MAVZU: O‘ZBEKISTON TA’LIM TIZIMIDA RAQAMLI INFRATUZILMA XAVFSIZLIGINI BAHOLASH UCHUN AI-MONITORING MODELI ISHLAB CHIQISH

Muallif: Palvaniyazova Dilbar Ametjanovna

Kirish

So‘nggi yillarda O‘zbekiston ta’lim tizimi raqamlashtirish jarayonida sezilarli o‘zgarishlarga erishdi. Maktablar, oliy ta’lim muassasalari va ilmiy markazlarda elektron jurnallar, masofaviy ta’lim platformalari, bulutli ma’lumotlar bazalari faol joriy etilmoqda. Shu bilan birga, raqamli infratuzilma kengaygani sari axborot xavfsizligi tahdidlari ham ortib bormoqda.

Masofaviy o‘quv tizimlariga noqonuniy kirish, foydalanuvchi ma’lumotlarining o‘g‘irlanishi, fishing, zararli dasturlar orqali hujumlar va server zaifliklari ta’lim muassasalarining ishonchliligiga jiddiy xavf tug‘dirmoqda. Shu bois, ta’lim tizimi infratuzilmasini himoyalashda **sun’iy intellekt (AI)** asosida ishlovchi **monitoring modellari**ni ishlab chiqish dolzarb vazifadir.

Asosiy qism

1. Ta’lim tizimi raqamli infratuzilmasining asosiy tahdidlari

Ta’lim muassasalari infratuzilmasida quyidagi xavf omillari mavjud:

- Zaif autentifikatsiya tizimlari (foydalanuvchi parollari oddiy yoki qayta ishlatilgan holatlar);
- Masofaviy o‘quv platformalarida (Moodle, ZiyoNet, EduMarket va b.) himoyasiz API interfeyslar;
- Ma’lumotlarni saqlashda bulutli xavfsizlik sertifikatlarining yetishmasligi;
- Ichki tarmoqlarda monitoringning cheklanganligi.

Bu holatlarda **AI-monitoring modeli** real vaqt rejimida tarmoqdagi faoliyatni kuzatib, xavf belgilarini avtomatik tahlil qilishi mumkin.

2. AI-monitoring modeli arxitekturasi

Tadqiqot natijalariga ko‘ra, ishlab chiqilayotgan AI-monitoring modeli quyidagi tarkibiy qismlardan iborat:

1. **Ma’lumot to‘plash moduli** – tarmoqdan kelayotgan loglar, foydalanuvchi kirish ma’lumotlari va server javoblarini yig‘adi.
2. **AI-tahlil moduli** – mashinali o‘rganish algoritmlari asosida odatiy xatti-harakat modelini shakllantiradi.
3. **Xavf aniqlash moduli** – real vaqt rejimida noodatiy faoliyatni (noqonuniy kirish, katta hajmli yuklab olish, API so‘rovlaridagi g‘ayritabiiylik) aniqlaydi.
4. **Ogohlantirish va qaror qabul qilish moduli** – tizim administratoriga avtomatik bildirishnoma yuboradi va xavfni bloklaydi.

Modelning asosiy afzalligi – inson omilini kamaytirib, xavfli faoliyatni **oldindan prognozlash** imkonini berishidir.

3. Modelning amaliy qo‘llanilishi

Ushbu AI-monitoring modeli:

- O‘zbekiston ta’lim tarmog‘i (ZiyoNet, my.edu.uz) kabi markazlashtirilgan platformalarda sinovdan o‘tkazilishi mumkin;
- Universitet serverlari (masalan, Nukus DPI, TATU filiallari) uchun maxsus modul sifatida integratsiya qilinadi;
- Mahalliy axborot tizimlarida ma’lumotlar oqimini tahlil qilib, xavf darajasini foiz ko‘rsatkichda baholaydi.

Natijada, ta’lim muassasalarining raqamli infratuzilmasi ustidan doimiy **sun’iy intellekt asosli nazorat** o‘rnatiladi.

Xulosa

O‘zbekiston ta’lim tizimida raqamli infratuzilmaning tezkor rivojlanishi bilan birga, axborot xavfsizligini ta’minlashda avtomatlashtirilgan AI-monitoring tizimlarini joriy etish zarurati ortib bormoqda. Taklif etilgan model tarmoqdagi xavf-xatarlarni real vaqt rejimida aniqlash, foydalanuvchi faoliyatini tahlil qilish va tezkor javob choralarini ko‘rish imkonini beradi.

Kelgusida ushbu tizimni ta’lim sohasidagi barcha raqamli platformalarga moslashtirish orqali **axborot xavfsizligi madaniyatini oshirish** va **raqamli ta’lim tizimining barqarorligini ta’minlash** mumkin bo‘ladi.

FOYDALANGAN ADABIYOTLAR

European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024: The Role of Artificial Intelligence in Cybersecurity.* Athens: ENISA Publications, 2024.

☞ Rasmiy manba: https://www.enisa.europa.eu/publications

 UNESCO Institute for Information Technologies in Education (IITE). *Cybersecurity in Digital Education Systems: Global Policy Review.* Paris, 2024.

☞ Rasmiy manba: https://iite.unesco.org

 Kaspersky. *Machine Learning in Cybersecurity: Global Threat Report H1 2024.* Kaspersky Security Bulletin, 2024.

☞ Rasmiy manba: https://www.kaspersky.com/about/press-releases

 National Cybersecurity Center of Uzbekistan. *Cyber Threat Landscape of Uzbekistan 2024.* Tashkent: MITC, 2024.

☞ Rasmiy manba: https://cybersecurity.uz

 Kadirov, A. I. “Blockchain Technology and Information Security in Uzbekistan’s Digital Economy.” *International Journal of Asian Economic Light (JAEL)*, Vol. 12, Issue 3, May 2024.

☞ Rasmiy manba: https://eprajournals.com

 Microsoft Security. *AI-Driven Cyber Defense for Education and Research Institutions.* Technical Whitepaper, 2024.

☞ Rasmiy manba: https://www.microsoft.com/security/blog

 OECD. *Digital Education and Data Protection: Policy Insights 2023.* Paris: OECD Publishing, 2023.

☞ Rasmiy manba: https://www.oecd.org/education