Научная статья
УДК 338.2:338.46
DOI: 10.25683/VOLBI.2025.73.1469

Dmitry Alexandrovich Nikolaev
Candidate of Economics,
Associate Professor of the Department of Economic Security and Risk Management,
Financial University
under the Government of the Russian Federation
Moscow, Russian Federation
DNikolaev@fa.ru

Дмитрий Александрович Николаев
канд. экон. наук,
доцент кафедры экономической безопасности и управления рисками,
Финансовый университет
при Правительстве Российской Федерации
Москва, Российская Федерация
DNikolaev@fa.ru

Aisa Arkadyevna Sandzhieva
Student of the Department of Economic Security and Risk Management,
field of training
38.03.01 — Economics,
Financial University
under the Government of the Russian Federation
Moscow, Russian Federation
a.sandzhieva2004@mail.ru

Айса Аркадьевна Санджиева
студент кафедры экономической безопасности и управления рисками,
направление подготовки
38.03.01 — Экономика,
Финансовый университет
при Правительстве Российской Федерации
Москва, Российская Федерация
a.sandzhieva2004@mail.ru

ОТ KYC К eKYC: КАК БИОМЕТРИЯ И ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ УКРЕПЛЯЮТ ФИНАНСОВУЮ ПРОЗРАЧНОСТЬ

5.2.3 — Региональная и отраслевая экономика

Аннотация. *В условиях цифровой трансформации финансового сектора система идентификации клиентов претерпевает фундаментальные изменения. Статья посвящена комплексному анализу эволюции процедур KYC от традиционных к современным решениям в области электронной идентификации (eKYC) с акцентом на проблемы и перспективы их внедрения в России и за рубежом. Особое внимание уделяется технологическим аспектам eKYC, включая биометрическую верификацию, использование искусственного интеллекта и блокчейн-решений. Проведен сравнительный анализ международного опыта внедрения систем цифровой идентификации в различных юрисдикциях: от индийской системы Aadhaar и сингапурского SingPass до европейских стандартов eIDAS и африканских решений для финансовой инклюзии. Выявлены как успешные кейсы, так и системные проблемы, связанные с кибербезопасностью и цифровым неравенством. В контексте российской практики детально рассмотрены этапы становления Единой биометрической системы и нормативной базы, регулирующей дистанционную идентификацию. На основе проведенных расчетов продемонстрирована экономическая эффективность внедрения eKYC: при первоначальных инвестициях в 15 млн руб. и горизонте планирования 3 года чистая приведенная стоимость проекта достигает положительна и значительна, показатель ROI высокий. Сформулированы ключевые вызовы, включая риски утечек биометрических данных, необходимость преодоления цифрового разрыва и этические дилеммы. Предложены направления развития, среди которых — внедрение децентрализованных моделей идентификации, совершенствование регуляторной базы и формирование общественного доверия. Доказано, что eKYC становится стратегическим активом для повышения финансовой инклюзии, прозрачности и безопасности банковского сектора.*

Ключевые слова: *eKYC, цифровая идентификация, биометрия, финансовая прозрачность, банковский сектор, удаленная идентификация, цифровые технологии, безопасность данных, финансовая инклюзия, искусственный интеллект*

Для цитирования: Николаев Д. А., Санджиева А. А. От KYC к eKYC: как биометрия и цифровая идентификация укрепляют финансовую прозрачность // Бизнес. Образование. Право. 2025. № 4(73). С. 149—156. DOI: 10.25683/VOLBI.2025.73.1469.

Original article

FROM KYC TO eKYC: HOW BIOMETRICS AND DIGITAL IDENTIFICATION STRENGTHEN FINANCIAL TRANSPARENCY

5.2.3 — Regional and sectoral economy

Abstract. *In the context of the digital transformation of the financial sector, the customer identification system is undergoing fundamental changes. The article is devoted to a comprehensive analysis of the evolution from traditional KYC procedures to modern solutions in the field of electronic identification (eKYC), with an emphasis on the problems and prospects of their implementation in Russia and abroad. Special attention is paid to the technological aspects of eKYC,*

including biometric verification, the use of artificial intelligence and blockchain solutions. A comparative analysis of international experience in the implementation of digital identification systems in various jurisdictions is conducted: from the Indian Aadhaar system and Singapore's SingPass to European eIDAS standards and African solutions for financial inclusion. Successful cases as well as systemic problems related to cybersecurity and digital divide are identified. In the context of Russian practice, the stages of formation of the Unified Biometric System (UBS) and the regulatory framework governing remote identification are considered in detail. Based on our own calculations, the economic efficiency of implementing eKYC has been demonstrated: with an initial investment of 15 million rubles and a planning horizon of 3 years, the net present value of the project is positive and significant, the ROI indicator is high. Key challenges are formulated, including the risks of biometric data leaks, the need to bridge the digital divide, and ethical dilemmas. The directions of development are proposed, including the introduction of decentralized identification models (SSI), the improvement of the regulatory framework and the formation of public trust. It has been proven that eKYC is becoming a strategic asset for increasing financial inclusion, transparency and security of the banking sector.

Keywords: *eKYC, digital identification, biometrics, financial transparency, banking sector, remote identification, digital technologies, data security, financial inclusion, artificial intelligence*

For citation: Nikolaev D. A., Sandzhieva A. A. From KYC to eKYC: how biometrics and digital identification strengthen financial transparency. *Biznes. Obrazovanie. Pravo = Business. Education. Law*. 2025;4(73):149—156. DOI: 10.25683/VOLBI.2025.73.1469.

