УДК 004.056:004.89
DOI 10.17513/snt.40773

ИНТЕГРАЦИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ НА БАЗЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА С СИСТЕМАМИ КОНТРОЛЯ ДОСТУПА НА ПРОМЫШЛЕННОМ ПРЕДПРИЯТИИ «ТЮМЕНСКИЕ МОТОРОСТРОИТЕЛИ»

Вязов Е. С., Тарханова О. В., Сенкевич Л. Б.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тюменский индустриальный университет», Тюмень, Российская Федерация, e-mail: liydmila1@yandex.ru

Рассмотрен практический опыт модернизации системы контроля доступа на промышленном предприятии «Тюменские моторостроители» путем интеграции подсистемы распознавания лиц на базе искусственного интеллекта с существующей автоматизированной системой управления технологическими процессами и системой контроля управления доступа. Проанализированы недостатки традиционной радиочастотной идентификации по прокси-картам, проведен сравнительный анализ биометрических методов (распознавание по лицу, отпечаткам пальцев, радужной оболочке глаза, голосу) по ключевым критериям: стоимость внедрения, точность алгоритма, скорость обработки данных, соответствие 152-ФЗ, удобство для пользователя. Обоснован выбор метода распознавания лиц как оптимального для промышленных условий с точки зрения «прозрачной» аутентификации – анализа видеопотока с камеры цехового терминала без активного участия сотрудника. Приведены количественные оценки ошибок первого и второго рода, детально описаны поэтапный процесс интеграции подсистемы на предприятии, архитектура решения, сценарии использования в нотации UML. Результаты пилотного внедрения подсистемы подтверждают снижение числа инцидентов, связанных с компрометацией идентификаторов, передачи прокси-карт и повышением скорости процесса идентификации. Статья предлагает метод модернизации информационной инфраструктуры реального промышленного объекта для его интеграции с интеллектуальной системой.

Ключевые слова: идентификация, аутентификация, искусственный интеллект, биометрия, сверточные нейронные сети, контроль доступа, промышленная безопасность, интеграция систем

INTEGRATION OF ARTIFICIAL INTELLIGENCE-BASED INTELLIGENT SYSTEMS WITH ACCESS CONTROL SYSTEMS AT INDUSTRIAL ENTERPRISE «TYUMEN MOTOR BUILDERS»

Vyazov E. S., Tarkhanova O. V., Senkevich L. B.

Federal State Budgetary Educational Institution of Higher Education "Tyumen Industrial University", Tyumen, Russian Federation, e-mail: liydmila1@yandex.ru

The article discusses the practical experience of modernizing the access control system at the «Tyumen motor builders» industrial enterprise by integrating an artificial intelligence-based facial recognition subsystem with the existing automated process control system and access control system. The article examines the disadvantages of traditional radio frequency identification using proxy cards and conducts a comparative analysis of biometric methods (facial recognition, fingerprint recognition, iris recognition, and voice recognition) based on key criteria: The cost of implementation, the accuracy of the algorithm, the speed of data processing, compliance with Federal Law №152, and user-friendliness have all been considered. The choice of face recognition as the optimal method for industrial conditions has been justified in terms of "transparent" authentication, which involves analyzing the video stream from the workshop terminal camera without the active participation of an employee. The article proposes a method for upgrading the information infrastructure of a real industrial facility to integrate it with an intelligent system.

Keywords: identification, authentication, artificial intelligence, biometrics, convolutional neural networks, access control, industrial security, system integration

Введение

Современные промышленные предприятия, такие как «Тюменские моторостроители» (Предприятие), характеризуются высокой степенью автоматизации технологических процессов. Обеспечение безопасности и разграничения прав доступа к автоматизированным системам управления технологическими процессами (АСУ ТП) является критически важной задачей для бесперебойности и безопасности производственного цикла. До недавного времени на Предприятии использовалась система идентификации и аутентификации на основе RFID-карт стандарта Em-Marine, интегрированная с СКУД «Орион» платформой «1С: Предприятие» (конфигурации «Производство» и «Кадры») [1]. Данная система, несмотря на свою экономическую эффективность, показала ряд уязвимостей: случаи переда-

чи карт, потеря карт, несанкционированное копирование идентификаторов [2]. В связи с этим руководством Предприятия была поставлена задача модернизации системы с применением биометрических технологий на базе искусственного интеллекта.

