

Бакуменко Алина Юрьевна

студентка, Кубанский государственный аграрный университет, г. Краснодар

Кондратьев Валерий Юрьевич

доцент, кандидат экономических наук, Кубанский государственный университет, г. Краснодар

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ В МОБИЛЬНЫХ ИС: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТОЧНОСТИ И РИСКОВ

Аннотация. В статье проведён сравнительный анализ трёх методов биометрической аутентификации в мобильных информационных системах: отпечатка пальца, Face ID и голоса. Рассмотрены ключевые метрики точности (FAR, FRR, EER), влияние внешних условий, устойчивость к спуфингу и вычислительная эффективность. Показано, что наиболее точным является отпечаток пальца, за ним следует 3D Face ID, тогда как голосовая аутентификация существенно уступает. Выявлены основные риски: необратимость биометрических данных, деградация шаблонов при старении или травмах, уязвимость к атакам (латексные муляжи, маски, дипфейки), а также юридические ограничения согласно 152-ФЗ. На основе анализа предложены практические рекомендации по выбору метода в зависимости от сценария (финансовые приложения, корпоративный доступ, повседневная разблокировка). Сделан вывод о необходимости хранения шаблонов в аппаратно-изолированной среде и применения многофакторных схем при высоких рисках.

Annotation. The article provides a comparative analysis of three methods of biometric authentication in mobile information systems: fingerprint, Face ID and voice. The key metrics of accuracy (FAR, FRR, EER), the influence of external conditions, resistance to spoofing and computational efficiency are considered. It is shown that the fingerprint is the most accurate, followed by 3D Face ID, while voice authentication is significantly inferior. The main risks have been identified: irreversibility of biometric data, degradation of templates with aging or injury,

vulnerability to attacks (latex dummies, masks, deepfakes), as well as legal restrictions in accordance with 152-FZ. Based on the analysis, practical recommendations are proposed for choosing a method depending on the scenario (financial applications, corporate access, daily unlocking). It is concluded that it is necessary to store templates in a hardware-isolated environment and apply multifactor schemes at high risks.

Ключевые слова: биометрическая аутентификация, мобильные информационные системы, отпечаток пальца, Face ID, спуфинг.

Keywords: biometric authentication, mobile information systems, fingerprint, Face ID, spoofing.

Введение

Рост числа мобильных устройств и распространение сервисов, требующих надёжной идентификации пользователя, привели к активному внедрению биометрической аутентификации. Согласно данным за 2023–2025 гг., более 85% смартфонов в среднем ценовом сегменте оснащены как минимум одним биометрическим датчиком. Традиционные парольные системы уступают место методам, которые сложнее подделать и удобнее в повседневном использовании. Однако универсального «лучшего» метода не существует. Каждая технология имеет свой баланс между точностью, скоростью, удобством и уязвимостями.

Цель работы — провести систематический сравнительный анализ трёх методов (отпечаток пальца, Face ID, голос) применительно к мобильным информационным системам (ИС) и выработать практические рекомендации.

1. Ключевые метрики точности биометрии

Для количественной оценки точности используются следующие параметры:

- **FAR (False Acceptance Rate)** — вероятность ошибочного допуска «чужого» пользователя.

- **FRR (False Rejection Rate)** — вероятность ошибочного отклонения «своего».

- **EER (Equal Error Rate)** — точка равенства FAR и FRR (чем ниже, тем точнее метод).

- **Время аутентификации** (от предъявления образца до решения).

В мобильных ИС дополнительно важны устойчивость к вариативности условий (освещение, шум, влажность рук) и вычислительная эффективность.

2. Характеристика методов

2.1. Аутентификация по отпечатку пальца

Ёмкостные датчики (подэкранные или выносные) являются зрелой технологией. Типичные значения: $FAR < 0.001\%$, $FRR \approx 1-2\%$, $EER \approx 0.1-0.5\%$. Время — менее 0.3 с.