Введение

Актуальность. Финансовая система XXI в. переживает кардинальные трансформации, вызванные цифровизацией экономики, ростом числа глобальных транзакций и ужесточением регуляторных требований. Если раньше контроль за финансовыми потоками в основном лежал на государственных органах, сегодня основная ответственность постепенно переносится на банки, страховые компании и финтех-компании. В этом контексте ключевым инструментом остается концепция «Знай своего клиента» (*KYC*). Значение *KYC* выходит за рамки простого контроля за мошенничеством — это важная часть глобальной системы противодействия отмыванию доходов и финансированию терроризма (далее — ПОД/ФТ). Международные организации, включая Группу разработки финансовых мер борьбы с отмыванием денег (*Financial Action Task Force on Money Laundering*, *FATF*) и Базельский комитет по банковскому надзору, постоянно обновляют стандарты, стимулируя финансовые институты внедрять всё более строгие процедуры идентификации [1].

Однако традиционный *KYC*, основанный на бумажных документах и личных визитах клиентов, в условиях цифровой экономики показал себя недостаточно эффективным. Особенно ярко это проявилось во время пандемии *COVID*-19: ограниченный доступ к офисам, высокие издержки, медленные процессы и уязвимость к подделкам документов подчеркнули необходимость нового подхода. На этом фоне появился *eKYC* — электронная проверка клиентов, основанная на цифровых документах, биометрии и современных технологиях.

Изученность проблемы. Вопросы цифровой идентификации и внедрения электронных систем *KYC* (*eKYC*) находятся в центре внимания современных исследований, что отражено в работах ведущих отечественных и зарубежных специалистов. Так, Е. Н. Денисевич и И. И. Фищенко подробно анализируют влияние *AML/CFT* на повышение финансовой безопасности государства [1]. Е. Н. Барашко и Р. А. Парагульгов исследуют актуальные технологии идентификации в финансовом секторе, подчеркивая значимость биометрических решений [2]. Т. Ю. Мазурина и Е. И. Шаманина акцентируют внимание на рисках цифровизации и необходимости правового регулирования новых форм легализации доходов [3]. Работа В. В. Егина посвящена проблемам внедрения биометрии в банковской сфере, выявляя перспективные направления развития [4]. Особое значение приобретает региональное сотрудничество в области цифровой идентификации, о чем свидетельствуют исследования О. И. Долгановой в азиатском регионе [5]. Нормативно-правовые аспекты *e*-платежей рассмотрели И. О. Харуна, П. А. Айдоноджи, О. Д. Бейда — это вносит важный вклад в понимание регуляторного поля [6]. Н. А. Ковалева, Н. В. Ермакова, Д. Д. Тулаева проводят комплексный анализ биометрических технологий, подчеркивая их роль в обеспечении безопасности банковских операций [7]. Е. Н. Храмов и О. В. Вершинина рассматривают биометрию как фактор конкурентоспособности и безопасности в современных условиях [8]. Е. И. Шаманина и Ю. С. Захаренко выделяют биометрические методы как перспективное средство улучшения удаленного банковского обслуживания [9]. Важен также правовой аспект, изученный А. Р. Попковой, в части использования биометрических данных [10]. Н. В. Кузнецов фокусируется на применении биометрии в борьбе с отмыванием денег и финансированием терроризма, подкрепляя актуальность темы [11]. Аналитические отчеты *McKinsey Global Institute* подтверждают значимость цифровой идентификации для социально-экономического развития и усиления финансовой инклюзии.

Таким образом, современная литература демонстрирует широкий и глубокий анализ технологических, правовых и организационных аспектов *eKYC*, что создает прочную теоретическую базу и подчеркивает актуальность дальнейших исследований в данной области.

Целесообразность разработки темы. Сегодня *eKYC* воспринимается не просто как технологическая новинка, но и как важный инструмент обеспечения прозрачности и устойчивости финансовых систем. Он сочетает удобство для клиента, безопасность для компании и контроль для регулятора. В отличие от классического *KYC*, который требовал личного визита, паспортных документов, справок о доходах и ручной проверки сотрудниками банка, *eKYC* автоматизирует процесс и минимизирует человеческий фактор.

Цель исследования — комплексно проанализировать эволюцию процедур *KYC* к *eKYC*, оценить их проблемы и перспективы внедрения, а также продемонстрировать экономическую эффективность данного перехода.

Задачи исследования: проанализировать преимущества и недостатки традиционного *KYC* и *eKYC*; исследовать технологические аспекты *eKYC* (биометрия, искусственный интеллект, блокчейн); провести сравнительный анализ международного опыта внедрения *eKYC*; рассмотреть специфику российского опыта внедрения *eKYC* [Единая биометрическая система (далее — ЕБС), законодательство]; выявить ключевые вызовы и риски, связанные с *eKYC* (кибербезопасность, цифровое неравенство, этические дилеммы); предложить направления дальнейшего развития *eKYC*; оценить экономическую эффективность внедрения *eKYC* на основе расчетов.

Научная новизна заключается в комплексном анализе эволюции *KYC* к *eKYC* с учетом технологических, регуляторных, этических и экономических аспектов, а также в проведении собственных расчетов экономической эффективности и предложении направлений развития, учитывающих специфику российской экономики.

