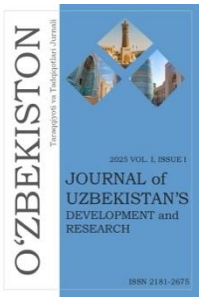

Journal of Uzbekistan's Development and Research (JUDR)

Journal home page: https://ijournal.uz/index.php/judr

O‘ZBEKISTONDA RAQAMLI IQTISODIYOT SHAROITIDA IQTISODIY XAVFSIZLIKNI TA’MINLASH

Saidova Gulchexra[1]

Oriental universiteti

KEYWORDS

raqamli iqtisodiyot, iqtisodiy xavfsizlik, sun’iy intellekt, SIEM, axborot xavfsizligi, log tahlil.

ABSTRACT

Ushbu maqolada O‘zbekiston korxonalarining raqamli iqtisodiyot sharoitida iqtisodiy xavfsizlikni ta’minlashdagi muammolari tahlil qilinadi. Asosiy e’tibor eskirgan axborot infratuzilmasi, zaif dasturiy ta’minot va inson omiliga bog‘liq xavf-xatarlarga qaratilgan. Muallif sun’iy intellektga asoslangan SIEM tizimlarining joriy etilishi orqali tahdidlarni real vaqt rejimida aniqlash, avtomatlashtirilgan xavfsizlik monitoringi va texnologik barqarorlikni oshirish imkoniyatlarini ko‘rsatadi. Shuningdek, milliy kadrlar tayyorlash va mahalliy texnologiyalarni rivojlantirishning dolzarbligi ta’kidlanadi.

2181-2675/© 2025 in XALQARO TADQIQOT LLC.
DOI: **10.5281/zenodo.15731935**

Ko‘plab O‘zbekiston korxonalarida axborot infratuzilmasi 10 yildan ortiq eskirgan texnologiyalarga asoslangan. Serverlarining aksariyati doimiy yangilanmaydi, zaif shifrlash protokollaridan foydalaniladi va ehtiyot rejimdagi (backup) tizimlar mavjud emas.

Bu quyidagi muammolarga olib keladi:

- Kirish nazoratining sustligi (authentication)
- Dasturiy yamoqlarning o‘z vaqtida o‘rnatilmasligi
- Serverlarning tez ishdan chiqishi yoki ortiqcha yuklanish

Korxonalar tomonidan foydalanilayotgan dasturiy ta’minotning ko‘pchiligi:

- Litsenziyasiz
- Yangilanishsiz
- Himoyasiz ochiq kod asosida yozilgan

Bu holat “zero-day” ekspluatatsiyalar uchun qulay sharoit yaratadi. 2023-yil davomida AKT vazirligi auditiga ko‘ra, 15 mingdan ortiq kichik korxonada o‘rnatilgan buxgalteriya

[1] Oriental universiteti 2-boshqich magistri

va savdo dasturlarida kritik xavfsizlik zaifliklari aniqlangan.

Ko‘pchilik korxonalarda ERP, CRM, BI kabi tizimlar alohida-alohida ishlaydi, ularning o‘zaro ma’lumot almashinuvi mavjud emas. Bu ma’lumotlarning chalg‘ishiga, dublikat bazalarning shakllanishiga va xavfsizlik monitoringining izchilligi buzilishiga sabab bo‘ladi.

Texnik xavfsizlik choralarini kuchaytirish uchun integratsiyalashgan va xavfsizlik mezonlariga mos infratuzilma, muntazam texnik auditlar va IT-sertifikatli kadrlar zarur.

Axborot xavfsizligining 60% dan ortiq tahdidlari inson omiliga, xususan xodimlar xatti-harakatiga bog‘liq. Ular uch toifaga bo‘linadi:

- Ataylab zarar yetkazuvchilar (sabotaj)
- Bilmasdan noto‘g‘ri harakat qiluvchilar (e-mail orqali ma’lumot yuborish, zaif parollar)
- Ilgari ishdan bo‘shagan, ammo tizimga kirish imkoniyati saqlanib qolganlar

IBM (2022) ma’lumotiga ko‘ra, bitta ichki tahdidning o‘rtacha aniqlanish va bartaraf qilish muddati 77 kun, bu esa korxona uchun vaqt va mablag‘ sarfi demakdir.

