

ЦИФРОВЫЕ ИННОВАЦИИ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК НОВЫЕ ФАКТОРЫ ОБЕСПЕЧЕНИЯ ФИНАНСОВОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ГЛОБАЛЬНЫХ РИСКОВ

Ходжарахманова Назира Бахтияр кизи
Магистрант 2 курса Ташкентского государственного
экономического университета

Аннотация: В статье анализируются современные подходы к обеспечению финансовой безопасности в условиях активной цифровизации экономики. Рассматривается роль искусственного интеллекта и облачных технологий в создании устойчивой системы защиты финансовых институтов, а также их влияние на повышение эффективности внутреннего контроля и снижение киберрисков. Отмечено, что внедрение ИИ способствует переходу к предиктивной аналитике и проактивным мерам противодействия угрозам, однако сопровождается новыми вызовами — зависимостью от поставщиков, рисками централизации данных и необходимостью прозрачности алгоритмов. В исследовании подчеркивается важность комплексного подхода, включающего сочетание технологических инноваций с механизмами риск-менеджмента и регуляторного надзора для достижения устойчивой финансовой безопасности.

Ключевые слова: финансовая безопасность, искусственный интеллект, облачные технологии, цифровизация, риск-менеджмент, киберустойчивость, Zero-Trust.

GLOBAL RIVOJLANISH SHAROITIDA MOLIYAVIY XAVFSIZLIKNI TA'MINLASHNING YANGI OMILLARI SIFATIDA RAQAMLI INNOVATSIYALAR VA SUN'IY INTELEKT

Xodjaraxmanova Nazira Baxtiyar qizi
Toshkent davlat iqtisodiyot universiteti 2-kurs magistranti

Annotatsiya: Maqolada iqtisodiyotning raqamlashtirilishi sharoitida moliyaviy xavfsizlikni ta'minlashning zamonaviy yondashuvlari tahlil qilinadi. Sun'iy intellekt va bulut texnologiyalarining moliya institutlari himoya tizimini mustahkamlashdagi roli hamda ichki nazorat samaradorligini oshirish va kiberxavflarni kamaytirishdagi ahamiyati ko'rsatib o'tiladi. Sun'iy intellektidan foydalanish tahliliy prognozlash va proaktiv xavfsizlik choralariga o'tish imkonini bersa-da, bu jarayon texnologiya yetkazib beruvchilarga qaramlik, ma'lumotlarning markazlashuvi va algoritmlarning shaffofligi kabi yangi chaqiriqlarni keltirib chiqaradi. Tadqiqotda moliyaviy

xavfsizlikni ta'minlash uchun texnologik innovatsiyalarni xavf-xatarlarni boshqarish va nazorat tizimlari bilan uyg'unlashtirish zarurligi ta'kidlanadi.

Kalit so'zlar: moliyaviy xavfsizlik, sun'iy intellekt, bulut texnologiyalari, raqamlashtirish, xavf-xatarlarni boshqarish, kiberbarqarorlik, Zero-Trust.

DIGITAL INNOVATIONS AND ARTIFICIAL INTELLIGENCE AS NEW FACTORS IN ENSURING FINANCIAL SECURITY UNDER GLOBAL RISKS

Xodjaraxmanova Nazira Bakhtiyar kizi
2nd-year Master's student, Tashkent State University of Economics

Abstract: The article analyzes modern approaches to ensuring financial security in the context of economic digitalization. It explores the role of artificial intelligence and cloud technologies in building resilient protection systems for financial institutions and enhancing internal control and cybersecurity effectiveness. The study highlights that AI implementation enables predictive analytics and proactive threat prevention but also introduces new challenges, such as vendor dependency, data centralization risks, and the need for algorithmic transparency. The research emphasizes the importance of a comprehensive approach that combines technological innovation with effective risk management and regulatory oversight to achieve sustainable financial security.

Keywords: financial security, artificial intelligence, cloud technologies, digitalization, risk management, cyber resilience, Zero-Trust.

ВВЕДЕНИЕ

Рост цифровизации и активное внедрение искусственного интеллекта (ИИ) в финансовом секторе трансформируют не только бизнес-модели, но и подходы к обеспечению финансовой безопасности. Согласно данным компании **Gartner**, глобальные расходы на информационную безопасность и управление рисками в 2025 году достигнут **212 млрд долларов**, что на 15 % больше, чем в 2024 году — это отражает растущую осознанность угроз, связанных с цифровой инфраструктурой [1]. Финансовые институты всё чаще переходят на использование облачных сервисов, систем машинного обучения и аналитических платформ для выявления мошенничества, оценки кредитных рисков и оптимизации внутренних процессов. Например, стратегическое партнёрство между **Euroclear** и **Microsoft** направлено на модернизацию инфраструктуры финансовых операций через облачные технологии и искусственный интеллект [2].

