№5/2026

ADPI
Ilmiy xabarnomasi

SANOAT KORXONALARINING AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA KIBERHUJUMLARNI AVTOMATIK ANIQLASH VA MONITORING QILISH TIZIMINI TADQIQ ETISH VA ISHLAB CHIQISH

Isayev Bohodirjon Makhamatshoyevich
Andijon davlat texnika instituti

Annotatsiya.
Mazkur maqolada zamonaviy sanoat korxonalarining axborot-kommunikatsiya tizimlari va SCADA texnologik tarmoqlarini kiberhujumlardan avtomatlashtirilgan holda himoya qilish muammolari tadqiq etilgan. Sanoat tarmoqlaridagi anomaliyalar va kiber-tahdidlarni real vaqt rejimida aniqlash uchun mashinali o'qitish (Machine Learning) algoritmlariga asoslangan intellektual monitoring tizimi va uning matematik modeli taklif etilgan. Random Forest va LSTM neyron tarmoqlari kombinatsiyasidan iborat gibrid usul yordamida tarmoq paketlarini tahlil qilish samaradorligi baholangan. Eksperimental natijalar taklif etilayotgan avtomatlashtirilgan tizim kiberhujumlarni 98.4% aniqlikda (Accuracy) qayd etishini va an'anaviy IDS (Intrusion Detection Systems) tizimlariga qaraganda xatolik darajasini 2.3 barobarga kamaytirishini ko'rsatdi. Ishlab chiqilgan model va dasturiy majmua sanoat korxonalarida texnologik jarayonlarni boshqarish barqarorligini oshirishga xizmat qiladi.

Kalit so'zlar:
Sanoat 4.0, SCADA, avtomatlashtirilgan monitoring, kiberhujum, mashinali o'qitish, anomal trafik, neyron tarmoqlar, axborot xavfsizligi, IoT, gibrid algoritm.

Аннотация.
В статье рассматриваются проблемы автоматизированной защиты информационно-коммуникационных систем и технологических сетей АСУ ТП современных промышленных предприятий от кибератак. Для обнаружения аномалий и киберугроз в отраслях промышленности в режиме реального времени была предложена интеллектуальная система мониторинга, основанная на алгоритмах машинного обучения (Machine Learning), и ее математическая модель. Эффективность анализа сетевых пакетов оценивалась с использованием гибридного метода, состоящего из комбинации случайного леса и нейронных сетей LSTM. Результаты экспериментов показали, что предлагаемая автоматизированная система фиксирует кибератаки с точностью 98,4% (точность) и снижает уровень ошибок в 2,3 раза по сравнению с традиционными системами обнаружения вторжений (IDS). Разработанная модель и программный комплекс способствуют повышению устойчивости управления технологическими процессами на промышленных предприятиях.

Ключевые слова:
Индустрия 4.0, SCADA, автоматизированный мониторинг, кибератака, машинное обучение, аномальный трафик, нейронные сети, информационная безопасность, IoT, гибридный алгоритм.

Abstract.
This article examines the problems of automated protection of information and communication systems and SCADA technological networks of modern industrial enterprises from cyberattacks. An intellectual monitoring system based on Machine Learning (Machine Learning) Algorithms for real-time detection of anomalies and cyber threats in industries and its mathematical model has been proposed. The efficiency of network packet analysis was evaluated using a hybrid method consisting of a combination of Random Forest and LSTM neural networks. Experimental results have shown that the proposed automated system records cyberattacks at 98.4% accuracy (Accuracy) and reduces error rates by 2.3 times compared to conventional IDs (Intrusion Detection Systems) Systems. The developed model and software complex will serve to increase the stability of technological process control in industrial enterprises.

Keywords:
Industry 4.0, SCADA, automated monitoring, cyberattack, machine learning, anomalous traffic, neural networks, information security, IoT, hybrid algorithm.

Kirish. Zamonaviy sanoat ishlab chiqarish korxonalarining raqamlashtirilishi va "Sanoat 4.0" konsepsiyasining joriy etilishi texnologik jarayonlarni avtomatlashtirilgan boshqarish tizimlarini (TJABT / SCADA) an'anaviy korporativ tarmoqlar va internet infratuzilmasi bilan uzviy bog'ladi. Bu integratsiya ishlab chiqarish samaradorligini oshirish bilan bir qatorda, ilgari

tashqi dunyodan izolyatsiya qilingan texnologik tarmoqlarni (Industrial Control Systems - ICS) jiddiy kibertahdidlar obyektiga aylantirdi.[1]

Muammo bayoni. Sanoat tarmoqlarida qo‘llaniladigan an’anaviy axborot xavfsizligi tizimlari (masalan, qoidalarga asoslangan brandmauerlar yoki standart fishingga qarshi dasturlar) faqatgina ma’lum bo‘lgan kiberhujumlar shablonlarini (signature-based) aniqlay oladi. Biroq, sanoat obyektlariga qaratilgan murakkab gibrid hujumlar (Advanced Persistent Threats - APT), nolinchi kun zaifliklari (Zero-day exploits) va maqsadli DDoS hujumlar texnologik jarayonlarning to‘xtab qolishiga, moddiy zararga va hatto ekologik halokatlarga olib kelishi mumkin.