AI integratsiyalangan SIEM tizimi (Security Information and Event Management) tashkilotning barcha IT infratuzilmasidagi voqealarni (events) va xavflarni markazlashtirilgan holda to‘playdi, ularni real vaqt rejimida tahlil qiladi va tahdid mavjud bo‘lsa, signal uzatadi. Asosiy afzalliklari quyidagilardan iborat:

- Ma’lumotlar ombori (data lake) dan millionlab loglar asosida real vaqt monitoring
- Yolg‘on ijobiy (false positive) signal darajasini kamaytirish
- Mashina o‘rganish algoritmlari orqali doimiy takomillashuv

Mashhur SIEM tizimlariga misollarni IBM QRadar, Splunk Enterprise Security, Azure Sentinel, Elastic SIEM korxonalari misolida ko‘rish mumkin. Ushbu platformalar O‘zbekiston korxonalari uchun moslashtirilgan holda mahalliy bulutli infratuzilmaga o‘rnatilishi mumkin.

Har bir operatsion tizim (Windows, Linux, Android, iOS), veb-server (Apache, Nginx), router, firewall, va ilovalar o‘zining log-fayllarini generatsiya qiladi. Ular juda katta hajmga ega va inson tomonidan qo‘lda kuzatish deyarli imkonsiz.

AI asosidagi log-tahlil tizimi quyidagicha:

- Har daqiqada hosil bo‘ladigan minglab log yozuvlarini avtomatik o‘qiydi
- Xavfsizlik buzilishi mumkin bo‘lgan holatlarni (login urinishlari, port scanning, unauthorized access) aniqlaydi
- Kontekstual tahlil orqali loglar orasida yashiringan anomaliyalarni aniqlaydi

Misol uchun bir foydalanuvchi odatda Toshkentda ishlaydi, lekin bir kunda Xorazm va xorij IP manzilidan kirishga urinsa – tizim bu holatni tahdid sifatida qayd etadi.

Bu modul “oddiydan chetga chiqish”ni aniqlash orqali yangi, hali ma’lum bo‘lmagan tahdidlarni ham aniqlashga xizmat qiladi. Masalan:

Oddiy kunlarda foydalanuvchi faqat Excel fayl ochadi, bir kun kelib esa 100 ta PDF va SQL fayl yuklay boshlasa – bu anomal faollik;

Serverga kechasi odatda hech kim kirmaydi, lekin birdaniga 300 ta login urinish kuzatilsa – bu hujum belgisi;

AI bu xatti-harakatlarni o‘rganadi (baselining) va shunga asoslanib avtomatik o‘zgarishlarni ko‘rib chiqadi. Bu model zero-day attacklar yoki APT (advanced persistent threat) ni aniqlashda ayniqsa foydalidir.

Tizim tahdid aniqlangan zahoti xavfsizlik xodimlariga avtomatik ogohlantirish yuboradi. Ogohlantirishlar:

- Telegram orqali yuboriladi – bu ayniqsa lokal korxonalarda tez va qulay;
- Email va SMS orqali yuboriladi – menejment darajasidagi ogohlantirishlar;
- Dashboard orqali vizual holatda ko‘rsatiladi – voqea (incident) soni, joyi, darajasi va holati.

Kutilayotgan natijalar quyidagilardan iborat:

a) Kiberhujum va ichki xavflarni 70–80% tez aniqlash. Sun’iy intellekt loglar va trafikdagi anomal xatti-harakatlarni insondan 100 barobar tez tahlil qiladi. Bu hujumni boshlanish bosqichida to‘xtatishga imkon beradi;

b) Inson xatolarini kamaytirish. Ko‘p holatlarda xodimlar ogohlantirishni o‘tkazib yuboradi, noto‘g‘ri baholaydi yoki kech harakat qiladi. AI asosidagi tizim doimiy, xatolikdan holi va mustahkam monitoring ta’minlaydi;

c) Operatsion barqarorlik va ishonchni oshirish. Xavfsizlik monitoringi aniq va uzluksiz bo‘lsa, ishlab chiqarish, moliya va mijozlar xizmatidagi barqarorlik ortadi. Investitsion muhit yaxshilanadi, regulatorlar ishonchi mustahkamlanadi.

