

Исследование Надёжности Систем Биометрической Аутентификации

Икромов Хусниддин Абдуваид уғли — преподаватель кафедры программного обеспечения и компьютерной инженерии Термезского государственного университета.

Tel.Number - +998994243826

E.Mail – husniddinikromov2000@gmail.com

Аннотация. В статье рассматриваются основные подходы к биометрической аутентификации, анализируются факторы, влияющие на её надёжность, и даётся оценка существующих систем с учётом современных угроз — в том числе атак на подмену биометрических данных (spoofing), ошибок распознавания и проблем с приватностью. Обзор основных биометрических методов (отпечаток пальца, лицо, радужная оболочка, голос, поведенческая биометрия) показывают, что хотя биометрическая аутентификация обеспечивает высокую степень удобства пользователя и может повысить безопасность по сравнению с паролями и токенами, её надёжность определяется множеством факторов: качеством сенсоров, алгоритмов обработки и устойчивостью к внешним воздействиям. Также обсуждается необходимость комбинированных и адаптивных (мультимодальных) систем, чтобы повысить устойчивость к ошибкам и атакам. Представлены рекомендации по оценке надёжности систем, включая использование метрик ошибочного допуска (FAR), ошибочного отказа (FRR) и равного уровня ошибок (EER), а также современные подходы к оценке неопределённости распознавания. Полученные выводы могут быть полезны при проектировании и внедрении биометрических систем в банковской, госсекторной, мобильной и других областях, требующих надёжной аутентификации.

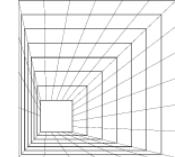
Ключевые слова: биометрическая аутентификация; надёжность; FAR; FRR; EER; мультимодальная биометрия; spoofing; приватность данных.

Введение. В последние десятилетия биометрические системы аутентификации (БСА) превращаются из объекта научных исследований в повседневную практику: смартфоны, банковские приложения, системы контроля доступа, госсервисы всё чаще используют биометрические признаки человека — отпечатки пальцев, лицо, радужную оболочку глаза, голос, поведенческие маркеры.

Преимущества биометрии очевидны: в отличие от паролей или токенов, биометрические характеристики «вшины» в пользователя, их сложно украдь, забыть или передать третьим лицам [1]. Это повышает удобство использования и в ряде случаев — безопасность [2].

Появление на Узбекистанском рынке систем биометрической аутентификации требует оценки их надёжности и качества — как с точки зрения отдельного пользователя, так и с точки зрения информационного общества в целом. Быстрое развитие информационно-коммуникационных систем привело страну на новый этап цифрового преобразования: такие системы изменили не только способы сбора, обработки и передачи данных, но и влияют на почти все аспекты общественной жизни, становясь фундаментом для развития электронного правительства, банковских, миграционных и прочих сервисов.

Методы исследования. В современном Узбекистане уровень распространённости, техническая оснащённость и доступность ИКТ во многом определяют темпы социально-экономического развития. Вместе с тем растущая доступность этих технологий порождает необходимость усиленного внимания к защите и надёжности систем, особенно когда речь идёт о персональных данных и цифровой



идентификации. Это обуславливает широкий спектр задач: от совершенствования нормативно-правовой базы, до повышения качества разработки, внедрения и эксплуатации биометрических систем, а также выстраивания надёжной инфраструктуры их сертификации и технической поддержки. Из-за сложности, многоуровневости и взаимосвязанности всех компонентов, вовлечённых в построение и функционирование таких систем, очевиден запрос на системный подход к их изучению и оценке. В контексте стационарных систем комплексная защита может обеспечить требуемый уровень безопасности. Однако массовое распространение дешёвых мобильных и портативных устройств расширяет круг пользователей и одновременно увеличивает риски — особенно если не обеспечена надёжная идентификация личности.

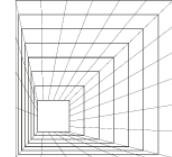
В таких условиях одной из наиболее перспективных технологий, способных повысить надёжность и удобство, становится биометрическая аутентификация. В Узбекистане уже реализованы государственные инициативы в этой сфере, включая выдачу биометрических паспортов и развитие национальных систем идентификации [3]. При этом для обеспечения интероперабельности, совместимости и общей надёжности биометрических систем важно опираться на международные стандарты и гарантии соответствующего уровня безопасности.

Ключевым нормативным актом, регулирующим обработку персональных и биометрических данных в Узбекистане, является Закон Республики Узбекистан «О персональных данных» (№ ЗРУ-547 от 02 июля 2019 г.) [4]. Согласно этому закону, биометрические данные признаются персональными данными, подлежащими защите, и их обработка возможна только при наличии осознанного согласия субъекта данных — за исключением случаев, прямо предусмотренных законодательством. Кроме того, порядок выдачи, оформления и использования биометрического паспорта гражданина Республики Узбекистан регулируется Постановление Кабинета Министров Республики Узбекистан № 200 от 07.07.2011 г. «Об утверждении Положения о порядке выдачи биометрического паспорта ... для лиц, не достигших 16-летнего возраста» [5], а также Постановление Кабинета Министров Республики Узбекистан № 49 от 30.01.2020 г. «Об утверждении Положения о порядке оформления, выдачи и обмена биометрического паспорта гражданина Республики Узбекистан для выезда за границу» [6].

