ТЕХНИКАЛЫҚ ҒЫЛЫМДАР ЖӘНЕ ТЕХНОЛОГИЯЛАР

УДК 004.8:004.5
МРНТИ 20.01.45

DOI: https://doi.org/10.37788/2026-2/86-92

А.Т. Берикова[1]*, М.М. Илипов[2]
[1]Казахский агротехнический университет имени С. Сейфуллина, Казахстан
(e-mail: aruzhan8787@gmail.com)

Интеллектуальная система контроля доступа на основе распознавания лиц и анализа поведения пользователя с использованием методов глубокого обучения

Аннотация.

Актуальность: Современные системы контроля доступа уже не справляются с требованиями к безопасности, если опираются только на пароли, PIN-коды и другие классические способы аутентификации. Такие методы легко украсть, подобрать или передать другим людям, поэтому они становятся слабым звеном защиты. На этом фоне особенно востребованы решения, которые используют биометрию и умеют «понимать» поведение пользователя, а не только сверять введённые данные.

Цель: В работе создаётся программная система, которая не просто идентифицирует человека по биометрическим признакам, но и оценивает, насколько типично он себя ведёт при попытке входа. Задача состоит в том, чтобы получить инструмент, способный вовремя заметить подозрительную активность и автоматически усилить защиту.

Методы: В качестве технической основы выбраны методы компьютерного зрения и глубокого обучения, которые применяются для распознавания лиц в видеопотоке. Дополнительно используется модуль поведенческого анализа, отслеживающий последовательность и частоту попыток входа, время и контекст доступа. Система структурирована на несколько взаимосвязанных модулей: распознавание лиц, проверка прав по времени и зоне, оценка уровня риска.

Результаты: Разработанный прототип показывает, что сочетание биометрии и поведенческих признаков позволяет заметно повысить качество контроля доступа. Если количество ошибок или необычных действий превышает заданный порог, система автоматически блокирует пользователя и запускает тревожный сценарий. Такой подход уменьшает вероятность несанкционированного входа и снижает нагрузку на администратора безопасности за счёт частичной автоматизации реагирования.

Научная новизна: Предложенная система объединяет распознавание лиц и поведенческий анализ не как два отдельных слоя защиты, а как элементы единой архитектуры принятия решения. Это позволяет одновременно учитывать биометрические характеристики пользователя и контекст его действий – от времени и места доступа до паттернов неудачных попыток. Такой интегрированный подход формирует более гибкий и «умный» контур безопасности по сравнению с классическими однофакторными решениями.

Ключевые слова: распознавание лиц, контроль доступа, поведенческий анализ, биометрия, компьютерное зрение, глубокое обучение, Python.

Введение

В условиях быстрого развития цифровых технологий и возрастания требований к информационной и физической безопасности особую актуальность приобретают системы контроля доступа. Традиционные методы аутентификации – пароли и PIN-коды – обладают рядом существенных недостатков: они подвержены утечкам, могут быть утрачены или переданы третьим лицам. В связи с этим всё большее распространение получают биометрические технологии, в частности системы распознавания лиц, обеспечивающие бесконтактную и более надёжную идентификацию пользователей [1].

Вместе с тем применение единственного биометрического признака не всегда гарантирует достаточный уровень защиты, что обусловливает необходимость интеграции

распознавания лиц с анализом поведения пользователя. Поведенческий анализ позволяет выявлять аномальные действия: попытки несанкционированного доступа, вход в запрещённые зоны или активность в нерабочее время [2]. Нормативные аспекты управления правами доступа также требуют учёта соответствующих ограничений, что подтверждается современными подходами к биометрической идентификации [3]. Совместное применение биометрии и поведенческой аналитики повышает надёжность системы и снижает вероятность ошибок первого и второго рода [4].

