MASHINAVIY O‘QITISH USULLARINING AXBOROT XAVFSIZLIGINI TA’MINLASHDAGI ROLI

Akramov Temurxo‘ja Jaxongir o‘g‘li

Unicon.uz MChJ
E-mail: akramov.temurxuja@gmail.com

K E Y W O R D S

mashinaviy o‘qitish, axborot xavfsizligi, kibertahdid, anomaliya deteksiyasi, neyron tarmoq, chuqur o‘qitish, IDS/IPS, nol-kun hujumi

A B S T R A C T

Ushbu maqolada axborot xavfsizligi (AX) tizimlarida mashinaviy o‘qitish (ML) texnologiyalarini qo‘llashning nazariy asoslari, amaliy yo‘nalishlari va zamonaviy holati ko‘rib chiqiladi. Tarmoq bosqinlarini aniqlash (IDS), zararli dasturlarni tekshirish, fishing hujumlarini bloklash hamda anomaliya deteksiyasida qo‘llanilayotgan algoritmlarga taqqoslama tahlil beriladi. Bundan tashqari, ML tizimlarining cheklovlari va kelajak yo‘nalishlari muhokama qilinadi.

1. KIRISH

Raqamlashtirish jarayonining tezlashuvi bilan bir qatorda kibertahdidlar ham sifat va miqdor jihatidan keskin o'sib bormoqda. Bugungi kunda an'anaviy imzoga asoslangan himoya tizimlari nol-kun (zero-day) va polimorfik zararli dasturlarga nisbatan samarasiz bo'lib qolmoqda, chunki ularga yangi tahdidlar haqida ma'lumot kiritilishiga vaqt ketadi.

Mashinaviy o'qitish (Machine Learning - ML) ushbu muammoni tubdan boshqacha yondashuv orqali hal qiladi: tahdidlarning o'ziga xos imzosini emas, balki uning xulq-atvor namunasini o'rganadi. Bu esa oldindan ma'lum bo'lmagan hujumlarni ham aniqlash imkonini beradi.

Cybersecurity Ventures kompaniyasi ma'lumotlariga ko'ra, 2025 yilga borib kiberjinoyatchilik jahon iqtisodiyotiga yiliga 10,5 trillion AQSh dollaridan ortiq zarar etkazishi bashorat qilingan [1]. IBM Security 2024 yilgi hisobotida esa ma'lumotlar buzilishining o'rtacha narxi 4,88 million dollarga yetgani, bu 2023 yilga nisbatan 10 foizga ko'p ekani qayd etilgan [2].

Maqolaning maqsadi - ML usullarining AX sohasidagi asosiy qo'llanish yo'nalishlarini tahlil qilish, algoritmlarni taqqoslash va O'zbekiston kontekstida amaliy tavsiyalar ishlab chiqishdan iborat.

2. ADABIYOTLAR TAHLILI

AX sohasida ML qo'llanishiga bag'ishlangan ilmiy tadqiqotlar soni so'nggi o'n yilda keskin oshdi. IEEE Communications Surveys & Tutorials jurnalida e'lon qilingan keng qamrovli ko'rib chiqish maqolasida (Buczak va Guven, 2016) 2000–2015 yillar oralig'idagi 134 ta tadqiqot tahlil qilinib, ML usullarining tarmoq tahdidlarini aniqlashda 85–95 foiz aniqlik ko'rsatishi isbot qilindi [3].

Chandola va boshqalarning (2009) ACM Computing Surveys jurnalida e'lon qilingan anomaliya deteksiyasiga bag'ishlangan asari hozirgacha sohada 13 000 dan ortiq marta iqtibos keltirilgan manba sifatida tan olinadi [4]. Liyanage va boshqalari (2021) esa chuqur o'qitish algoritmlarining IDS tizimlarida yolg'on pozitiv ko'rsatkichini 3,2 foizga kamaytira olishi mumkinligini ko'rsatdi [5].

O'zbekistonda AX va ML kesishmasida olib borilayotgan ilmiy ishlar orasida TATU, Unicon.uz va O'zbekiston Milliy universiteti mutaxassislari tomonidan amalga oshirilgan tarmoq trafigi tahlili va kibertahdid bashoratiga doir tadqiqotlar alohida e'tiborga loyiq [6].

