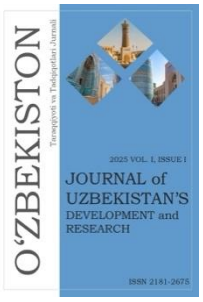


Journal of Uzbekistan's Development and Research (JUDR)

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

# O‘ZBEKISTONDA RAQAMLI IQTISODIYOT SHAROITIDA IQTISODIY XAVFSIZLIKNI TA’MINLASH

Kosimov Xasan[1]

*Oriental universiteti*

KEYWORDS

raqamli iqtisodiyot, iqtisodiy xavfsizlik, kiberxavfsizlik, raqamli transformatsiya, iqtisodiy suverenitet, axborot xavfsizligi, digital risk, texnologik xavf, raqamli boshqaruv, O‘zbekiston strategiyasi.

ABSTRACT

Maqolada O‘zbekistonda raqamli iqtisodiyotning rivojlanishi va uning iqtisodiy xavfsizlikka ta’siri tahlil qilinadi. Raqamlashtirish jarayonida yuzaga kelayotgan asosiy tahdidlar, jumladan, kiberxavfsizlik, axborot asimmetriyasi, raqamli suverenitet muammolari va ularni bartaraf etish mexanizmlari ko‘rib chiqiladi. Tadqiqotda “Raqamli O‘zbekiston – 2030” strategiyasining xavfsizlik aspektlari, iqtisodiy subyektlar faoliyatida raqamli risklarni boshqarish, hamda xalqaro tajribalardan foydalanish zarurati asoslab berilgan. Maqolada iqtisodiy xavfsizlikni mustahkamlashda institutsional yondashuv, normativ-huquqiy baza va texnologik tayyorgarlik darajasining o‘zaro uyg‘unligi tahlil qilingan.



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 va savdo

[1] Oriental universiteti magistranti

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.

- 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.

- 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. O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash to‘g‘risidagi PF–6079-sonli Farmoni. 2020 yil, 5 oktyabr.
2. Tursunov, B. O. (2023). “Raqamli iqtisodiyot sharoitida iqtisodiy xavfsizlikni ta’minlashning institutsional asoslari.” Iqtisodiyot va innovatsion texnologiyalar jurnali, №2, 57–64.
3. Karimov, I. & Yusupova, D. (2022). “Raqamli xavfsizlik va iqtisodiy mustahkamlik o‘zaro bog‘liqligi.” Milliy xavfsizlik va strategik tadqiqotlar, №4, 33–41.
4. OECD (2021). Digital Security Risk Management for Economic and Social Prosperity. OECD Publishing, Paris.
5. World Economic Forum (2022). Global Cybersecurity Outlook 2022. WEF Annual Report.
6. Qodirov, A. Sh. (2024). “Axborot xavfsizligini ta’minlashda raqamli texnologiyalar roli.” TDIU ilmiy axborotlari, №1, 89–97.
7. GOST R ISO/IEC 27001-2021. “Axborot xavfsizligi menejmenti tizimlari – Talablar.” Moskva, 2021.
8. Murodov, S. (2023). “O‘zbekistonda iqtisodiy suverenitetni raqamlashtirish sharoitida ta’minlash muammolari.” Iqtisodiy tadqiqotlar jurnali, №3, 102–110.
9. UNCTAD (2022). Digital Economy Report 2022: Cross-border data flows and development. Geneva.
10. Xudayberganov, B. R. (2023). “Raqamli iqtisodiyotning makroiqtisodiy barqarorlikka ta’siri.” Iqtisodiy taraqqiyot, №2, 21–30.