



МЕТОДЫ РАСПОЗНАВАНИЯ ЛЮДЕЙ ПО ПАРАМЕТРАМ КАНАЛА WI-FI: ПРИМЕНИМОСТЬ В СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Белкин Е. Н. ORCID ID 0009-0007-5848-5433

*Акционерное общество «АЛГОНТ», Калуга, Российская Федерация,
e-mail: belkinen@algont.ru*

Актуальность исследования обусловлена развитием безустройственных методов математической и программной обработки параметров радиоканала беспроводной локальной сети для распознавания человека и необходимостью оценить переносимость лабораторных результатов в контур физического доступа. Цель работы – определить применимость таких методов для проверки владельца бесконтактной идентификационной карты в шлюзовой кабине, архитектурном шлюзе и турникете со шлюзованием, а также для распознавания личности без предъявления идентификатора. Выполнен структурированный обзор рецензируемых публикаций и стандартов. Сопоставлялись источник радиопризнаков, постановка индивидуальной верификации и поиска по базе, размер выборки, разделение обучающих и проверочных данных, устойчивость к смене ракурса и радиосреды, одновременное присутствие нескольких людей и биометрические показатели ошибок. Установлено, что наивысшие опубликованные результаты относятся главным образом к закрытой классификации в контролируемой радиосреде и не подтверждают требуемые для самостоятельного решения о допуске вероятность ложного совпадения, межсессионную устойчивость и корректный отказ неизвестному лицу. Наиболее обоснованным направлением является дополнительная проверка владельца карты в изолированной зоне одиночного прохода. Для архитектурного шлюза и турникета применимость зависит от пространственной изоляции, стабильности траектории и синхронизации с механикой. Идентификация у обычной двери или турникета пока не имеет достаточной доказательной базы. Радиопризнаки целесообразно использовать как скрытый дополнительный фактор или основание для усиленной проверки, но не как единственный фактор допуска.

Ключевые слова: радиобиометрическое распознавание, беспроводное зондирование, состояние радиоканала, обратная связь лучеформирования, машинное обучение, управление доступом, верификация личности, идентификация личности

HUMAN RECOGNITION METHODS BASED ON WI-FI CHANNEL PARAMETERS: APPLICABILITY TO ACCESS CONTROL AND MANAGEMENT SYSTEMS

Belkin E. N. ORCID ID 0009-0007-5848-5433

Joint Stock Company ALGONT, Kaluga, Russian Federation, e-mail: belkinen@algont.ru

The relevance of the study is determined by the development of device-free mathematical and software methods for processing wireless local-area-network channel parameters for human recognition and by the need to assess whether laboratory results can be transferred to physical access control. The purpose is to determine the applicability of these methods to verifying the holder of a contactless identification card in a security portal cabin, an architectural interlock, and an interlocking turnstile, as well as to recognizing a person without presenting an identifier. A structured review of peer-reviewed publications and standards was conducted. The comparison covered the radio-feature source, individual verification and database-search formulations, sample size, separation of training and test data, robustness to viewpoint and radio-environment changes, simultaneous presence of several people, and biometric error measures. The highest published results were found to relate mainly to closed-set classification in a controlled radio environment and not to demonstrate the false-match probability, cross-session stability, or correct rejection of an unknown person required for an independent access decision. The best-supported direction is supplementary verification of a cardholder in an isolated single-person passage zone. Applicability to architectural interlocks and turnstiles depends on spatial isolation, trajectory stability, and synchronization with the mechanism. Identification at an ordinary door or turnstile lacks sufficient evidence. Radio features should be used as a covert supplementary factor or a trigger for enhanced verification, not as the sole access factor.

Keywords: radio-biometric recognition, wireless sensing, channel state information, beamforming feedback, machine learning, access control, identity verification, person identification

Введение

Технологии беспроводного зондирования используют не только передачу данных, но и зависимость радиоканала от объектов в зоне распространения сигнала. Тело человека отражает, поглощает и рассеивает радиоволны, а движение изменяет многолучевую структуру канала. По временным по-

следовательностям этих изменений модели машинного обучения обнаруживают присутствие, оценивают активность, восстанавливают элементы походки и пытаются различать людей. Современные обзоры относят к основным нерешенным проблемам одновременное присутствие нескольких пользователей, изменение состава зарегистри-

стрированной группы, работу вне прямой видимости и перенос между помещениями, конфигурациями оборудования и пользователями [1–3].