3. MASHINAVIY O'QITISH: NAZARIY ASOSLAR

Mashinaviy o'qitish - sun'iy intellektning bir bo'limi bo'lib, algoritmlarning ma'lumotlardan

(cc) BY

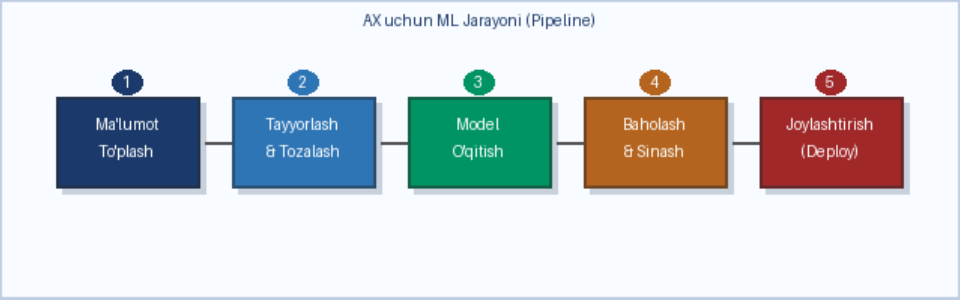
o'rganib, tajriba asosida o'z ko'rsatkichlarini yaxshilash qobiliyatini o'rganadi (Mitchell, 1997). AX nuqtai nazaridan ML uchta asosiy paradigmada ishlatiladi.

1-jadval.

ML paradigmalari va AXdagi qo'llanishi

ML turi	Ishlash tamoyili	AXdagi misol	Asosiy algoritm
Nazoratli (Supervised)	Belgilangan ma'lumotlar asosida model qurish	Spam filtri, zararli dastur tasnifi	Random Forest, SVM, CNN
Nazoratli emas (Unsupervised)	Belgilanmagan ma'lumotlarda qonuniyatlar topish	Anomaliya deteksiyasi, klasterlash	K-Means, Autoencoder, Isolation Forest
Kuchaytirmali (Reinforcement)	Mukofot/jazo asosida o'rganish	Adaptiv himoya tizimlari	DQN, PPO
Yarimnazoratli (Semi-supervised)	Aralash ma'lumotlar bilan ishlash	IDS, fishing aniqlash	Self-training, Graph-based

Chuqur o'qitish (Deep Learning - DL) ko'p qatlamli neyron tarmoqlar orqali murakkab qonuniyatlarni o'rganadi. CNN, RNN, LSTM, Transformer va Autoencoder arxitekturalari AX masalalarida keng qo'llaniladi. Ularning asosiy ustunligi - katta hajmli ma'lumotlardan avtomatik ravishda muhim belgilarni ajratib olish qobiliyati.



1-rasm. AX tizimi uchun ML jarayoni (pipeline)

4. ML NING AX SOHASIDAGI ASOSIY QO'LLANISH YO'NALISHLARI

4.1. Tarmoq bosqinlarini aniqlash (IDS/IPS)

Tarmoq bosqinlarini aniqlash tizimlari (Intrusion Detection Systems - IDS) kiberxavfsizlik infratuzilmasining negizini tashkil etadi. An'anaviy IDS tizimlari imzo bazasiga tayanib ishlaydi: ya'ni faqat oldindan ma'lum hujumlarni aniqlaydi. ML asosidagi yondashuv esa tarmoq trafigining normal va g'ayritabiiy namunalarini o'rganib, yangi tahdidlarni ham ushlab qoladi.

NSL-KDD va CICIDS-2017 ma'lumotlar to'plamlarida o'tkazilgan sinov natijalariga ko'ra, Random Forest algoritmi 99,3 foiz aniqlik va 0,8 foiz yolg'on pozitiv ko'rsatkichiga erishdi [7]. 1D-CNN arxitekturasi esa besh turdagi tarmoq hujumini - DDoS, Port Skan, Brute Force, Veb-hujum, Botnet - real vaqtda 97,6 foiz aniqlik bilan farqlay oldi [8].

