

RAQAMLI BANKLAR MA'LUMOTLARI XAVFSIZLIGINI NAZORAT QILUVCHI VA MONITORING QILUVCHI SUN'IY INTELLEKT MODELLARI VA VOSITALARI

Sh.R.Shirinov

University of Business and Science (UBS)

"Aniq va tabiiy fanlar" kafedrası

Dasturlash asoslari fani o'qituvchisi shsherali92@mail.ru

Suyunova Zamira

"Aniq va tabiiy fanlar" kafedrası

Dasturlash asoslari fani o'qituvchisi

Annotatsiya. Ushbu maqola raqamli banklar ma'lumotlari xavfsizligini nazorat qilish va monitoring qilish uchun qo'llaniladigan sun'iy intellekt modellari va vositalarini kompleks tahlil qiladi. Zamonaviy bank sektori kiberxavfsizlik tahdidlariga tobora ko'proq duch kelmoqda, bu esa innovatsion himoya mexanizmlarini talab qiladi. Tadqiqot natijalari moliya muassasalari uchun sun'iy intellekt asosidagi xavfsizlik tizimlarini joriy etish bo'yicha amaliy tavsiyalar va kelajakdagi istiqbollarni taqdim etadi.

Kalit so'zlar: raqamli banklar, sun'iy intellekt, ma'lumotlar xavfsizligi, kiberxavfsizlik, mashinali o'rganish (machine learning), monitoring tizimlari, anomaliyalarni aniqlash (anomaly detection), firibgarlikni oldini olish (fraud prevention).

Аннотация. Данная статья представляет комплексный анализ моделей и инструментов искусственного интеллекта, применяемых для контроля и мониторинга безопасности данных цифровых банков. Исследование методологически изучает системы мониторинга на основе искусственного интеллекта, их базовую архитектуру, области внедрения и показатели эффективности. На основе анализа литературы раскрывается фундаментальная роль моделей искусственного интеллекта в обеспечении безопасности

банковских данных, возможности идентификации угроз в режиме реального времени, мониторинга аномалий и оптимизации стратегий кибербезопасности. Результаты исследования предоставляют практические рекомендации и перспективы на будущее по внедрению систем безопасности на основе искусственного интеллекта для финансовых учреждений.

Ключевые слова: цифровые банки, искусственный интеллект, безопасность данных, кибербезопасность, машинное обучение, системы мониторинга, обнаружение аномалий, предотвращение мошенничества.

Abstract. This article provides a comprehensive analysis of artificial intelligence models and tools used for monitoring and controlling digital bank data security. Based on literature analysis, the fundamental role of artificial intelligence models in ensuring bank data security, capabilities for real-time threat identification, anomaly monitoring, and optimization of cybersecurity strategies are revealed. The research results provide practical recommendations and future perspectives on implementing artificial intelligence-based security systems for financial institutions.

Keywords: digital banks, artificial intelligence, data security, cybersecurity, machine learning, monitoring systems, anomaly detection, fraud prevention.

KIRISH

Zamonaviy bank sektori raqamli transformatsiya jarayonida chuqur strukturaviy o'zgarishlarga uchramoqda. Raqamli texnologiyalarning keng joriy etilishi va moliyaviy xizmatlarning virtuallashuvi natijasida banklar mijozlarga yanada qulayroq, tezkor va samarali xizmatlarni taqdim etish bilan bir qatorda, ma'lumotlar xavfsizligi bilan bog'liq jiddiy muammolarga ham duch kelmoqda [1]. Accenture kompaniyasining empirik tadqiqotlariga ko'ra, so'nggi ikki yil ichida bank sektori kiberxavfsizlik choralariga sarflanadigan mablag'lar hajmini 140% ga oshirgan, biroq shunday bo'lsa-da, 54% banklar uchinchi tomon tomonidan kiberhujumlarga uchraganligi qayd etilgan [2]. Bank mijozlarining shaxsiy va moliyaviy ma'lumotlari, tranzaksiya tarixlari, to'lov tizimi ma'lumotlari, kredit tarixi kabi sensitiv ma'lumotlar zamonaviy kiberjinoatchilar uchun jozibali nishonga aylangan, ular esa tobora

murakkab texnologik usullardan foydalanib, an'anaviy xavfsizlik tizimlarining zaif tomonlarini ekspluatatsiya qilmoqda.

