УДК 004.891.2+006.9
DOI: 10.26102/2310-6018/2026.57.6.014

Миварная экспертная система для системы контроля и управления доступом на основе биометрической идентификации по венам ладони

К.Д. Григоренко[1], А.А. Горенков[1], И.А. Беляев[1], О.О. Варламов[1,2]✉

[1]Московский государственный технический университет имени Н.Э. Баумана, Москва, Российская Федерация
[2]Научно-исследовательский институт вычислительных комплексов имени М.А. Карцева, Москва, Российская Федерация

Резюме. В статье рассмотрена задача построения системы контроля и управления доступом (СКУД), способной принимать обоснованные решения не только на основе биометрического шаблона, но и с учетом контекста: уровня прав сотрудника, зоны доступа, временного режима и истории аутентификации. Предложена архитектура комплексной интеллектуальной системы, объединяющей нейросетевой и логический уровни искусственного интеллекта. Биометрическая идентификация реализована с помощью сверточной нейронной сети ResNet18, адаптированной для grayscale-изображений вен ладони и обученной на датасете из 834 субъектов (8 340 снимков) с использованием триплетного метрического обучения и классификационной головы; достигнута точность Top-1 Accuracy = 87,47 %, Top-5 = 96,58 %, Top-10 = 98,14 %, ROC-AUC = = 0,9985 и EER = 1,64 % при среднем уровне уверенности правильных совпадений 0,908. Степень уверенности нейронной сети совместно с пятью контекстными параметрами передается в миварную экспертную систему (МЭС), реализованную в среде КЭСМИ Wi!Mi Разуматор. МЭС содержит три независимых отношения с общими входными параметрами, формирующих решение о доступе, уровень тревоги и оценку надежности биометрии. Общие входы порождают перекрестные дуги в двудольном графе решения, что отражает многоаспектность принятия решений в комплексном искусственном интеллекте. Разработан алгоритм принятия решений из 32 правил, распределенных по пяти группам приоритета. Проведено тестирование МЭС на трех репрезентативных сценариях, демонстрирующих три различные топологии графа решения – от вырожденной до полной двудольной. Результаты подтверждают корректность миварного логического вывода и масштабируемость базы знаний без изменения нейросетевого модуля. Практическая значимость полученных результатов состоит в возможности построения аудируемых биометрических СКУД, сочетающих точность глубокого обучения и прозрачность логического вывода миварных баз знаний.

Ключевые слова: миварная экспертная система, СКУД, биометрическая идентификация, вены ладони, ResNet18, триплетное обучение, комплексный искусственный интеллект, КЭСМИ, Wi!Mi, нейросимволический искусственный интеллект.

Благодарности: Авторы выражают благодарность кафедре ИУ-5 «Системы обработки информации и управления» МГТУ им. Н.Э. Баумана за поддержку исследования и предоставление вычислительных ресурсов, а также НИИ Мивар за консультации по разработке миварной экспертной системы в среде КЭСМИ Wi!Mi Разуматор.

Для цитирования: Григоренко К.Д., Горенков А.А., Беляев И.А., Варламов О.О. Миварная экспертная система для системы контроля и управления доступом на основе биометрической идентификации по венам ладони. *Моделирование, оптимизация и информационные технологии.* 2026;14(6). URL: https://moitvivt.ru/ru/journal/article?id=2393 DOI: 10.26102/2310-6018/2026.57.6.014

Mivar expert system for an access control system based on palm vein biometric identification

K.D. Grigorenko[1], A.A. Gorenkov[1], I.A. Belyaev[1], O.O. Varlamov[1,2]✉

[1]Bauman Moscow State Technical University, Moscow, the Russian Federation
[2]Kartsev Research Institute of Computing Complexes, Moscow, the Russian Federation

Abstract. The paper addresses the task of designing an access control system (ACS) capable of making informed decisions not only on the basis of a biometric template but also taking into account the context: employee access level, zone of access, time-of-day policy and authentication history. An architecture of a complex intelligent system combining neural-network and logical levels of artificial intelligence is proposed. Biometric identification is implemented using a ResNet18 convolutional neural network adapted for grayscale palm-vein images and trained on a dataset of 834 subjects (8,340 images) using triplet metric learning with a classification head; Top-1 accuracy of 87.47 %, Top-5 of 96.58 %, Top-10 of 98.14 %, ROC-AUC of 0.9985 and EER of 1.64 % are achieved with an average confidence of correct matches equal to 0.908. The neural-network confidence together with five contextual parameters is passed to a mivar expert system (MES) implemented in the KESMI Wi!Mi Razumator environment. The MES contains three independent relations with shared inputs that produce an access decision, an alert level and a biometric reliability estimate. Shared inputs induce cross-edges in the bipartite solution graph, reflecting the multi-aspect nature of decision making in complex AI. A decision algorithm of 32 rules grouped into five priority tiers is developed. Testing on three representative scenarios demonstrates three distinct topologies of the solution graph – from a degenerate case to a full bipartite one. The results confirm the correctness of mivar logical inference and the scalability of the knowledge base without any change to the neural-network module.

Keywords: mivar expert system, ACS, biometric identification, palm veins, ResNet18, triplet learning, complex artificial intelligence, KESMI, Wi!Mi, neurosymbolic artificial intelligence.

Acknowledgments: The authors thank the IU-5 Department of Information Processing and Control Systems of Bauman MSTU for supporting the research and providing computational resources, and the Mivar Research Institute for consultations on the development of the mivar expert system in the Wi!Mi Razumator environment.

For citation: Grigorenko K.D., Gorenkov A.A., Belyaev I.A., Varlamov O.O. Mivar expert system for an access control system based on palm vein biometric identification. *Modeling, Optimization and Information Technology.* 2026;14(6). (In Russ.). URL: https://moitvivt.ru/ru/journal/article?id=2393 DOI: 10.26102/2310-6018/2026.57.6.014

Введение

Системы контроля и управления доступом (СКУД) традиционно рассматриваются как инфраструктурная задача физической безопасности [1]. С расширением парка корпоративных объектов и переходом на биометрические методы идентификации задача СКУД перестает сводиться к сравнению шаблона и превращается в задачу принятия контекстных решений: одно и то же совпадение биометрии должно интерпретироваться по-разному в зависимости от уровня прав сотрудника, зоны доступа, времени суток и истории аутентификации. Чисто нейросетевые решения плохо справляются с такими контекстными правилами – они обучаются на задаче соответствия и не обеспечивают прозрачного логического вывода, необходимого для аудита и сертификации систем безопасности.