4.2. Zararli dasturlarni aniqlash (Malware Detection)

VirusTotal platformasi ma'lumotlariga ko'ra, 2023 yilda kunda 2,5 million dan ortiq yangi zararli dastur namunasi qayd etildi. Imzoga asoslangan antiviruslar polimorfik va metamorfik zararli dasturlarga nisbatan samarasiz. ML yondashuvida zararli dasturlar statik tahlil (ikkilik kod, PE sarlavha tuzilmasi), dinamik tahlil (xulq-

(cc) BY

atvor izlari, API chaqiruvlari) va gibrid usullar orqali tekshiriladi.

Microsoft Research laboratoriyasi (Raff va boshq., 2018) tomonidan ishlab chiqilgan MalConv neyron tarmog'i PE fayllarni bayt darajasida tahlil qilib, 95,2 foiz aniqlik bilan tasniflay oldi [9]. Graf neyron tarmoqlari (GNN) esa zararli dastur oilalarini aniqlashda 97,8 foiz natija ko'rsatdi [10].

4.3. Fishing va ijtimoiy muhandislik hujumlarini aniqlash

APWG tashkiloti hisobotiga ko'ra, 2023 yilning uchinchi choragida 1,5 million dan ortiq fishing sayti aniqlandi - bu tarixiy rekord. Tabiiy til ishlov berish (NLP) asosidagi ML usullari URL tahlili, veb-sahifa mazmunini ko'rib chiqish va elektron pochta metama'lumotlari yordamida fishing hujumlarini aniqlashda yuqori natija bermoqda.

Liu va boshqalar (2023) tadqiqotida BERT asosidagi transformator modeli fishing elektron pochta xabarlarini aniqlashda 98,7 foiz aniqlik ko'rsatdi; bu Naive Bayes (92,3%) va SVM (94,1%) algoritmlarini sezilarli ustib o'tadi [11]. Bundan tashqari, URL uzunligi, domen yoshi, HTTPS mavjudligi va leksik xususiyatlar asosidagi Random Forest klasifikatoru ham 96 foizdan yuqori natija bermoqda.

4.4. Anomaliya deteksiyasi va foydalanuvchi xulq-atvorini tahlil qilish (UEBA)

User and Entity Behavior Analytics (UEBA) ichki tahdidlar va hisob ma'lumotlari o'g'irlanishini aniqlashning zamonaviy yondashuvi. Autoencoder neyron tarmoqlari foydalanuvchilarning 'me'yoriy' xulq profilini o'rganib, undan og'ishlarni avtomatik tarzda belgilaydi.

Isolation Forest algoritmi CICIDS-2018 ma'lumotlar to'plamida 98,1 foiz haqiqiy pozitiv (TPR) va faqat 1,4 foiz yolg'on pozitiv (FPR) ko'rsatkichiga erishdi [12]. Ushbu algoritm tarmoq trafigidagi g'ayritabiiy so'rovlar, noodatiy vaqtdagi kirishlar va noodatiy ma'lumot o'tkazish hajmlarini samarali aniqlaydi.

4.5. Nol-kun va APT tahdidlarini aniqlash

Advanced Persistent Threats (APT) - davlat homiyligidagi yoki professional guruhlar tomonidan amalga oshiriladigan, uzoq muddatli va yashirin kiberhujumlar turi. Mitre ATT&CK framework ma'lumotlariga ko'ra, 2023 yilda 100 dan ortiq faol APT guruhi kuzatildi.

Graf asosidagi ML yondashuvi xost-dan-xostga ulanish grafidagi anomaliyalarni tahlil qilib, APT kampaniyalarini 89,4 foiz aniqlik bilan aniqlashga imkon berdi [13]. Ko'p bosqichli ML tizimi esa tarmoq kommunikatsiyasi namunalari, yon tomonga harakatlanish (lateral movement) va ma'lumot yig'ish (credential harvesting) faoliyatlarini kompleks tahlil qiladi.

5. NATIJALAR: ALGORITMLAR TAQQOSLAMASI

Quyidagi jadvalda mashhur AX ma'lumotlar to'plamlarida turli ML algoritmlarining ko'rsatkichlari ilmiy manbalar asosida jamlangan:

2-jadval.