Целью данной работы является разработка интеллектуальной системы контроля доступа на основе совместного использования распознавания лиц и анализа поведения пользователя. Для её достижения поставлены следующие задачи: провести анализ современных методов биометрической идентификации; исследовать подходы к поведенческому анализу; разработать архитектуру системы; реализовать программную модель и оценить её эффективность. В разработанной системе используются библиотеки компьютерного зрения для распознавания лиц, а также модуль поведенческого анализа, учитывающий количество неудачных попыток входа и другие факторы риска [5]. Дополнительно реализована верификация по времени и зоне доступа, что позволяет принимать во внимание контекст использования системы [6].

Методы и материалы

В рамках данного исследования разработана интеллектуальная система контроля доступа на основе методов распознавания лиц и анализа поведения пользователя. Основными инструментами реализации послужили язык программирования Python и библиотеки компьютерного зрения – OpenCV и face_recognition. Основу системы составляет алгоритм распознавания лиц, реализованный с использованием библиотеки face_recognition.

Процесс распознавания включает следующие этапы: захват изображения с камеры; обнаружение лица посредством HOG-детектора; извлечение 128-мерного вектора признаков; сравнение с базой данных известных пользователей по евклидову расстоянию. При нахождении совпадения в пределах установленного порогового значения определяется имя пользователя, в противном случае в доступе отказывается.

Дополнительно в системе реализован метод поведенческого анализа, основанный на отслеживании действий пользователя: по мере накопления неудачных попыток входа система последовательно повышает уровень риска (низкий → средний → высокий → критический) и при достижении критического порога блокирует учётную запись, активируя сигнал тревоги. Для реализации системы использовались: веб-камера, персональный компьютер под управлением Windows 10, библиотеки OpenCV и face_recognition, стандартные библиотеки Python. База данных пользователей представлена в виде словаря, содержащего имя, роль, доступные зоны и временны́е ограничения. Сбор данных осуществляется в реальном времени: при запуске системы захватывается видеопоток, извлекается кадр, изображение преобразуется в формат RGB, после чего выполняется поиск и идентификация лиц. Функция проверки прав доступа показана на рисунке 1.

```
def check_access(user, zone):

    if user is None:
        return False, "Нет в базе"

    if user["zone"] != zone and user["zone"] != "all":
        return False, "Нет доступа в эту зону"

    hour = datetime.now().hour

    if hour < user["time_start"]:
        return False, "Рано"

    if hour > user["time_end"]:
        return False, "Поздно"

    return True, "Доступ разрешён"
```

Рисунок 1. – Функция проверки прав доступа

Все действия пользователей сохраняются в журнале для последующего ретроспективного анализа и выявления аномалий. Итоговый набор функций системы включает: успешный вход, отказ в доступе по зоне, отказ по времени и блокировку пользователя.

Результаты и их обсуждение

В ходе исследования реализована интеллектуальная система контроля доступа, объединяющая распознавание лиц и анализ поведения пользователя. В процессе тестирования система продемонстрировала стабильную работу в четырёх ключевых сценариях.

1. Успешная идентификация пользователя. При корректном распознавании лица и наличии необходимых прав система разрешает вход. В журнале зафиксировано значительное число успешных попыток доступа, как показано на рисунке 2.