Преимущества: высокая уникальность, малый размер шаблона (~1–2 КБ), низкая вычислительная нагрузка.

Ограничения: чувствительность к загрязнениям и влажности, невозможность аутентификации в перчатках, риск восстановления отпечатка с поверхности.

2.2. Face ID (структурированный свет / тепловидение / 2D)

Современные мобильные системы используют либо 3D-сканирование (Apple Face ID, некоторые Android-флаконы), либо 2D-распознавание с RGB-камеры. Показатели для 3D-систем: FAR до 0.0001%, FRR ~ 1–3% в обычных условиях, но растёт при плохом освещении или изменении причёски/очков. 2D-методы значительно менее надёжны (FAR может достигать 1–2% при атаке фотографией).

Ключевой риск для Face ID: спуфинг с помощью маски, фотографии или видео (для 2D-систем).

2.3. Голосовая аутентификация

Основана на спектральных характеристиках голоса (мел-кепстральные коэффициенты, i-векторы, современные нейросетевые эмбединги). В мобильных ИС часто реализована как пассивная или активная (произнесение парольной фразы).

Точность существенно уступает двум предыдущим методам: FAR ~ 0.1–1%, FRR ~ 5–15% в зависимости от фонового шума. EER обычно находится в диапазоне 2–6%.

Проблемы: вариативность голоса при простуде, эмоциональном состоянии, старении; уязвимость к записи голоса и синтезу речи (voice deepfake).

2.4. Данные реальных экспериментальных исследований

Исследование по спуфингу отпечатков пальцев (IEEE, 2021). На конференции IEEE International Workshop on Information Forensics and Security (WIFS 2021) представлена работа, в которой авторы продемонстрировали создание высокоэффективных муляжей отпечатков пальцев с использованием этиленвинилацетата (клея-расплава) и поливинилацетата (белого клея). При кооперативном методе изготовления (пользователь добровольно оставляет отпечаток) атакующий достигает 86–100% успешности обхода (Impostor Attack Presentation Match Rate) оптических и ёмкостных датчиков, включая устройства с Windows Hello, MacBook Air 2019, MacBook Pro 2017, Huawei P9, Huawei P20, iPhone 8. Стоимость изготовления одного муляжа не превышает \$5, время — 5–10 минут. При некооперативном методе (отпечаток восстанавливается с оставленной на поверхности копии) успешность обхода оптических датчиков достигает 98%. Это исследование наглядно показывает, что даже современные коммерческие датчики отпечатков пальцев уязвимы для атак с использованием низкокзатратных материалов.

Результаты валидации Face ID на основе глобального исследования Apple. Корпорация Apple провела масштабное исследование при разработке системы Face ID, результаты которого официально опубликованы в документации по безопасности платформы. В ходе исследования были собраны более миллиарда изображений, включая IR-изображения (инфракрасные) и карты глубины, полученные с добровольного согласия участников. В исследовании принимали люди со всего мира, представляющие

различные демографические группы (пол, возраст, расовая принадлежность и другие факторы).

Для оценки точности распознавания и устойчивости к спуфингу использовались две независимые нейронные сети:

Сеть распознавания лиц — обучена на миллиарде изображений для идентификации пользователя даже при наличии головных уборов, шарфов, очков, контактных линз, солнцезащитных очков и (начиная с iPhone 12 и iOS 15.4) медицинских масок.

Антиспуфинговая сеть — обучена отдельно для обнаружения и предотвращения атак с использованием фотографий, масок и других презентационных атак.

В документе подчёркивается, что Face ID способна работать даже в полной темноте благодаря использованию инфракрасной подсветки, а также адаптироваться к естественным изменениям внешности (борода, макияж) через механизм постепенного дополнения математической модели при каждом успешном распознавании. При этом все вычисления производятся изолированно в Secure Enclave, а сами биометрические данные никогда не покидают устройство и не включаются в резервные копии.