An'anaviy xavfsizlik tizimlari va qoidalarga asoslangan yondashuvlar (rule-based approaches) zamonaviy tahdidlarni aniqlab, ularga tezkor javob berish imkoniyatini fundamental darajada cheklab qo'ymoqda. Bu sharoitda sun'iy intellekt (SI) va mashinali o'rganish (machine learning) texnologiyalari bank ma'lumotlari xavfsizligini ta'minlashda innovatsion paradigma sifatida rivojlanmoqda. Sun'iy intellekt algoritmlari ulkan hajmdagi strukturalashgan va strukturalashmagan ma'lumotlarni real vaqt rejimida tahlil qilib, shubhali faoliyatni aniqlash, tahdidlarni bashorat qilish va identifikatsiyalash hamda ularga javob berish jarayonlarini avtomatlashtirish imkonini beradi [3]. Bu texnologiyalar bank xavfsizlik tizimlarining operatsion samaradorligini oshirish, inson faktori bilan bog'liq xatolarni minimallashtirish va tezkor qarorlar qabul qilish protsesslarini optimallashtirish imkoniyatlarini taqdim etmoqda, bu esa zamonaviy kiberhujumlar kontekstida muhim ahamiyat kasb etadi. 2023-yilgi statistik ma'lumotlarga ko'ra, mashinali o'rganish algoritmlarini firibgarlikni aniqlash tizimlarida (fraud detection systems) qo'llash soxta ogohlantirishlar (false positives) sonini 75% gacha kamaytirish va operatsion xarajatlarni sezilarli darajada qisqartirish imkonini bergan [4].

METODOLOGIYA VA ADABIYOTLAR TAHLILI

Ushbu tadqiqot metodologik asosi sistematik adabiyotlar tahlili (systematic literature review) strategiyasiga asoslangan bo'lib, mavjud ilmiy nashrlar, empirik tadqiqot ishlari, soha ekspertlari tomonidan tayyorlangan analitik hisobotlar va bank sektorida implementatsiya qilinayotgan sun'iy intellekt texnologiyalari bo'yicha kompleks ma'lumotlarni o'z ichiga oladi.

Sun'iy intellekt va mashinali o'rganish texnologiyalari bank sektorida xavfsizlikni ta'minlash maqsadida tobora intensiv tarzda adaptatsiya qilinmoqda, bu esa ko'plab tadqiqotchilar e'tiborini jalb qilgan tematik yo'nalishga aylandi. Ferumal (2018) o'z fundamental tadqiqotlarida sun'iy intellektning kiberxavfsizlikdagi transformativ rolini tahlil qilib, ushbu texnologiyalar bank sektorida kiberhujumlarni preventiv identifikatsiyalash va proaktiv mitigation strategiyalarini implementatsiya qilish imkoniyatlarini sezilarli darajada oshirishini empirik ma'lumotlar asosida

argumentatsiya qilgan [5]. Ryzhkova va uning hamkasblari (2020) tomonidan o'tkazilgan kompleks tadqiqotlar shuni ko'rsatdiki, bank sektorida kiberhujumlar intensivligi va taktik sofistikatsiyasi tobora ortib bormoqda, bu esa deterministik modellarga asoslangan an'anaviy himoya mexanizmlarining fundamental limitations qayta ko'rib chiqish zaruriyatini yuzaga keltirmoqda [6]. Ular mashinali o'rganish texnologiyalariga asoslangan adaptiv xavfsizlik tizimlarining an'anaviy tizimlardan katta margin bilan ustunligini komparativ analiz orqali isbotlashgan, bunda birinchi navbatda real-time learning va model adaptability aspektlariga alohida e'tibor qaratilgan.