Теоретическая значимость исследования заключается в систематизации знаний о *eKYC*, его технологических основах, преимуществах и недостатках. Вклад в понимание влияния цифровой трансформации на финансовый сектор. **Практическая значимость** заключается в том, что результаты исследования могут быть использованы финансовыми институтами при принятии решений о внедрении *eKYC*, регуляторами при разработке нормативной базы, а также для формирования стратегии развития цифровых сервисов в банковском секторе.

Основная часть

Методология исследования. Данное исследование представляет собой комплексный анализ, основанный на сочетании методов. В ходе анализа научной литературы использованы труды российских и зарубежных ученых, статьи в научных журналах, материалы конференций для обзора существующих подходов к *KYC* и *eKYC*, а также анализ проблем и перспектив. Проведен сравнительный анализ международного опыта внедрения систем цифровой идентификации в различных юрисдикциях (Индия, Сингапур, Европейский Союз, Африка) для выявления успешных кейсов и системных проблем. В результате статистического анализа (включая экономическое моделирование) на основе данных о затратах и выгодах традиционного *KYC* и *eKYC* (включая данные *McKinsey Global Institute*) выполнен расчет экономической эффективности внедрения *eKYC* (*NPV*, *ROI*) для гипотетической когорты клиентов. В результате системного анализа изучены этапы становления ЕБС в России и нормативной базы, регулирующей дистанционную идентификацию, для понимания российского контекста. Индуктивный и дедуктивный подходы применялись для формирования общих выводов на основе частных наблюдений (анализ конкретных кейсов) и для применения общих принципов к конкретным проблемам (например, применение принципов кибербезопасности к *eKYC*).

Результаты исследования и их обсуждение. Преимущества *eKYC* очевидны: скорость процедуры — минуты вместо дней; точность благодаря алгоритмам распознавания лиц и машинному обучению; сокращение затрат на персонал и бумажный документооборот; гибкость и интеграция с государственными цифровыми сервисами, такими как цифровой паспорт и налоговые реестры; соответствие международным стандартам благодаря проверке клиентов по санкционным и риск-спискам в режиме реального времени [2].

Особое место в *eKYC* занимает биометрическая идентификация, позволяющая связать цифровую запись с конкретным человеком через уникальные физические или поведенческие признаки, такие как отпечатки пальцев, распознавание лиц, сканирование радужной оболочки и голосовая биометрия. Эти методы повышают точность и безопасность, но кибербезопасность становится критически важной, т. к. утечку биометрии нельзя исправить сменой пароля.

Внедрение *eKYC* сопровождается вызовами: киберугрозы, т. к. базы биометрии — лакомая цель для хакеров; цифровое неравенство — не у всех есть доступ к современным устройствам и интернету; высокая стоимость внедрения и регуляторные сложности из-за отсутствия единых правовых стандартов; а также этические вопросы, связанные с опасениями чрезмерного контроля и угрозы личной свободе [3]. Тем не менее риски — это также возможности. Защиту биометрии лучше строить на многоуровневой системе: децентрализация данных (хранение на устройстве пользователя), технологии определения живости (чтобы отсеивать подделки) и многофакторная аутентификация, где биометрия лишь один из элементов.

В отличие от пароля, биометрию невозможно изменить после утечки, что создает пожизненные риски для пострадавших граждан. Яркой иллюстрацией этой проблемы стал мировой прецедент 2019 г. — масштабная утечка из системы *BioStar* 2, когда были компрометированы 28 млн биометрических записей, включая отпечатки пальцев и данные распознавания лиц. Этот инцидент, наряду со случаями взлома системы распознавания лиц *Apple iPhone X*, наглядно демонстрирует уязвимость даже технологически продвинутых платформ [4]. Не менее реальны и презентационные атаки, когда злоумышленники используют высококачественные маски или фотографии для обмана системы верификации. Добавим сюда риски перехвата данных при передаче и изощренные атаки на сами алгоритмы машинного обучения — и картина киберугроз становится абсолютно конкретной и требующей безотлагательных решений как на технологическом, так и на регуляторном уровне.

Конкретность этих угроз позволяет выработать и столь же конкретные меры противодействия. Решение видится не в отказе от биометрии, а в построении многоуровневой системы защиты. Стратегическим вектором здесь является отход от рискованной централизации в сторону моделей децентрализованной идентификации (*Self-Sovereign Identity*, *SSI*), где биометрический шаблон хранится на самом устройстве пользователя, а не на удаленном сервере. Это делает саму кражу данных бессмысленной. Тактически же пользователей защищают технологии определения живости (*liveness detection*), анализирующие микродвижения и пульсацию крови для отсеивания муляжей, и безусловный принцип многофакторной аутентификации, где биометрия — лишь один из элементов, дополняемый владением устройством и знанием *PIN*-кода.

Особую сложность представляют этические дилеммы: страх потери анонимности и алгоритмическая дискриминация, при которой алгоритмические модели дают несправедливые или предвзятые результаты, приводя к неравному отношению к различным социальным группам [12]. Решение лежит в прозрачности, информированном согласии, праве на цифровое забвение, аудитах алгоритмов и минимизации сбора данных, что создаст более устойчивую, безопасную и справедливую систему цифровой идентификации.

В России создание ЕБС стало важным этапом цифровизации финансового сектора. С ее помощью клиенты могут проходить удаленную идентификацию в банках с использованием голоса и лица. Несмотря на вопросы приватности, проект демонстрирует стремление государства построить цифровую инфраструктуру доверия.