Цель исследования – анализ существующего решения идентификации личности на промышленном объекте «Тюменские моторостроители» и разработка метода его модернизации и интеграции средствами искусственного интеллекта (ИИ) с обеспечением «прозрачной» аутентификации – анализа видеопотока с камеры цехового терминала, выделения лица и его аутентификации без активного участия сотрудника.

Материалы и методы исследования

В работе использованы методы:

1. Анализ научно-технической литературы и документации по системам RFID, биометрической идентификации, нейросетевым методам распознавания лиц (CNN, FaceNet, VGGFace).

2. Сбор и разметка экспериментального набора данных – 1000 изображений лиц сотрудников цеха № 14 Предприятия в различных условиях освещения, ракурсах и с частичными перекрытиями (защитные очки, каски).

3. Экспериментальное тестирование предобученной модели FaceNet с дообучением на собранном датасете. Оценка качества по метрикам FAR (вероятность ложного допуска) и FRR (вероятность ложного отказа) на контрольной выборке (20 % от общего объема).

4. Сравнительный анализ биометрических методов по критериям: стоимость внедрения (рубли), среднее время идентификации (секунды), FAR/FRR (%), необходимость контакта с оборудованием, соответствие 152-ФЗ [3].

5. Моделирование бизнес-процессов в виде диаграммы вариантов использования нотации UML.

6. Пилотное внедрение на одном участке (цех № 14) с последующей оценкой экономической эффективности, выраженной в сокращении инцидентов и экономии рабочего времени.

Результаты исследования и их обсуждение

Для выбора оптимального решения проведен сравнительный анализ четырех биометрических технологий и радиочастотной идентификации. В качестве критериев оценки выбраны стоимость внедрения, среднее время идентификации, FAR, FRR и соответствие законодательству о персональных данных [4; 5].

Как следует из данных таблицы, метод распознавания лиц, основанный на применении глубокого обучения и сверточных нейронных сетей (CNN), обеспечивает оптимальный баланс между стоимостью, скоростью работы и точностью идентификации для промышленных условий, а также позволяет реализовать «прозрачную» аутентификацию – идентификацию по видеопотоку без необходимости активного действия сотрудника (прикладывания карты, касания сканера) [6; 7]. Радиочастотная идентификация дешевле, но уязвима к компрометации носителя и другим человеческим факторам. Идентификация по отпечаткам пальцев требует контакта со сканером, что негигиенично и снижает скорость потока в цехах с повышенным загрязнением воздуха [8; 9]. Метод сканирования радужной оболочки слишком дорогой для внедрения. Голосовая идентификация ненадежна при высоком уровне шума (87–95 дБ в цехе) [10].

Сравнительные характеристики методов идентификации

Метод	Стоимость внедрения на 1 пост (тыс. руб.)	Среднее время идентификации (с)	FAR, %	FRR, %	Контактность	Соответствие 152-ФЗ (доп. меры)
RFID (прокси-карта)	5–10	1–2	0,01 (при копировании – до 100)	0,1	контактный	не требуется
Распознавание лиц (CNN)	80–150	0,5–1,5	0,001–0,01	0,1–1,0	бесконтактный	требуется
Отпечаток пальца	30–60	1–2	0,0001–0,001	0,5–2,0	контактный	требуется
Радужная оболочка глаза	150–300	1–3	< 0,0001	0,01–0,1	бесконтактный, но требует фиксации	требуется
Голосовая идентификация	20–50	3–5	1 – 5	2–8	бесконтактный	требуется

Примечание: составлена авторами на основе полученных данных в ходе исследования.