Afzalliklar	**Tahdid va cheklovlar**
- Real vaqtli monitoring	- SIEM tizimi litsenziyasi qimmat bo‘lishi mumkin
- O‘z-o‘zini o‘rganuvchi model	- Mahalliy kadrlar malakasi yetishmasligi
- Insonga nisbatan ancha barqaror	- Sun’iy intellektni noto‘g‘ri sozlash noto‘g‘ri signalga olib keladi
- Audit, tahlil, hisobotlar avtomatik	- Har bir tizim uchun individual moslash talab etiladi

Jadval 1. SIEM tizimining afzalliklar va tahdidlar

Mahalliy texnoparklarda ochiq manba SIEM (masalan, ELK stack: Elasticsearch, Logstash, Kibana) asosida loyihalar yaratilishi mumkin. Davlat idoralari uchun maxsus Telegram-bot asosida tahdid monitoringi ishlab chiqish qulay va amaliy bo‘ladi. Oliy ta’lim muassasalari bilan hamkorlikda AI xavfsizlik laboratoriyalari tashkil qilish — kadr tayyorlash va milliy texnologiyalarni rivojlantirish uchun zarur.

Sun’iy intellekt asosidagi xavfsizlik monitoring platformasi korxonalarning raqamli transformatsiyada ishonchli va barqaror faoliyat yuritishini ta’minlovchi eng samarali zamonaviy vositalardan biridir. U nafaqat xavflarni aniqlaydi, balki ularni oldindan bashorat qilish, tezkor choralar ko‘rish va tizimni real vaqt rejimida himoya qilish imkonini beradi.

Ushbu model O‘zbekiston uchun universal bo‘lib, bank, sanoat, ta’lim, sog‘liqni saqlash va boshqa tarmoqlar uchun moslashtirilgan holda joriy etilishi mumkin. Strategik va amaliy

jihatdan bu yondashuv mamlakatning raqamli suvereniteti, iqtisodiy xavfsizligi va texnologik mustaqilligini ta’minlashga xizmat qiladi.

Foydalanilgan adabiyotlar ro‘yxati

1. ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. International Organization for Standardization, Geneva.
2. ISO 22301:2019 – Security and Resilience – Business Continuity Management Systems – Requirements. ISO, Geneva.
3. COSO (2017) – Enterprise Risk Management: Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission (COSO), USA.
4. NIST (2018) – Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA.
5. General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679 of the European Parliament and of the Council, European Union.
6. Republic of Uzbekistan (2021) – Law on Information Security [“Axborot xavfsizligi to‘g‘risida” Qonuni]. National Legislative Database, www.lex.uz.
7. Cabinet of Ministers of Uzbekistan (2022) – Cybersecurity Strategy of the Republic of Uzbekistan 2022–2025. Tashkent: Ministry for Development of Information Technologies and Communications.
8. Ministry of Digital Technologies of the Republic of Uzbekistan (2023) – National Digital Economy Development Report. Tashkent.
9. World Bank (2022) – Cybersecurity Capacity Review: Central Asia Report. Washington, DC.
10. European Union Agency for Cybersecurity (ENISA) (2023) – Threat Landscape Report. Athens.
11. IBM Security (2023) – Cost of a Data Breach Report. IBM Corporation, USA.
12. https://www.ibm.com/security/data-breach
13. Kaspersky Lab (2023) – Cybersecurity Trends in CIS Countries. Moscow.
14. Statistika agentligi huzuridagi Statkom (2023) – Axborot texnologiyalaridan foydalanish bo‘yicha statistik tahlil. Tashkent.
15. Kapitalbank Annual Report (2023) – IT Security and Risk Management Division. Tashkent.
16. Singh, A., & Sidhu, B. (2020) – Cybersecurity Governance in Developing Countries: Case Studies from Asia. International Journal of Information Management, 54, 102139. https://doi.org/10.1016/j.ijinfomgt.2020.102139
17. Clarke, R., & Knake, R. (2019) – Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins.
18. Almukhambetov, A. (2022) – Institutionalizing Cybersecurity in Central Asia: Challenges and Perspectives. Central Asian Affairs, 9(1), 53–74.

19. Bohoslavsky, P. (2021) – Digital Sovereignty and Institutional Capacity in Emerging Economies. Journal of Global Policy, 12(S1), 77–92.
20. Uzbekistan National Statistics Agency (2023) – Raqamli texnologiyalarni joriy qilgan korxonalar statistikasi. www.stat.uz
21. The World Economic Forum (2023) – Global Cybersecurity Outlook. Geneva: WEF.