Следует разграничивать распознавание человека и обнаружение принадлежащего ему устройства. Отслеживание MAC-адреса телефона, радиометки или сетевой активности устанавливает присутствие технического идентификатора и фактически дублирует фактор владения. Безустройственное распознавание, рассматриваемое в настоящей работе, предполагает, что проходящий не носит специального передатчика, а его личность оценивается по воздействию тела и движений на сигнал между стационарными узлами Wi-Fi.

Интерес к применению технологии в системах контроля и управления доступом (СКУД) усилился после публикации результатов BFId: для информации обратной связи формирования луча была заявлена точность $99,5 \pm 0,38$ % на наиболее крупной для данного направления выборке [4]. Однако общая точность классификации не эквивалентна вероятности ложного допуска. СКУД должна связать предъявленный идентификатор с конкретным человеком, отвергнуть незарегистрированное лицо, обработать непригодный образец и сохранить характеристики при смене дня, одежды, траектории и радиосреды. Предметом обзора являются алгоритмы выделения признаков из информации о состоянии канала (Channel State Information, CSI) и информации обратной связи формирования луча (Beamforming Feedback Information, BFI), модели машинного обучения и программные методы принятия решения, то есть компоненты математического и программного обеспечения вычислительных комплексов и компьютерных сетей, применяемые в СКУД. Поэтому научная оценка требует сопоставления экспериментальной постановки с эксплуатационным сценарием, а не непосредственного переноса максимальной опубликованной точности.

Для пропускных пунктов принципиально различаются две задачи. При предъявлении бесконтактной карты система получает заявленную личность и выполняет верификацию 1:1 – сравнение текущего радиообраза с шаблоном владельца карты. При отсутствии карты требуется идентификация 1:N с поиском по базе и одновременным решением, принадлежит ли человек зарегистрированному множеству. Вторая задача существенно сложнее, поскольку рост базы увеличивает число сравнений и риск случайно высокого совпадения, а открытая зона прохода затрудняет ассоциацию сигнала

с одним телом. В отличие от существующих обзоров [1–3], в настоящей работе опубликованные алгоритмы и протоколы сопоставляются не только между собой, но и с конкретными режимами СКУД. Научная новизна состоит в разграничении доказательности для верификации владельца карты и открытой идентификации, а также в формировании условий переноса результатов в шлюзовую кабину, архитектурный шлюз и турникет со шлюзованием.

Цель исследования – на основе рецензируемых публикаций и стандартов определить границы применимости алгоритмов выделения признаков из CSI/BFI, моделей машинного обучения и программных методов принятия решения для верификации владельцев бесконтактных карт в шлюзовой кабине, архитектурном шлюзе и турникете со шлюзованием, а также оценить готовность технологии к идентификации 1:N у двери или турникета.

Материалы и методы исследования

Работа выполнена как структурированный научный обзор. Поиск охватывал публикации 2016–2026 гг., опубликованные не позднее 31 августа 2026 г. На платформах ACM Digital Library, IEEE Xplore, ScienceDirect, Springer Nature, MDPI и PubMed по названию, аннотации и ключевым словам использовались сочетания: WiFi human identification, WiFi person authentication, CSI gait recognition, beamforming feedback identity, multi-user WiFi authentication, cross-domain WiFi sensing и их смысловые варианты. Дополнительная проверка полноты выполнена по спискам литературы обзоров [1–3], прямым и обратным цитированиям, а также по запросам: WiFi individual identification, identity legitimacy authentication, open-set WiFi recognition, unknown user, device-free fast identification и path-independent gait recognition. DOI, состав авторов, тип публикации и выходные сведения проверялись по страницам издателей.