Альтернативой является комплексный (нейросимволический, гибридный) искусственный интеллект (ИИ) [2], объединяющий нейронную сеть, отвечающую за восприятие, и логический модуль, отвечающий за принятие решения по набору правил. Такой подход особенно актуален для биометрических СКУД, поскольку он позволяет

разделить две подзадачи: распознавание шаблона (область сильной стороны нейронных сетей) и контекстное принятие решения (область сильной стороны экспертных систем).

Из современных биометрических модальностей вены ладони привлекают все больший интерес промышленных разработчиков. В отличие от отпечатков пальцев и других пальцевых биометрических признаков, вены расположены под кожей и практически не подделываются; в отличие от распознавания лица, биометрия вен не зависит от освещения, макияжа и старения; в отличие от радужной оболочки, сенсоры для сканирования вен контактны или бесконтактны с короткой дистанцией и проще вписываются в СКУД на проходных. Обзорные работы по распознаванию вен ладони [3] и оригинальные исследования глубоких сверточных сетей для пальцевых вен [4, 5] демонстрируют высокую точность на закрытых множествах и устойчивость к шумам сенсора. Современные обзоры методов глубокого обучения [6] и сравнительные исследования биометрии по изображениям пальцев [7] подтверждают применимость сверточных архитектур для биометрических задач.

Миварные технологии [8] логического ИИ на протяжении последних лет последовательно расширяют область применения. Миварные экспертные системы (МЭС) реализуются в задачах планирования действий автономных роботов и других интеллектуальных систем [9]. Миварный подход отличается переходом к двудольным ориентированным графам миварных сетей и линейной вычислительной сложностью относительно числа правил «если-то» [10], что позволяет масштабировать базы знаний без деградации производительности и обеспечивает прозрачность логического вывода.

Несмотря на накопленный задел, применение МЭС в составе СКУД с биометрической идентификацией по венам ладони ранее не рассматривалось. Цель настоящей работы – разработать архитектуру комплексной (гибридной) интеллектуальной СКУД, в которой степень уверенности нейронной сети распознавания вен ладони поступает в миварную экспертную систему в качестве одного из входных параметров наряду с контекстом, а МЭС формирует три независимых выхода: решение о доступе, уровень тревоги и оценку надежности биометрии. В работе решаются следующие задачи: обучение нейронной сети ResNet18 на датасете вен ладони с применением триплетного обучения; формализация входных и выходных параметров МЭС, разработка алгоритма принятия решений из 32 правил; тестирование системы на трех репрезентативных сценариях, демонстрирующих различные режимы работы миварного решателя; анализ топологии двудольного графа решения. Таким образом, тема работы актуальна и обладает практической полезностью.

Материалы и методы

Предлагаемая архитектура комплексной СКУД состоит из двух последовательных уровней. Первый уровень – нейронная сеть биометрической идентификации по венам ладони, формирующая на выходе степень уверенности в совпадении предъявленного образца с шаблоном в галерее. Второй уровень – миварная экспертная система, получающая степень уверенности совместно с контекстными параметрами и формирующая три выхода: решение о доступе, уровень тревоги и оценку надежности биометрии.

Датасет и предобработка. Для обучения и тестирования использована авторская база изображений вен ладони, содержащая 834 субъекта по 10 снимков ладони на каждого: суммарно 8 340 изображений в формате BMP, grayscale, исходное разрешение 640×480. Разбиение набора выполнено по фотографиям внутри каждого субъекта в соотношении 8/2 (6 672 обучающих и 1 668 тестовых изображений). Предобработка включает приведение к grayscale и ресайз до 224×224 и адаптивное контрастное

преобразование CLAHE [11] с параметрами clipLimit = 2,0 и tileGridSize = 8×8, подчеркивающее рисунок вен. Аугментации при обучении: случайный поворот в пределах ±15°, изменение яркости и контраста в диапазоне ±20 %, упругие искажения и перспективные преобразования.

Архитектура нейронной сети. Нейронная сеть основана на архитектуре ResNet18 [12], предварительно обученной на ImageNet. Для работы с grayscale-изображениями первый сверточный слой адаптирован: число входных каналов изменено с 3 на 1, начальные веса получены усреднением RGB-весов предобученной сети по измерению каналов. Первые слои сверточной части заморожены; обучение ведется на последних слоях основной сети и на эмбеддинг-голове. Эмбеддинг-голова реализует последовательность Linear(512→256) → BatchNorm1d → ReLU → Dropout(0,3) → Linear(256→512) → BatchNorm1d; выход головы подвергается L2-нормализации и используется как 512-мерный дескриптор в пространстве косинусных расстояний.

Обучение проведено комбинированным методом: триплетное метрическое обучение (Triplet Loss [13], маргин 0,25) совместно с классификационной головой и функцией CrossEntropyLoss. Оптимизатор Adam ($\beta_1 = 0{,}9$, $\beta_2 = 0{,}999$), начальный коэффициент обучения 0,01, планировщик ReduceLROnPlateau (фактор 0,5, патентс 5), градиентная обрезка нормой 1,0, mixed precision на GPU, batch_size = 64, до 100 эпох с ранней остановкой (patience = 40), зафиксированный random seed = 42. Идентификация на этапе вывода выполняется поиском ближайшего соседа в галерее по косинусному расстоянию; порог верификации > 0,85.

Метрики распознавания. В качестве основной метрики используется Top-1 Accuracy – доля запросов, для которых первый кандидат в рейтинге косинусных близостей соответствует целевому субъекту. Дополнительно отслеживается среднее значение уверенности при правильном совпадении – численно равное косинусному сходству между эмбеддингом запроса и ближайшим эмбеддингом галереи. Достигнутые на отложенной тестовой выборке из 1 668 изображений 834 субъектов значения составляют: Top-1 = 87,47 %, Top-5 = 96,58 %, Top-10 = 98,14 %, средняя уверенность правильных совпадений 0,908, межкандидатная разность 0,190; в задаче верификации на 13 344 genuine-парах и 11 115 552 impostor-парах достигнуто ROC-AUC = 0,9985 и EER = = 1,64 % при пороге 0,486. Степень уверенности сети, выраженная в процентах (X_1), передается в миварную экспертную систему как первичный входной параметр.