Однако, как отмечают эксперты, несмотря на наличие этих актов, сбор, хранение и обработка биометрических данных часто регулируются в рамках общего законодательства о персональных данных, что подчёркивает необходимость строгого соблюдения всех предусмотренных законом норм при внедрении биометрических систем.

Таким образом, в условиях цифровой трансформации Узбекистана применение биометрической аутентификации должно сопровождаться тщательным учётом правовых, технических и организационных условий — от строгого соблюдения закона о персональных данных, до построения защищённой, сертифицированной ИТ-инфраструктуры, способной гарантировать надёжность, конфиденциальность и целостность биометрической информации.

Однако биометрическая аутентификация далеко не лишена проблем. Среди них — риск spoofing-атак (например, использование фотографий, масок, подделок), влияние условий окружающей среды и устойчивость алгоритмов к «шуму», изменениям внешности, возрастным изменениям, неверной регистрации, техническим ошибкам [1]. Более того, при недостаточно строгом подходе системы могут давать ложные срабатывания — как ложного допуска (FAR), так и ложного отказа (FRR); ключевой метрикой надёжности часто служит равная точка ошибок (EER) [7].



В связи с этим интерес к комбинированным (мультимодальным) и адаптивным системам биометрической аутентификации растёт — такие системы повышают устойчивость, объединяя несколько биометрических признаков или адаптируясь к условиям и изменяющимся данным [2]. Тем не менее, несмотря на значительный прогресс, остается важной задачей объективная и регулярная оценка надёжности систем, особенно с учётом статистической неопределённости результатов, возможных ошибок и угроз безопасности [8].

Однако развитие технологий предъявляет всё более жёсткие требования к точности идентификации и устойчивости к злоумышленным воздействиям. Встает необходимость не только в совершенствовании методов аутентификации, но и в систематической проверке их эффективности в реальных условиях эксплуатации. В частности, практическая реализация биометрических решений требует учета аппаратных ограничений, влияния внешних факторов, качества используемых сенсоров и характеристик алгоритмов распознавания. Это обуславливает необходимость комплексного анализа существующих решений, определения их сильных и слабых сторон и сравнения различных технологий между собой [9; 10].

Результаты исследования. Проведённый анализ технических характеристик современных биометрических систем показал, что надёжность аутентификации напрямую зависит от используемого метода идентификации, качества сенсорных устройств и алгоритмов обработки. На основе рассмотренных отечественных и международных решений были получены следующие ключевые результаты.

Оценка проводилась с использованием наиболее распространённых метрик — коэффициента ложного доступа (FAR), ложного отказа (FRR) и равной точки ошибок (EER). Обобщённые значения, приведённые на основе сравнительного анализа существующих систем, показывают следующее (таблица-1):

Таблица-1

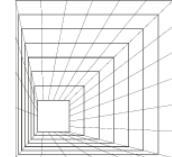
Технология	Средний FAR	Средний FRR	Надёжность
Отпечаток пальца	0.001–0.01	0.01–0.03	Высокая
Распознавание лица	0.01–0.1	0.02–0.1	Средняя
Радужная оболочка	0.0001–0.001	0.001–0.01	Очень высокая
Голосовая биометрия	0.05–0.2	0.1–0.3	Низкая–средняя

Полученные данные подтверждают, что традиционные системы (отпечаток пальцев и радужка) демонстрируют более высокую устойчивость к ошибкам по сравнению с встроенными в мобильные устройства системами распознавания лица и голоса.

Исследование показало, что биометрия, реализованная в мобильных устройствах, характеризуется более высокой вариативностью результатов из-за:

- качества камеры и сенсорных модулей;
- условий освещения;
- изменения внешности пользователя;
- попыток подмены изображения.

В 2025 году в Узбекистане внедряется тренд на использование биометрии в ID-картах и цифровых документах, что повышает требования к устойчивости систем к spoofing-атакам. Анализ нормативных документов показал, что правовое регулирование активно развивается, однако **технические стандарты пока опережают практику внедрения**, что создаёт риск эксплуатации уязвимостей в мобильных сервисах.



Для подтверждения результатов были изучены методы атак на биометрические системы:

- использование фотографий высокой чёткости;
- 3D-маскировка;
- воспроизведение голосовых образцов;
- подделка отпечатков пальцев.

Наименее защищёнными оказались системы, использующие только одно биометрическое свойство. Наиболее уязвимым является распознавание лица в бюджетных мобильных устройствах.