Включались рецензируемые исследования безустройственной идентификации, аутентификации или повторной идентификации человека по параметрам серийных беспроводных локальных сетей; обзоры предметной области; работы о переносе между доменами, многопользовательском режиме и составительных воздействиях; стандарты зондирования и биометрических испытаний. Первичный поиск зарегистрировал 38 записей; дополнительная проверка полноты выявила 6 уникальных релевантных работ, поэтому итоговый массив составил 44 записи. Были удалены 7 дубликатов по DOI, а при его отсутствии – по названию

и составу авторов, проверены 37 записей; 7 исключены как не относящиеся к распознаванию личности. Полнотекстово оценены 30 публикаций; 9 исключены: 4 – без задачи установления личности, 2 – по радиомодальностям вне семейства Wi-Fi, 2 – об идентификации устройства, 1 – без окончательной рецензируемой публикации на дату поиска. В качественный синтез включена 21 рецензируемая работа – 18 первичных исследований и 3 обзора; отдельно использованы 4 стандарта.

Для каждого исследования кодировались источник радиопризнаков, способ предварительной обработки, архитектура модели и правило принятия решения; число участников; режим 1:1 или 1:N; закрытый либо открытый набор; разделение обучающих и тестовых данных; смена помещения, ракурса и траектории; наличие нескольких людей; длительность наблюдения; показатели ложного совпадения и ложного несовпадения; задержка и доступность кода или данных. Дополнительно формировался профиль доказательности по наличию независимых межсессионных испытаний, неизвестных лиц, смены радиосреды, многопользовательского режима, стандартизованных биометрических метрик и достаточного размера выборки; единый суммарный балл не рассчитывался. Из-за неоднородности выборок, протоколов и метрик метаанализ не проводился; применен качественный синтез с проверкой соответствия опытов трем эксплуатационным сценариям. Под архитектурным шлюзом понимается тамбур из двух взаимозависимых дверей, образованный строительными конструкциями, а под турникетом со шлюзованием – управляемая полоса, ограничивающая одновременный проход.

Результаты исследования и их обсуждение

Физическая основа и развитие методов

Наиболее распространенным источником данных является информация о состоянии канала (Channel State Information, CSI) – комплексные оценки амплитуды и фазы для поднесущих и пар передающих и приемных антенн. Временной ряд CSI содержит одновременно признаки движения человека и конкретной геометрии многолучевого распространения. Ранние системы подтвердили принципиальную различимость на малых закрытых выборках. В WiFi-ID средняя точность уменьшалась примерно с 93 до 77 % при росте числа кандидатов с двух до шести [5]. WifiU преобразовывал CSI в спектрограммы поход-

ки и сообщил точность первого результата 79,28 %, а попадание в первые три результата – 93,05 % [6]. FreeSense сочетал метод главных компонент, дискретное вейвлет-преобразование и динамическое выравнивание времени; для девяти участников точность составляла 88,9–94,5 % в зависимости от размера множества кандидатов [7]. Радиобиометрический подход показывал различимость через стену [8], а WiPIN – около 92 % для 30 участников при времени решения менее 300 мс [9]. Совокупно эти результаты подтверждают наличие индивидуально зависимых радиопризнаков, но также демонстрируют чувствительность к размеру класса и условиям регистрации.

Последующие работы уменьшали зависимость от направления и траектории, применяли перенос обучения, метрическое представление и открытое распознавание. Gate-ID учитывал зеркальное изменение радиосигнатуры при противоположных направлениях движения [10], GaitSense – разные скорости и траектории [11], CAUTION – маловыборочную открытую аутентификацию [12], подход повторной идентификации – сиамскую модель [13], а WiTL – перенос обучения между сценами и активностями [14]. MetaGanFi объединил условно-циклическую генеративно-состязательную сеть и доменно-независимое метаобучение: при одном и пяти регистрационных примерах точность составляла 87,25 и 93,50 % при изменении траектории и многолучевой среды, а также 86,84 и 91,25 % при изменении расположения устройств [15]. WiDFF-ID применял глубокую сверточную сеть с повторным использованием признаков и достиг средней точности 98 % для 42 участников [16]. Multi-WiIR использовал многоветвевую нейронную сеть и индивидуальные бинарные классификаторы для отказа незарегистрированным лицам; при числе легитимных пользователей до четырех достигнута точность 85,11 % [17]. Wi-GPD сочетал вариационное модальное разложение и плотность точек комплексного сигнала; для 5–20 участников сообщено 84,75–99,5 % [18]. Эти методы улучшают переносимость, снижают объем регистрации и учитывают неизвестных лиц, однако остаются привязаны главным образом к частным наборам данных и общей точности. Ни одна включенная работа одновременно не подтвердила крупную открытую выборку, независимые долговременные сессии, смену радиосреды, многопользовательскую ассоциацию и стандартизованные показатели допуска.