Миварная экспертная система. Миварная модель знаний представима как двудольный ориентированный граф G = (V ∪ R, E), где множество вершин-параметров V соответствует переменным состояния системы, множество вершин-правил R – продукциям типа «если-то», а ребра E связывают параметры с правилами (входные и выходные). Вычислительная сложность миварного решателя линейна относительно числа правил, что позволяет строить объемные базы знаний без деградации производительности [10]. База знаний разработанной системы реализована в среде КЭСМИ Wi!Mi Разуматор.

МЭС содержит шесть входных параметров (Таблица 1) и три выходных параметра (Таблица 2). Входные параметры охватывают как биометрические (X_1, X_6), так и контекстные (X_2 – статус сотрудника, X_3 – уровень прав, X_4 – зона доступа, X_5 – режим рабочего времени) характеристики.

Таблица 1 – Входные параметры МЭС
Table 1 – Input parameters of the MES

№	Обозн.	Параметр/Parameter	Тип/Type	Значения/Values
1	X_1	Уверенность нейронной сети / NN confidence, %	Число/ Numeric	0–100
2	X_2	Статус сотрудника / Employee status	Текст/Text	active, blocked
3	X_3	Уровень прав доступа / Access rights level	Текст/Text	low, medium, high
4	X_4	Запрашиваемая зона / Requested zone	Текст/Text	main, secure, server
5	X_5	Рабочее время / Working hours	Логический/ Boolean	true, false
6	X_6	Ошибочные попытки / Failed attempts	Число/ Numeric	0, 1, 2, 3+

Таблица 2 – Выходные параметры МЭС
Table 2 – Output parameters of the MES

№	Обозн.	Параметр/Parameter	Тип/Type	Значения/Values
1	Y_1	Решение о доступе / Access decision	Текст/Text	allowed, warning, denied
2	Y_2	Уровень тревоги / Alert level	Текст/Text	none, alert, lockdown
3	Y_3	Надежность биометрии / Biometric reliability	Текст/Text	trusted, uncertain, suspicious, compromised, failed

МЭС содержит три отношения типа «prog», каждое из которых реализует независимый аспект принятия решения и формирует один выходной параметр. Общие входные параметры порождают перекрестные дуги в двудольном графе решения КЭСМИ, отражая многоаспектность комплексного ИИ.

Алгоритм принятия решений. Отношение 1 «Решение о доступе» (X_1, X_2, X_3, X_4, $X_5 \rightarrow Y_1$) объединяет 32 правила, распределенные по пяти группам приоритета с цепочкой if-else в порядке убывания приоритета:

– Группа 5 (4 правила, наивысший приоритет) – защита от подбора: срабатывает при количестве ошибочных попыток (X_6) ≥ 1 или при статусе сотрудника (X_2) = blocked с попытками;

– Группа 4 (3 правила) – абсолютный запрет при статусе сотрудника (X_2) = blocked для любой зоны доступа;

– Группа 3 (7 правил) – обработка сомнений нейронной сети: уверенность $X_1 < 50\ \% \rightarrow$ denied; $50\ \% \leq X_1 < 80\ \% \rightarrow$ warning;

– Группа 2 (9 правил) – ограничения вне рабочего времени при X_5 = false;

– Группа 1 (9 правил) – штатное разграничение доступа при $X_1 \geq 80\ \%$, X_2 = active, X_5 = true, с учетом уровня прав X_3 и зоны X_4.

Отношение 2 «Уровень тревоги» (X_2, $X_6 \rightarrow Y_2$) оценивает угрозу безопасности независимо от решения о доступе: $X_6 \geq 3 \rightarrow$ lockdown; $X_2 =$ blocked и $X_6 > 0 \rightarrow$ lockdown; $X_2 =$ blocked $\rightarrow$ alert; $X_6 = 1$ или $2 \rightarrow$ alert; иначе $\rightarrow$ none.

Отношение 3 «Надежность биометрии» (X_1, $X_6 \rightarrow Y_3$) классифицирует качество биометрической идентификации: $X_6 \geq 3 \rightarrow$ compromised; $X_1 \geq 80$ % и $X_6 = 0 \rightarrow$ trusted; $X_1 \geq 80$ % и $X_6 > 0 \rightarrow$ suspicious; $50\ \% \leq X_1 < 80\ \% \rightarrow$ uncertain; $X_1 < 50$ % $\rightarrow$ failed.

Параметр X_2 является общим входом для отношений 1 и 2, параметр X_1 – для отношений 1 и 3, параметр X_6 – для отношений 2 и 3. Благодаря общим входам миварный решатель КЭСМИ формирует двудольный граф с перекрестными дугами, топология которого отражает архитектуру комплексного ИИ и переиспользование биометрических и контекстных данных между независимыми аспектами принятия решений.

Результаты

Оценка эффективности комплексной системы проведена по двум направлениям: метрики биометрической идентификации на уровне нейронной сети и корректность логического вывода на уровне миварной экспертной системы.

Результаты нейросетевой идентификации. Задача идентификации решена в режиме open-set: каждая проба сравнивается с галереей из 8 эмбеддингов на субъекта, итоговая близость с субъектом берётся как максимум косинусного сходства по его галерее. На отложенной выборке из 1 668 проб 834 субъектов (по 2 снимка на субъекта) достигнуты следующие показатели идентификации: Top-1 = 87,47 %, Top-5 = 96,58 %, Top-10 = 98,14 %. Средняя уверенность (косинусное сходство) для правильных совпадений составляет 0,908, для ошибочных – 0,794; средняя межкандидатная разность (margin между рангами 1 и 2) для правильных совпадений 0,190, для ошибочных 0,053. Высокая разность margin между правильными и ошибочными распознаваниями подтверждает, что ошибки модели концентрируются на снимках, близких в пространстве эмбеддингов, и могут быть отсечены порогом по margin.

