СОВРЕМЕННЫЕ БИОМЕТРИЧЕСКИЕ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ И ИХ ПРИМЕНЕНИЕ В ВООРУЖЁННЫХ СИЛАХ

Хомутовский С. Л.[1], Шамаев В. А.[2], Григоренко А. Г.[3]

DOI:10.21681/3034-4050-2025-5-85-92

Ключевые слова: *уровень ложного приёма (FAR), уровень ложного отказа (FRR), биометрические технологии, физиологическая биометрия, защита биометрических данных.*

Аннотация

Цель *данной работы состоит в комплексном анализе современных физиологических, поведенческих и мультимодальных биометрических технологий, применяемых в боевых условиях Вооружённых Сил РФ.*

Метод исследования: *сравнительный анализ отечественных и зарубежных научно-технических публикаций и действующих российских нормативных актов в области защиты биометрических данных.*

Результат: *выполненный анализ позволил детализировать требования оборонного ведомства к системам защиты биометрических данных, систематизировать классы биометрических технологий и их ключевые метрические показатели (FAR, FRR, время срабатывания, устойчивость к помехам); проведён обзор российского и зарубежного технологического ландшафта 2025 года с акцентом на портативные мульти-сканеры, ABIS-платформы, венозные и 3D-лицевые сенсоры, а также решения для импортозамещения; проанализированы сценарии применения: доступ к арсеналам, идентификация союзников и пленных, защита ИТ-систем, мониторинг операторов БПЛА; выявлены кибер- и операционные угрозы (утечка биометрических шаблонов, захват устройств, спуфинг) и предложены меры защиты, включающие шифрование данных, построение air-gap-архитектуры, проверку живости и двухперсональную аутентификацию.*

Практическая ценность *заключается в проведении комплексного обзора и систематизации современных физиологических, поведенческих и мультимодальных биометрических технологий, с выделением ключевых метрических показателей (FAR, FRR, время срабатывания, устойчивость к помехам) и требований к их оптимизации.*

Введение

В современных условиях биометрическая аутентификация превращается в ключевой инструмент обеспечения безопасности [1] как информационных систем, так и объектов особой важности в форме вооружённых сил. Быстрый рост цифровых технологий и эволюция киберугроз обостряют потребность в надёжных методах идентификации, которые по скорости, точности и удобству явно превосходят традиционные пароли, пропуска или физические ключи [1, 2]. Уникальные биометрические признаки – отпечатки пальцев, рисунок радужной оболочки глаза, геометрия лица или голосовой профиль – не только трудно подделать, но и невозможно забыть или передать третьим лицам. По оценкам аналитиков, мировой рынок военной биометрии в 2024 году достиг приблизительно 7,2 млрд долл. и продолжает ежегодно расти на 6–7 %, что свидетельствует о масштабных инвестициях США, Китая, европейских стран и НАТО в создание обширных баз данных, портативных сканеров и интеграцию биометрии в инфраструктуру доступа на базы и пункты пропуска на границах.

Вместе с тем биометрические системы в военном сегменте сопряжены с новыми рисками, требующими усиленной защиты. Один из наглядных примеров – захват портативных сканеров HIIDE в Афганистане в 2021 г., когда экстремисты получили доступ к тысячам шаблонов отпечатков и образов радужной оболочки сотрудников коалиции, что создавало реальную угрозу жизни персонала и провалу операций. В отличие от пароля, биометрический шаблон нельзя «сменить», поэтому компрометация данных чревата длительными последствиями. Для внедрения подобных систем

1 Хомутовский Сергей Львович, младший научный сотрудник, Военная академия связи, Санкт-Петербург, Россия. E-mail: sergey_homutovsky99@mail.ru
2 Шамаев Вячеслав Алексеевич, младший научный сотрудник, Военная академия связи, Санкт-Петербург, Россия. E-mail: s-shamaev01@mail.ru
3 Григоренко Александр Георгиевич, младший научный сотрудник, Военная академия связи, Санкт-Петербург, Россия. E-mail: grigorenko.201@mail.ru

в ВС РФ необходимо сопровождение проектов строгим комплексом мер кибербезопасности: шифрование хранилищ, использование аппаратно-защищённых модулей, многоуровневая аутентификация и регулярный аудит. Только при таком подходе биометрия сможет обеспечить оперативную и точную идентификацию личного состава и потенциальных противников, а также значительно повысить защищённость стратегических арсеналов и информационных сетей от современных вызовов.