Вторым источником является информация обратной связи формирования луча

(Beamforming Feedback Information, BFI). Клиент вычисляет по оценке канала сжатое представление, необходимое точке доступа для направленной передачи. В отличие от CSI, извлечение BFI может не требовать модифицированной прошивки приемника, а передаваемые отчеты доступны в радиоэфире. Это снижает аппаратный барьер и одновременно создает угрозу скрытого наблюдения. Принятый в 2025 г. IEEE 802.11bf формализует процедуры зондирования беспроводной локальной сетью, но не устанавливает биометрические пороги, правила регистрации личности или пригодность результата для управления доступом [19].

Доказательность опубликованных результатов

Наиболее сильный количественный результат получен в BFId, где были записаны данные 197 участников, а пригодные BFI-последовательности сохранились для 161 чел. [4]. Для обычной ходьбы модель обучалась и проверялась после случайного разделения последовательностей каждого участника, и была получена точность $99,5 \pm 0,38$ %. Авторы дополнительно исследовали быстрый проход, рюкзак, перенос ящика и турникет. Этот эксперимент убедительно доказывает информативность BFI и масштабируемость закрытой классификации лучше прежних малых выборок.

Вместе с тем BFId исследовал угрозу раскрытия личности, а не биометрический контроллер доступа. Случайное разделение последовательностей 80:20 не отделяло регистрацию и проверку по независимым дням; примененный softmax-классификатор выбирал одного из известных участников и не обеспечивал полноценного отказа для неизвестного лица. Участникам предписывалось не носить свободную одежду, юбки, платья и обувь на каблуке. При обучении на одном ракурсе и проверке на другом большинство результатов было ниже 5 %, то есть радиосигнатура оказалась тесно связана с конкретной парой радиоприборов и геометрией прохода. Влияние долговременного дрейфа, перемещаемых объектов и других сетей оставлено открытым [4]. Поэтому заявленные 99,5 % нельзя интерпретировать как вероятность правильного допуска на реальной проходной.

Отдельная проблема возникает при нескольких людях. MultiAuth разделял многолучевые компоненты и аутентифицировал до трех пользователей, однако сообщил среднюю точность 86,2 % и показатель ложного принятия (false acceptance rate, FAR) 9,5 % [20]. Для СКУД остается задача пространственной ассоциации: радиоизмере-

ние должно относиться к человеку, предъявившему карту, а не к ожидающему рядом сотруднику. Библиотеки и сравнительные тесты также показывают сильную зависимость результатов от оборудования, набора данных и глубины модели [21], а исследования переноса относят смену помещения и конфигурации к главным барьерам [3].

Следовательно, общая точность классификации недостаточна для решения о допуске. Стандарты биометрического тестирования требуют отдельно оценивать вероятность ложного совпадения (false match rate, FMR), вероятность ложного несовпадения (false non-match rate, FNMR), долю непригодных образцов, пропускную способность и доверительные интервалы [22]. Обозначение FAR в отдельных публикациях сохраняется здесь только при воспроизведении авторской метрики и не считается автоматически тождественным стандартизированной FMR. Для сценария контроля доступа дополнительно важны длительность транзакции и испытания в условиях, соответствующих реальному потоку людей [23]. ГОСТ Р 51241-2008 устанавливает общие требования и методы испытаний средств и систем контроля и управления доступом, однако специальной радиобиометрической модальности не выделяет [24]. До появления воспроизводимых оценок по этим метрикам Wi-Fi-распознавание нельзя считать самостоятельным средством биометрического допуска.

Переход от классификации к задаче СКУД

Предъявление карты существенно улучшает постановку. Идентификатор задает один эталон, поэтому радиомодель должна ответить не «кто находится в зоне?», а «согласуется ли текущий образ с владельцем карты?». Верификация 1:1 уменьшает число сравнений и позволяет формировать индивидуальный порог. Однако она не устраняет необходимость подтвердить одиночность прохода и качество измерения. Практически оправдана трехисходная логика: совпадение, несовпадение и неопределенный результат. Последний не должен автоматически означать нарушение; он должен инициировать проверку лица, радужной оболочки глаза, персонального кода либо оператором.