Mashinali o'rganish algoritmlari bank ma'lumotlari xavfsizligini ta'minlashda markaziy komponenta sifatida funktsionallashmoqda. Kaloudi va Li (2020) tomonidan o'tkazilgan empirik tadqiqotlarda mashinali o'rganish texnologiyalari asosida yaratilgan defence systemlarining operational advantageslar hamda functional limitationslar kompleks ravishda o'rganilgan [7]. Ular tomonidan taklif etilgan kontseptual modellar real vaqt rejimida anomal operatsiyalarni identifikatsiyalash, potentsial threatlarni proaktiv bashorat qilish va deviant patternlarni detektiv aniqlash imkoniyatlarini demonstratsiya qilgan. Adabiyotlar tahlili asosida quyidagi mashinali o'rganish algoritmlari bank ma'lumotlari xavfsizligini ta'minlashda eng ko'p qo'llaniladigan instrumentlar sifatida identifikatsiya qilindi: Support Vector Machines (SVM, Tayanch Vektor Mashinalari) - firibgarlik operatsiyalarini (fraudulent transactions) klassifikatsiyalash uchun; Recurrent Neural Networks (RNN, Rekurrent Neyron Tarmoqlari) - temporal anomaliyalarni aniqlash va bashorat qilish uchun; Hidden Markov Models (HMM, Yashirin Markov Modellar) - mijozlar xulq-atvorini (customer behavior) probabillistik modellashtirish uchun; Local Outlier Factor (LOF, Lokal Outlier Faktori) - noodatiy operatsiyalarni (anomalous operations) multivariate space da identifikatsiyalash uchun [8]. Al-Mhiqani va boshqalar (2018) o'z tadqiqotlarida bank sektorida SI asosidagi kiberxavfsizlik tizimlarini joriy etishning ikkita fundamental paradigmasini konseptualizatsiya qilishgan [9].

NATIJALAR VA MUHOKAMA

Tadqiqot natijalariga ko'ra, bank sektorida ma'lumotlar xavfsizligini ta'minlash uchun qo'llaniladigan sun'iy intellekt modellarini funksional xarakteristikalariga asosida quyidagi fundamental kategoriyalarga sistematsizatsiya qilish mumkin: anomaliyalarni aniqlash algoritmlari (anomaly detection algorithms), bashorat qiluvchi modellar (predictive models), xulq-atvorni tahlil qiluvchi tizimlar (behavioral analysis systems) va kiberxujumlarni aniqlash tizimlari (cyberattack detection systems). Har bir kategoriya o'ziga xos funktsional xarakteristikalariga ega bo'lib, bank ma'lumotlari xavfsizligini ta'minlashning turli aspektlarini qamrab oladi. Anomaliyalarni aniqlash algoritmlari asosan mijozlar operatsiyalari va bank tizimlaridagi noodatiy faoliyatni identifikatsiyalash uchun qo'llaniladi va ularning asosiy qo'llanilish sohalari firibgarlik operatsiyalarini aniqlash (fraud detection) va ichki tahdidlarni monitoring qilish (internal threat monitoring) hisoblanadi. Bashorat qiluvchi modellar ma'lumotlar analizi asosida potentsial tahdidlarni proaktiv bashorat qilish uchun xizmat qiladi va risk management hamda xavfsizlik strategiyasini optimization qilishda keng qo'llaniladi. Xulq-atvorni tahlil qiluvchi tizimlar mijozlar va xodimlarning interaktiv xulq-atvorini kontinual monitoring qilish orqali ichki tahdidlarni aniqlash va autentifikatsiya jarayonlarini takomillashtirish imkonini beradi. Kiberxujumlarni aniqlash tizimlari esa bank tizimlariga bo'layotgan external attacklarni real vaqt rejimida identifikatsiyalash va bloklash uchun qo'llaniladi, asosan tarmoq xavfsizligi (network security) va DDoS hujumlarini mitigation qilish funksiyalarini bajaradi. Ushbu kategoriyalar va ularning asosiy xarakteristikalariga 1-jadvalda keltirilgan.

1-jadval.

Bank ma'lumotlari xavfsizligini ta'minlash uchun qo'llaniladigan SI modellari tasnifi

Model turi	Asosiy vazifasi	Qo'llanilish sohalari	Afzalliklari
Anomaliyalarni aniqlash algoritmlari	Noodatiy operatsiyalar va xulq-atvorni aniqlash	Firibgarlikni aniqlash, ichki tahdidlarni monitoring qilish	Real vaqt rejimida monitoring, yuqori aniqlik

Bashorat qiluvchi modellar	Potensial tahdidlarni oldindan bashorat qilish	Risklar boshqaruvi, xavfsizlik strategiyasini rejalashtirish	Proaktiv himoya, xavflarni minimallashtirish
Xulq-atvorni tahlil qiluvchi tizimlar	Mijozlar va xodimlar xulq-atvorini monitoring qilish	Ichki tahdidlar monitoringi, autentifikatsiya	Foydalanuvchilar profili asosida anomaliyalarni aniqlash
Kiberxujumlarni aniqlash tizimlari	Tizimga bo'layotgan hujumlarni aniqlash	Tarmoq xavfsizligi, DDoS hujumlarini aniqlash	Hujumlarni real vaqtda aniqlash va bloklash