Международный опыт показывает, что модели внедрения *eKYC* сильно различаются. В Индии национальная система *Aadhaar* охватывает более 99 % граждан страны начиная с пятилетнего возраста и интегрирована с финансовыми и социальными сервисами, что значительно ускоряет доступ граждан к банковским продуктам [5]. В Сингапуре система *SingPass* обеспечивает единый цифровой идентификатор для доступа к государственным и коммерческим сервисам, позволяя открывать счета за считанные минуты [5]. В странах Европейского Союза регламент *eIDAS* создает единое правовое поле для электронных идентификаторов, а в США частные и государственные компании развивают биометрические сервисы с акцентом на защиту персональных данных и согласие клиентов. В Африке и Латинской Америке *eKYC* активно используют для финансовой инклюзии. Например, система *Bank Verification Number* в Нигерии дала миллионам граждан первый доступ к банковским услугам [6].

Однако международный опыт внедрения *eKYC* не является исключительно позитивным и сталкивается с существенными вызовами, анализ которых критически важен для формирования сбалансированной регуляторной политики. Ярким примером системных трудностей может служить первоначальная реализация системы *Aadhaar* в Индии, которая столкнулась с масштабными проблемами защиты персональных данных и многочисленными утечками информации, что привело к судебным разбирательствам и требовало значительных доработок в области кибербезопасности для обеспечения конфиденциальности. В Великобритании попытка внедрения универсальной цифровой идентификации *Verify* оказалась коммерчески неуспешной, не достигнув планируемого охвата пользователей, и была закрыта из-за низкого уровня принятия населением, сложности пользовательского интерфейса и конкуренции с частными решениями, что демонстрирует важность удобства и экономической целесообразности. В ряде стран Африки, таких как Кения, несмотря на успех мобильного банкинга, развертывание национальных систем *eKYC* тормозится из-за низкого качества интернет-соединения в удаленных районах и проблем с верификацией биометрических данных у населения, занятого физическим трудом, что ограничивает полноту охвата и подчеркивает зависимость технологии от инфраструктурных условий.

Эффективность современного *eKYC* в России обеспечивается комплексом передовых технологий: *OCR*, такие как отечественные решения от ЦРТ или «НаноСкан», точно считывают данные даже с поврежденных документов, в то время как алгоритмы компьютерного зрения, основанные на архитектурах глубокого обучения типа *Siamese Neural Networks*, сравнивают селфи и фото из паспорта с высочайшей точностью, минимизируя ложные отказы. Искусственный интеллект, представленный предиктивными моделями машинного обучения (например, градиентный бустинг от *CatBoost*), анализирует паттерны транзакций для выявления аномалий, а блокчейн-платформы, вроде решений на базе *Masterchain*, обеспечивают целостность и безопасное хранение верифицированных данных. Обработка *Big Data* позволяет строить динамические поведенческие профили, повышая точность скоринга. В будущем ожидается интеграция с концепцией *SSI*, где пользователи самостоятельно контролируют свои цифровые идентификаторы через децентрализованные решения, что кардинально повысит доверие и снизит риски злоупотреблений за счет исключения единой точки отказа.

История *eKYC* в России тесно связана с цифровизацией государственного управления и банковской сферы (табл. 1). В 2012 г. была создана Единая система идентификации и аутентификации (далее — ЕСИА) на портале «Госуслуги», обеспечившая основу для удаленной идентификации граждан. Поправки 2017 г. к Федеральному закону от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» закрепили возможность дистанционной проверки клиентов банков. В 2018 г. заработала ЕБС, а в 2021 г. компания *Smart Engines* предложила технологию идентификации по одной фотографии. В 2022—2023 гг. усилилось внимание к кибербезопасности и концепции «Суверенной биометрии». Сейчас *eKYC* развивается через интеграцию ЕБС с финтех-сервисами и переход к гибридным моделям, сочетающим централизованные платформы и децентрализованные идентификаторы (*DID*, *SSI*) [7].

Таблица 1

История возникновения и развития *eKYC* в России

Год	Событие	Комментарий
2012	Создание ЕСИА на портале «Госуслуги»	Основа для удаленной идентификации граждан
2017	Поправки к № Федеральному закону от 7 августа 2001 г. № 115-ФЗ	Возможность дистанционной проверки клиентов банков
2018	Запуск ЕБС Банком России и «Ростелекомом». Начат сбор данных по лицу и голосу	Россия стала одной из первых стран, внедривших национальную биометрическую платформу
2019	Первые банки подключились к ЕБС для удаленного открытия счетов и предоставления услуг	Начался реальный переход от теории к практике: клиенты получили возможность пользоваться услугами без визита в офис
2020	Расширение функционала ЕБС, активное внедрение в коммерческих банках; новые нормативные акты Центрального Банка РФ	Появились первые стандарты взаимодействия банков с ЕБС, что обеспечило единые правила игры
2021	Появление отечественных технологий *eKYC*, например, *Smart Engines* (идентификация по селфи с паспортом)	Россия начала развивать собственные инновационные решения, снижая зависимость от зарубежных технологий
2022	Усиление регуляторного контроля: новые требования к защите биометрии, обсуждение концепции «Суверенной биометрии»	В центре внимания оказались вопросы безопасности и доверия общества к государственным платформам

Окончание табл. 1

Год	Событие	Комментарий
2023	Массовое внедрение биометрии в банковский сектор; рост общественной дискуссии о конфиденциальности данных	Общество активно обсуждало риски утечек, что подчеркнуло необходимость прозрачности и независимого контроля
2024	Пилотные проекты по интеграции ЕБС с коммерческими сервисами; тестирование мультифакторных *eKYC*-схем	Появились решения, совмещающие биометрию, госуслуги и коммерческие финтех-продукты
2025	Развитие ЕБС, интеграция с финтех-платформами и переход к децентрализованным идентификаторам (*DID*, *SSI*)	Россия делает ставку на будущее: сочетание централизованных госрешений и инновационных децентрализованных технологий

Примечание: сост. авторами на основе [7].