Радиопризнак нельзя считать независимым от среды в том же смысле, что изображение радужки или контрольные точки отпечатка. В шаблон неизбежно входят особенности тела и походки вместе с геометрией помещения, положением антенн, состоянием дверей и окружающими отражателями. Поэтому регистрацию следу-

ет выполнять отдельно для каждой полосы и направления, в несколько дней и при различной одежде, обуви, скорости и переносимых предметах. Автоматическое пополнение шаблона каждым успешным проходом не следует применять без контроля качества, защиты от ошибочного сопоставления и механизма отката эталона, поскольку ошибка может постепенно изменить шаблон.

Оценка сценариев применения

Шлюзовая кабина является наиболее благоприятным сценарием. Закрытая первая дверь и независимый датчик заполнения позволяют подтвердить присутствие одного человека, зафиксировать состояние механизмов и выделить стабильное временное окно. Карта однозначно связывается с текущей транзакцией. Ограничениями остаются малая длина траектории, сильные отражения от металлоконструкций, изменение канала при движении створок и зависимость от одежды, груза или временного наруше-

ния походки. Поэтому кабина пригодна для теневого пилота и последующего применения радиопризнака как дополнительного фактора 1:1, но не как единственного основания для открытия второй двери.

Архитектурный шлюз потенциально предоставляет более длинный участок ходьбы, но хуже изолирует радиосреду. Через стекло и легкие перегородки на измерение воздействуют очередь, проходящие рядом люди и перемещаемое оборудование; траектория внутри тамбура обычно варьирует. Применение возможно лишь при гарантированном одиночном нахождении, ограниченной зоне чувствительности и регистрации шаблона именно для данного шлюза. В обычном широком тамбуре более реалистичны функции обнаружения присутствия, освобождения зоны и совместного прохода, а не подтверждение личности.

Ключевые экспериментальные результаты и ограничения их переноса в СКУД представлены в таблице.

Сопоставление ключевых исследований
безустройственного распознавания человека по Wi-Fi

Работа	Радиопризнаки, метод и дизайн	Основной результат	Ограничение для СКУД
BFI [4]	BFI; 197 участников, пригодные данные 161; закрытая 1:N	99,5 ± 0,38 %; случайное разбиение 80:20	Нет полноценного отказа неизвестному; разбиение не межсессионное; зависимость от ракурса
WiFi-ID [5]	CSI, походка; 2–6 чел.; закрытая 1:N	Точность ≈ 93–77 % при росте базы	Малая выборка; фиксированная траектория
MetaGanFi [15]	CSI; генеративная сеть и метаобучение; 1/5 примеров; смена домена	87,25–93,50%; решение около 0,1 с	Требуется регистрационный пример; нет нормированных FMR/FNMR
WiPIN [9]	CSI, стоящий человек; сопоставление признаков; 30 участников	Около 92 %; решение менее 300 мс	Закрытый набор; междневная переносимость не доказана
Gate-ID [10]	CSI; нормализация направления; 6–20 чел.	90,7–75,7 % при росте базы	Снижение при масштабировании; фиксированная установка
GaitSense [11]	CSI, признаки походки; 5–11 чел.	93,2 % (5); 76,2 % (11)	Малая выборка; закрытая классификация
CAUTION [12]	CSI; маловыборочное открытое распознавание	Порог неизвестного; 1/5 обучающих данных аналогов	Нет нормированных FMR/FNMR для проходной; ограниченная выборка
Person Re-ID [13]	CSI; сиамская модель, повторная идентификация	Сопоставление радиосигнатур между наблюдениями	Частный набор; нет метрик допуска и масштабного открытого теста
WiTL [14]	CSI; перенос обучения; разные сцены и активности	Более 93 % между сценами; более 97 % между активностями	Собственный протокол; нет стандартизованных показателей СКУД
Multi-WiIR [17]	CSI; многоветвевая сеть и бинарные классификаторы; до 4 пользователей	Точность до 85,11%; низкая задержка	Общая точность не задает ложный допуск; ассоциация «карта – тело» не решена
MultiAuth [20]	CSI; разделение многолучевых компонентов; до 3 чел. одновременно	86,2 %; авторами указано FAR 9,5 %	Недостаточно для единственного фактора; проблема ассоциации «карта – тело»

Примечание: составлена автором по источникам, указанным в графе «Работа»; показатели приведены в терминологии исходных публикаций и непосредственно не сопоставимы из-за различий выборок, протоколов и правил расчета метрик.