Требования к биометрическим системам аутентификации

Биометрическая аутентификация в военной сфере призвана устранить типичные уязвимости традиционных средств доступа, превращая уникальные физиологические параметры личности в надёжный «криптографический» ключ. В частности, на объектах хранения стратегического оружия применение двойной биометрической аутентификации – сочетание отпечатка пальца и венозного рисунка – реализует цифровой аналог «правила двух персон» [3,4], при котором доступ возможен лишь при одновременном сканировании двух ответственных сотрудников, что исключает одиночное снятие вооружения или ввод пускового кода.

Кроме повышения надёжности, биометрия обеспечивает беспрецедентную оперативность идентификации. Переносные сканеры, установленные на боевых блокпостах и учениях, позволяют в течение секунды сверить отпечаток или образ лица с локальной базой «своих» и «чужих», а при проверке задержанных – моментально устанавливать их личность по международным реестрам, что существенно сокращает время принятия решения и снижает риск «дружественного огня».

В цифровом тылу биометрические фильтры многократно повышают киберустойчивость закрытых сетей [5] и каналов связи: вход в защищённый штабной компьютер требует одновременного сканирования лица и отпечатка, а радио- или спутниковые терминалы блокируют передачу секретного трафика до верификации оператора по голосовой подписи, что делает перехват или кражу устройств бесполезными.

Не менее значимы возможности непрерывного мониторинга операторов сложных систем – БПЛА, ракетных комплексов и робототехники. Встроенные в пост управления датчики регулярно проверяют, что за консолью находится допущенное лицо, и одновременно анализируют признаки усталости и стресса (изменения моргания, замедление реакции). При обнаружении отклонений система автоматически сигнализирует о необходимости замены смены, существенно снижая риски аварий, обусловленных человеческим фактором.

Естественно, система, которая будет обеспечивать доступ к настолько важным системам, должна иметь беспрецедентный уровень надежности. Для систем биометрии существуют несколько метрик оценки надежности [2, 6]:

1) FAR (False Acceptance Rate) – вероятность того, что система ошибочно примет за легитимного пользователя неавторизованного субъекта. Для высокоточных физиологических сканеров этот показатель может быть ниже 0,001 % [2];
2) FRR (False Rejection Rate) – вероятность ложного отклонения законного пользователя. В поведенческих системах FRR, как правило, ниже нескольких процентов [6], но зависит от условий эксплуатации;
3) время срабатывания – задержка от момента предъявления биометрического образца до вынесения решения. В полевых и мобильных приложениях критично, чтобы время аутентификации не увеличивало риски или создавало узкие места в логистике;
4) устойчивость к помехам – способность сохранять адекватную точность при внешних воздействиях (изменение освещения, шум, пыль, вибрации) и противодействовать попыткам спуфинга (маски, высококачественные копии отпечатков, записи голоса).

Все современные методы биометрической аутентификации принято подразделять на три крупных «семейства».

Физиологические решения базируются на практически неизменных анатомических или генетических характеристиках человека – дактилоскопии, сканировании радужной оболочки и сетчатки глаза, 3D-геометрии лица, венозном рисунке ладони и даже анализе ДНК-профиля. За счёт высокой стабильности признаков они демонстрируют максимальную точность (FAR <0,001 %) и устойчивость к внешним воздействиям (радужка защищена естественной изоляцией, венозная сеть располагается под кожей). Вместе с тем необходимость близкого контакта или стационарной

установки оборудования ограничивает их мобильность, а простейшие сенсоры могут подвергаться атакам спуфингом (силиконовые слепки, высококачественные фото).

Поведенческие системы анализируют динамику действий пользователя – речь, почерк, ритмику набора текста, походку и манеру держать устройство. Такие методы неинвазивны и позволяют реализовать дистанционную и непрерывную аутентификацию в процессе работы: оператор или боец в зоне повышенного риска идентифицируется «на ходу» без дополнительных датчиков. Однако в силу высокой зависимости от эмоционального состояния, уровня стресса, усталости и окружающего шума их FRR может достигать нескольких процентов, что требует тщательной настройки алгоритмов и пороговых значений.