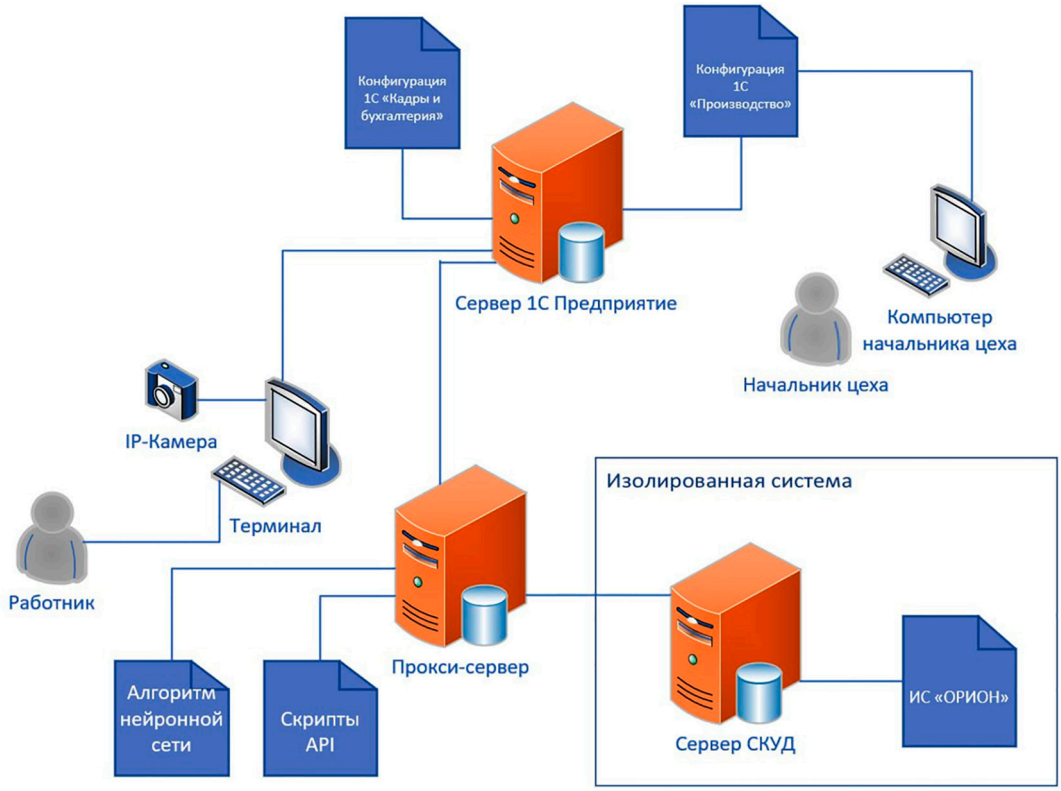

Рис. 1. Схема интеграции АСУ ТП и интеллектуальной системы идентификации личности
Примечание: составлен авторами по результатам данного исследования

Рис. 2. Цеховой терминал
Примечание: фото авторов (21.10.2025)

Для дообученной модели FaceNet на тестовой выборке из 1000 изображений (500 – сотрудники цеха, 500 – посторонние люди) получены следующие значения ошибок первого и второго рода:

– FAR = 0,005 % (5 ложных допусков на 100 000 попыток);

– FRR = 0,35 % (35 ложных отказов на 10 000 попыток аутентичных сотрудников).

Причинами FRR являются: сильное изменение освещения, частичное перекрытие лица каской, поворот головы > 30°. Для снижения FRR до 0,2 % предложено использовать многокадровую проверку (анализ трех последовательных кадров с камеры терминала) и установку дополнительного бокового освещения [11; 12].

На основе выбранного метода разработана и внедрена на Предприятии интеллектуальная подсистема идентификации и аутентификации личности (рис. 1) [13; 14].

Подсистема включает в себя следующие компоненты:

– IP-камеры (Hikvision, 2 Мп, 30 к/с) на цеховых терминалах (рис. 2);

– прокси-сервер с GPU (NVIDIA T4) для выполнения CNN-модели [15];

– модуль liveness detection (антиспуфинг) на основе анализа микродвижений лица;

– шлюз для обмена данными с СКУД «Орион» и 1С [16; 17].

Ключевой особенностью реализованной системы является «прозрачная» аутентификации. Работник цеха не прикладывает карту, так как система в фоновом режиме анализирует видеопоток с камеры терминала.