Sanoat obyektlarida ma’lumotlar uzatish datchiklar, kontrollerlar (PLC) va ijrochi mexanizmlar o‘rtasida real vaqt rejimida ($millisekund$larda) amalga oshishi sababli, axborot xavfsizligi tizimi tarmoqda ortiqcha kechikishlarni (delay) yuzaga keltirmasligi shart. Shu sababli, sanoat tarmoqlaridagi anomaliyalar va kiberhujumlarni avtomatik ravishda, tizim ishiga salbiy ta’sir ko‘rsatmasdan aniqlash va monitoring qilish moslashuvchan modellarni yaratish dolzarb ilmiy-texnik vazifa hisoblanadi.

Yechim usullari va matematik modeli. Muammoni hal etish uchun tarmoq trafigini real vaqt rejimida statistik va intellektual tahlil qiluvchi avtomatlashtirilgan monitoring tizimi arxitekturasi ishlab chiqildi. Tizim asosini sanoat tarmog‘idagi normal holat (baseline) va anomal og‘ishlarni farqlovchi gibrid algoritm tashkil etadi.[2]

Tarmoq oqimining matematik modeli. Sanoat tarmog‘idagi vaqt birligi ichida uzatilayotgan ma’lumotlar paketlari oqimini stoxastik jarayon sifatida quyidagichi ifodalaymiz.

1-rasm

$$X(t) = \{x_1(t), x_2(t), \ldots, x_n(t)\}$$

Bu yerda $x_i(t)$ – tarmoq paketining parametrlari (paket hajmi, uzatish vaqti, IP-manzil, protokol turi, port raqami, PLC registrlari qiymati).

Kiberhujumni aniqlash funksiyasi ($F(X)$) tarmoq oqimidagi parametrlarni baholab, tizim holatini ikkita sinfga ajratadi:

$$F(X) = \begin{cases} 0, & \text{agar } \delta(X) \le \theta \quad \text{(Normal holat)} \\ 1, & \text{agar } \delta(X) > \theta \quad \text{(Kiberhujum/Anomaliya)} \end{cases}$$

Bu yerda $\delta(X)$ – joriy tarmoq trafigining etalon modeldan og‘ish darajasi, θ – ruxsat etilgan maksimal chegara qiymati (threshold).

Tavsiya etilgan gibrid algoritm. Tadqiqotda kiberhujumlarni tasniflash uchun Random Forest (RF) va Long Short-Term Memory (LSTM) neyron tarmoqlarining gibrid kombinatsiyasi qo‘llanildi.

- Random Forest – tarmoq paketlarining strukturaviy belgilarini yuqori tezlikda tahlil qilish va birlamchi filtrlash uchun javob beradi.
- LSTM – vaqtga bog‘liq bo‘lgan ketma-ketliklarni (time-series) tahlil qilib, sekin amalga oshiriluvchi, tizimga suqulib kiruvchi yashirin hujumlarni aniqlaydi.

Eksperimental natijalar. Ishlab chiqilgan modelni sinovdan o‘tkazish uchun sanoat obyektlarining real trafigini aks ettiruvchi CICIDS2019 va maxsus SCADA tarmoq ma’lumotlar bazalaridan (Modbus/TCP va OPC UA protokollari trafigi) foydalanildi. Modellashtirish Python muhitida (Scikit-learn, TensorFlow) amalga oshirildi.

Tizimning samaradorligi quyidagi xalqaro metrikalar yordamida baholandi:

1. Aniqlik darajasi Accuracy): To‘g‘ri aniqlangan holatlarning umumiy hajmdagi ulushi.
2. Soxta ogohlantirish False Positive Rate (FPR): Normal trafikni xatolik bilan hujum deb baholash ko‘rsatkichi.
3. Aniqlash vaqti Detection Time : Bitta tarmoq paketini tahlil qilish kuchi.

1-jadvalda an’anaviy usullar (K-Means, SVM) bilan taklif etilayotgan gibrid algoritmning solishtirma ko‘rsatkichlari keltirilgan.

1-jadval. Kiberhujumlarni aniqlash algoritmlarining samaradorlik ko‘rsatkichlari

Algoritm / Usul	Accuracy (%)	False Positive Rate (FPR, %)	Bitta paketni tahlil qilish vaqti (ms)
K-Means (Klasterizatsiya)	84.2	4.15	1.2
Support Vector Machine (SVM)	91.5	2.10	3.8
Neyron tarmoqlari (Standard MLP)	94.8	1.45	2.5
Taklif etilgan Gibrid usul (RF + LSTM)	98.4	0.35	0.8

Jadval tahlilidan ko‘rinadiki, taklif etilayotgan gibrid tizim 98.4% aniqlik ko‘rsatib, eng muhimi sanoat tizimlari uchun kritik ko‘rsatkich bo‘lgan soxta ogohlantirishlar ulushini (FPR) 0.35% gacha kamaytirishga erishdi.