Турникет со шлюзованием фиксирует направление и положение проходящего лучше обычной двери. BFId показал сохранение информативности BFI при проходе через турникет [4]. Однако вращающийся ротор или створки сами изменяют радиоканал, человек адаптирует шаг к механике, а соседние полосы и очередь создают смешанные отражения. Перспективен выделенный канал, в котором измерение синхронизировано с положением механизма и выполняется до его движения либо после остановки. Решение следует использовать как вторичный фактор, а не переносить на многополосную проходную без пространственной изоляции. Режим идентификации 1:N у обычной двери или турникета в рассмотренных публикациях пока не получил достаточного экспериментального обоснования. Открытая радиозона не обеспечивает устойчивой связи между измерением и конкретным человеком, неизвестный посетитель должен быть корректно отвергнут, а междневная и межпозиционная стабильность не доказана на выборках масштаба промышленной СКУД. Даже высокая закрытая классификация не решает эту задачу. Достаточная точность может быть заявлена только после независимых испытаний открытого набора с предварительно заданными FMR и FNMR, а таких результатов для серийно применяемой системы пока нет.

Архитектура внедрения и программа испытаний

Рекомендуемая архитектура включает выделенные радиоустройства, формирующие воспроизводимый измерительный трафик; синхронизацию BFI или CSI с событием карты и состоянием двери или турникета; независимый датчик одиночного заполнения; модуль оценки качества; защищенное сравнение 1:1; политику усиленной проверки. Использование случайного офисного трафика нежелательно, поскольку частота отчетов зависит от нагрузки сети. Передача измерений должна иметь контроль целостности и времени, а сервер – запрещать решение по данным вне окна текущей транзакции.

Информационная безопасность должна учитывать как атаки на тракт измерения, так и состязательные воздействия на модель. Для классификаторов активности экспериментально показана деградация при специально сформированных возмущениях CSI [25]. Применительно к СКУД радиопомехи и подмена телеметрии являются прямыми угрозами; повтор записанных последовательностей и постепенное отравление эта-

лона следует рассматривать как проектные модели угроз, практическая реализуемость которых требует отдельной проверки. BFI, передаваемая в радиоэфире, одновременно облегчает внедрение и создает риск скрытого распознавания. Радиошаблоны, используемые для установления или подтверждения личности, целесообразно минимизировать, разграничивать и защищать на уровне, сопоставимом с иными биометрическими шаблонами; их конкретная правовая квалификация зависит от цели и организации обработки.

Пилотные испытания целесообразно начинать в теновом режиме без управления исполнительным устройством. Обучающие и тестовые проходы разделяются по дням, а не случайным фрагментам одной сессии. Отдельно проверяются неизвестные лица, чужие карты, зимняя и специальная одежда, сумки и грузы, разная скорость, остановки, изменение походки, соседняя полоса, движение дверей, перестановка оборудования и долговременный дрейф. До сбора данных задаются целевая вероятность ложного совпадения, допустимая вероятность ложного несовпадения, доля неопределенных результатов и предельная задержка. Только достижение этих показателей с доверительными интервалами позволяет переходить к ограниченному эксплуатационному применению.

Заключение

Проведенный обзор показывает, что безустройственное распознавание человека по CSI и BFI имеет достоверную физическую основу и способно различать людей в контролируемых экспериментах. Вместе с тем радиосигнатура объединяет особенности тела и движения с конфигурацией помещения, поэтому достигнутая закрытая точность не подтверждает эксплуатационные показатели биометрической СКУД.