Интеграция биометрических технологий в процессы удаленной идентификации представляет собой наиболее перспективное направление совершенствования системы финансового мониторинга. Согласно исследованию Е. Н. Храмова и О. В. Вершининой, внедрение единых биометрических стандартов в архитектуру *eKYC* способствует не только повышению уровня безопасности финансовых операций, но и укреплению конкурентоспособности национальной финансовой инфраструктуры [8]. Особое значение биометрическая аутентификация приобретает в контексте развития дистанционного банковского обслуживания, где, по мнению Е. И. Шаманиной и Ю. С. Захаренко, она выступает ключевым фактором обеспечения надежной верификации клиентов при одновременном сохранении пользовательского удобства [9].

Правовой аспект использования биометрических данных в процедурах *eKYC* детально проанализирован А. Р. Попковой, которая выделяет необходимость соблюдения сложного баланса между технологическими возможностями и защитой прав субъектов персональных данных [10]. Этот вывод получает развитие в исследовании Н. В. Кузнецова, где обоснована эффективность применения биометрической идентификации в рамках реализации требований ПОД/ФТ, особенно в части создания единого защищенного пространства для обмена данными между финансовыми организациями [11].

Однако процесс внедрения передовых *eKYC*-решений сталкивается с существенными барьерами, требующими комплексного преодоления. В. Е. Косарев и Э. С. Русило идентифицируют многоуровневую структуру факторов, сдерживающих развитие биометрии в банковском секторе, включая технологические ограничения, недостаточность нормативного регулирования и сохраняющийся низкий уровень доверия населения к дистанционным каналам обслуживания [13]. Дополнительные риски, связанные с конфиденциальностью персональных данных и потенциальными уязвимостями систем удаленной идентификации, выделены в работе В. В. Егина, где подчеркивается необходимость создания отказоустойчивой архитектуры *eKYC*-платформ [4].

С. С. Фешина и А. С. Славянов акцентируют внимание на системных проблемах цифровизации экономики, проявляющихся в возрастающей сложности выявления преступных схем и необходимости фундаментальной адаптации контрольно-надзорных механизмов к новым реалиям [14]. Эти вызовы особенно рельефно проявляются в контексте развития концепции цифровых валют центральных банков, где, как отмечает З. И. Хисамова, требования *AML/KYC* приобретают особую значимость в связи с потенциальными рисками анонимизации расчетов [15].

Трансформация финансовых услуг в условиях цифровой экономики находит свое отражение в исследовании С. В. Митрофанова с соавторами, где анализируются новые возможности бизнес-моделей, основанных на платформенных решениях. Авторы убедительно демонстрируют, что цифровые платформы не только оптимизируют операционные процессы, но и создают предпосылки для внедрения более эффективных систем мониторинга и контроля, основанных на технологиях распределенного реестра и смарт-контрактов [16].

Особого внимания заслуживает регуляторный аспект цифровой трансформации в сфере ПОД/ФТ, подробно рассмотренный П. С. Шараевым. Исследователь обоснованно указывает на необходимость развития адаптивного регулирования, способного учитывать стремительную эволюцию финансовых технологий при сохранении эффективности контрольно-надзорных функций. Этот подход представляется особенно актуальным в контексте формирования технологического суверенитета, где разработка отечественных стандартов и решений в области *eKYC* становится не только вопросом экономической эффективности, но и элементом национальной безопасности [17].

Формирование устойчивой системы финансовой безопасности сегодня требует комплексного подхода, объединяющего технологические инновации и постоянное совершенствование нормативного регулирования. Перспективно развивать отечественные *eKYC*-решения на базе биометрии и платформенных архитектур, которые обеспечат соответствие международным стандартам ПОД/ФТ и укрепят технологический суверенитет России в условиях растущей геоэкономической нестабильности.

В России цифровая идентификация является приоритетным направлением развития финансового сектора. Центральный банк активно продвигает концепцию удаленной идентификации, а создание ЕБС стало основой для *eKYC*.

Перспективы внедрения *eKYC* можно рассматривать через три взаимосвязанных направления. Во-первых, необходимо обеспечить инфраструктурное развитие, включая масштабируемость ЕБС и ее интеграцию с коммерческими сервисами, что позволит расширить охват пользователей и повысить эффективность дистанционной идентификации.

Во-вторых, важным аспектом является законодательное совершенствование: требуется адаптация норм о персональных данных, уточнение правил хранения и обработки биометрической информации, а также расширение полномочий регуляторов для контроля за соблюдением этих стандартов. Наконец, ключевым фактором успеха является формирование социального доверия, которое достигается через информирование

населения о преимуществах *eKYC*, прозрачность процедур и создание надежных гарантий защиты личной информации. Если эти условия будут выполнены, Россия сможет не только сократить риски финансовых преступлений, но и повысить доступность банковских услуг для миллионов граждан.