Tadqiqot natijalariga ko'ra, bank sektorida ma'lumotlar xavfsizligini ta'minlash uchun quyidagi mashinali o'rganish algoritmlari yuqori empirik samaradorlikni demonstratsiya qilmoqda: Deep Learning (Chuqur o'rganish) - murakkab pattern recognition va fraud detection operatsiyalarida yuqori accuracy ko'rsatadigan neural network-based algoritmlar, bank sektorida phishing detection, credit card fraud monitoring va customer behavior analysis kabi sophisticated use case-lar uchun adaptatsiya qilingan [10]; Random Forest (Tasodifiy o'rmonlar) - ensemble learning metodologiyasiga asoslangan qaror daraxti algoritmlarining kombinatsiyasi bo'lib, data classification va anomaly detection use-case-larida yaxshi natijalar ko'rsatgan, bu algoritmlar classificationning robust va interpretable xarakteristikalariga ega bo'lib, false positive rate minimallashtirishda samarali hisoblanadi; Genetic Algorithms (Genetik algoritmlar) - evolyutsion paradigmaga asoslangan global optimizatsion algoritmlar bo'lib, complex security problemlarini solving qilish va tarmoq konfiguratsiyasini optimallashtirishda qo'llaniladi, Qatar banklarida bu algoritmlar network traffic analizi uchun implementatsiya qilinganligi empirik ma'lumotlar bilan tasdiqlangan; Natural Language Processing (NLP, Tabiiy tilni qayta ishlash) - lingvistik ma'lumotlarni qayta ishlash texnologiyasi bo'lib, phishing emaillarni identifikatsiyalash, social media-dagi fraud activitylarni monitoring qilish va financial crime detectionda keng qo'llaniladi.

Sun'iy intellekt asosidagi monitoring tizimlarining operatsion samaradorligi (operational efficiency) turli empirik tadqiqotlarda keng o'rganilgan. ZestFinance kompaniyasi tomonidan amalga oshirilgan kompleks tadqiqot natijalariga ko'ra,

mashinali o'rganish algoritmlarini kredit skoringda integratsiya qilish an'anaviy rule-based metodlar bilan taqqoslaganda 27% ko'proq arizalarni approve qilish va 16% pastroq foiz stavkalarini (interest rates) taklif etish imkonini bergan, bu esa kredit operatsiyalarining iqtisodiy samaradorligini sezilarli darajada oshirgan. Greenhill investitsiya banki tomonidan adaptatsiya qilingan CrowdStrike kompaniyasining Falcon platformasi cloud-scale mashinali o'rganish algoritmlariga asoslangan bo'lib, bank IT-sistemasidagi potentsial tahdidlarni proaktiv identifikatsiyalash uchun implementatsiya qilingan. Bu tizimni joriy etish natijasida false alertlar soni 75% ga reduksiya qilingan va annual operatsion xarajatlar taxminan 300,000 dollar miqdorida optimallashtirilib, bank xavfsizlik tizimining efficacy indikatorlari sezilarli darajada yaxshilangan. Ushbu va boshqa empirik ma'lumotlar asosida, sun'iy intellekt asosidagi monitoring tizimlarining operatsion samaradorlik ko'rsatkichlari 2-jadvalda sistematizatsiya qilingan

2-jadval.

Sun'iy intellekt asosidagi monitoring tizimlarining samaradorlik ko'rsatkichlari

SI modeli	Qo'llanilish sohasi	Samaradorlik ko'rsatkichi
ML-based Fraud Detection	Firibgarlikni aniqlash	Soxta ogohlantirishlar 75% ga kamaygan
AI Credit Scoring	Kredit skoringi	27% ko'proq kredit arizalari tasdiqlangan
AI-based Cybersecurity	Kiberxavfsizlik	Kiberhujumlarni aniqlash vaqti 60% ga qisqargan
NLP for Phishing Detection	Phishing hujumlarni aniqlash	Aniqlash samaradorligi 85% dan 95% ga ko'tarilgan

Bank sektorida sun'iy intellekt asosidagi xavfsizlik tizimlarini implementatsiya qilish kompleks protsess bo'lib, tadqiqot natijalariga ko'ra, bu jarayonda quyidagi fundamental qiyinchiliklar identifikatsiya qilingan: texnologik murakkablik (technical complexity) - SI sistemalarini deploy qilish va maintenance qilish uchun high-skilled specialists va sophisticated technical infrastructure talab etiladi, bu esa

banklar uchun resource-intensive investitsiyalarni talab qiladi; ma'lumotlar sifati va availability - SI modellarining accuracy va reliability xarakteristikalari foydalaniladigan ma'lumotlar sifati va hajmiga bevosita dependency ko'rsatadi, sifatsiz, noisy yoki biased ma'lumotlar modellarda accuracy degradationga olib kelishi mumkin; regulatory compliance va privacy concerns - =

