – учитель, повар, охранник и т.п.); биометрические данные: эталонное изображение лица, загружаемое пользователем при регистрации в личном кабинете; учётные данные для входа в приложение; история событий доступа: временные метки и результат каждой попытки прохода (успех/отказ), а также отметки о ручном подтверждении охраной.

Моделирование СКУД

Процесс получения доступа строится на двухфакторной схеме идентификации, включающей последовательные этапы:

– идентификация по QR-коду: пользователь авторизуется в мобильном приложении, после чего генерируется динамический QR-код, содержащий зашифрованный идентификатор пользователя и временную метку; код предъявляется считывателю на турникете; система расшифровывает код, определяет личность и загружает соответствующий биометрический шаблон;

– верификация по лицу: камера, установленная на турникете, делает снимок лица предъявителя; алгоритм сравнивает полученное изображение с эталонным шаблоном, а также с накопленными вариациями; результат сравнения (оценка сходства) передаётся на сервер принятия решений.

Для защиты от повторного использования кодов предусмотрено автоматическое обновление QR-кода через заданные интервалы времени (каждые 60 секунд), что исключает возможность применения скриншота или ранее сохранённого изображения.

На начальном этапе внедрения, когда система ещё не накопила достаточное количество вариаций внешности пользователей, вводится механизм обучения с участием оператора. При сомнительном результате сравнения решение о допуске принимает сотрудник охраны. Он видит на мониторе эталонное фото из личного кабинета и текущее изображение с камеры, после чего подтверждает или отклоняет проход. В случае подтверждения система сохраняет новый снимок как дополнительный образец для данного пользователя. По мере накопления таких образцов точность распознавания повышается, и доля сомнительных случаев снижается. Этот процесс является ключевым элементом адаптивной биометрической верификации.

В отличие от алгоритмов контроля, которые осуществляют непосредственно верификацию личности в момент прохода, алгоритмы управления отвечают за подготовительные и регламентирующие функции: регистрация пользователей, генерация идентификаторов, назначение ограничений и поддержание актуальности учётных данных.

Алгоритмы контроля доступа составляют ядро разрабатываемой системы, обеспечивая непосредственную проверку личности пользователя в момент прохода через турникет. Процесс контроля доступа инициируется в момент, когда пользователь подносит смартфон с отображённым QR-кодом к считывателю на турникете. Последовательность выполняемых операций может быть представлена следующим образом:

1. Считывание и первичная обработка QR-кода.
2. Поиск пользователя и загрузка биометрических данных.
3. Захват текущего изображения лица. Если на изображении не удаётся обнаружить лицо (например, пользователь отвернулся или закрыл лицо), система выдаёт соответствующее сообщение и предлагает повторить попытку.
4. Детекция лица и извлечение признаков.
5. Вычисление степени сходства.

6. Принятие решения на основе пороговых значений.

7. Обработка ручного подтверждения.

Логика принятия решения на основе пороговых значений реализуется таким образом: если оценка сходства превышает заданный порог, то пользователь считается успешно верифицированным и турникет получает команду на открытие, событие доступа фиксируется в базе данных с результатом «успех», а текущее изображение добавляется в коллекцию шаблонов данного пользователя; если оценка оказывается ниже порога, то доступ запрещается и фиксируется событие «отказ», пользователю может быть предложено повторить попытку или обратиться к охране. При нажатии охранником кнопки «Подтвердить» доступ разрешается и турникет открывается, а событие фиксируется с пометкой «подтверждено охраной» и указанием идентификатора оператора. Текущее изображение добавляется в коллекцию шаблонов пользователя, что позволяет системе в будущем учитывать данную вариацию внешности.

Предложенные алгоритмы контроля доступа обеспечивают точность идентификации благодаря использованию современных методов распознавания лиц и двухфакторной схемы верификации. Постепенное накопление вариаций внешности пользователей повышает самостоятельность работы алгоритмов к изменениям причёски, наличию бороды, очков и других факторов, что делает систему удобной и надёжной в долгосрочной эксплуатации.

Выводы. Главная особенность разрабатываемой СКУД – это ее способность обучаться: она накапливает разные варианты внешности одного человека (например, с бородой или без, в очках и без них) и со временем начинает узнавать его точнее. На начальном этапе, если система сомневается, решение принимает сотрудник охраны, а удачные примеры сохраняются и используются для дообучения. Предложенный механизм обучения системы с участием оператора в «серой зоне» обеспечивает адаптацию к изменениям внешности пользователей и повышение точности распознавания в процессе эксплуатации.

Разработанные алгоритмы и прототип системы можно применять для построения автоматизированных СКУД в различных организациях. Результаты исследования могут быть использованы разработчиками, системными интеграторами и службами безопасности для повышения эффективности пропускного режима и защиты персональных данных.

Список использованных источников:

1. Boonkrong, S. Authentication and Access Control : Practical Cryptography Methods and Tools / S. Boonkrong. – Berkeley, CA : Apress, 2021. – 236 p.

2. QRPassport: умные пропуска и электронные сертификаты : [сайт]. – URL: https://www.qrpassport.tech

3. СКУД Гейт: автоматизация проходной по QR-коду : [сайт]. – URL: https://skd-gate.ru/