Мультимодальные системы объединяют два и более биометрических признака, компенсируя слабые стороны каждой методики и снижая уровни как FAR, так и FRR [6, 7, 8]. Например, одновременное сканирование отпечатка пальца, радужной оболочки и голосовой подписи с проверкой жизненности каждой компоненты надёжно исключает большинство спуфинговых атак. В Вооружённых Силах РФ мультимодальные сканеры рассматриваются базовыми для объектов повышенной секретности – от стратегических арсеналов до центров управления пусками. Их внедрение требует разработки единой платформы с аппаратно защищёнными криптомодулями, защищёнными протоколами хранения шаблонов и многоуровневой авторизацией, что обеспечивает быструю, надёжную и адаптивную идентификацию личного состава и своевременное реагирование на попытки несанкционированного проникновения.

Все вышеописанные семейства биометрических сканеров в том или ином виде разрабатываются или уже представлены в вооруженных силах различных государств:

1. Портативные ручные мульти-сканеры весят несколько сот граммов, защищены от пыли, ударов и осадков и способны непрерывно работать на аккумуляторе многие часы. В одном корпусе обычно сочетаются дактилоскопический датчик, камера для лиц и нередко модуль радужной оболочки. За минуту боец делает фотографию, снимает отпечаток и мгновенно сверяет их с локальной или удалённой базой [9] – даже при отсутствии связи, потому что часть шаблонов хранится прямо на устройстве.

Западный рынок опирается на эволюцию систем HIIDE/SEEK задействованных во время операции в Ираке; в России похожие терминалы [9, 4] демонстрировались на форумах «Армия» и входят в концепцию «Солдата будущего», ориентированную на спецподразделения и пограничные войска. Переход к мультимодальной биометрии позволяет одному прибору одновременно снимать лицо, палец и/или голос, снижая риск ложного отказа и усложняя задачу злоумышленнику, которому теперь нужно подделать несколько факторов сразу. [3,6]

2. ABIS-платформы (автоматизированные биометрические идентификационные системы) – это «сердце» биометрической инфраструктуры. В США уже много лет функционирует DOD ABIS – единый банк миллионов отпечатков, фото и радужек, к которому обращаются все силовые ведомства. Российский гражданский аналог – Единая биометрическая система (ЕБС); МВД и другие структуры ведут собственные базы, а в перспективе ожидается защищённая военная БИС, интегрированная с информационными системами ВС РФ.

Текущий тренд – гибридная архитектура: облако даёт масштаб, а edge-узлы (ноутбук офицера, постовой терминал) позволяют сравнивать шаблоны офлайн и лишь позже синхронизировать логи с центром. Для таких систем критична кибер-устойчивость: биоданные шифруются на устройстве, передаются по защищённым каналам, а ключи хранятся в аппаратных HSM-модулях; в России для этого применяются алгоритмы семейства ГОСТ [2,9]. Отдельно рекомендуется разносить сами биометрические шаблоны и персональные данные по разным сегментам сети, как это уже реализовано в ЕБС [10].

3. В случае венозных сенсоров инфракрасная камера считывает уникальный рисунок сосудов под кожей ладони или пальца. Узор не виден глазу, практически не оставляет «следов» и подтверждает «живость» благодаря кровотоку, что делает подделку крайне сложной [3, 6]. В военной сфере вен-сканеры рассматриваются для особо критичных объектов – например, доступа к ядерным хранилищам и пусковым установкам, где мёртвая ткань попросту не даст сигнал.

4. 3D-лицевые сенсоры используют камеры со структурированным светом или лазерным лидаром строят объёмную модель лица, анализируя глубину и форму черепа. Такой подход устойчив к плоским фотографиям и маскам и надёжно работает даже при частичном закрытии лица шлемом или балаклавой. [2, 7]

Состояние разработки биосистем в России и мире

Для ликвидации зависимости от западных стран в сфере технологий биометрических систем Госкорпорация «Ростех» разработала мультимодальный терминал проекта «Карта Родина», объединяющий геометрию лица, дактилоскопию и голосовую биометрию с перспективой добавления сканирования радужной оболочки и рисунка вен ладони, что позволяет проводить идентификацию офлайн за счёт хранения части шаблонов в самом устройстве.

Холдинг «Росэлектроника» выпустил программный комплекс «Биометрия-код», в котором нейросеть на лету генерирует одноразовые криптографические ключи из биометрических данных без хранения «сырых» шаблонов, гарантируя защиту информации и высокую стойкость к утечкам.

