Секция «43.14 Экономика инноваций»

За пределами удобства: детерминанты принятия биометрической аутентификации в России

Заявка № 1670279

Технологии биометрической аутентификации (ТБА) стали рутинным элементом цифрового ландшафта. Согласно исследованиям ВЦИОМ, рост одобрения с 27% в 2023 до 50% в 2025 г. [1,3] Однако, несмотря на технологическую зрелость и позитивный сдвиг в общественном мнении, фактический уровень проникновения в России остается крайне низким: на начало 2026 г. в Единой биометрической системе (ЕБС) зарегистрировано лишь ∼6% населения.[2] Этот разрыв между позитивным отношением и реальным использованием указывает на существование глубинных барьеров, не сводимых к техническим или правовым аспектам, которые были частично нивелированы Федеральным законом № 572-ФЗ. [4]

Существующие исследования биометрии преимущественно сфокусированы на алгоритмической надежности и безопасности инфраструктуры. Социокультурные детерминанты принятия — институциональное доверие, восприятие рисков утраты телесной идентичности, культурные нормы — остаются на периферии научного дискурса.

Цель работы — разработать расширенную версию модели принятия и использования технологий UTAUT2 [5], на основе выявленных установок и паттернов поведения пользователей в ходе эмпирического исследования, и адаптировать для анализа принятия «чувствительных» инноваций.

В ходе исследования были проведены глубинные полуструктурированные интервью с респондентами 23–48 лет, стратифицированными по уровню вовлеченности в ТБА (активные/слабые пользователи и не пользователи). Сценарный дизайн интервью охватывал как низкорисковые практики (оплата проезда, доступ на работу), так и высокорисковые транзакции (дистанционные сделки с недвижимостью). Анализ проводился методом осевого кодирования с последующей интеграцией данных в теоретическую рамку модели UTAUT2.

ТБА относятся к «чувствительной» категории инноваций, так как затрагивают фундаментальные аспекты приватности и идентичности. Это делает стандартные предикторы UTAUT2 недостаточными для объяснения вариативности пользовательского выбора. Преодоление этого ограничения потребовало расширения исходной модели путем интеграции дополнительных конструктов. В данном исследовании были выдвинуты следующие факторы: институционального доверия, перцептивных рисков и границ приватности.

Анализ интервью подтвердил значимость как базовых, так и расширенных конструктов модели. Факторы UTAUT2 такие как удобство и скорость (ожидаемая полезность) драйвят принятие в рутине, но технические сбои могут снижать этот эффект. Социальное влияние работает как индикатор безопасности («если все пользуются, значит, безопасно»). Значимость гедонистической мотивациии нивелирована среди не пользователей ТБА, но приобретает важное значение среди пользователей.

В ходе исследования была выявлена критическая роль расширенных конструктов. Было обнаружено, что институциональное доверие асимметрично. Государство (ЕБС) воспринимается как более надежный гарант сохранности данных по сравнению с коммерческими структурами, что легитимирует централизацию биометрии.

Также необходимо отметить существующую иерархию рисков. Наибольшую тревогу вызывают дипфейки и подделка лица/голоса. При этом наблюдается «технологический фетишизм»: методы, воспринимаемые как более сложные для подделки (сетчатка, отпечаток пальца), вызывают большее доверие, чем лицо.

Жесткие границы неприемлемости активируются в высокорисковых сценариях (крупные сделки), где респонденты требуют дополнительных гарантий или предпочитают отсрочить использование технологии.

Основным результатом является разработка контекстуально-чувствительной расширенной версии модели UTAUT2 для биометрической аутентификации. Показано, что включение блоков институционального доверия, восприятия рисков телесной идентичности и социокультурных границ позволяет объяснить вариативность принятия ТБА там, где базовая модель демонстрирует объяснительный разрыв.

Полученные выводы свидетельствуют о формировании в России гибридной модели принятия: рациональный выбор, основанный на удобстве (ядро UTAUT2), опосредуется глубокими культурными паттернами отношения к государству, риску и телесной приватности.

Источники и литература

1) Биометрия — новый стандарт безопасности? // URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/biometrija-novyi-standart-bezopasnosti?ysclid=mlxstwfja3446332036 (дата обращения: 20.02.2026).
2) Биометрия в МФО может улучшить качество портфеля задолженностей // rbc URL: https://companies.rbc.ru/news/6dHqI5nFwa/biometriya-v-mfo-mozhet-uluchshit-kachestvo-portfelya-zadolzhennostej/?ysclid=mlxsq9p6fw385464677 (дата обращения: 20.02.2026).
3) Делиться биометр Федеральный закон "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" от 29.12.2022 N 572-ФЗ (последняя редакция)ическими данными: выгоды и риски // Wciom URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/delitsja-biometricheskimi-dannymi-vygody-i-riski?ysclid=mlxs92g5ss264916620 (дата обращения: 20.02.2026).
4) Федеральный закон "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" от 29.12.2022 N 572-ФЗ (последняя редакция)
5) Venkatesh V., Thong J.Y.L., Xu X. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology // MIS Quarterly. – 2012. – Vol. 36, No 1. – P. 157–178.