Однако вместе с ростом цифровизации появляются новые уязвимости. Исследование **Reserve Bank of India (RBI)** отмечает, что классические модели информационной защиты больше не соответствуют современным вызовам: возрастают риски утечки данных, зависимости от поставщиков технологий (vendor lock-ins), а также алгоритмические и этические риски, возникающие при использовании ИИ [3]. В ответ на это RBI рекомендовал финансовым организациям переходить на модель «**Zero-Trust**» и формировать систему защиты, «осведомлённую об ИИ» (AI-aware defence), что подразумевает постоянную верификацию доступа и проактивное управление киберугрозами [4].

Международные консалтинговые компании, включая **McKinsey & Company**, подчеркивают, что применение ИИ и генеративных технологий может приносить финансовым организациям сотни миллиардов долларов добавленной стоимости, но без выстроенной системы управления рисками это создаёт опасность для стабильности финансовых потоков и репутации [5]. В связи с этим ключевым направлением становится развитие адаптивных механизмов контроля — от внутреннего аудита до оценки устойчивости облачных систем и внедрения многофакторной аутентификации.

Цель данного тезиса — определить роль ИИ и облачных технологий в повышении уровня финансовой безопасности предприятий и финансовых институтов. Современные цифровые инновации становятся неотъемлемым элементом инфраструктуры финансовой защиты, однако эффективность их применения напрямую зависит от способности организаций интегрировать технологические решения с комплексной системой риск-менеджмента, внутреннего контроля и регуляторного надзора.

ОСНОВНАЯ ЧАСТЬ

Современные тенденции в сфере финансовой безопасности характеризуются активным внедрением новейших технологических решений, направленных на минимизацию цифровых рисков. Среди ключевых инструментов выделяются генеративный искусственный интеллект, технологии многофакторной аутентификации и системы киберзащиты с ИИ-поддержкой. Так, 91 % банков США уже применяют ИИ для обнаружения мошенничества, и 83 % специалистов по борьбе с мошенничеством планируют внедрить генеративный ИИ (GenAI) к 2025 году. Эти технологии позволяют автоматически анализировать большие объёмы транзакций, выявлять аномальные шаблоны и предупреждать мошенничество значительно быстрее, чем традиционные системы [6].



Рис 1. Использование ИИ и мульт-факторной аутентификации для предотвращения мошенничества в банковской сфере¹

Примером интеграции инновационных решений является стратегическое партнёрство между Euroclear и Microsoft, направленное на модернизацию облачных систем хранения данных и обеспечение более высокого уровня киберустойчивости финансовых операций. Наряду с этим, Reserve Bank of India (RBI) рекомендует финансовым организациям внедрять архитектуру «Zero-Trust» и формировать «ИИ-осведомлённую» стратегию киберзащиты, что отражает тенденцию к адаптации защиты под современные цифровые вызовы. Стратегии включают постоянную проверку доступа, контроль третьих лиц и обеспечение устойчивости к вендор-зависимости [7].

При этом применение ИИ и облачных технологий как элементов финансовой безопасности приносит не только преимущества, но и заметные вызовы. Согласно отчёту Financial Stability Board (FSB), использование GenAI и облачных сервисов создаёт новые уязвимости: концентрация поставщиков, опирание многих организаций на одни и те же модели данных, непрозрачность алгоритмов и возможность системных сбоев. Кроме того, исследования показывают, что хотя ИИ-системы значительно увеличивают точность выявления мошенничества, они сталкиваются с проблемами качества данных, алгоритмической предвзятости, ограниченного охвата (особенно в малых организациях) и необходимостью прозрачности и объяснимости моделей [8].

Развитие искусственного интеллекта и облачных технологий в финансовом секторе открывает новые возможности для повышения устойчивости и защищённости финансовых институтов. Эти технологии позволяют переходить