Наиболее реалистично применение в шлюзовой кабине как дополнительной верификации 1:1 после предъявления карты и независимого подтверждения одиночного нахождения. Архитектурный шлюз пригоден только при радиопропространственной изоляции и стабильной траектории. Турникет со шлюзованием перспективен в выделенной полосе при синхронизации измерения с механикой. Во всех трех случаях неопределенный или отрицательный радиорезультат должен вести к другому биометрическому фактору либо операторской проверке. Использование Wi-Fi как единственного фактора допуска и идентификация 1:N у обычной двери или турникета преждевременны. Для изменения этого вы-

вода необходимы межсессионные и долговременные испытания открытого набора на крупных выборках, нормированные показатели ложного совпадения и несовпадения, проверка многопользовательской ассоциации и устойчивости к преднамеренным воздействиям. До получения таких доказательств рациональная роль технологии – скрытый дополнительный фактор, сигнал риска и средство инициирования усиленной проверки.

Список литературы

1. Wei Z., Chen W., Ning S., Lin W., Li N., Lian B., Sun X., Zhao J. A Survey on WiFi-based Human Identification: Scenarios, Challenges, and Current Solutions // *ACM Transactions on Sensor Networks*. 2025. Vol. 21. Is. 1. Art. 10. P. 1–32. DOI: 10.1145/3708323.
2. Mosharaf M., Kwak J. B., Choi W. WiFi-Based Human Identification with Machine Learning: A Comprehensive Survey // *Sensors*. 2024. Vol. 24. Is. 19. Art. 6413. DOI: 10.3390/s24196413.
3. Chen C., Zhou G., Lin Y. Cross-Domain WiFi Sensing with Channel State Information: A Survey // *ACM Computing Surveys*. 2023. Vol. 55. Is. 11. Art. 231. P. 1–37. DOI: 10.1145/3570325.
4. Todt J., Morsbach F., Strufe T. BFIId: Identity Inference Attacks Utilizing Beamforming Feedback Information // *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*. 2025. P. 2399–2413. DOI: 10.1145/3719027.3765062.
5. Zhang J., Wei B., Hu W., Kanhere S. S. WiFi-ID: Human Identification Using WiFi Signal // *Proceedings of the 12th International Conference on Distributed Computing in Sensor Systems*. 2016. P. 75–82. DOI: 10.1109/DCOSS.2016.30.
6. Wang W., Liu A. X., Shahzad M. Gait Recognition Using WiFi Signals // *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 2016. P. 363–373. DOI: 10.1145/2971648.2971670.
7. Xin T., Guo B., Wang Z., Li M., Yu Z. FreeSense: Indoor Human Identification with Wi-Fi Signals // *2016 IEEE Global Communications Conference*. 2016. P. 1–7. DOI: 10.1109/GLOCOM.2016.7841847.
8. Xu Q., Chen Y., Wang B., Liu K. J. R. Radio Biometrics: Human Recognition Through a Wall // *IEEE Transactions on Information Forensics and Security*. 2017. Vol. 12. Is. 5. P. 1141–1155. DOI: 10.1109/TIFS.2016.2647224.
9. Wang F., Han J., Lin F., Ren K. WiPIN: Operation-Free Passive Person Identification Using Wi-Fi Signals // *2019 IEEE Global Communications Conference*. 2019. P. 1–6. DOI: 10.1109/GLOBECOM38437.2019.9014226.
10. Zhang J., Wei B., Wu F., Dong L., Hu W., Kanhere S. S., Luo C., Yu S., Cheng J. Gate-ID: WiFi-Based Human Identification Irrespective of Walking Directions in Smart Home // *IEEE Internet of Things Journal*. 2021. Vol. 8. Is. 9. P. 7610–7624. DOI: 10.1109/JIOT.2020.3040782.
11. Zhang Y., Zheng Y., Zhang G., Qian K., Qian C., Yang Z. GaitSense: Towards Ubiquitous Gait-Based Human Identification with Wi-Fi // *ACM Transactions on Sensor Networks*. 2022. Vol. 18. Is. 1. Art. 1. P. 1–24. DOI: 10.1145/3466638.