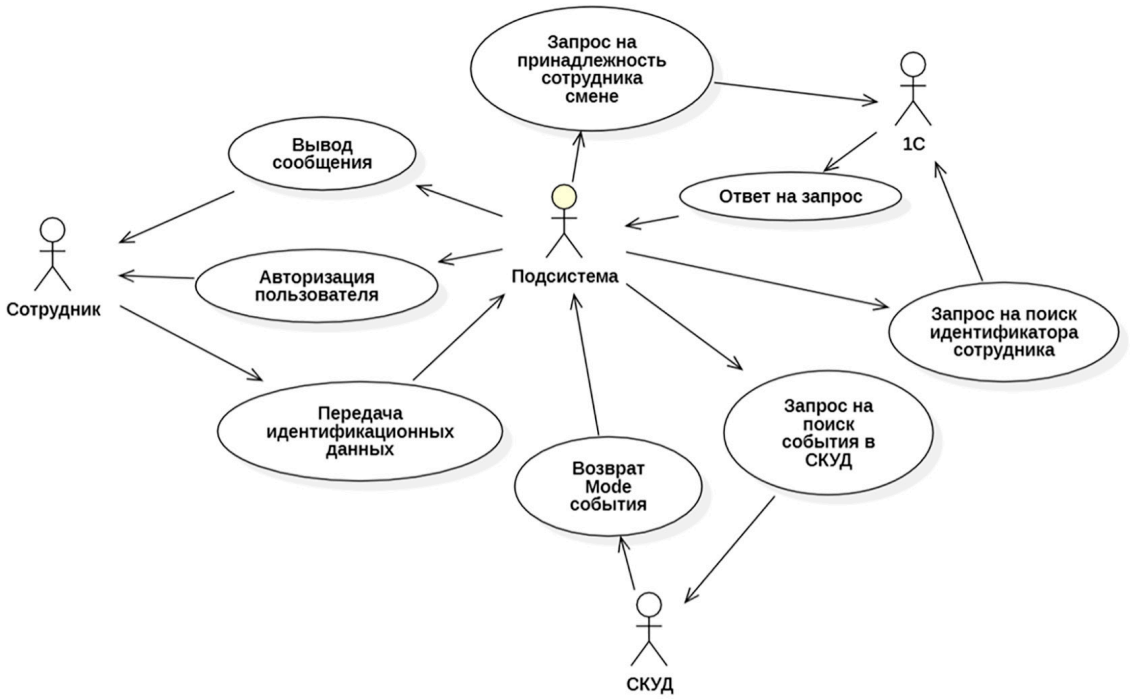

Рис. 3. Диаграмма вариантов использования «Процесс идентификации и аутентификации пользователя»
Примечание: составлен авторами по результатам данного исследования

Как только лицо сотрудника попадает в зону детекции (расстояние 0,5–1,2 м), алгоритм (MTCNN) выделяет лицо, нормализует изображение, извлекает эмбеддинг (FaceNet) и сравнивает с базой данных фотографий сотрудников [18; 19].

При успешной идентификации (порог косинусного сходства > 0,75) система автоматически авторизует работника и передает в 1С событие «Начало работы». Время от появления лица до открытия доступа – 0,8 с. В случае неуверенности системы, когда эмбеддинг находится на границе порога, система запрашивает у сотрудника RFID-карту в качестве второго фактора. Диаграмма вариантов использования идентификации и аутентификации работника в нотации UML представлена на рис. 3 [20, с. 172].

Выводы

Проведенное исследование и пилотное внедрение на Предприятии показывают, что интеграция интеллектуальной системы распознавания лиц с существующей инфраструктурой АСУ ТП и СКУД позволяет:

1. Устранить уязвимости, связанные с компрометацией RFID-карт.

2. Реализовать «прозрачную» аутентификацию, повышающую скорость отклика системы и удобство процесса получения доступа.

3. Обеспечить требуемый уровень точности (FAR = 0,005 %, FRR = 0,35 %) при условии дообучения модели на данных предприятия и установки хорошего освещения.

4. Достичь экономической эффективности за счет снижения инцидентов и экономии рабочего времени.