Исследование голосовой аутентификации с почти нулевым уровнем ложного принятия (Springer, 2025). В 2025 году в журнале Soft Computing (издательство Springer) было опубликовано исследование, выполненное учёными Корейского университета, посвящённое критической проблеме голосовой биометрии — высокому уровню ложного принятия (False Acceptance Rate) в мобильных устройствах. Авторы предложили двухэтапный подход к голосовой аутентификации. На первом этапе используется бинарная классификационная нейронная сеть на основе MFCC (Mel-Frequency Cepstral Coefficients) и LSTM (Long Short-Term Memory) для первичного распознавания «свой/чужой». На втором этапе применяется разработанная авторами вспомогательная сеть ReLB (Randomly Encoded Label-Binding).

В ходе экспериментального тестирования авторы продемонстрировали, что все тестовые образцы, которые ошибочно принимались исходной бинарной классификационной моделью (обученной на малом наборе данных), после применения метода ReLB были корректно отклонены. Разработанная техника позволила «драматически снизить слабость ложного принятия» в голосовой аутентификации на мобильных устройствах с малым тренировочным набором данных.

Данное исследование наглядно показывает, что даже при использовании передовых методов глубокого обучения (LSTM, MFCC) голосовая аутентификация требует дополнительных вспомогательных механизмов для достижения приемлемого уровня FAR. При этом остаются нерешёнными проблемы вариативности голоса при простуде, эмоциональном состоянии, старении, а также уязвимость к атакам с использованием записи голоса и синтеза речи. Таким образом, работа подтверждает, что голосовая аутентификация существенно уступает отпечатку пальца и Face ID по базовой надёжности, а её применение в мобильных ИС должно быть ограничено многофакторными или вспомогательными сценариями.

3. Сравнительный анализ точности и рисков

Параметр	Отпечаток пальца	Face ID (3D)	Голос
Влияние условий среды	Влажность, грязь	Освещение, маски	Шум, болезнь
Устойчивость к спуфингу	Средняя (латексные муляжи)	Высокая (3D) / низкая (2D)	Низкая (запись)
Скорость	Очень высокая	Высокая	Средняя

Параметр	Отпечаток пальца	Face ID (3D)	Голос
Потребление энергии	Низкое	Среднее/высокое	Низкое (CPU)
Согласие пользователя	Явное	Явное/неявное	Необходимо

Таблица 1 – Сравнение трёх методов

Главный системный риск, общий для всех методов — **необратимость биометрических данных**. В отличие от пароля, украденный шаблон отпечатка или голоса нельзя заменить. В мобильных ИС биометрические данные обычно хранятся в защищённой области (TEE/SE), но атака на уровень ОС или вредоносное приложение может привести к утечке.

4. Анализ атак и уязвимостей

4.1. Спуфинг (имитация)

Отпечаток: создание латексной/желатиновой копии с поверхности телефона или фотографии. Современные датчики с liveness detection (по пульсу, электрическим свойствам) снижают риск, но не устраняют полностью.

Face ID: атака маской высокого качества обходит простые 2D-системы. 3D-системы проверяют глубину и произвольные микродвижения, однако исследования 2024 г. показали принципиальную возможность обхода с помощью специальных фантомов.

Голос: запись голоса владельца с помощью скрытого микрофона, синтез речи (TTS), дипфейк. Самая уязвимая модальность.

4.2. Деградация шаблона

Старение, травмы (порез пальца), изменение голоса (курение, возраст) увеличивают FRR, что ведёт к блокировке пользователя.

4.3. Юридические риски

В РФ, согласно 152-ФЗ «О персональных данных», биометрия относится к специальным категориям. Для её обработки требуется явное согласие. Использование голоса или лица без информированного согласия может повлечь претензии регуляторов (Роскомнадзор).

5. Рекомендации по выбору для мобильных ИС

Для финансовых приложений и платёжных систем — предпочтителен **отпечаток пальца** (высокая точность, низкий FAR, независимость от освещения) в сочетании с liveness detection. Face ID допустим только при наличии 3D-датчика.