Тестирование МЭС. Оценка задачи верификации проведена на всех парах проба-галерея: 13 344 genuine-пар (проба и изображение галереи одного субъекта) и 11 115 552 impostor-пар (разные субъекты). Порог косинусного сходства варьировался в диапазоне [−1, 1], по каждому значению рассчитывались показатели FAR (false accept rate) и FRR (false reject rate). Достигнутые показатели: ROC-AUC = 0,9985, равный уровень ошибок EER = 1,64 % при пороге 0,486; при FAR = 0,1 % значение FRR = 8,28 % (порог 0,674); при FRR = 0,1 % значение FAR = 17,45 % (порог 0,196). Высокое значение ROC-AUC и низкий EER указывают на хорошую разделимость распределений genuine- и impostor-сходств (Рисунок 1) и применимость модели в режиме реальной СКУД. Для высокозащищенных зон рекомендуется оперировать на пороге 0,674 (FAR ≤ 0,1 %), что соответствует условию $X_1 \geq 67$ % в правилах МЭС.

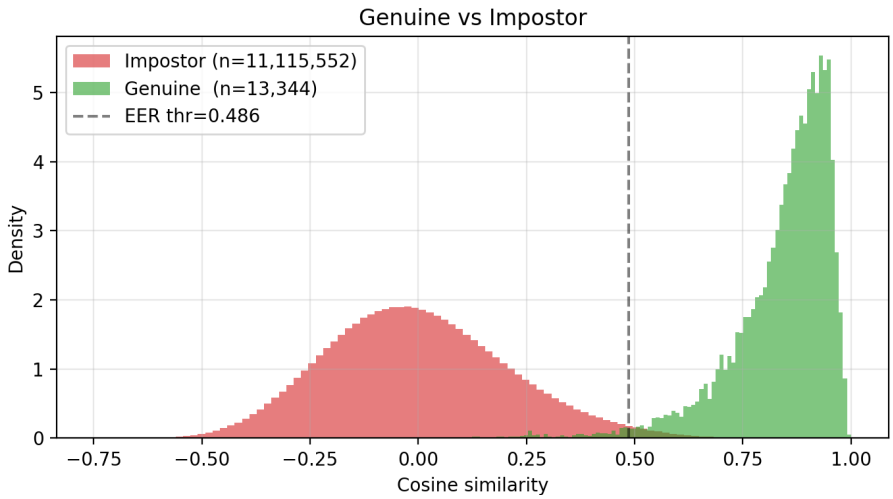

Рисунок 1 – Распределения косинусного сходства для genuine- и impostor-пар; вертикальная линия – порог EER = 0,486
Figure 1 – Cosine similarity distributions for genuine and impostor pairs; vertical line indicates the EER threshold = 0.486

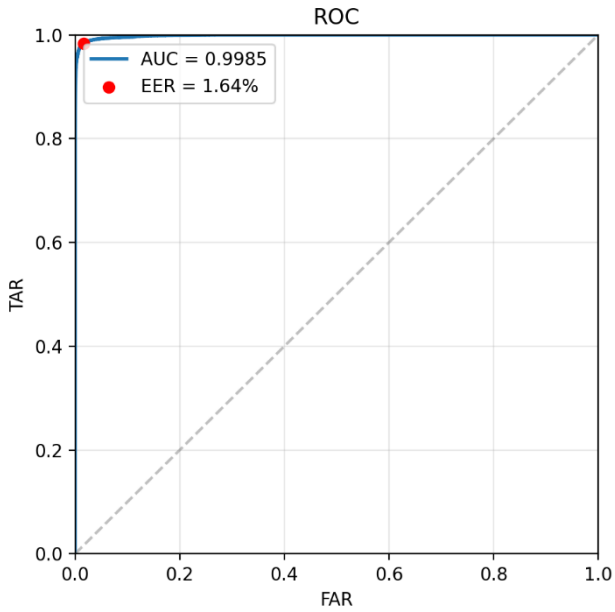

Рисунок 2 – ROC-кривая биометрической верификации; ROC-AUC = 0,9985, EER = 1,64 %
Figure 2 – ROC curve for biometric verification; ROC-AUC = 0.9985, EER = 1.64 %

Сводные показатели нейросетевой идентификации и верификации приведены в Таблице 3. ROC-кривая и точка EER представлены на Рисунке 2.

Таблица 3 – Сводные метрики биометрической идентификации и верификации
Table 3 – Summary of biometric identification and verification metrics

№	Метрика/Metric	Значение/Value
1	Top-1 Accuracy (идентификация / identification)	87,47 %
2	Top-5 Accuracy	96,58 %
3	Top-10 Accuracy	98,14 %

Таблица 3 (продолжение)
Table 3 (continued)

4	Средняя уверенность правильных / Mean conf. of correct	0,908
5	Средняя уверенность ошибочных / Mean conf. of wrong	0,794
6	Средний margin правильных / Mean margin of correct	0,190
7	ROC-AUC (верификация / verification)	0,9985
8	Equal Error Rate (EER)	1,64 %
9	FRR @ FAR = 0,1 %	8,28 % (порог/thr = 0,674)
10	FAR @ FRR = 0,1 %	17,45 % (порог/thr = 0,196)

Тестирование МЭС проведено в среде КЭСМИ Wi!Mi Разуматор на трех репрезентативных сценариях, отражающих различные режимы работы комплексного ИИ. КЭСМИ строит граф по активным отношениям, поэтому каждый сценарий дает структурно отличающийся граф: от простейшего (одно отношение с двумя входами) до сложного с тремя параллельными правилами и шестью входами, объединёнными перекрестными дугами через общие параметры.

Сценарий 1 – оценка надежности биометрии. В тестовой панели КЭСМИ заданы только два параметра: уверенность нейронной сети $X_1 = 65$ % и количество ошибочных попыток $X_6 = 2$; для расчета запрошен единственный выход Y_3. Миварный решатель активирует только отношение 3 и строит минимальный граф (Рисунок 3): два входных эллипса X_1 и X_6, один прямоугольник правила «var x_1, x_6, y_3», один выходной эллипс Y_3 = uncertain. Вырожденный граф демонстрирует, что при отсутствии контекста (уровень доступа, зона, режим работы) МЭС способна выдать автономную оценку качества биометрии.