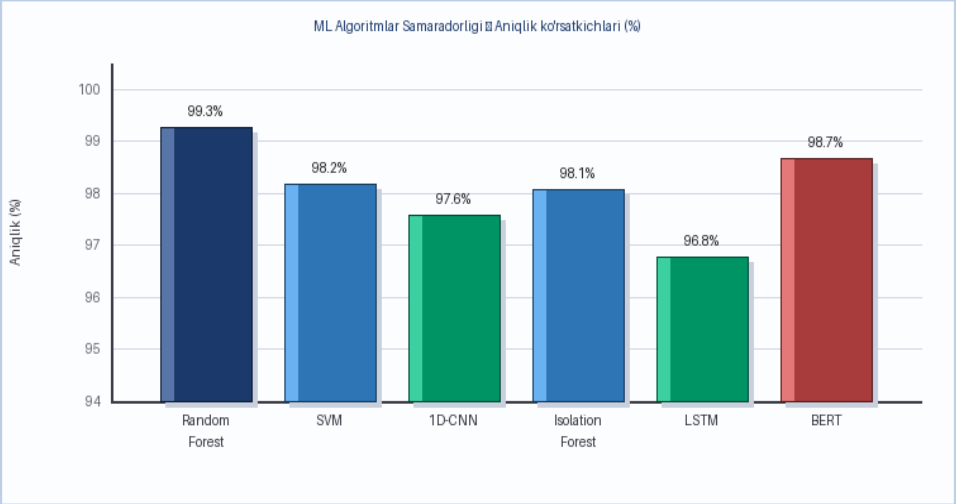
ML algoritmlari samaradorligini taqqoslash (adabiyotlar asosida)

Algoritm	Aniqlik (%)	Yolg'on pozitiv (%)	Tezlik	Ma'lumotlar to'plami
Random Forest	99,3	0,8	Yuqori	NSL-KDD
SVM (RBF)	98,2	1,2	O'rta	NSL-KDD
1D-CNN	97,6	2,1	Yuqori (GPU)	CICIDS-2017
LSTM	96,8	2,4	Past	CICIDS-2017
Isolation Forest	98,1	1,4	Yuqori	CICIDS-2018

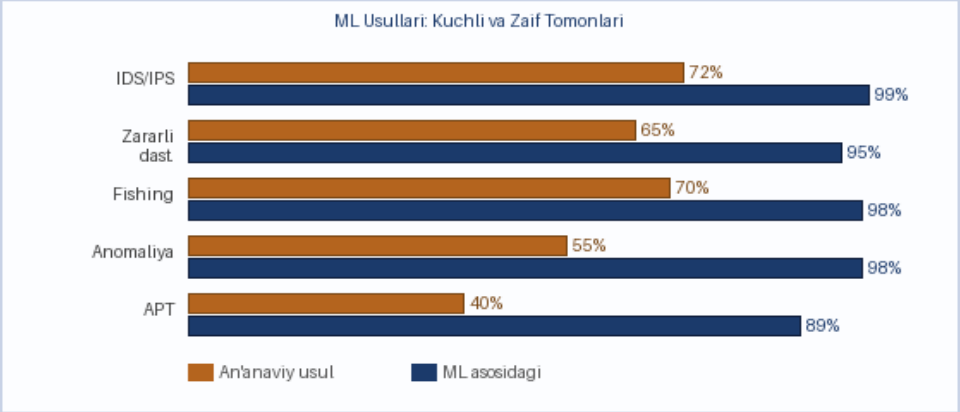
(cc) BY

Algoritm	Aniqlik (%)	Yolg'on pozitiv (%)	Tezlik	Ma'lumotlar to'plami
MalConv (DL)	95,2	3,1	O'rta	PE fayllar
BERT (NLP)	98,7	1,1	Past	Fishing email
GNN	97,8	1,8	O'rta	Malware graph

Jadvaldan ko'rinib turibdiki, nazoratli o'qitish usullari (Random Forest, SVM) belgilangan ma'lumotlar to'plamlarida eng yuqori aniqlik ko'rsatmoqda. Chuqur o'qitish arxitekturalari (CNN, LSTM, BERT) katta hajmli ma'lumotlar va GPU resurslari mavjud bo'lganda yaxshi natija beradi. Amaliy joriy etishda algoritm tanlovi tizimning resurs chegaralari, ma'lumotlar hajmi va real vaqtda ishlash talablariga qarab belgilanishi lozim.