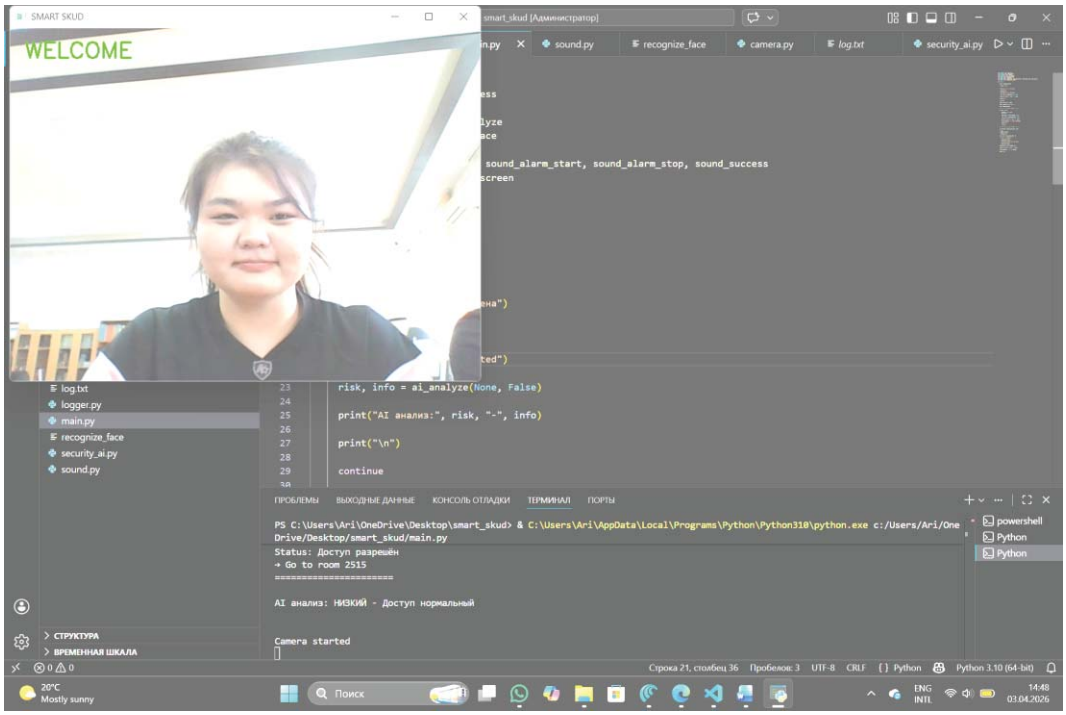

Рисунок 2. – Журнал успешной авторизации

2. Отказ в доступе по зоне. При попытке входа в запрещённую зону система корректно отклоняет запрос без увеличения счётчика риска, поскольку личность пользователя уже подтверждена, как показано на рисунке 3.

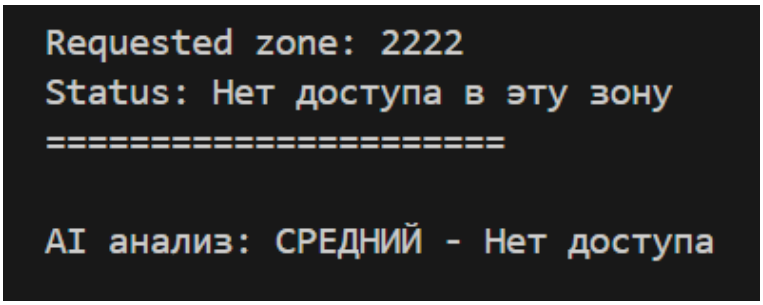

Рисунок 3. – Отказ в доступе по зоне

3. Отказ в доступе по времени. Система учитывает временные ограничения и блокирует вход вне разрешённого периода, возвращая сообщение об отказе с указанием причины, как показано на рисунке 4.

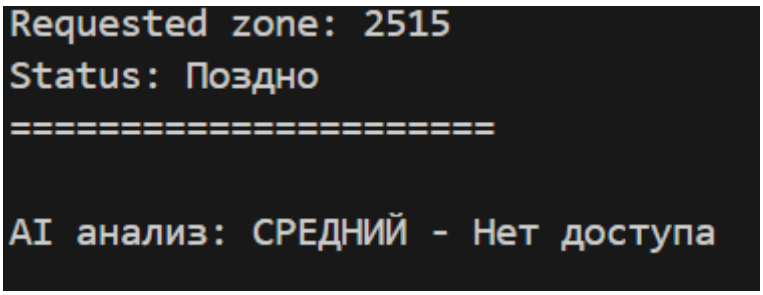

Рисунок 4. – Отказ в доступе по времени

4. Неуспешное распознавание лица. При отсутствии совпадения в базе данных система фиксирует ошибку и увеличивает счётчик риска, как показано на рисунке 5.