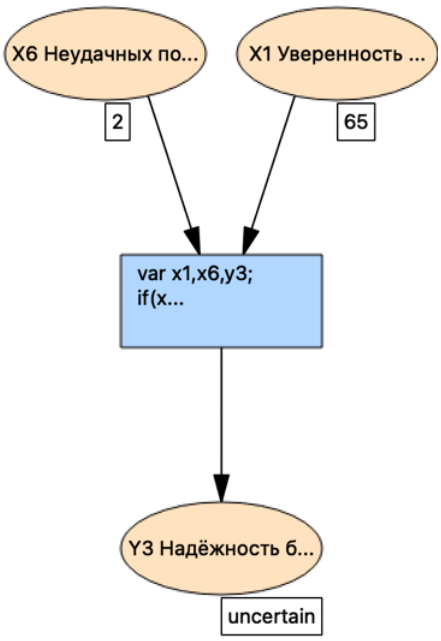

Рисунок 3 – Минимальный граф решения: $X_1 = 65$ %, $X_6 = 2 \rightarrow Y_3$ = uncertain
Figure 3 – Minimal solution graph: $X_1 = 65$ %, $X_6 = 2 \rightarrow Y_3$ = uncertain

Сценарий 2 – решение о доступе без биометрического контекста. В тестовой панели заданы пять параметров: X_1 = 91 %, X_2 = blocked, X_3 = medium, X_4 = main, X_5 = true; запрошен только Y_1. Миварный решатель активирует отношение 1 и строит граф с пятью входами, сходящимися в один прямоугольник «var x_1, x_2, x_3, x_4, x_5» (Рисунок 4). Результат Y_1 = denied формируется правилом группы 4: статус X_2 = blocked блокирует доступ независимо от высокой уверенности нейросети (X_1 = 91 %). Структура графа принципиально отличается от сценария 1: пять входов вместо двух, один прямоугольник, один выход – веерная топология.

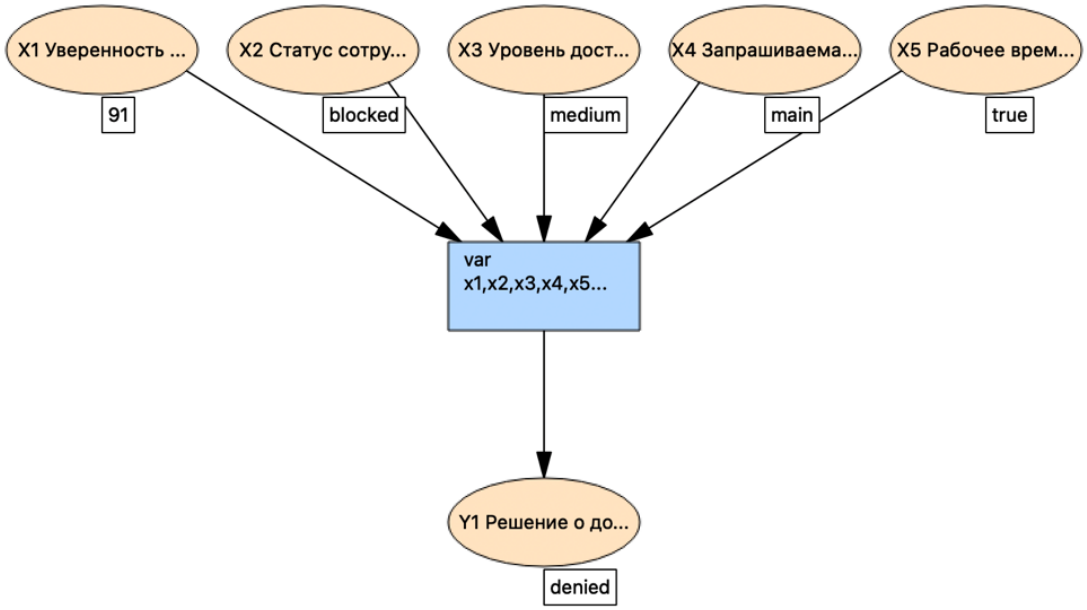

Рисунок 4 – Веерный граф решения: X_1 = 91 %, X_2 = blocked, X_3 = medium, X_4 = main, X_5 = true → Y_1 = denied
Figure 4 – Fan-shaped solution graph: X_1 = 91 %, X_2 = blocked, X_3 = medium, X_4 = main, X_5 = true → Y_1 = denied

Сценарий 3 – полная оценка комплексного ИИ. В тестовой панели заданы все шесть входных параметров: X_1 = 85 %, X_2 = active, X_3 = high, X_4 = server, X_5 = true, X_6 = 0; запрошены все три выхода Y_1, Y_2, Y_3. Миварный решатель активирует все три отношения и строит полный двудольный граф решения (Рисунок 5). Граф содержит шесть входных эллипсов, три прямоугольника правил и три выходных эллипса, соединённых перекрестными дугами: X_1 передаётся в отношения 1 и 3, X_2 – в отношения 1 и 2, X_6 – в отношения 2 и 3. Такая топология характерна для миварных сетей: один и тот же входной параметр влияет на несколько независимых выходов. Результаты сценария: Y_1 = allowed (штатный доступ в серверную), Y_2 = none (угроз нет), Y_3 = trusted (биометрия надежна).

