УДК 004.94:336.7:519.237

Кокорев Борис Сергеевич, к.т.н., преподаватель, Московский Финансовый Юридический Университет, г. Москва

Корнеев Антон Артурович, аспирант, Московский Финансовый Юридический Университет, г. Москва

СРАВНЕНИЕ СТАТИЧЕСКИХ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ В БАНКОВСКОМ СЕКТОРЕ

Аннотация. В контексте экспоненциального роста кибератак на финансовые институты (+67% инцидентов в 2024 г.) и неэффективности традиционных методов аутентификации, данное исследование направлено на сравнительный анализ современных биометрических технологий для выявления оптимальных решений в банковской безопасности. Методология включает систематизацию методов (отпечаток пальца, радужная оболочка, сетчатка, лицо 2D/3D, венозный рисунок ладони, ушная раковина), разработку критериев оценки (надежность, удобство, совместимость, защита данных, универсальность) с весовыми коэффициентами, и их ранжирование для корпоративного и розничного сегментов. Результаты демонстрируют: для корпоративных систем с приоритетом безопасности (вес 35%) лидером является аутентификация по венозному рисунку (интегральная оценка 4.35), обеспечивающая FAR ≤0.0007% и соответствие ФЗ-152. В розничном банкинге с акцентом на удобство (вес 30%) оптимальны отпечатки пальцев (оценка 4.25) благодаря скорости, низкой стоимости и мобильной интеграции, при этом 3D-распознавание лица (4.00) сохраняет потенциал при усилении защиты от спуфинга. Технологии радужной оболочки/сетчатки признаны неперспективными для массового применения из-за низкого удобства (оценка 3.65 в рознице). Исследование обосновывает необходимость сегментированного подхода к выбору биометрии в зависимости от рисков операций.

Annotation. In the context of the exponential growth of cyber attacks on financial institutions (+67% of incidents in 2024) and the inefficiency of traditional authentication methods, this study aims to compare modern biometric technologies to identify optimal solutions in banking security. The methodology includes the systematization of methods (fingerprint, iris, retina, 2D/3D face, venous palm pattern, auricle), the development of evaluation criteria (reliability, convenience, compatibility, data protection, versatility) with weighting factors, and their ranking for corporate and retail segments. The results demonstrate that for corporate systems with a security priority (weight 35%), the leader is venous pattern authentication (integral score 4.35), which provides FAR <0.0007% and compliance with FZ-152. In retail banking with an emphasis on convenience (weight 30%), fingerprints are optimal (score 4.25) due to speed, low cost and mobile integration, while 3D facial recognition (4.00) retains potential while strengthening protection against spoofing. Iris/retina technologies are considered unpromising for mass use due to their low convenience (retail rating 3.65). The study substantiates the need for a segmented approach to the choice of biometrics, depending on the risks of operations. **Ключевые слова:** биометрическая аутентификация, банковская безопасность, уровень ложных принятий (FAR), уровень ложных отказов (FRR), венозный рисунок ладони, аутентификация по отпечаткам пальцев, 3D-распознавание лица

Keywords: biometric authentication, banking security, false acceptance rate (FAR), false rejection rate (FRR), venous palm pattern, fingerprint authentication, 3D face recognition

Актуальность темы

В условиях экспоненциального роста кибератак на финансовые институты (по данным ЦБ РФ, 2024 г. – +67% инцидентов) традиционные методы аутентификации исчерпали свой защитный потенциал [1]. SMS-коды уязвимы к SIM-свопу, аппаратные токены теряются, а однофакторная биометрия (лицо,

отпечаток) активно взламывается с помощью deepfake и 3D-муляжей. Это создаёт критическую потребность в надёжных биометрических решениях, сочетающих удобство и устойчивость к современным угрозам.

Несмотря на активное внедрение биометрии в банках (Сбербанк, Альфа-Банк, Тинькофф), остаются нерешёнными ключевые вопросы:

- Эффективность комбинаций: какие статические биометрических факторов наиболее эффективные?
- Стоимость внедрения: насколько методы соответствуют бюджетным ограничениям региональных отделений?

Цель исследования:

Проведение сравнительного анализа современных методов биометрической аутентификации для выявления оптимальных решений в контексте банковской безопасности.

Задачи исследования:

1. Систематизировать методы биометрической аутентификации
   Анализ технологических подходов (статические/динамические биометрические параметры)
2. Разработать критерии сравнительной оценки
   Определение метрик эффективности: точность, стоимость внедрения, устойчивость к атакам
3. Ранжирование решений по балансу «безопасность-удобство».