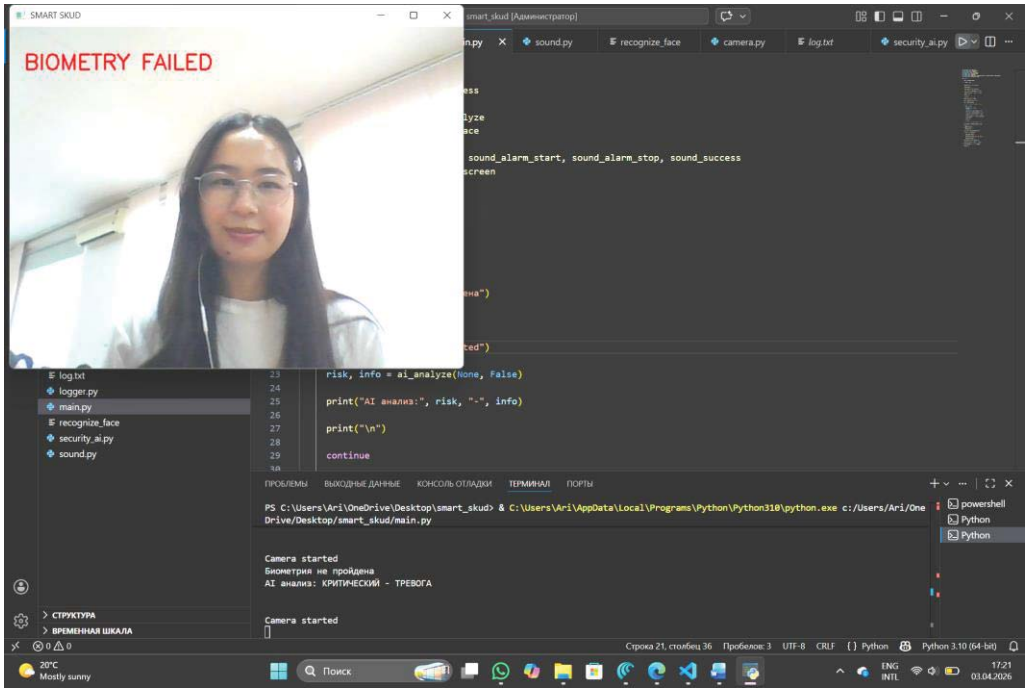

Рисунок 5. – Неуспешное распознавание лица

Процесс распознавания лица реализован в виде, представленном на рисунках 6 и 7. Алгоритм итерирует по всем областям лиц в текущем кадре, вычисляет совпадения с эталонными дескрипторами и извлекает имя пользователя при выполнении условия допуска.

```
faces = face_recognition.face_locations(rgb)
```

Рисунок 6 – Фрагмент кода распознавания лиц (часть 1)

```
encodings = face_recognition.face_encodings(rgb, faces)
```

Рисунок 7. – Фрагмент кода распознавания лиц (часть 2)

При обнаружении совпадения доступ предоставляется и событие регистрируется в журнале, как показано на рисунке 8.

```
result = face_recognition.compare_faces(
    [enc[0]],
    cam_encoding,
    tolerance=0.5
)
```

Рисунок 8. – Совпадение найдено: доступ разрешён

Логика поведенческого анализа и активации сигнала тревоги представлена на рисунке 9. Система последовательно отслеживает накопленное число ошибочных попыток и при достижении критического порога автоматически переходит в режим блокировки.

```
if name is None:

    attempts += 1

    if attempts == 1:
        return "СРЕДНИЙ", "Лицо не найдено"

    if attempts == 2:
        return "ВЫСОКИЙ", "Подозрительное поведение"

    if attempts >= 3:
        blocked = True
        return "КРИТИЧЕСКИЙ", "ТРЕВОГА"
```

Рисунок 9. – Поведенческий анализ и логика сигнализации

Полученные результаты свидетельствуют о том, что разработанная система эффективно распознаёт пользователей, корректно ограничивает доступ по времени и зонам, успешно обнаруживает подозрительное поведение и автоматически реагирует на угрозы. Особую значимость представляет поведенческий анализ, который существенно расширяет возможности классических биометрических систем, учитывая контекст действий пользователя. Таким образом, результаты эксперимента подтверждают эффективность разработанного подхода: объединение распознавания лиц и анализа поведения позволяет повысить надёжность контроля доступа и снизить вероятность несанкционированного входа.