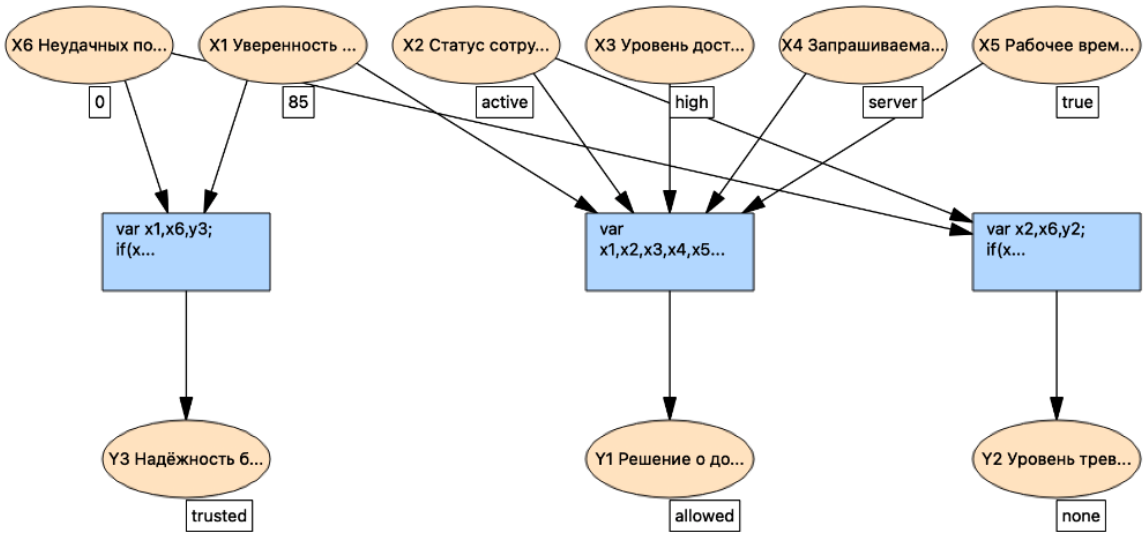

Рисунок 5 – Полный двудольный граф решения с перекрестными дугами: $X_1 = 85$ %, X_2 = active, X_3 = high, X_4 = server, X_5 = true, $X_6 = 0 \rightarrow Y_1$ = allowed, Y_2 = none, Y_3 = trusted
Figure 5 – Full bipartite solution graph with cross-edges: $X_1 = 85$ %, X_2 = active, X_3 = high, X_4 = server, X_5 = true, $X_6 = 0 \rightarrow Y_1$ = allowed, Y_2 = none, Y_3 = trusted

Сценарии подобраны таким образом, чтобы продемонстрировать три различные топологии графа решения и, соответственно, три режима работы миварного решателя: вырожденный (одно отношение с двумя входами), веерный (одно отношение с множеством входов) и полный двудольный (три отношения с общими входами и перекрёстными дугами). Все три сценария подтвердили корректность миварного логического вывода (Таблица 4).

Таблица 4 – Результаты тестирования МЭС СКУД на трех сценариях
Table 4 – Testing results of the ACS MES on three scenarios

№	Сценарий/ Scenario	Входные параметры/ Inputs	Активные отношения / Active relations	Результат/ Result	Топология графа / Graph topology
1	Надёжность биометрии / Biometric reliability	$X_1 = 65$ %, $X_6 = 2$	Отношение 3 / Relation 3	Y_3 = uncertain	2 → 1 → 1 (вырожденный / degenerate)
2	Доступ без биометрического контекста / Access without bio-context	$X_1 = 91$ %, X_2 = blocked, X_3 = medium, X_4 = main, X_5 = true	Отношение 1 / Relation 1	Y_1 = denied	5 → 1 → 1 (веерный / fan-shaped)
3	Полная оценка комплексного ИИ / Full complex-AI evaluation	$X_1 = 85$ %, X_2 = active, X_3 = high, X_4 = server, X_5 = true, $X_6 = 0$	Отношения 1, 2, 3 / Relations 1, 2, 3	Y_1 = allowed, Y_2 = none, Y_3 = trusted	6 → 3 → 3 (полный двудольный / full bipartite)

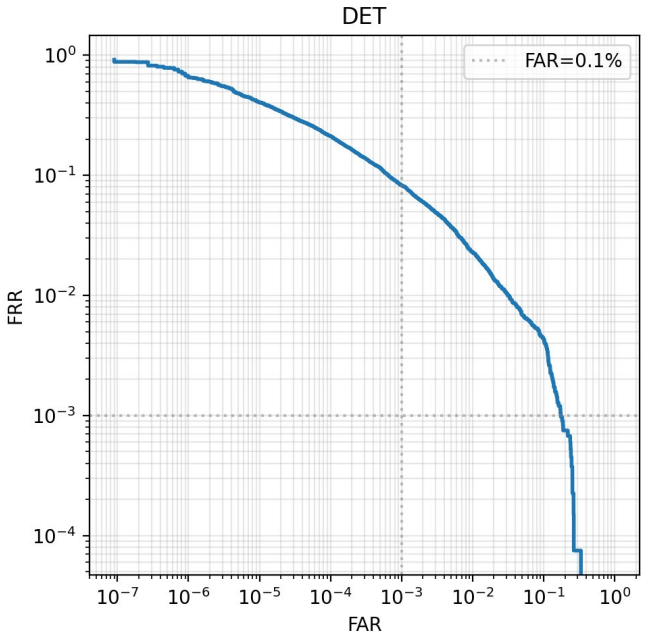

Рисунок 6 – DET-кривая (log-log): зависимость FRR от FAR; точки FAR = 0,1 % и FRR = 0,1 % обозначены пунктиром

Figure 6 – DET curve (log-log): FRR as a function of FAR; FAR = 0.1 % and FRR = 0.1 % operating points are shown by dashed lines

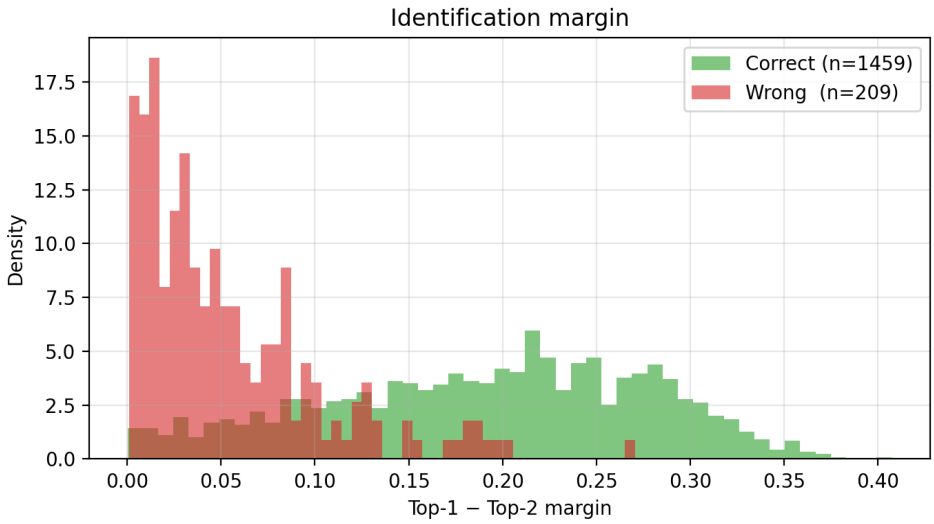

Рисунок 7 – Гистограмма межкандидатной разности (margin = Top-1 − Top-2) для правильных и ошибочных распознаваний