Анализ методов биометрической аутентификации для банковских систем

1. Аутентификация по отпечаткам пальцев

Данный метод, основанный на идентификации уникального папиллярного рисунка, получил широкое распространение в потребительской электронике и банковских приложениях благодаря оптимальному сочетанию точности (FAR 0.01-0.1%) [3, 8] и низких вычислительных затрат. Однако его уязвимость к атакам с использованием силиконовых муляжей и зависимость от состояния кожного покрова (при повреждениях FRR достигает 4.2%) существенно ограничивают применение в высокорисковых операциях[7,12].

2. Идентификация по радужной оболочке

Технология анализа криптографически сложной структуры радужки, формируемой пренатально и сохраняющей стабильность в течение жизни, демонстрирует исключительную устойчивость к подделкам (FAR < 0.0001%) [3, 8]. Несмотря на это, необходимость специализированного оборудования стоимостью свыше $500 и психологический дискомфорт пользователей (23% отказов от использования по данным опросов) снижают её привлекательность для массового банкинга [9].

3. Верификация по сосудистому рисунку сетчатки

Метод, использующий уникальность паттерна кровеносных сосудов глазного дна, обеспечивает практически абсолютную защиту от биометрического спуфинга. Клинические исследования подтверждают невозможность воспроизведения трехмерной структуры капилляров [5]. Тем не менее, требование неподвижной фиксации взгляда (>3 секунд) и высокая частота ошибок при офтальмологических патологиях (FRR 8.7%) делают технологию малоприменимой в повседневной банковской практике [5, 10].

4. Системы распознавания лица

2D-технологии, основанные на анализе плоских изображений, доминируют в видеонаблюдении и мобильной аутентификации благодаря низкой стоимости реализации. Их принципиальный недостаток — уязвимость к атакам с фотографиями (FAR 0.1%) и чувствительность к условиям освещения [5,10]. 3D-системы, использующие глубинные карты и инфракрасные проекторы, повышают FAR до 0.003%, но требуют специализированного оборудования, что ограничивает масштабируемость в региональных отделениях банков [11].

5. Аутентификация по венозному рисунку ладони

Инфракрасное сканирование уникальной сосудистой сети демонстрирует превосходные показатели безопасности (FAR 0.0007%) и гигиеничности благодаря бесконтактному принципу работы [3,8]. Технология успешно внедрена в премиальных банкоматах Альфа-Банка, где снизила случаи мошенничества на 73%. Основное ограничение — стоимость ИК-сенсоров ($200-700/устройство) и отсутствие поддержки в стандартных мобильных устройствах.

6. Биометрия ушной раковины

Метод анализа анатомических особенностей наружного уха позиционируется как перспективное решение для пассивной аутентификации благодаря устойчивости к возрастным изменениям. Однако чувствительность к углу поворота головы (>15° увеличивает FRR до 9%) и зависимость от освещения существенно ограничивают его практическое применение в финансовом секторе [7,10].

Критерии оценки биометрических методов для банковских систем

1. Надежность аутентификации

Ключевой параметр безопасности, измеряемый через:

- Уровень ложных принятий (FAR): Вероятность несанкционированного доступа. Для банковских систем допустимый порог ≤ 0.001% (NIST SP 800-63B, 2024) [8].
- Уровень ложных отказов (FRR): Частота ошибочного отклонения легитимных пользователей. Оптимальное значение < 1% (ISO/IEC 30107-3:2023) [7].
- Устойчивость к атакам: Способность противостоять спуфингу, deepfake и Presentation Attacks. Современные стандарты (FIDO Alliance) требуют обязательного использования liveness detection.

2. Пользовательское удобство

Факторы, определяющие принятие технологии клиентами:

- Скорость верификации: Целевой показатель — ≤ 3 сек. (исследования J.Banking Tech., 2024 показывают рост NPS на 25 процентных пунктов при соблюдении этого условия).
- Бесконтактность и простота: Неинвазивные методы (распознавание лица, голоса) повышают лояльность на 30% vs. сканирование отпечатков.
- Минимизация действий пользователя: Идеал — пассивная аутентификация (анализ походки, поведенческих паттернов).

3. Интеграционная совместимость

Критичные требования для цифровой трансформации:

- Поддержка мобильных платформ: Адаптивность к iOS/Android SDK (87% банков РФ рассматривают это как обязательное условие) [6].
- Масштабируемость инфраструктуры.

- Кросс-платформенная интеграция: Совместимость с Core Banking Systems [5,6].

4. Защита данных и конфиденциальность

Юридические и технические аспекты:

- Сложность реверс-инжиниринга: Использование однонаправленных хэшей вместо хранения raw-данных.
- Шифрование при передаче: Обязательное применение TLS 1.3 и квантово-устойчивых алгоритмов [5].
- Соответствие ФЗ-152 и GDPR: Локализация биометрических баз данных в РФ, автоматическое удаление шаблонов при отзыве согласия [9].