Заключение

В данной работе разработана интеллектуальная система контроля доступа на основе методов распознавания лиц и анализа поведения пользователя. В ходе исследования рассмотрены современные подходы к биометрической идентификации и поведенческой аналитике, реализована программная модель, объединяющая указанные технологии в единую систему. Результаты экспериментов подтвердили корректность идентификации пользователей и эффективность управления доступом с учётом временных ограничений и зон.

Реализация поведенческого анализа повысила уровень безопасности за счёт своевременного выявления подозрительных действий и автоматической блокировки при превышении порогового числа ошибок. Практическая значимость работы определяется возможностью внедрения системы в учебных заведениях, офисах, на производственных предприятиях и иных объектах, требующих надёжного контроля доступа. Применение биометрических технологий повышает удобство пользователей и снижает зависимость от традиционных средств аутентификации.

Научная новизна состоит в интеграции методов распознавания лиц и поведенческого анализа в единой системе принятия решений о допуске, что позволяет одновременно учитывать как биометрические, так и поведенческие характеристики пользователя. Данный подход

повышает надёжность системы и снижает вероятность несанкционированного входа. Перспективными направлениями дальнейших исследований являются расширение набора биометрических модальностей, интеграция с облачными сервисами управления идентификацией и разработка адаптивных моделей обнаружения аномалий на основе рекуррентных нейронных сетей.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Распознование лиц: польза или вред? // Mobikom.ru. – URL: https://www.mobicom.ru
2 UEBA: анализ поведения защищает // Habr. – URL: https://habr.com
3 Распознование лиц: законно ли видеонаблюдение с II // CVC.ai. – URL: https://cvc.ai
4 Биометрическая идентификация: утверждены правила её использования // Zakon.kz. – URL: https://www.zakon.kz
5 Мультимодальные биометрические системы аутентификации // Wikipedia. – URL: https://ru.wikipedia.org
6 Выравнивание лица: что это такое // AIEW.ru. – URL: https://aiew.ru

REFERENCES

1 Raspoznavanie lits: polza ili vred? [Facial recognition: benefit or harm?]. Mobikom.ru. – URL: https://www.mobicom.ru
2 UEBA: analiz povedeniya zashchishchaet dannye [UEBA:behavior analysis protects]. Habr. – URL: https://habr.com
3 Raspoznavanie lits: zakonno li videonablyudenie s II [Facial Recognition: Is Video Surveillance Legal with II]. CVC.ai. – URL: https://cvc.ai
4 Biometricheskaya identifikatsiya: utverzhdeny pravila ee ispolzovaniya [Biometric identification: rules for its use have been approved]. Zakon.kz. – URL: https://www.zakon.kz
5 Multimodalnye biometricheskie sistemy autentifikatsii [Multimodal biometric authentication systems]. Wikipedia. – URL: https://ru.wikipedia.org
6 Vyravnivanie litsa: chto eto takoe [Facial alignment: what is it?]. AIEW.ru. – URL: https://aiew.ru

А.Т. Берикова[1]*, М.М. Илипов[1]
[1]Қазақ агротехникалық университеті С. Сейфуллин атындағы, Қазақстан

Терең оқыту әдістерін пайдалана отырып бет-әлпет тану және пайдаланушы мінез-құлқын талдауға негізделген интеллектуалды қолжетімділікті басқару жүйесі

Қазіргі кезде қолжетімділікті бақылау жүйелері тек парольдер мен PIN-кодтарға сүйенген кезде қауіпсіздік талаптарына толық жауап бере алмайды. Мұндай дәстүрлі әдістерді ұрлау, болжап табу немесе басқа адамға беру оңай, сондықтан олар қорғаныс жүйесінің әлсіз буынына айналады. Осы жағдайда пайдаланушының тек деректерін ғана емес, оның өзін қалай ұстайтынын да «түсіне алатын» биометриялық және поведенциялық тәсілдер ерекше сұранысқа ие болып отыр.

