ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ИИ В БАНКОВСКУЮ ИДЕНТИФИКАЦИЮ

Давирова Ш.Ш.
PhD, ст.преп.
Ахмедов Достонбек Исламович
Магистрант второго курса
Ташкентский государственный экономический университет
akhmedov9894@gmail.com
+998979083330

Аннотация: *В тезисе рассматриваются перспективы внедрения искусственного интеллекта (ИИ) в процессы банковской идентификации и верификации клиентов в условиях цифровой трансформации финансового сектора. Актуальность исследования обусловлена ростом дистанционных каналов обслуживания, усилением требований к противодействию мошенничеству и необходимостью повышения операционной эффективности банков. В работе анализируются интеллектуальные методы распознавания биометрических данных, автоматической проверки документов и поведенческой аналитики. Представлены количественные модели оценки качества идентификации, экономической эффективности и управления рисками. Показано, что применение ИИ позволяет существенно сократить время идентификации, повысить точность принятия решений и снизить операционные затраты при условии соблюдения требований информационной безопасности и нормативного регулирования. Практическая значимость исследования заключается в возможности использования предложенных моделей при проектировании интеллектуальных платформ e-KYC и цифровой идентификации.*

Ключевые слова: *искусственный интеллект; банковская идентификация; e-KYC; биометрия; машинное обучение; управление рисками; цифровая трансформация; информационная безопасность; автоматизация; финтех.*

Искусственный интеллект становится ключевым драйвером модернизации процессов банковской идентификации, обеспечивая переход от регламентированных процедур к интеллектуальным системам принятия решений. Современные алгоритмы машинного обучения и компьютерного зрения позволяют автоматизировать распознавание лиц, анализ подлинности документов, оценку поведенческих паттернов и выявление аномалий в режиме реального времени. Это способствует снижению человеческого фактора, ускорению клиентского онбординга и повышению точности верификационных процедур.

Качество интеллектуальной идентификации оценивается с использованием стандартных метрик ошибок:

$$FAR = \frac{N_{FA}}{N}, \quad FRR = \frac{N_{FR}}{N}, \quad Accuracy = 1 - (FAR + FRR)$$

где N_{FA} — количество ложных допусков,

N_{FR} — количество ложных отказов,

N — общее количество проверок.

Экономическая эффективность внедрения ИИ определяется показателями возврата инвестиций и чистой приведённой стоимости:

$$ROI = \frac{P - I}{I} \times 100\%, \quad NPV = \sum_{t=1}^{T} \frac{CF_t}{(1+r)^t} - I$$

где P — прибыль от автоматизации,

I — инвестиции в ИИ-платформу,

CF_t — денежный поток,

r — ставка дисконтирования.

Для оценки совокупного риска интеллектуальной идентификации применяется интегральная модель:

$$R_{AI} = \sum_{i-1}^{n} w_i r_i$$

где r_i — отдельные риски (кибернетические, правовые, алгоритмические),

w_i — их весовые коэффициенты.

$$S = \alpha S_{bio} + \beta S_{doc} + \gamma S_{beh}$$

где S_{bio} — биометрическая достоверность,

S_{doc} — качество верификации документов,

S_{beh} — поведенческая стабильность.

Практика показывает, что внедрение ИИ позволяет сократить время идентификации в 5–10 раз, снизить операционные затраты до 40–60 % и повысить уровень обнаружения мошеннических операций. Вместе с тем усиливаются риски утечки персональных данных, смещения алгоритмов и правовой неопределённости, что требует внедрения механизмов интерпретируемости моделей, сертификации алгоритмов и постоянного мониторинга качества данных.

Таким образом, перспективы внедрения искусственного интеллекта в банковскую идентификацию связаны с формированием интеллектуальных экосистем e-KYC, интеграцией с государственными цифровыми реестрами и развитием нормативных стандартов цифрового доверия. Дальнейшие исследования целесообразно направить на разработку адаптивных моделей управления рисками и оценку социальной устойчивости интеллектуальных идентификационных систем.

СПИСОК ИСТОЧНИКОВ:

1. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. — Cambridge : MIT Press, 2016. — 800 p.

2. Bishop C. M. *Pattern Recognition and Machine Learning*. — New York : Springer, 2006. — 738 p.

3. National Institute of Standards and Technology (NIST). *Digital Identity Guidelines : SP 800-63*. — Gaithersburg, 2020. — URL: https://pages.nist.gov/800-63-3/ (дата обращения: 12.09.2025).

4. Financial Action Task Force (FATF). *Guidance on Digital Identity*. — Paris, 2020. — URL: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html (дата обращения: 15.09.2025).

5. European Union Agency for Cybersecurity (ENISA). *Cybersecurity for Digital Identity*. — Athens, 2021. — URL: https://www.enisa.europa.eu/publications/cybersecurity-for-digital-identity (дата обращения: 18.09.2025).

6. ISO/IEC 27001:2018. *Information security management systems — Requirements*. — Geneva : ISO, 2018. — URL: https://www.iso.org/standard/54534.html (дата обращения: 21.09.2025).

7. World Bank. *Digital ID and Financial Inclusion*. — Washington : World Bank Group, 2020. — URL: https://www.worldbank.org/en/topic/financialinclusion/brief/digital-id (дата обращения: 25.09.2025).

8. Gartner. *Digital Identity Market Trends 2023*. — Stamford : Gartner Inc., 2023. — URL: https://www.gartner.com/en/documents/digital-identity-market-trends-2023 (дата обращения: 28.09.2025).

9. McKinsey & Company. *Artificial Intelligence in Banking*. — New York : McKinsey Global Institute, 2022. — URL: https://www.mckinsey.com/industries/financial-services/our-insights/artificial-intelligence-in-banking (дата обращения: 02.10.2025).

10. Deloitte. *AI and Digital Identity in Financial Services*. — London : Deloitte, 2023. — URL: https://www2.deloitte.com/global/en/pages/financial-services/articles/ai-digital-identity.html (дата обращения: 05.10.2025).

11. World Economic Forum. *Global Identity Framework*. — Geneva, 2022. — URL: https://www.weforum.org/reports/global-identity-framework (дата обращения: 09.10.2025).

12. UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. — Paris, 2021. — URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137 (дата обращения: 12.10.2025).