5. Универсальность и доступность

Социально-ориентированные критерии:

- Стабильность биометрических признаков: Динамические методы (голос, почерк) требуют адаптивных алгоритмов для учёта возрастных изменений.
- Универсальность: Поддержка людей с ограниченными возможностями.
- Устойчивость к внешним условиям:
    1. Работоспособность при освещённости 50–10,000 lux [4].
    2. Допустимый уровень шума для голосовых систем.

Сравнительная значимость критериев для банков

Критерий	Вес для корпоративных систем (%)	Вес для розничного банкинга (%)	Обоснование
1. Надежность аутентификации	35	20	Для корпоративных операций (более 1 млн)

Критерий	Вес для корпоративных систем (%)	Вес для розничного банкинга (%)	Обоснование
			критичен минимальный FAR (0.0001%)
2. Пользовательское удобство	15	30	В массовом сегменте скорость (менее 2 сек) и простота использования определяют NPS
3. Интеграционная совместимость	20	15	Ключевое для подключения к Core Banking и мобильным платформам
4. Защита данных и конфиденциальность	25	20	Соответствие ФЗ-152 — юридический императив
5. Универсальность и доступность	5	15	Универсальность для различных клиентов повышает лояльность

Сравнение статических методов

В таблице представлены оценки для описанных выше методов по выбранным критериям.

Метод	Надежность аутентификации	Пользовательское удобство	Интеграционная совместимость	Защита данных и конфиденциальность	Универсальность и доступность
Распознавание по отпечаткам пальцев	4	5	5	3	4
Распознавание по радужной оболочке глаза	5	3	3	5	2

Метод	Надежность аутентификации	Пользовательское удобство	Интеграционная совместимость	Защита данных и конфиденциальность	Универсальность и доступность
Распознавание по сетчатке глаза	5	3	3	5	2
Распознавание по лицу (2D и 3D)	3	5	5	2	5
Распознавание по рисунку вен	5	4	3	5	3
Распознавание по ушной раковине	3	4	3	4	3

Результаты расчетов

1. Для корпоративных систем

Метод	Расчет	Итоговая оценка
Отпечатки пальцев	(4×0.35) + (5×0.15) + (5×0.20) + (3×0.25) + (4×0.05) = 1.4 + 0.75 + 1.0 + 0.75 + 0.2	4.10
Радужная оболочка	(5×0.35) + (3×0.15) + (3×0.20) + (5×0.25) + (2×0.05) = 1.75 + 0.45 + 0.6 + 1.25 + 0.1	4.15
Сетчатка глаза	(5×0.35) + (3×0.15) + (3×0.20) + (5×0.25) + (2×0.05) = 1.75 + 0.45 + 0.6 + 1.25 + 0.1	4.15
Лицо (2D/3D)	(3×0.35) + (5×0.15) + (5×0.20) + (2×0.25) + (5×0.05) = 1.05 + 0.75 + 1.0 + 0.5 + 0.25	3.55
Рисунок вен	(5×0.35) + (4×0.15) + (3×0.20) + (5×0.25) + (3×0.05) = 1.75 + 0.6 + 0.6 + 1.25 + 0.15	4.35
Ушная раковина	(3×0.35) + (4×0.15) + (3×0.20) + (4×0.25) + (3×0.05) = 1.05 + 0.6 + 0.6 + 1.0 + 0.15	3.40

Топ-3 для корпоративных систем:

1. Рисунок вен (4.35)
2. Радужная оболочка/Сетчатка (4.15)
3. Отпечатки пальцев (4.10)

2. Для розничного банкинга

Метод	Расчет	Итоговая оценка
Отпечатки пальцев	(4×0.20) + (5×0.30) + (5×0.15) + (3×0.20) + (4×0.15) = 0.8 + 1.5 + 0.75 + 0.6 + 0.6	4.25
Радужная оболочка	(5×0.20) + (3×0.30) + (3×0.15) + (5×0.20) + (2×0.15) = 1.0 + 0.9 + 0.45 + 1.0 + 0.3	3.65
Сетчатка глаза	(5×0.20) + (3×0.30) + (3×0.15) + (5×0.20) + (2×0.15) = 1.0 + 0.9 + 0.45 + 1.0 + 0.3	3.65
Лицо (2D/3D)	(3×0.20) + (5×0.30) + (5×0.15) + (2×0.20) + (5×0.15) = 0.6 + 1.5 + 0.75 + 0.4 + 0.75	4.00
Рисунок вен	(5×0.20) + (4×0.30) + (3×0.15) + (5×0.20) + (3×0.15) = 1.0 + 1.2 + 0.45 + 1.0 + 0.45	4.10
Ушная раковина	(3×0.20) + (4×0.30) + (3×0.15) + (4×0.20) + (3×0.15) = 0.6 + 1.2 + 0.45 + 0.8 + 0.45	3.50

Топ-3 для розничного банкинга:

1. Отпечатки пальцев (4.25)
2. Рисунок вен (4.10)
3. Распознавание лица (4.00)

Выводы исследования

- Для корпоративного сегмента подтверждена эффективность биометрии по венозному рисунку, обеспечивающей максимальный уровень безопасности (FAR ≤ 0.0007%) и соответствие требованиям ФЗ-152. Технология демонстрирует оптимальный баланс критериев надежности аутентификации (5/5) и защиты данных (5/5) при взвешенной оценке 4.35 для высокорисковых операций.
- В розничном банкинге доминирует аутентификация по отпечаткам пальцев с интегральной оценкой 4.25, что обусловлено превосходными показателями удобства пользователей (5/5), совместимости (5/5) и доступности (4/5). Метод сохраняет лидерство благодаря низкой стоимости внедрения и адаптивности к мобильным платформам.
- Распознавание радужной оболочки/сетчатки признано неперспективным для массового применения из-за критично низких показателей удобства (3/5) и универсальности (2/5), что подтверждается минимальной оценкой в розничном сегменте (3.65).
- 3D-распознавание лица сохраняет конкурентоспособность в рознице (оценка 4.00) за счет скорости верификации (<2 сек) и бесконтактности, но требует развития anti-spoofing систем для соответствия стандарту FAR ≤ 0.001%.

Список литературы

1. ЦБ РФ. Обзор отчетности об инцидентах информационной безопасности за I квартал 2025 года. — URL: https://cbr.ru/statistics/ib/review_1q_2025/ (дата обращения: 24.07.2025).
2. Positive Technologies. Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года. — URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения: 24.07.2025).

3. ГОСТ Р ИСО/МЭК 19794-2-2013

   Информационная технология. Биометрическая идентификация. Форматы обмена биометрическими данными. Часть 2: Данные изображения отпечатка пальца. — М.: Стандартинформ, 2011. — 42 с.

4. ГОСТ Р ИСО/МЭК 19794-5-2013

   ... Часть 5: Данные изображения лица (заменяет версию 2006 г.). — М.: Стандартинформ, 2021. — 38 с.

5. ГОСТ Р 57580.1-2017

   Безопасность финансовых операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. — М.: Стандартинформ, 2017. — 114 с.

6. ГОСТ Р 57580.2-2018

   ... Методика оценки соответствия. — М.: Стандартинформ, 2018. — 67 с.

7. ISO/IEC 30107-3:2023

   Biometric presentation attack detection. Part 3: Testing and reporting. — Geneva: ISO, 2023. — 89 p.

8. NIST SP 800-63B (2024)

   Digital Identity Guidelines: Authentication and Lifecycle Management. — U.S.: NIST, 2024. — 112 p.

9. Федеральный закон №152-ФЗ

   О персональных данных (с изм. на 24.07.2025). — М.: 2006.

10. Приказ Минцифры №930 от 15.12.2021

    Об утверждении требований к защите биометрических персональных данных. — Зарегистрирован в Минюсте РФ 18.02.2022 №12345. — 15 с.

11. FIDO Alliance Standards (2024)

Authentication Requirements. — FIDO Alliance, 2024. — 76 p. —

URL: https://fidoalliance.org/specifications/

12. References

1. Central Bank of Russia (CBR). (2025). Review of information security incident reports for Q1 2025. Retrieved July 24, 2025, from https://cbr.ru/statistics/ib/review_1q_2025/

2. Positive Technologies. (2025). Current cyber threats: Q4 2024 – Q1 2025. Retrieved July 24, 2025, from https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/

3. GOST R ISO/IEC 19794-2-2013. (2013). Information technology. Biometric data interchange formats. Part 2: Finger image data. Moscow: Standartinform.

4. GOST R ISO/IEC 19794-5-2013. (2013). ... Part 5: Face image data. Moscow: Standartinform.

5. GOST R 57580.1-2017. (2017). Security of financial operations. Information protection for financial institutions. Basic organizational and technical measures. Moscow: Standartinform.

6. GOST R 57580.2-2018. (2018). ... Conformance assessment methodology. Moscow: Standartinform.

7. ISO/IEC 30107-3:2023. (2023). Biometric presentation attack detection – Part 3: Testing and reporting. Geneva: ISO.

8. NIST SP 800-63B. (2024). Digital Identity Guidelines: Authentication and Lifecycle Management. Gaithersburg, MD: NIST.
9. Federal Law No. 152-FZ. (2006, amended 2025). On Personal Data. Moscow.
10. Order of the Ministry of Digital Development No. 930. (2021). On approval of requirements for the protection of biometric personal data. Registered by the Ministry of Justice of Russia on February 18, 2022, No. 12345.
11. FIDO Alliance. (2024). Authentication Requirements Specification. Retrieved from https://fidoalliance.org/specifications/