С точки зрения финансового анализа, ключевым аргументом в пользу внедрения *eKYC* является не только технологическое совершенство, но и его прямая экономическая эффективность для кредитных организаций. Первоначальные инвестиции в развертывание *eKYC*-платформы, включающие затраты на лицензирование программного обеспечения, интеграцию с государственными платформами (например, ЕСИА) и аппаратное обеспечение, могут быть значительными. Однако они должны рассматриваться в контексте долгосрочной экономии операционных расходов. Традиционный *KYC* характеризуется высокими переменными издержками на одного клиента: ручная проверка документов, содержание физических отделений для идентификации, затраты на бумажный документооборот и труд сотрудников комплаенс-подразделений. По мнению *McKinsey Global Institute*, внедрение *eKYC* позволяет радикально сократить эти затраты, автоматизируя до 80 % процессов верификации, что снижает стоимость онбординга нового клиента в разы — по оценкам российских банков-первопроходцев, с нескольких тысяч до нескольких сотен рублей.

Ключевой источник экономии в *eKYC* — сокращение мошенничества. Машинное обучение и биометрия ускоряют процесс и выявляют подделки на регистрации, снижая финансовые потери и судебные издержки. Автоматизация позволяет переводить сотрудников с рутинных проверок на сложные задачи, улучшая контроль.

Кроме того, *eKYC* способствует финансовой инклюзии, привлекая клиентов из удаленных регионов без затрат на физические отделения, расширяя клиентскую базу и увеличивая обороты.

Такой подход повышает надежность, экономит ресурсы и открывает новые рынки, делая *eKYC* важным инструментом для бизнеса и финансовых институтов.

В контексте цифровой трансформации финансового сектора и ужесточения регуляторных требований к верификации клиентов, анализ экономической эффективности различных моделей *KYC* приобретает особую актуальность для стратегического управления затратами и рисками. В табл. 2 систематизированы расчеты, позволяющие количественно оценить преимущества *eKYC* по сравнению с традиционным очным форматом за трехлетний горизонт планирования. Моделирование построено на гипотетической когорте в 100 000 новых клиентов и отражает не только прямую операционную экономию за счет автоматизации, но и сопутствующие эффекты — снижение потерь от мошенничества и возможность монетизации ранее недоступных клиентских сегментов из удаленных регионов.

Таблица 2

Сравнение затрат и выгод традиционного *KYC* и *eKYC* за трехлетний период, руб. (расчет на 100 000 новых клиентов)

Показатель	*KYC*	*eKYC*	Комментарий
Инвестиции (*CAPEX*): внедрение (лицензии, программное обеспечение, интеграция)	0	15 000 000	Разовые затраты в «год 0»
Операционные расходы (*OPEX*): стоимость верификации одного клиента	2 500	300	Труд операторов, бумага, проверка вручную/ стоимость запросов в ЕСИА, биометрия, *AI*-анализ (*eKYC*)
Общие *OPEX* на 100 000 клиентов	250 000 000	30 000 000	100 000 чел. × стоимость верификации 1 клиента
Прямая экономия на *OPEX*	—	220 000 000	Экономия = *OPEX KYC* – *OPEX eKYC* = = 250 млн – 30 млн = 220 млн
Сокращение потерь от мошенничества (в год)	5 000 000	1 000 000	Оценочное снижение на 80 % за счет выявления фрода на входе
Общая экономия от снижения фрода за 3 года	—	12 000 000	(5 млн — 1 млн) × 3 = 12 млн
Привлеченные клиенты из удаленных регионов (дополнительный доход)	—	50 000 000	Оценочный дополнительный доход от монетизации новых сегментов (кредиты, карты, вклады)
Общая экономия и дополнительный доход	—	282 000 000	Экономия *OPEX* + Экономия от фрода + + Дополнительный доход = 220 млн + 12 млн + + 50 млн = 282 млн
Чистый экономический эффект (*NPV* за 3 года)	—	267 000 000	Общий эффект – *CAPEX* = 282 млн – 15 млн = = 267 млн
ROI (*Return on Investment*)	—	1 780 %	Чистый эффект / *CAPEX* × 100 % = 267 млн / 15 млн × × 100 % = 1 780 %

Примечание: сост. авторами на основе методики *McKinsey Global Institute*.

Расчет экономического эффекта от внедрения *eKYC*-платформы выполнен автором на основе сравнительного моделирования затрат традиционного и дистанционного онбординга в 100 000 новых клиентов с горизонтом планирования 3 года. Объем первоначальных инвестиций (*CAPEX*) в размере 15 млн руб. обоснован среднерыночной стоимостью лицензий на программное обеспечение для биометрической верификации и его интеграции с ЕСИА и внутренними системами банка. Кардинальное снижение операционных расходов (*OPEX*) с 2 500 до 300 руб. на клиента аргументировано переходом от трудоемкого ручного процесса проверки документов к автоматизированному сценарию, что исключает затраты на бумажный документооборот и существенно сокращает фонд оплаты труда фронт-персонала. Консервативная оценка сокращения ежегодных потерь от мошенничества на 80 % (с 5 млн до 1 млн руб.) подтверждается исследованиями, демонстрирующими, что использование

алгоритмов *AI* для анализа «цифрового следа» и верификации «живого лица» минимизирует риски принятия фальсифицированных документов на этапе идентификации. Прогнозируемый дополнительный доход в 50 млн руб. от монетизации клиентов из удаленных регионов моделировался исходя из их среднего срока жизни и потенциала кросс-продаж финансовых продуктов. Совокупный положительный денежный поток в 282 млн руб. и впечатляющий показатель *ROI* на уровне 1 780 % наглядно демонстрируют не только операционную эффективность, но и стратегические конкурентные преимущества, получаемые кредитной организацией в результате цифровой трансформации клиентского сервиса.