Figure 7 – Histogram of rank-1 minus rank-2 margin for correct and incorrect identifications

Форма DET-кривой на Рисунке 6 (log-log масштаб) иллюстрирует поведение системы в области низких FAR, что критично для промышленных СКУД: в точке FAR = 10^{-3} значение FRR составляет 8,28 %, то есть при требовании одного ложного пропуска на 1 000 импостор-попыток система отвергает около 8 % легитимных предъявлений. Гистограмма разности margin (Рисунок 7) показывает, что правильные распознавания сконцентрированы в области margin ≥ 0,10, тогда как ошибочные – в узком диапазоне margin < 0,05; это дает основание для введения вторичного порога по margin в миварных правилах: пары $X_1 \geq$ порог и margin ≥ 0,10 могут классифицироваться как trusted (Y_3), а $X_1 \geq$ порог, margin < 0,05 – как suspicious (Y_3).

Обсуждение

Достигнутые метрики нейросетевого модуля – Top-1 = 87,47 %, ROC-AUC = = 0,9985, EER = 1,64 % на датасете из 834 субъектов и 8 340 изображений – сопоставимы с показателями работ по распознаванию вен ладони [3] и современных глубоких сверточных моделей бесконтактной аутентификации по венам ладони [14]. Полученный показатель не является пределом: расширение датасета, применение более глубоких архитектур (ResNet50/101), использование специализированных функций потерь (ArcFace, CosFace) [15] и hard-negative mining в триплетном обучении потенциально могут поднять точность на несколько процентных пунктов. Для задач настоящей работы важнее не абсолютное значение Top-1, а поставка нейронной сетью интерпретируемого скаляра уверенности, который может быть использован логическим модулем в качестве одного из входов.

Ключевое отличие предложенной архитектуры от типовых биометрических СКУД с пороговым принятием решения состоит в том, что МЭС не просто применяет фиксированный порог к уверенности нейронной сети, а интерпретирует ее в контексте пяти других параметров. Это дает качественно новые возможности: биометрия с низкой уверенностью может быть допущена в малочувствительную зону при наличии прав доступа и режима рабочего времени; высокая уверенность не является достаточным условием для доступа при заблокированном статусе сотрудника; один и тот же входной параметр одновременно участвует в принятии решения о доступе и в оценке качества биометрии, что отражается в двудольном ориентированном графе КЭСМИ перекрестными дугами.

Предложенный подход обладает характерным для миварных технологий преимуществом линейной вычислительной сложности O(N) относительно числа правил [10], что принципиально отличает его от продукционных систем с экспоненциальным ростом. Это критично для промышленных СКУД: расширение базы знаний до сотен и тысяч правил (например, при добавлении новых зон доступа, временных режимов, категорий сотрудников) не приводит к деградации производительности решателя. Кроме того, добавление новых правил не требует переобучения нейронной сети – нейросетевой и логический модули развиваются независимо.

К ограничениям настоящего исследования следует отнести: использование авторской базы изображений, что ограничивает воспроизводимость результатов; отсутствие оценки устойчивости системы к атакам spoofing (презентационным атакам с использованием фотографий или искусственных моделей ладоней); отсутствие кросс-датасетного тестирования и оценки обобщающей способности модели на других популяциях; сравнительно небольшой набор контекстных параметров. Указанные ограничения не затрагивают общности архитектурного решения и являются направлениями дальнейшего развития работы.

Выбор миварного подхода вместо классических продукционных оболочек (CLIPS, Drools) или логических языков (Prolog) в разработанной СКУД мотивирован тремя факторами. Первый – линейная вычислительная сложность миварного решателя относительно числа правил [10], что позволяет безболезненно масштабировать базу знаний до сотен правил без потери производительности, характерной для forward-chaining продукционных систем. Второй – эволюционная природа миварного информационного пространства [8], позволяющая изменять набор параметров и отношений без переписывания кода: в нашей системе добавление новой зоны доступа или временного режима сводится к расширению перечня значений параметра X_3 или X_5 и дописыванию соответствующих правил. Третий – развитая экосистема КЭСМИ Wi!Mi, обеспечивающая визуализацию графа решения и отладку базы знаний без написания

дополнительного кода, что важно для инженеров СКУД без глубокой подготовки в области логического программирования.

Заключение

Разработана архитектура комплексной интеллектуальной системы контроля и управления доступом, объединяющая нейросетевой модуль биометрической идентификации по венам ладони и миварную экспертную систему. Нейронная сеть ResNet18, адаптированная для grayscale-изображений и обученная методом триплетного метрического обучения совместно с классификационной головой, обеспечивает биометрическую идентификацию с точностью Top-1 = 87,47 % и ROC-AUC = 0,9985 на датасете из 834 субъектов. Миварная экспертная система, реализованная в среде КЭСМИ Wi!Mi Разуматор, содержит три независимых отношения и формирует три выходных параметра: решение о доступе (Y_1), уровень тревоги (Y_2) и оценку надежности биометрии (Y_3). Общие входные параметры X_1, X_2 и X_6 порождают перекрестные дуги в двудольном графе решения КЭСМИ, что отражает многоаспектность принятия решений в комплексном ИИ.

Тестирование системы на трех репрезентативных сценариях подтвердило изменяемость топологии графа решения в зависимости от запрошенных выходов и заданных входов – от вырожденного графа с одним отношением до полного двудольного графа с перекрестными связями. Применение миварного подхода обеспечило линейную вычислительную сложность O(N) и эволюционируемость системы: расширение базы знаний выполняется без изменения нейросетевого модуля. Практическая значимость работы состоит в демонстрации применимости нейросимволического комплексного ИИ для задач биометрических СКУД, требующих одновременно высокой точности распознавания и прозрачного контекстного принятия решений, пригодного для аудита и сертификации.