12. Wang D., Yang J., Cui W., Xie L., Sun S. CAUTION: A Robust WiFi-Based Human Authentication System via Few-Shot Open-Set Recognition // *IEEE Internet of Things Journal*. 2022. Vol. 9. Is. 18. P. 17323–17333. DOI: 10.1109/JIOT.2022.3156099.
13. Avola D., Cascio M., Cinque L., Fagioli A., Petrioli C. Person Re-Identification Through Wi-Fi Extracted Radio Biometric Signatures // *IEEE Transactions on Information Forensics and Security*. 2022. Vol. 17. P. 1145–1158. DOI: 10.1109/TIFS.2022.3158058.
14. Lin C., Wang P., Ji C., Obaidat M. S., Wang L., Wu G., Zhang Q. A Contactless Authentication System Based on WiFi CSI // *ACM Transactions on Sensor Networks*. 2023. Vol. 19. Is. 2. Art. 29. P. 1–20. DOI: 10.1145/3532095.
15. Zhang J., Chen Z., Luo C., Wei B., Kanhere S. S., Li J. MetaGanFi: Cross-Domain Unseen Individual Identification Using WiFi Signals // *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 2022. Vol. 6. Is. 3. Art. 152. P. 1–21. DOI: 10.1145/3550306.
16. Wu Z., Xiao X., Lin C., Gong S., Fang L. WiDFF-ID: Device-Free Fast Person Identification Using Commodity WiFi // *IEEE Transactions on Cognitive Communications and Networking*. 2023. Vol. 9. Is. 1. P. 198–210. DOI: 10.1109/TCCN.2022.3222193.
17. Wei Z., Dong Y. Multi-WiIR: Multi-User Identity Legitimacy Authentication Based on WiFi Device // *Future Internet*. 2024. Vol. 16. Is. 4. Art. 127. P. 1–17. DOI: 10.3390/fi16040127.
18. Liu Y., Cao Z., Cai J., He Y., Hu M. Wi-GPD Identification System Based on Gait Point Density // *ACM Transactions on Embedded Computing Systems*. 2025. Vol. 24. Is. 4. Art. 61. P. 1–24. DOI: 10.1145/3746639.
19. IEEE 802.11bf-2025. IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 4: Enhancements for Wireless LAN Sensing. New York: IEEE, 2025. 228 p. DOI: 10.1109/IEEESTD.2025.11184214.
20. Kong H., Lu L., Yu J., Chen Y., Xu X., Lyu F. Toward Multi-User Authentication Using WiFi Signals // *IEEE/ACM Transactions on Networking*. 2023. Vol. 31. Is. 5. P. 2117–2132. DOI: 10.1109/TNET.2023.3237686.
21. Yang J., Chen X., Zou H., Lu C. X., Wang D., Sun S., Xie L. SenseFi: A Library and Benchmark on Deep-Learning-Empowered WiFi Human Sensing // *Patterns*. 2023. Vol. 4. Is. 3. Art. 100703. DOI: 10.1016/j.patter.2023.100703.
22. ISO/IEC 19795-1:2021. Information technology – Biometric performance testing and reporting. Part 1: Principles and framework. Geneva: International Organization for Standardization, 2021. 76 p. URL: <https://www.iso.org/standard/73515.html> (дата обращения: 02.09.2026).
23. ISO/IEC 19795-5:2011. Information technology – Biometric performance testing and reporting – Part 5: Access control scenario and grading scheme. Geneva: International Organization for Standardization, 2011. 36 p. [Электронный ресурс]. URL: <https://www.iso.org/standard/51768.html> (дата обращения: 02.09.2026).
24. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Введ. 2009-09-01. М.: Стандартинформ, 2009. (с Изменением № 1, введ. 2025-02-01). [Электронный ресурс]. URL: <https://protect.gost.ru/gost/details/b6aab7df-fac3-40d3-8c34-42e037e737c5> (дата обращения: 02.09.2026).
25. Ambalkar H., Wang X., Mao S. Adversarial Human Activity Recognition Using Wi-Fi CSI // *2021 IEEE Canadian Conference on Electrical and Computer Engineering*. 2021. P. 1–5. DOI: 10.1109/CECE53047.2021.9569098.

Конфликт интересов: Автор заявляет об отсутствии конфликта интересов.

Conflict of interest: The author declares that there is no conflict of interest.

Финансирование: Автор заявляет об отсутствии внешнего финансирования.

Financing: The research was performed without external funding.