Бұл жұмыста адамның бет-әлпеті бойынша ғана емес, сонымен қатар оның жүйеге кіру кезіндегі мінез-құлқына сүйеніп шешім қабылдайтын бағдарламалық жүйе әзірленеді. Мақсат – күмәнді әрекеттерді дер кезінде байқап, қолжетімділікті автоматты түрде шектеуге қабілетті құрал жасау.

Техникалық негіз ретінде бейнеағыннан бет-әлпетті тану үшін компьютерлік көру мен терең оқыту әдістері қолданылады. Сонымен бірге, уақыт, аймақ және сәтсіз әрекеттердің жинақталуын ескеретін мінез-құлықты талдау модулі іске асырылған. Жүйе бірнеше өзара байланысты бөліктерден тұрады: бет-әлпетті тану, қолжетімділікті уақыт пен аймақ бойынша тексеру және тәуекел деңгейін бағалау.

Жасалған прототип биометриялық және поведенциялық белгілерді біріктіру қолжетімділікті бақылаудың сапасын айтарлықтай жақсартатынын көрсетті. Егер қате әрекеттер саны немесе әдеттен тыс қадамдар белгіленген шектен асып кетсе, жүйе пайдаланушыны автоматты түрде бұғаттап, дабыл сценарийін іске қосады. Осылайша,

рұқсатсыз кіру ықтималдығы азаяды, ал қауіпсіздік әкімшісінің жүктемесі жүйенің дербес әрекеті есебінен төмендейді.

Ұсынылған тәсілдің ғылыми жаңалығы – бет-әлпетті тану мен мінез-құлықты талдауды бірегей шешім қабылдау архитектурасында біріктіруінде. Бұл пайдаланушыға қолжетімділік беру туралы шешім қабылдағанда биометриялық сипаттамаларды да, оның әрекет контекстін де (кіру уақыты, орны, сәтсіз талпыныстардың құрылымы) қатар ескеруге мүмкіндік береді. Мұндай интеграцияланған тәсіл дәстүрлі бір факторлы жүйелермен салыстырғанда анағұрлым икемді және «зияткерлік» қауіпсіздік контурын қалыптастырады.

Түйін сөздер: бетті тану, қолжетімділікті бақылау, мінез-құлық талдауы, биометрия, компьютерлік көру, терең оқыту.

A.T. Berikova[1]*, M.M. Ilipov[1]
[1]S. Seifullin Kazakh Agro Technical Research University, Kazakhstan

Intelligent access control system based on face recognition and user behavior analysis using deep learning methods

Today, access control systems that rely only on passwords and PIN codes can no longer keep up with growing security requirements. These traditional methods are easy to steal, guess, or share with someone else, which turns them into the weakest link in the protection chain. In this context, solutions that use biometrics and can also “understand” user behavior, rather than just verify entered data, are becoming especially relevant.

This study develops a software system that makes decisions not only based on a person’s biometric features, but also on how they behave when trying to log in. The aim is to obtain a tool that can detect suspicious activity in time and automatically strengthen access restrictions when necessary.

As a technical foundation, computer vision and deep learning methods are used to recognize faces in a video stream. In addition, a behavioral analysis module is implemented that tracks the sequence and frequency of login attempts, as well as the time and context of access. The system is structured into several interconnected modules: face recognition, time- and zone-based access verification, and risk level assessment.

The prototype shows that combining biometric and behavioral features can significantly improve the quality of access control. When the number of errors or atypical actions exceeds a predefined threshold, the system automatically blocks the user and triggers an alarm scenario. In this way, the probability of unauthorized access is reduced, while part of the routine work of the security administrator is offloaded to the system itself.

The scientific novelty of the proposed approach lies in integrating face recognition and behavioral analysis not as two separate layers of protection, but as components of a single decision-making architecture. This makes it possible to consider both the user’s biometric characteristics and the context of their actions-such as time, location, and patterns of failed attempts-simultaneously when deciding whether to grant access. Compared to classical single-factor solutions, such an integrated approach forms a more flexible and intelligent security perimeter.

Keywords: face recognition, access control, behavioral analysis, biometrics, computer vision, deep learning, Python.

Дата поступления рукописи в редакцию: 13.04.2026 г.