Представленный в статье опыт демонстрирует практическую применимость предложенного подхода на аналогичных промышленных предприятиях. Дальнейшие исследования могут быть направлены на повышение устойчивости алгоритмов к задымлению, запыленности и использование мультимодальной биометрии (лицо и голос) для критически важных зон. Статья обобщает успешный опыт инженерного внедрения, что может быть полезно специалистам по автоматизации и промышленной безопасности.

Список литературы

1. Царегородцев К. Д. Анализ режимов шифрования для реализации в устройствах RFID // ПДМ. Приложение. 2020. № 13. URL: https://cyberleninka.ru/article/n/analiz-rezhimov-shifrovaniya-dlya-realizatsii-v-ustroystvah-rfid (дата обращения: 05.02.2026). DOI: 10.17223/2226308X/13/20.

2. Смушкин А. Б. Кибербезопасность: понятие, структура, механизм правового обеспечения // Правоприменение. 2025. № 3. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-ponyatie-struktura-mehanizm-pravovogo-obespecheniya (дата обращения: 07.02.2026). DOI: 10.52468/2542-1514.2025.9(3).114-123.

3. Кутейников Д. Л., Ижаев О. А., Лебедев В. А., Зенин С. С. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности // Lex russica. 2022. Т. 75. № 2. С. 121–131. URL: https://cyberleninka.ru/article/n/neprikosnovennost-chastnoy-zhizni-v-usloviyah-ispolzovaniya-sistem-iskusstvennogo-intellekta-dlya-udalennoy-biometricheskoy (дата обращения: 09.02.2026). DOI: 10.17803/1729-5920.2022.183.2.121-131.

4. Лютикова Л. А., Ибрагим А. С. Применение нейросетевого подхода для решения задачи аутентификации пользователя // Известия КБНЦ РАН. 2020. № 4 (96). URL: https://cyberleninka.ru/article/n/primenenie-neyrosetevogo-podhoda-dlya-resheniya-zadachi-autentifikatsii-polzovatelya (дата обращения: 24.02.2026). DOI: 10.35330/1991-6639-2020-4-96-5-10.

5. Гареева Г. А., Хамидуллин М. Р., Джибладзе З. Г., Ахметов Л. М. Развертывание искусственного интеллекта по распознаванию лиц // Научно-технический вестник Поволжья. 2022. № 8. С. 50–53. URL: https://lib.dm-centre.ru/lib/document/gpntb/ESVODT/060ca749785cc2869409ec9362a7cc3f/ (дата обращения: 24.02.2026).

6. Нуржанов Ф. Р. Применение методов искусственного интеллекта в идентификации личности по изображению лица // Universum: технические науки. 2024. № 5 (122). С. 55–58. URL: https://cyberleninka.ru/article/n/primenenie-metodov-iskusstvennogo-intellekta-v-identifikatsii-lichnosti-po-izobrazheniyu-litsa (дата обращения: 25.02.2026). DOI: 10.32743/UniTech.2024.122.5.17624.

7. Саяпин В. О. Интеллектуальные нейросети – будущий потенциал цивилизационного развития цифрового мира // Вестник Челябинского государственного университета. 2023. Т. 7 (477). № 2. С. 21–26. URL: https://cyberleninka.ru/article/n/intellektualnye-neyroseti-buduschiy-potentsial-tsivilizatsionnogo-razvitiya-tsifrovogo-mira/viewer (дата обращения: 26.02.2026). DOI: 10.47475/1994-2796-2023-477-7-21-26.

8. Руднев И. С., Королев Л. Ю., Соболев Н. С. Разработка системы контроля доступа на основе биометрических данных для сервисного центра // Вестник науки. 2026. Т. 4. № 1 (94). С. 1125–1131. URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-kontrolya-dostupa-na-osnove-biometricheskih-dannyh-dlya-servisnogo-tsentra (дата обращения: 26.02.2026).

9. Глаженков А. И. Алгоритм безопасного управления доступом на объектах электроэнергетики // Инновационная наука. 2026. Т. 1. № 2–2. С. 77–80. URL: https://aeterna-ufa.ru/sbornik/IN-2026-02-2-1.pdf (дата обращения: 26.02.2026).