XULOSA

Ushbu kompleks tadqiqot raqamli banklar ma'lumotlari xavfsizligini nazorat qiluvchi va monitoring qiluvchi sun'iy intellekt modellari va instrumentlarini sistematzirlashgan tahlil qilish orqali quyidagi fundamental konkluziyalarga kelindi: sun'iy intellekt va mashinali o'rganish texnologiyalari bank ma'lumotlari xavfsizligini ta'minlashda transformativ rol o'ynab, fraud detection, anomaly monitoring va threat prediction kapabilitylarini significant darajada enhancement qilmoqda; bank sektorida prevalent kiberxavfsizlik tahdidlari orasida insider threats, distributed denial of service (DDoS) attacks, ransomware, phishing attacks va social engineering kabi sophisticated attack vectorlar dominantlik qiladi, bu tahdidlarning evolving xarakteri va increasing sophisticationli an'anaviy security paradigmalarining fundamental limitatsiyalarini demonstratsiya qilmoqda; banking security provisioningda Support Vector Machines (SVM), Recurrent Neural Networks (RNN), Hidden Markov Models (HMM) va Local Outlier Factor (LOF) kabi mashinali o'rganish algoritmlari yuqori empirik samaradorlikni ko'rsatmoqda, bu algoritmlarning komplementar implementatsiyasi banklarning xavfsizlik sistemalari efficacysini comprehensive ravishda optimization qilish imkonini beradi.

Xulosa qilib aytganda, sun'iy intellekt texnologiyalari bank ma'lumotlari xavfsizligini provision qilishda paradigmatic transformationlarni kataliz qilmoqda. SI modellarini effective leveraging qilish orqali banklar kiberxavfsizlik tahdidlariga qarshi proaktiv stanceni adopt qilish, tahdidlarni real-time rejimida identifikatsiyalash va preventiv defence strategiyalarini implementatsiya qilish kapabilitylarini enhancement qilmoqda. Biroq, bu texnologiyalardan optimall foydalanish uchun organizatsion, texnologik va regulatory dimensionlardagi kompleks challengelarni comprehensive addresslash imperative hisoblanadi. =

Adabiyotlar ro'yxati

1. Barkadehi, M.Q., Saberi, M., Hamzelou, K., Smith, K.J. "The Role of Trust and Security in Electronic Banking and Customer Loyalty", International Journal of Electronic Commerce, 2018, Vol. 12, pp. 214-242.
2. Accenture Research. "Guardians of Trust: Navigating Cybersecurity in Banking", 2025.
3. Ryzhkova, A., Makarov, P., Kovalchuk, S. "Cybersecurity Challenges in Digital Banking", Journal of Banking Technology, 2020, Vol. 25, No. 3, pp. 145-163.
4. He, W., Tian, X., Chen, Y., Choo, K.R. "Securing Online Banking Services: A Comprehensive Review", IEEE Communications Surveys & Tutorials, 2020, Vol. 22, No. 2, pp. 944-973.
5. Li, J., Che, W., Li, X. "A Survey of AI-based Cybersecurity Solutions", Computer Science Review, 2024, Vol. 42, pp. 100-121.
6. Perumal, S. "A Comprehensive Analysis of AI for Cybersecurity", International Journal of Cyber Security, 2018, Vol. 2, No. 1, pp. 67-89.
7. Ryzhkova, A., Makarov, P., Kovalchuk, S. "Analysis of Cyber Security Threats in Banking Industry", Journal of Banking Security, 2020, Vol. 15, No. 2, pp. 78-96.
8. Accenture. "Guardians of Trust Survey: Navigating Cybersecurity in Banking", 2025.
9. Kaloudi, N., Li, J. "The AI-Based Cyber Threat Landscape: A Survey", ACM Computing Surveys, 2020, Vol. 53, No. 1, pp. 1-34.
10. Begley, T.A., Srinivasan, A. "Network Analysis and Machine Learning Applications in Banking Security", Journal of Financial Stability, 2019, Vol. 40, pp. 111-135