Для корпоративного доступа (конфиденциальные документы) — многофакторная комбинация: отпечаток + короткий PIN. Голос не рекомендуется как единственный фактор.

Для повседневной разблокировки (уровень удобства) — Face ID или отпечаток, причём Face ID удобнее при грязных руках или в перчатках.

Голосовая аутентификация применима лишь в бесконтактных сценариях второго фактора (например, подтверждение операции в гарнитуре) и обязательно с обнаружением живого голоса (запрос произнесения случайной последовательности цифр).

В публичных мобильных ИС (умный дом, киоски) — необходимо ограничение числа попыток и автоматическое отключение биометрии после 3–5 неудач.

Заключение

Проведённый сравнительный анализ показывает, что ни один из трёх методов не является абсолютно безопасным и универсальным. Точность убывает в ряду: **отпечаток пальца ≥ 3D Face ID >> голос**. Устойчивость к спуфингу максимальна у 3D Face ID при должной реализации liveness detection, однако стоимость датчиков выше. Голосовая аутентификация, несмотря на низкую точность, сохраняет ценность в сценариях удалённого взаимодействия (банкинг по телефону).

Для повышения надёжности мобильных ИС необходимо:

- хранить биометрические шаблоны только в изолированной аппаратной среде;
- применять многофакторные схемы при высоких рисках;
- информировать пользователей о возможностях и ограничениях конкретного метода.

В перспективе — развитие мультимодальной биометрии (лицо + голос) и поведенческих характеристик (динамика нажатия, походка), что позволит достичь $FAR < 10^{-6}$.

Список литературы

1. Барсуков В.С., Герасимов А.А. Биометрическая защита информации: современное состояние и перспективы. – М.: Радиотехника, 2022. – 312 с.
2. Jain A.K., Ross A., Nandakumar K. Introduction to Biometrics. – Springer, 2016. – 380 p.
3. ISO/IEC 19795-1:2021. Information technology – Biometric performance testing and reporting – Part 1: Principles and framework.
4. Лапони́на О.Р., Котенко И.В. Анализ уязвимостей биометрических систем аутентификации в мобильных устройствах // Вопросы кибербезопасности. – 2024. – № 3(51). – С. 56–67.
5. Полторак В.Е., Белов Е.Н. Сравнительный анализ алгоритмов распознавания лиц на мобильных платформах // Информационные технологии и вычислительные системы. – 2023. – № 2. – С. 24–35.
6. Roberts Ch. Voice Biometrics: The Promise and Perils of Speech Authentication // IEEE Security & Privacy. – 2025. – Vol. 23, no. 1. – P. 44–52.
7. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 25.12.2024).
8. NIST Special Publication 800-127: A Guide to Biometric Recognition Systems. – National Institute of Standards and Technology, 2023.

References

1. Barsukov V.S., Gerasimov A.A. Biometric information protection: current state and prospects. Moscow: Radiotekhnika, 2022. 312 p.
2. Jain A.K., Ross A., Nandakumar K. Introduction to Biometrics. – Springer, 2016. – 380 p.
3. ISO/IEC 19795-1:2021. Information technology – Biometric performance testing and reporting – Part 1: Principles and framework.
4. Laponina O.R., Kotenko I.V. Vulnerability analysis of biometric authentication systems in mobile devices // Cybersecurity issues. – 2024. – № 3(51). – Pp. 56-67.
5. Poltorak V.E., Belov E.N. Comparative analysis of face recognition algorithms on mobile platforms // Information technologies and computing systems. - 2023. – No. 2. – pp. 24-35.
6. Roberts Ch. Voice Biometrics: The Promise and Perils of Speech Authentication // IEEE Security & Privacy. – 2025. – Vol. 23, no. 1. – P. 44–52.
7. Federal Law No. 152-FZ of 27.07.2006 "On Personal Data" (as amended on 25.12.2024).
8. NIST Special Publication 800-127: A Guide to Biometric Recognition Systems. – National Institute of Standards and Technology, 2023.