Заключение

Проведенный анализ позволяет утверждать, что переход от традиционного *KYC* к электронной идентификации представляет собой не просто технологическую модернизацию, а стратегическую необходимость для построения устойчивой, прозрачной и доступной финансовой системы будущего. Однако его успешная реализация напрямую зависит от способности всех участников процесса — регуляторов, финансовых институтов и технологических компаний — адекватно ответить на комплекс выявленных проблем. Преодоление рисков информационной безопасности требует не просто усиления защиты, но и фундаментального пересмотра архитектуры хранения данных в сторону децентрализованных моделей, что минимизирует последствия потенциальных утечек и соответствует растущему общественному запросу на цифровой суверенитет. Проблема цифрового неравенства и высокой стоимости внедрения диктует необходимость развития государственно-частного партнерства для создания доступной и совместимой инфраструктуры, а также разработки гибких регуляторных режимов, позволяющих малым участникам постепенно внедрять решения электронной идентификации без критических затрат. Наконец, формирование социального доверия, подорванного инцидентами с утечками данных и этическими вопросами, невозможно без реализации принципа «безопасности изначально», максимальной прозрачности алгоритмов и создания понятных для пользователя механизмов контроля над их персональными данными. Таким образом, будущее электронной идентификации лежит в объединении технологий, экономической целесообразности и права: только сбалансированный подход, учитывающий российскую специфику и международный опыт, позволит раскрыть весь потенциал цифровой идентификации для укрепления финансовой прозрачности, безопасности и подлинной интеграции каждого гражданина в цифровую экономику.

СПИСОК ИСТОЧНИКОВ

1. Денисевич Е. Н., Фищенко И. И. Финансовая безопасность государства и ПОД/ФТ // Modern Science. 2022. № 5-3. С. 126—133.

2. Барашко Е. Н., Парагульгов Р. А. Системы идентификации личности человека в финансовом секторе // Colloquium-Journal. 2019. № 25(49)-2. С. 86—89.

3. Мазурина Т. Ю., Шаманина Е. И. Современные способы и схемы легализации доходов, полученных преступным путем, и влияние цифровой трансформации на процессы их выявления // Национальный экономический форум имени Д. С. Львова — «Львовский форум» : материалы Нац. экон. форума. М. : Гос. ун-т управления, 2025. С. 125—129.

4. Егин В. В. Применение биометрической идентификации в банках: проблемы и перспективы // Вестник Пензенского государственного университета. 2021. № 3(35). С. 69—73.

5. Долганова О. И. Сотрудничество стран Азии в области цифровой идентификации личности // Азия и Африка сегодня. 2023. № 7. С. 42—48. DOI: 10.31857/S032150750025123-7.

6. Харуна И. О., Айдоноджи П. А., Бейда О. Д. Проблемы и перспективы нормативного регулирования системы электронных платежей в Нигерии // Journal of Digital Technologies and Law. 2024. Т. 2. № 2. С. 372—393. DOI: 10.21202/jdtl.2024.19.

7. Ковалева Н. А., Ермакова Н. В., Тулаева Д. Д. Биометрическая идентификация в банковском секторе России: текущее состояние и перспективы развития // Финансовые рынки и банки. 2024. № 4. С. 197—204.

8. Храмов Е. Н., Вершинина О. В. Биометрические технологии как фактор повышения безопасности и конкурентоспособности в финансовой инфраструктуре России // Фундаментальные исследования. 2025. № 4. С. 69—79. DOI: 10.17513/fr.43814.

9. Шаманина Е. И., Захаренко Ю. С. Биометрические технологии как перспективное направление совершенствования дистанционного банковского обслуживания // Вестник университета. 2020. № 5. С. 193—199. DOI: 10.26425/1816-4277-2020-5-193-199.

10. Попкова А. Р. Правовой режим использования биометрических персональных данных при удаленной идентификации физических лиц банками // Молодой ученый. 2020. № 1(291). С. 183—185.

11. Кузнецов Н. В. Использование кредитными организациями биометрических данных для идентификации своих клиентов в рамках борьбы с отмыванием денежных средств и финансированием терроризма // Закон и власть. 2025. № 2. С. 48—50.

12. Фаллетти Э. Алгоритмическая дискриминация и защита неприкосновенности частной жизни // Journal of Digital Technologies and Law. 2023. Т. 1. № 2. С. 387—420. DOI: 10.21202/jdtl.2023.16.

13. Косарев В. Е., Русило В. Е. Биометрия в банках и факторы, сдерживающие ее развитие // Финансовые рынки и банки. 2021. № 3. С. 35—40.

14. Фешина С. С., Славянов А. С. Цифровизация экономики: проблемы и последствия // Экономика и управление: проблемы, решения. 2018. № 5. Т. 7. С. 159—163.