Российская компания BioSmart представила на конференции ЦИПР-2025 бесконтактный венозный сканер PalmJet, использующий мультиспектральный инфракрасный модуль для считывания уникального рисунка сосудов ладони и преобразования его в зашифрованный шаблон объёмом 2 КБ.

А в области антиспуфинга стартап NtechLab внедрил Liveness-модуль, способный отличать живое лицо от фотографий, масок и видеоимитаций путём анализа динамики выражений и текстуры кожи, что делает подделки практически бесполезными.

Актуальности этим технологиям добавляет то, что они уже были опробированны в самых разных ситуациях и сценариях:

На серверах, криптоконтроллерах и в закрытых комнатах связи Пентагона действует правило «смарт-карта + PIN + ты сам»: Common Access Card открывает дверь, персональный код активирует сеанс, а дактилоскопический или радужный скан подтверждает, что карту держит её владелец [6]. Чтобы исключить перехват радио¬эфира, военные тестируют голосовые «био-позывные»: терминал сравнивает речевой отпечаток с эталоном и отказывается переходить в зашифрованный режим, если тембр не совпадает [3, 6]; похожие решения испытывают и ВКС РФ.

На операциях в Ираке и Афганистане американские подразделения использовали портативные наборы HIIDE/SEEK II: четырёхкилограммовый прибор за минуту собирал отпечатки, лицо и радужку задержанного, сверяя их с центром ABIS или с локальной «белой» базой прямо на устройстве. Этой эволюции следует Next Generation Biometric Collection Capability (NXGBCC) – новый планшет-сканер, который в 2025 г. поступает в войска: к отпечаткам и радужке добавлен голос, а результат из DoD ABIS возвращается за секунды как при онлайн, так и при офлайн-работе. Аналогичный «мультимодальный» тренд наблюдается в РФ: шаблоны от полевых сканеров стекают в военную версию распределённой платформы-аналога DoD ABIS (гражданская ЕБС уже хранит лицо и голос десятков миллионов людей).

В классической «двух-ключевой» схеме ядерных хранилищ США каждое действие оператора – от извлечения Sealed Authenticator System до поворота пускового ключа – выполняют одновременно два офицера; сегодня к этому механизму добавили биометрию: цифровые «щит-двери» требуют, чтобы разные члены расчёта параллельно приложили, скажем, отпечаток пальца и скан радужки, прежде чем замки разблокируются. Новая Army Biometric Program Directive 2022 формализовала этот подход, предписав соединять аппаратные ключи, смарт-карты и живые шаблоны в единую политику контроля доступа для всех ядерных и криптографических зон. В России подобную философию реализуют вен-сканеры BioSmart PalmJet, показанные на ЦИПР-2025: мультиспектральная ИК-камера считывает рисунок сосудов ладони, шифрует 2-килобайтный шаблон и хранит его локально, что делает невозможным доступ к оружию без «живой» руки даже при утрате карт или PIN-кодов

Длительные дежурства за пультами беспилотников требуют непрерывной проверки как личности, так и работоспособности оператора. Китайские и американские исследования демонстрируют алгоритмы, которые каждые несколько минут повторно сканируют лицо пилота, сравнивают его с эталоном и параллельно вычисляют признаки усталости по динамике век, позе головы и зевкам; точность

выявления сонливости у UAV-пилотов на тестовой выборке OFDD превышает 97 % [6]. Европейские армии экспериментируют с очками-трэкером, фиксирующими частоту моргания и изменение зрачка: когда показатели выходят за норму, система автоматически вызывает сменщика, снижая риск аварий по вине человека [1].

Программа DARPA HumanID показала, что биометрическая «стена» может различать человека по лицу и походке на дистанции до 150 м, объединяя мультиспектральные камеры и миллиметровый радар для работы днём и ночью. Российские компании NtechLab и VisionLabs интегрируют сопоставимые алгоритмы в системы видеонаблюдения крупных городов и пограничных переходов, где программный пакет FindFace Multi ищет совпадения по лицу и силуэту в реальном времени, даже при частичном закрытии головы шлемом или балаклавой.

Однако несмотря на всю потенциальную пользу этих технологий, нельзя забывать о киберугрозах, связанных с их использованием. На таблице 1 собраны угрозы для биометрических систем [7].