¹ Разработано автором

от реактивных методов защиты к проактивным, когда угрозы предсказываются и предотвращаются ещё до того, как они наносят ущерб. Искусственный интеллект обеспечивает глубокий анализ больших данных, моделирование поведенческих сценариев клиентов и выявление отклонений, которые могут свидетельствовать о мошенничестве или попытках кибервзлома. Облачные решения, в свою очередь, способствуют гибкости и масштабируемости систем безопасности, позволяя быстро реагировать на изменения в цифровой среде и повышать уровень доступности и непрерывности финансовых операций. Однако с ростом технологической зависимости усиливаются и риски: централизация данных, возможные уязвимости облачных платформ, а также сложность аудита и контроля алгоритмических решений. Финансовые институты должны уделять особое внимание вопросам прозрачности алгоритмов, защите данных клиентов, устойчивости к сбоям в инфраструктуре и рискам сторонних поставщиков. Интеграция ИИ и облачных систем должна сопровождаться усилением корпоративного управления, постоянным мониторингом цифровых угроз, внедрением стандартов «Zero-Trust» и обучением персонала работе с новыми технологиями. В долгосрочной перспективе именно синергия технологических инноваций и эффективного риск-менеджмента будет определять уровень финансовой безопасности предприятий и банков. Создание адаптивных систем внутреннего контроля, использование ИИ для непрерывной оценки киберрисков и развитие сотрудничества между государственными регуляторами и частным сектором становятся ключевыми направлениями будущей финансовой архитектуры. Финансовая безопасность в эпоху цифровой экономики перестаёт быть статичным понятием — она становится динамическим процессом, основанным на постоянном обновлении технологий, регуляторных механизмов и корпоративной культуры доверия и ответственности.

ВЫВОДЫ

В условиях стремительной цифровизации финансового сектора искусственный интеллект и облачные технологии становятся ключевыми факторами укрепления финансовой безопасности. Их внедрение позволяет финансовым организациям перейти на качественно новый уровень управления рисками — от реактивного реагирования на угрозы к их прогнозированию и предупреждению. Использование ИИ повышает точность идентификации мошеннических операций, способствует оптимизации внутреннего контроля и обеспечивает непрерывный мониторинг транзакционной активности, что особенно важно для систем с высокой степенью автоматизации.

В то же время цифровая трансформация создаёт и новые уязвимости. Зависимость от облачных поставщиков, концентрация данных и сложность алгоритмических моделей увеличивают вероятность системных рисков и

требуют более строгих механизмов регулирования. Эффективность использования ИИ-технологий напрямую зависит от качества данных, прозрачности алгоритмов и способности организаций обеспечивать объяснимость решений.

Для достижения устойчивого баланса между инновациями и безопасностью финансовым институтам необходимо развивать комплексный подход: сочетать технологические инструменты с управленческими и регуляторными мерами. Это предполагает внедрение стандартов «Zero-Trust», развитие внутренней культуры киберустойчивости и тесное взаимодействие с регуляторами для формирования единой цифровой экосистемы доверия.

Дальнейшее развитие финансовой безопасности требует не только внедрения передовых технологий, но и системного переосмысления подходов к управлению рисками. Только интеграция ИИ, облачных решений и стратегий риск-ориентированного надзора позволит финансовым организациям обеспечить устойчивость, доверие клиентов и конкурентоспособность в условиях глобальной цифровой экономики.

Список источников

1. Gartner. *Global Information Security Spending Forecast 2025* [Электронный ресурс]. – 2024. – Режим доступа: <https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025>
2. *Euroclear strikes Microsoft tie-up for cloud modernization* // *Financial News London* [Электронный ресурс]. – 2024. – Режим доступа: <https://www.fnlondon.com/articles/euroclear-strikes-microsoft-tie-up-d68e5217>
3. *Cyber risks in financial sector: RBI calls for AI-aware defence and zero-trust approach* // *The Times of India* [Электронный ресурс]. – 2025. – Режим доступа: <https://timesofindia.indiatimes.com/business/cybersecurity/cyber-risks-in-financial-sector-rbi-calls-for-ai-aware-defence-and-zero-trust-approach-warns-of-systemic-threat-from-vendor-lock-ins/articleshow/122164857.cms>
4. *RBI urges adoption of risk-based supervision and zero-trust architecture* // *The Economic Times* [Электронный ресурс]. – 2025. – Режим доступа: <https://m.economictimes.com/news/economy/policy/adopt-risk-based-supervision-zero-trust-approach-to-curb-cyberfrauds-rbi/articleshow/122164631.cms>
5. McKinsey & Company. *Derisking Emerging Technologies in Financial Services* [Электронный ресурс]. – 2024. – Режим доступа: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services>

6. Financial Stability Board (FSB). Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector [Электронный ресурс]. – 10 Октября 2025. – Режим доступа: <https://www.fsb.org/uploads/P101025.pdf>
7. OECD & FSB Roundtable on Artificial Intelligence in Finance. Summary of Key Findings [Электронный ресурс]. – 30 Сентября 2024. – Режим доступа: <https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/digital-finance/OECD%20%E2%80%93%20FSB%20Roundtable%20on%20Artificial%20Intelligence%20%28AI%29%20in%20Finance.pdf>
8. Mirishli S. Regulating AI in Financial Services: Legal Frameworks and Compliance Challenges [Электронный ресурс]. – 2025. – Режим доступа: <https://arxiv.org/abs/2503.14541>