10. Гаязова С. Р., Ерохина К. С., Мельникова Д. А., Ермолина Л. В. Биометрические технологии в системах контроля доступа как фактор инновационного развития и повышения экономической безопасности предприятий топливно-энергетического комплекса // Экономика и предпринимательство. 2026. № 1 (186). С. 1295–1299. URL: https://parlib.duma.gov.ru/common/web_services/secure_download/Resource-210824/2026-06413.pdf (дата обращения: 27.02.2026).

11. Полковникова Н. А. Исследование методов и алгоритмов компьютерного зрения на основе сверточных и рекуррентных нейронных сетей // Эксплуатация морского транспорта. 2020. № 3. С. 154–168. URL: https://elibrary.ru/item.asp?id=44403281 (дата обращения: 27.02.2026). DOI: 10.34046/aumsuomt96/21.

12. Липин Ю. Н. Разработка алгоритма распознавания лиц с учетом особенностей работы человеческого мозга // Вестник Пермского университета. Серия: Математика. Механика. Информатика. 2023. № 2 (61). URL: https://cyberleninka.ru/article/n/razrabotka-algoritma-raspoznavaniya-lits-s-uchetom-osobennostey-raboty-chelovecheskogo-mozga (дата обращения: 27.02.2026). DOI: 10.17072/1993-0550-2023-2-59-64.

13. ГОСТ 34.602-2020. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы: межгосударственный стандарт. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200181804 (дата обращения: 27.02.2026).

14. ГОСТ 57193-2025. Системная и программная инженерия. Процессы жизненного цикла систем: национальный стандарт Российской Федерации [Электронный ресурс]. URL: https://docs.cntd.ru/document/1312112086 (дата обращения: 27.02.2026).

15. Стефанова Н. А., Силкина А. В. Система распознавания лиц как инструмент повышения уровня качества жизни населения и экономического развития // Региональная и отраслевая экономика. 2024. № 1. URL: https://cyberleninka.ru/article/n/sistema-raspoznavaniya-lits-kak-instrument-povysheniya-urovnya-kachestva-zhizni-naseleniya-i-ekonomicheskogo-razvitiya (дата обращения: 28.02.2026). DOI: 10.47576/2949-1916.2024.1.1.018.

16. Череватова Д. А., Куваева Е. Н. Обзор возможностей 1С: предприятие для автоматизации бизнес-процессов // Вестник науки. 2024. № 12 (81). URL: https://cyberleninka.ru/article/n/obzor-vozmozhnostey-1s-predpriyatie-dlya-avtomatizatsii-biznes-protsessov (дата обращения: 28.02.2026).

17. Документации АРМ «Орион Про» – «версия 1.20 сервисный пакет 3 обновление 8. М.: ЗАО НВП Болид, 2024. 1571 с. [Электронный ресурс]. URL: https://bolid.ru/files/373/566/rep_orion_pro_1.20.3.8_mar_25.pdf (дата обращения: 28.02.2026).

18. Qi S., Zuo X., Feng W., Naveen I. G. Face Recognition Model Based On MTCNN And Facenet // 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC). 2022. [Электронный ресурс]. URL: https://ieeexplore.ieee.org/document/10031806 (дата обращения: 11.02.2026). DOI: 10.1109/ICMNWC56175.2022.10031806.

19. Zuama L. R., Setiadi D. R. I. M., Susanto A., Santosa S., Gan H.-S., Ojugo A. A. High-Performance Face Spoofing Detection using Feature Fusion of FaceNet and Tuned DenseNet201 // Journal of Future Artificial Intelligence and Technologies. 2025. Vol. 1. № 4. P. 385–400. URL: https://faith.futuretechsci.org/index.php/FAITH/article/view/62 (дата обращения: 14.02.2026).

20. Путилин А. Б., Юрагов Е. А. Компонентное моделирование и программирование на языке UML. Практическое руководство по проектированию информационных систем М.: НТ Пресс, 2021. 664 с. [Электронный ресурс]. URL: https://rusneb.ru/catalog/010003_000061_e79cd252485c86e96e6d31e71ab12e2f/ (дата обращения: 24.02.2026). ISBN 5-477-00046-5.

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest: The authors declare that there is no conflict of interest.

Финансирование: Авторы заявляют об отсутствии внешнего финансирования.

Financing: The research was performed without external funding.