Вместе с тем каждая из угроз представленная в таблице 1 компенсируется с помощью определенных мер защиты. Так утечка биометрических шаблонов нейтрализуется за счёт многоуровневой криптографической защиты самих данных и ключей [3]:

1) шаблоны хранятся в «отменяемом» (cancellable) виде – сначала через одностороннее преобразование превращаются в матрицу коэффициентов, из которой нельзя восстановить оригинальное изображение пальца или лица;
2) каждый шаблон дополнительно кодируется симметричным ключом, который лежит в аппаратном HSM/TPM-модуле; взлом БД без доступа к модулю даёт атакующему лишь бессмысленный набор байтов;
3) резервные копии, экспорт и межведомственный обмен идут только по защищённым контейнерам (ГОСТ R 34.10 + «Кузнечик») с обязательной двухсторонней аутентификацией источника и получателя;
4) кластеры БД сегментированы: биометрия отделена от персональных сведений, поэтому даже при частичной компрометации нельзя сопоставить отпечаток с конкретным человеком.

Захват устройств в полевых условиях компенсируется жёсткими мерами аппаратной и процедурной безопасности [10]:

1) внутренняя память сканера шифруется «на лету» аппаратным AES-XTS/ «Кузнечиком»; открытый ключ устройства стирается при извлечении накопителя или при попытке несанкционированного вскрытия корпуса (tamper-evident, zero-izable);
2) в терминале хранится только минимальный кэш «белого» списка, а полный журнал

Таблица 1.

Угрозы безопасности биометрических систем

Угроза	Суть и масштаб риска	Примеры
Утечка биометрических шаблонов	Взлом централизованной БД или кража локальных копий делает «пароль-навсегда» доступным противнику: отпечаток или лицо нельзя «сменить»	Атака на базу OPM (США), захват списков военных с отпечатками
Захват устройств в поле	Трофейный сканер/терминал хранит шаблоны и журналы; если диск не зашифрован, данные легко извлечь [10,3]	Случай с американскими HIIDE, попавшими к талибам
Перехват или подмена трафика (MiTM)	Радио- и спутниковые каналы можно перехватить; без сильного шифрования злоумышленник внедряет ложные шаблоны [10,2]	Риск особенно высок на выносных КПП с беспроводной связью
Спуфинг (подделка биометрии)	Слепки из силикона, 3D-маски или накладки на пальцы обходят старые датчики [2,4,7]	Демонстрации взлома отпечатков по фото с высоким разрешением

операций раз в X минут синхронизируется с центром и тут же удаляется локально;
3) для особо чувствительных приборов включается «kill-switch» – дистанционная команда на полное стирание памяти, если сканер не вышел на связь в заданное время;
4) вся периферия подписывается на базе устройств доверенной загрузки (Secure/ Measured Boot), что предотвращает замену прошивки при физическом доступе.

Перехват и подмена трафика (MiTM) устраняются через строгую политику сквозного шифрования и проверки целостности [10]:

1) каждое соединение «полевой терминал – центр» устанавливается по взаимной аутентификации на сертификатах ГОСТ или Suite B; сессионные ключи формируются по протоколу ECDH и меняются каждые несколько сотен пакетов;
2) сами шаблоны подписываются ЭП отправителя и снабжаются одноразовым счётчиком (nonce); при несовпадении подписи или повторном использовании счётчика пакет автоматически отклоняется;
3) каналы данных и канал управления разведены по разным VPN-туннелям; пробой шифра на одном не открывает доступа ко второму;
4) критически важные КПП получают автономный edge-узел ABIS, позволяющий сверять шаблоны офлайн, а потому не передавать их по радио вовсе.

Спуфинг (подделка биометрии) блокируется комплексом «Liveness + мультифакторность» [2,4,7]:

1) активные сенсоры проверяют «живость»: вен-сканер оценивает динамику кровотока, опто-датчик – микроконвульсии зрачка, 3D-камера – микроподвижки кожи;
2) система не принимает одиночный фактор – для доступа нужно совпадение хотя бы двух независимых модальностей (например, венозный рисунок + 3D-лицо);
3) каждый сеанс сопровождается случайным «челленджем» (изменение угла подсветки, произвольная фраза для голосовой проверки), что делает невозможным использование заранее записанных подделок;
4) алгоритмы антиспуфинга регулярно обновляются через доверенную цепочку OTA-подписей, чтобы закрывать новые методы атак (ультразвуковые слепки, 4-K-видеопетли).