Направлениями дальнейшего исследования являются: расширение датасета и кросс-датасетное тестирование, интеграция модуля определения presentation attack, расширение набора контекстных параметров (журналы событий, данные кадрового учёта), а также апробация предложенной архитектуры на других биометрических модальностях (радужная оболочка, рисунок пальцевых вен) в рамках концепции комплексного (гибридного, нейросимволического) ИИ.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Jain A.K., Ross A.A., Nandakumar K. *Introduction to Biometrics.* New York: Springer; 2011. 312 p. https://doi.org/10.1007/978-0-387-77326-1
2. Garcez A.D., Lamb L.C. Neurosymbolic AI: the 3*rd* wave. *Artificial Intelligence Review.* 2023;56(11):12387–12406. https://doi.org/10.1007/s10462-023-10448-w
3. Wu W., Elliott S.J., Lin S., et al. Review of palm vein recognition. *IET Biometrics.* 2020;9(1):1–10. https://doi.org/10.1049/iet-bmt.2019.0034
4. Das R., Piciucco E., Maiorana E., et al. Convolutional Neural Network for Finger-Vein-Based Biometric Identification. *IEEE Transactions on Information Forensics and Security.* 2019;14(2):360–373. https://doi.org/10.1109/TIFS.2018.2850320
5. Huang H., Liu Sh., Zheng H., et al. DeepVein: Novel finger vein verification methods based on deep convolutional neural networks. In: *2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), 22–24 February 2017, New Delhi, India.* IEEE; 2017. https://doi.org/10.1109/ISBA.2017.7947683

6. Sarker I.H. Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. *SN Computer Science.* 2021;2(6):420. https://doi.org/10.1007/s42979-021-00815-1
7. Kumar A., Zhou Y. Human Identification Using Finger Images. *IEEE Transactions on Image Processing.* 2012;21(4):2228–2244. https://doi.org/10.1109/TIP.2011.2171697
8. Варламов О.О. *Эволюционные базы данных и знаний для адаптивного синтеза интеллектуальных систем. Миварное информационное пространство.* Москва: Радио и связь; 2002. 286 с.
9. Varlamov O., Aladin D. A New Generation of Rules-based Approach: Mivar-based Intelligent Planning of Robot Actions (MIPRA) and Brains for Autonomous Robots. *Machine Intelligence Research.* 2024;21(5):919–940. https://doi.org/10.1007/s11633-023-1473-1
10. Варламов О.О. Миварные технологии: переход от продукций к двудольным миварным сетям и реализация автоматического конструктора алгоритмов, управляемого потоком входных данных и обрабатывающего более трех миллионов правил. *Искусственный интеллект.* 2012;(4):11–33.
Varlamov O.O. Mivar technologies: transition from productions to bipartite graphs mivar nets and realization of automated constructor of algorithms handling more than three million production rules. *Artificial Intelligence.* 2012;(4):11–33. (In Russ.).
11. Pizer S.M., Amburn E.Ph., Austin J.D., et al. Adaptive histogram equalization and its variations. *Computer Vision, Graphics, and Image Processing.* 1987;39(3):355–368. https://doi.org/10.1016/S0734-189X(87)80186-X
12. He K., Zhang X., Ren Sh., et al. Deep Residual Learning for Image Recognition. In: *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 27–30 June 2016, Las Vegas, USA.* IEEE; 2016. P. 770–778. https://doi.org/10.1109/CVPR.2016.90
13. Schroff F., Kalenichenko D., Philbin J. FaceNet: A Unified Embedding for Face Recognition and Clustering. In: *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 07–12 June 2015, Boston, USA.* IEEE; 2015. P. 815–823. https://doi.org/10.1109/CVPR.2015.7298682
14. Obayya M.I., El-Ghandour M., Alrowais F. Contactless Palm Vein Authentication Using Deep Learning With Bayesian Optimization. *IEEE Access.* 2020;9:1940–1957. https://doi.org/10.1109/ACCESS.2020.3045424
15. Deng J., Guo J., Xue N., et al. ArcFace: Additive Angular Margin Loss for Deep Face Recognition. In: *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 15–20 June 2019, Long Beach, USA.* IEEE; 2019. P. 4685–4694. https://doi.org/10.1109/CVPR.2019.00482

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Григоренко Кирилл Дмитриевич, студент кафедры ИУ-5, Московский государственный технический университет имени Н.Э. Баумана, Москва, Российская Федерация.

Kirill D. Grigorenko, Student at the Department IU-5, Bauman Moscow State Technical University, Moscow, the Russian Federation.

Горенков Александр Александрович, студент кафедры ИУ-5, Московский государственный технический университет имени Н.Э. Баумана, Москва, Российская Федерация.

Aleksandr A. Gorenkov, Student at the Department IU-5, Bauman Moscow State Technical University, Moscow, the Russian Federation.

Беляев Иван Андреевич, студент кафедры ИУ-5, Московский государственный технический университет имени Н.Э. Баумана, Москва, Российская Федерация.

Ivan A. Belyaev, Student at the Department IU-5, Bauman Moscow State Technical University, Moscow, the Russian Federation.

Варламов Олег Олегович, доктор технических наук, профессор, МИРЭА – Российский технологический университет, Московский государственный технический университет им. Н.Э. Баумана; главный научный сотрудник, Научно-исследовательский институт вычислительных комплексов имени М.А. Карцева, Москва, Российская Федерация.
e-mail: ovar@yandex.ru
ORCID: 0000-0002-2858-1383

Oleg O. Varlamov, Doctor of Engineering Sciences, Professor, MIREA – Russian Technological University, Bauman Moscow State Technical University; Chief Researcher, Kartsev Research Institute of Computing Complexes, Moscow, the Russian Federation.

Статья поступила в редакцию 06.05.2026; одобрена после рецензирования 10.06.2026; принята к публикации 22.06.2026.

The article was submitted 06.05.2026; approved after reviewing 10.06.2026; accepted for publication 22.06.2026.