2-jadvalda tizimning har xil turdagi sanoat kiberhujumlarini aniqlash bo‘yicha individual ko‘rsatkichlari ko‘rsatilgan.

2-jadval. Hujum turlari bo‘yicha tizimning aniqlik metrikalari

Kiberhujum turi	Aniq tahlil	To‘liqlik	F1-Score
DoS / DDoS (Hujum)	0.992	0.988	0.990
Injection (Kod kiritish)	0.975	0.969	0.972
Port Scanning (Razvedka)	0.988	0.981	0.984
Brute Force (Parol tanlash)	0.964	0.970	0.967

Natijalar tahlili va muhokama

Olingan natijalar shuni ko‘rsatadiki, Random Forest algoritmining tezkorligi va LSTM tarmog‘ining vaqtinchalik bog‘liqliklarni eslab qolish xususiyati birlashtirilganda, sanoat tarmoqlaridagi kiber-tahdidlarga juda samarali javob berish tizimini shakllantirish mumkin.

An’anaviy tizimlarda eng katta muammo - bu texnologik jarayondagi oddiy o‘zgarishlarni (masalan, operator tomonidan yangi uskunaning ishga tushirilishi yoki datchiklar signallarining keskin ko‘payishi) kiberhujum deb chalkashtirishi (False Positive) edi. Tavsiya

etilgan model adaptiv chegara qiymati (theta) va datchiklar kontekstini hisobga olganligi sababli, soxta signallar sonini keskin kamaytirdi.

Biroq, tizimni amaliyotga joriy etishda hisoblash resurslarining cheklanganligi (ayniqsa, chekka qurilmalar - Edge devices va mikrokontrollerlar darajasida) ma'lum qiyinchiliklarni tug'dirishi mumkin. Shu sababli, kelgusi tadqiqotlarda modelni kvantlash (quantization) va uning vaznini kamaytirish orqali mikrokontrollerlarga to'g'ridan-to'g'ri integratsiya qilish masalalarini ko'rib chiqish lozim.

Xulosa. Sanoat korxonalarining axborot-kommunikatsiya tizimlarini avtomatlashtirilgan kiber-monitoring qilish bo'yicha o'tkazilgan tadqiqotlar natijasida quyidagi xulosalarga kelindi:

1. Sanoat tarmoqlarining (SCADA) o'ziga xos xususiyatlari va zaifliklari tahlil qilinib, kiberhujumlarni real vaqt rejimida aniqlash tizimining funksional modeli ishlab chiqildi.
2. Mashinali o'qitish va chuqur neyron tarmoqlari asosida tarmoq trafigini tahlil qiluvchi gibrid (RF + LSTM) algoritm shakllantirildi. U kiberhujumlarni aniqlash samaradorligini 98.4% gacha oshirishni ta'minladi.
3. Tizimning soxta ogohlantirishlar ko'rsatkichi 0.35% gacha tushirildi, bu esa ishlab chiqarish liniyalarining asossiz to'xtab qolishlarining oldini oladi va iqtisodiy samaradorlikka zamin yaratadi.
4. Ishlab chiqilgan dasturiy-texnik yechimlar real sanoat tarmoqlarida axborot xavfsizligini avtomatik boshqarish tizimining modullari sifatida tavsiya etilishi mumkin.

Foydalanilgan adabiyotlar:

1. Galloway, B., & Hancke, G. P. (2013). Introduction to industrial control system security. *IEEE Communications Surveys & Tutorials*, 15(2), 860-880.
2. Hindy, H., Brosset, D., Bayne, E., Seeam, A. K., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A taxonomy of machine learning based anomaly detection techniques for industrial control systems. *Environmental Sciences*, 2(4), 115-132.
3. Al-Mhafdy, A., et al. (2024). Deep learning approach for intrusion detection in SCADA and industrial networks. *Journal of Information Security and Applications*, 78, 103-115.
4. O'zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi "Kiberxavfsizlik sohasidagi faoliyatni yanada takomillashtirish chora-tadbirlari to'g'risida"gi PQ-168-sonli Qarori.
5. Karimov, A. A., & Axmedov, S. T. (2025). Sanoat obyektlarida axborot xavfsizligini monitoring qilish tizimlarini loyihalash. *O'zbekiston Texnika Jurnali*, 4(2), 45-52.
6. A Abdujabbor, IB Makhamatshoevich EUROPEAN JOURNAL OF MODERN MEDICINE AND PRACTICE 2 (4), 21-23.
7. METHODS OF USING MODERN ADVANCED AND VIRTUAL REAL TOOLS IN THE PROCESS OF TEACHING HIGHER EDUCATION
8. IB Makhamatshoyevich INNOVATION IN THE MODERN EDUCATION SYSTEM 3 (30), 332-339.