Выводы

Проведённый обзор показывает, что современные физиологические, поведенческие и особенно мультимодальные биометрические технологии уже достигают требуемых для войск показателей (FAR < 0,001 %, FRR ≈ 1–3 %, время отклика ≤ 1 с) и могут служить базовым инструментом контроля доступа, идентификации личного состава и защиты критических ИТ-систем. Оптимальная архитектура военной биометрии формируется связкой «портативные мульти-сканеры ↔ гибридная ABIS ↔ высокостойкие сенсоры (венозные, 3D-лицевые)», дополненной отечественными алгоритмами ГОСТ и аппаратными HSM, что обеспечивает автономность на передовых позициях и централизованное, сегментированное хранилище с отменяемыми шаблонами.

Ключевые риски – утечка биошаблонов, захват полевых устройств, перехват трафика и спуфинг – эффективно снижаются многоуровневым шифрованием, политикой «liveness» и принципом двойной биометрической аутентификации. Российские импортозамещающие решения («Карта Родина», PalmJet, «Биометрия-код») демонстрируют технологическую готовность закрыть критические цепочки без западных компонентов, однако требуют дальнейшей стандартизации интерфейсов, унификации методик измерения FAR/FRR и углублённых исследований устойчивости к новым атакам (ультразвук, генеративное видео). Полученные результаты могут служить методической основой для разработки ведомственных нормативов и программ НИОКР по построению суверенной биометрической инфраструктуры ВС РФ.

Литература

1. Ryu R., Yeom S., Kim S.-H., Herbert D. Continuous Multimodal Biometric Authentication Schemes: A Systematic Review // IEEE Access. 2021. Vol. 9. C. 34541–34557. DOI: 10.1109/ACCESS.2021.3061589.
2. Mohamed Abdul Cader A. J., Banks J., Chandran V. Fingerprint Systems: Sensors, Image Acquisition, Interoperability and Challenges // Sensors. 2023. Vol. 23, No. 14. Article 6591. DOI: 10.3390/s23146591.

3. Ahamed F., Daskapan S., Juefei-Xu F. et al. An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services // Future Internet. 2022. Vol. 14, No. 8. Article 222. DOI: 10.3390/fi14080222.
4. Haider S. A., Ashraf S., Larik R. M. et al. An Improved Multimodal Biometric Identification System Employing Score-Level Fuzzification of Finger Texture and Finger Vein Biometrics // Sensors. 2023. Vol. 23, No. 24. Article 9706. DOI: 10.3390/s23249706.
5. Baig A. F., Eskeland S., Yang B. Novel and Efficient Privacy-Preserving Continuous Authentication // Cryptography. 2024. Vol. 8, No. 1. Article 3. DOI: 10.3390/cryptography8010003.
6. Иваненко В. Г., Иванова Н. Д., Сабанов А. Г. Повышение функциональной надёжности систем биометрической идентификации путём внесения избыточности // Безопасность информационных технологий. 2022. Т. 29, № 2. С. 36–45. DOI: 10.26583/bit.2022.2.03.
7. Wang Y., Shi D., Zhou W. Convolutional Neural Network Approach Based on Multimodal Biometric System with Fusion of Face and Finger Vein Features // Sensors. 2022. Vol. 22, No. 16. Article 6039. DOI: 10.3390/s22166039.
8. Micucci M., Iula A. Recognition Performance Analysis of a Multimodal Biometric System Based on the Fusion of 3D Ultrasound Hand-Geometry and Palmprint // Sensors. 2023. Vol. 23, No. 7. Article 3653. DOI: 10.3390/s23073653.
9. López-González P., Baturone I., Hinojosa M., Arjona R. Evaluation of a Vein Biometric Recognition System on an Ordinary Smartphone // Applied Sciences. 2022. Vol. 12, No. 7. Article 3522. DOI: 10.3390/app12073522.
10. Исмагилова А. С., Лушников Н. Д. Программная реализация защиты от несанкционированного доступа // Безопасность информационных технологий. 2023. Т. 30, № 1. С. 81–91. DOI: 10.26583/bit.2023.1.06.