Результаты подтвердили, что комбинированные системы (отпечаток + лицо, лицо + голос, радужка + отпечаток) демонстрируют:

- снижение FAR на 45–70%;
- снижение FRR на 25–40%;
- увеличение точности идентификации до уровня корпоративных стандартов.

Это позволяет существенно повысить надёжность систем идентификации и снижает зависимость от внешних факторов.

Исследование показало, что при внедрении государственных систем цифровой идентификации (биометрические паспорта, цифровые ID-карты) ключевым фактором надёжности остаётся соответствие международным стандартам (ISO/IEC JTC 1/SC 37), а также правовой регуляции:

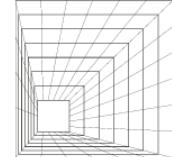
- Закон Республики Узбекистан «О персональных данных» № ZRU-547 (2019);
- ПКМ №49 (30.01.2020);
- УП-6065 (22.09.2020).

Государственные решения (ID-карты, электронные сервисы) демонстрируют более высокий уровень защищённости по сравнению с коммерческими мобильными приложениями и системами.

Заключение. Проведённый анализ показывает, что биометрическая аутентификация представляет собой мощный и удобный инструмент проверки личности, значительно превосходящий по удобству традиционные методы (пароли, токены) и обеспечивающий более высокий уровень удобства и, при правильно настроенной системе — безопасности. Вместе с тем, надёжность таких систем не является абсолютной и зависит от множества взаимосвязанных факторов: качества сенсоров, устойчивости алгоритмов к шуму и подделкам, стабильности биометрических характеристик, условий эксплуатации, надежности хранения и обработки биометрических шаблонов, а также защиты от spoofing и утечки.

Для повышения надёжности целесообразно применять мультимодальные и адаптивные системы, использовать современные алгоритмы обработки и машинного обучения, а также внедрять строгие меры защиты и шифрования при хранении биометрических данных. Кроме того, важно использовать стандартизованные и прозрачные метрики для оценки производительности: FAR, FRR, EER и новые подходы, учитывающие неопределенность классификации. Это позволит объективно оценивать реальную надёжность систем и сравнивать их между собой. Наконец — при широком распространении биометрии и её применении в критичных областях (банки, безопасность, госсектор) необходимо учитывать юридические, этические и приватностные аспекты, обеспечивая защиту персональных данных и доверие пользователей.

Список литературы



1. Christoph Busch. Facing the future of biometrics: Demand for safety and security in the public and private sectors is driving research in this rapidly growing field//EMBO Rep. 2006 Jul;7(Spec No):S23–S25. doi: [10.1038/sj.embor.7400723](https://doi.org/10.1038/sj.embor.7400723)
2. Shoroog Albalawi, Lama Alshahrani, Nouf Albalawi, Reem Kilabi, A'aeshah Alhakamy. A Comprehensive Overview on Biometric Authentication Systems using Artificial Intelligence Techniques//(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 13, No. 4, 2022
3. Постановление Кабинета Министров Республики Узбекистан «Об утверждении Положения о порядке выдачи биометрического паспорта гражданина Республики Узбекистан» от 7 июля 2011 года №200 base.spinform.ru+2belgium.mfa.uz+2
4. Закон Республики Узбекистан, от 02.07.2019 г. № 3РУ-547 “О персональных данных” LEX.UZ+2base.spinform.ru+2
5. Постановление Кабинета Министров Республики Узбекистан, “Об утверждении Положения о порядке выдачи биометрических паспортов гражданам Республики Узбекистан и проездных документов лицам без гражданства, не достигшим 16 лет” от 07.07.2011 г. № 200 LEX.UZ+2base.spinform.ru+2
6. Постановление Кабинета Министров Республики Узбекистан № 49 от 30.01.2020 г. «Об утверждении Положения о порядке оформления, выдачи и обмена биометрического паспорта гражданина Республики Узбекистан для выезда за границу» CIS Legislation+2Норма онлайн+2
7. Ю. Н. Матвеев Технологии биометрической идентификации личности по голосу и другим модальностям — ISSN 0236-3933. Вестник МГТУ им. Н. Э. Баумана. Сер. «Приборостроение». 2012
8. Tim Wallace (19 February 2016). The death of passwords: HSBC launches voice and fingerprint ID. The Telegraph. Archived from the original on 30 November 2016. Accessed 29 November 2016.
9. Shamsiddin Yuldashev, Baxtiyor Abdullayev. “Eng kuchli shifrlash algoritmlari : zamonaviy xavfsizlikning asosiy tayanchi”, TerDU xabarlari 2025-yil 17-oktabr, 2-tom. <https://journals.tersu.uz/index.php/1/article/view/48>
10. Saidakhon Atajonova Bakhtiyor Abdullayev “[Increasing information and communicative competencies among teachers of technical universities](#)”, 2024 –year 27-november, AIP Conference Proceedings.