15. Хисамова З. И. Концепция цифровых валют центральных банков: основные риски в части соблюдения требований AML («противодействия отмыванию денег») и KYC («знай своего клиента») // Актуальные проблемы экономики и права. 2020. Т. 14. № 3. С. 508—515. DOI: 10.21202/1993-047X.14.2020.3.508-515.

16. Митрофанов С. В., Арсаханова З. А., Гизятова А. Ш. Цифровые платформы в сфере финансовых услуг: новые возможности для бизнеса // Экономика и управление: проблемы, решения. 2025. № 5. Т. 14. С. 186—193. DOI: 10.36871/ek.up.p.r.2025.05.14.020.

17. Шараев П. С. Противодействие отмыванию (легализации) денежных средств в условиях цифровой трансформации (финансово-правовой аспект) // Юридический вестник Самарского университета. 2022. Т. 8. № 3. С. 94—100. DOI: 10.18287/2542-047X-2022-8-3-94-100.

REFERENCES

1. Denisevich E. N., Fishchenko I. I. Financial security of the state and AML/CFT. *Modern Science*. 2022;5-3:126—133. (In Russ.)

2. Barashko E. N., Paragulgov R. A. Human personality identification systems in the financial sector. *Colloquium-Journal*. 2019;25(49)-2:86—89. (In Russ.)

3. Mazurina T. Yu., Shamanina E. I. Modern methods and schemes for legalization of proceeds from crime and the impact of digital transformation on the processes of their detection. *National Economic Forum named after D. S. L`vov – "Lvov Forum". Proceedings of the National economic forum.* Moscow, State University of Management publ., 2025:125—129. (In Russ.)

4. Egin V. V. Application of biometric identification in banks: problems and prospects. *Vestnik Penzenskogo gosudarstvennogo universiteta = Vestnik of Penza State University*. 2021;3(35):69—73. (In Russ.)

5. Dolganova O. I. Cooperation between Asian countries in the field of digital identification of a person. *Aziya i Afrika segodnya = Asia and Africa today*. 2023;7:42—48. (In Russ.) DOI: 10.31857/S032150750025123-7.

6. Haruna I. O., Aidonojie P. A., Beida O. J. Prospects and Issues Concerning the Regulatory Regime of E-Payment System in Nigeria. *Journal of Digital Technologies and Law*. 2024;2(2):372—393. DOI: 10.21202/jdtl.2024.19.

7. Kovaleva N. A., Ermakova N. V., Tulaeva D. D. Biometric identification in the Russian banking sector: current state and development prospects. *Finansovye rynki i banki = Financial markets and banks*. 2024;4:197—204. (In Russ.)

8. Khramov E. N., Vershinina O. V. Biometric technologies as a factor in improving security and competitiveness in Russia's financial infrastructure. *Fundamental`nye issledovaniya = Fundamental research*. 2025;4:69—79. (In Russ.) DOI: 10.17513/fr.43814.

9. Shamanina E. I., Zakharenko Yu. S. Biometric technologies as a perspective direction of improving remote bank service. *Vestnik Universiteta*. 2020;5:193—199. (In Russ.) DOI: 10.26425/1816-4277-2020-5-193-199.

10. Popkova A. R. The legal regime for the use of biometric personal data in remote identification of individuals by banks. *Molodoi uchenyi = Young scientist*. 2020;1(291):183—185. (In Russ.)

11. Kuznetsov N. V. The use of biometric data by credit organizations to identify their clients in the framework of combating money laundering and terrorist financing. *Zakon i vlast` = Law and Power*. 2025;2:48—50. (In Russ.)

12. Falletti E. Algorithmic Discrimination and Privacy Protection. *Journal of Digital Technologies and Law*. 2023;1(2):387—420. DOI: 10.21202/jdtl.2023.16.

13. Kosarev V. E. Rusilo E. S. Biometry in banks and factors handling its development. *Finansovye rynki i banki = Financial markets and banks*. 2021;3:35—40. (In Russ.)

14. Feshina S. S., Slavyanov A. S. Economic digitalization: problems and consequences. *Ekonomika i upravlenie: problemy, resheniya*. 2018;5-7:159—163. (In Russ.)

15. Khisamova Z. I. Concept of digital currencies of Central Banks: main risks in observing the requirements of AML ("Anti-Money Laundering") and KYC ("Know Your Client"). *Aktual`nye problemy ekonomiki i prava = Actual Problems of Economics and Law*. 2020;14(3):508—515. (In Russ.) DOI: 10.21202/1993-047X.14.2020.3.508-515.

16. Mitrofanov S. V., Arsakhanova Z. A., Gizyatova A. Sh. Digital platforms in financial services: new opportunities for business. *Ekonomika i upravlenie: problemy, resheniya*. 2025;5-14:186—193. (In Russ.) DOI: 10.36871/ek.up.p.r.2025.05.14.020.

17. Sharaev P. S. Countering money laundering (legalization) in the context of digital transformation (financial legal aspect). *Yuridicheskii vestnik Samarskogo universiteta = Juridical Journal of Samara University*. 2022;8(3):94—100. (In Russ.) DOI: 10.18287/2542-047X-2022-8-3-94-100.

Статья поступила в редакцию 06.10.2025; одобрена после рецензирования 13.11.2025; принята к публикации 17.11.2025.
The article was submitted 06.10.2025; approved after reviewing 13.11.2025; accepted for publication 17.11.2025.