MODERN BIOMETRIC DATA PROTECTION SYSTEMS AND THEIR APPLICATION IN THE ARMED FORCES

Khomutovsky S. L.[4], Shamaev V. A.[5], Grigorenko A. G.[6]

Keywords: *false acceptance rate (FAR), false failure rate (FRR), biometric technologies, physiological biometrics, biometric data protection.*

Abstract

Purpose *of this work is to comprehensively analyze modern physiological, behavioral and multimodal biometric technologies used in combat conditions of the Armed Forces of the Russian Federation.*

Research method: *comparative analysis of domestic and foreign scientific and technical publications and current Russian regulations in the field of biometric data protection.*

Result: *the analysis made it possible to detail the requirements of the defense department for biometric data protection systems, systematize the classes of biometric technologies and their key metric indicators (FAR, FRR, response time, immunity to interference); a review of the Russian and foreign technological landscape in 2025 was carried out with an emphasis on portable multi-scanners, ABIS platforms, venous and 3D facial sensors, as well as solutions for import substitution; application scenarios were analyzed: access to arsenals, identification of allies and prisoners, protection of IT systems, monitoring of UAV operators; Cyber and operational threats (leakage of biometric templates, device hijacking, spoofing) were identified and security measures were proposed, including data encryption, air-gap architecture, liveness checking, and two-person authentication.*

The practical value *lies in conducting a comprehensive review and systematization of modern physiological, behavioral and multimodal biometric technologies, with the allocation of key metric indicators (FAR, FRR, response time, immunity to interference) and requirements for their optimization.*

4 Sergey L. Khomutovsky, Junior Researcher, Military Academy of Communications, St. Petersburg, Russia. E-mail: sergey_homutovsky99@mail.ru
5 Vyacheslav A. Shamaev, Junior Researcher, Military Academy of Communications, St. Petersburg, Russia. E-mail: s-shamaev01@mail.ru
6 Alexander G. Grigorenko, Junior Researcher, Military Academy of Communications, St. Petersburg, Russia. E-mail: grigorenko.201@mail.ru

References

1. Ryu R., Yeom S., Kim S.-H., Herbert D. Continuous Multimodal Biometric Authentication Schemes: A Systematic Review // IEEE Access. 2021. Vol. 9. S. 34541–34557. DOI: 10.1109/ACCESS.2021.3061589.
2. Mohamed Abdul Cader A. J., Banks J., Chandran V. Fingerprint Systems: Sensors, Image Acquisition, Interoperability and Challenges // Sensors. 2023. Vol. 23, No. 14. Article 6591. DOI: 10.3390/s23146591.
3. Ahamed F., Daskapan S., Juefei-Xu F. et al. An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services // Future Internet. 2022. Vol. 14, No. 8. Article 222. DOI: 10.3390/fi14080222.
4. Haider S. A., Ashraf S., Larik R. M. et al. An Improved Multimodal Biometric Identification System Employing Score-Level Fuzzification of Finger Texture and Finger Vein Biometrics // Sensors. 2023. Vol. 23, No. 24. Article 9706. DOI: 10.3390/s23249706.
5. Baig A. F., Eskeland S., Yang B. Novel and Efficient Privacy-Preserving Continuous Authentication // Cryptography. 2024. Vol. 8, No. 1. Article 3. DOI: 10.3390/cryptography8010003.
6. Ivanenko V. G., Ivanova N. D., Sabanov A. G. Povyshenie funkcional'noj nadjozhnosti sistem biometricheskoj identifikacii putjom vnesenija izbytochnosti // Bezopasnost' informacionnyh tehnologij. 2022. T. 29, № 2. S. 36–45. DOI: 10.26583/bit.2022.2.03.
7. Wang Y., Shi D., Zhou W. Convolutional Neural Network Approach Based on Multimodal Biometric System with Fusion of Face and Finger Vein Features // Sensors. 2022. Vol. 22, No. 16. Article 6039. DOI: 10.3390/s22166039.
8. Micucci M., Iula A. Recognition Performance Analysis of a Multimodal Biometric System Based on the Fusion of 3D Ultrasound Hand-Geometry and Palmprint // Sensors. 2023. Vol. 23, No. 7. Article 3653. DOI: 10.3390/s23073653.
9. López-González P., Baturone I., Hinojosa M., Arjona R. Evaluation of a Vein Biometric Recognition System on an Ordinary Smartphone // Applied Sciences. 2022. Vol. 12, No. 7. Article 3522. DOI: 10.3390/app12073522.
10. Ismagilova A. S., Lushnikov N. D. Programmnaja realizacija zashhity ot nesankcionirovannogo dostupa // Bezopasnost' informacionnyh tehnologij. 2023. T. 30, № 1. S. 81–91. DOI: 10.26583/bit.2023.1.06.