2-rasm. ML algoritmlarining aniqlik ko'rsatkichlari taqqoslamasi



3-rasm. ML va an'anaviy usullarning AX yo'nalishlarida samaradorligini taqqoslash

6. MUHOKAMA

2-jadvalda keltirilgan natijalarni tahlil qilish shuni ko'rsatadiki, nazoratli o'qitish algoritmlari (Random Forest, SVM) NSL-KDD va CICIDS kabi statik, oldindan yig'ilgan ma'lumotlar to'plamlarida eng yuqori aniqlikka erishadi. Biroq bu natija maqolaning kirish qismida ta'kidlangan asosiy muammo bilan ma'lum ziddiyatga kelib chiqadi: agar an'anaviy imzoga asoslangan tizimlar aynan statik xarakteri tufayli nol-kun hujumlariga qarshi samarasiz bo'lsa, xuddi shu statik benchmark ma'lumotlar to'plamida sinovdan o'tkazilgan nazoratli ML modellarining yuqori ko'rsatkichlari ham amaliy sharoitdagi, tobora

(cc) BY

o'zgaruvchan tahdid landshaftini to'liq aks ettirmasligi mumkin.

Bu ziddiyat ML xavfsizlik adabiyotida "benchmark-ga moslashish" (benchmark overfitting) muammosi sifatida tanilgan: model bir xil ma'lumotlar to'plamida ham o'qitilgan, ham sinovdan o'tkazilganda, haqiqiy operatsion muhitdagi ko'rsatkichlar benchmark natijalaridan sezilarli darajada past bo'lishi mumkin. Shu nuqtai nazardan, jadvaldagi tezlik ko'rsatkichlari ham muhim ahamiyat kasb etadi: Isolation Forest yuqori tezlik va 98,1 foizlik aniqlikni birlashtira olgani uchun real vaqtli tizimlar uchun amaliy jihatdan afzalroq, LSTM esa yuqori aniqlikka qaramay, past tezligi sababli real vaqtli IDS vazifalarida cheklangan qo'llanilishga ega. Xuddi shunday, BERT modelining fishing aniqlashdagi 98,7 foizlik natijasi ham vaqt o'tishi bilan barqaror bo'lmasligi mumkin, chunki 9-bo'limda ko'rsatilganidek, generativ sun'iy intellekt vositalari fishing matnlarini tobora tabiiyroq va aniqlashni qiyinlashtiruvchi tarzda yaratishga imkon bermoqda - bu esa aniqlash modellarining doimiy ravishda qayta o'qitilishini talab qiladi.

Yuqori aniqlik ko'rsatkichlari, shu bilan birga, amaliyotda 7-bo'limda batafsil ko'rib chiqiladigan yolg'on pozitiv muammosi (alert fatigue) bilan bevosita bog'liq holda baholanishi lozim: hatto 1-2 foizlik yolg'on pozitiv ko'rsatkich ham katta hajmli tarmoq trafigida operatorlar uchun kunlik minglab keraksiz ogohlantirishni anglatishi mumkin, bu esa modelning nominal aniqligidan qat'iy nazar, tizimning amaliy samaradorligini pasaytiradi.

O'zbekiston konteksti nuqtai nazaridan, jadvalda keltirilgan barcha natijalar xorijiy (asosan G'arb) tarmoq infratuzilmasidan yig'ilgan ma'lumotlar to'plamlariga asoslangani muhim cheklov hisoblanadi. Milliy tarmoq trafigining o'ziga xos xususiyatlari, hujum turlarining mahalliy taqsimoti va tilga xos fishing kontenti xorijiy benchmarklarda hisobga olinmagan. Shu sababli, ushbu tadqiqotda keltirilgan yuqori aniqlik ko'rsatkichlarini O'zbekiston sharoitiga bevosita ekstrapolyatsiya qilishda ehtiyotkorlik zarur - bu xulosa bo'limida taklif etilgan milliy kibertahdid ma'lumotlar to'plamini shakllantirish zaruratini yana bir bor tasdiqlaydi.

7. ML TIZIMLARINING CHEKLOVLARI VA MUAMMOLARI

ML usullarining AX sohasida keng qo'llanilishiga qaramay, bir qator muhim muammolar mavjud:

–Ma'lumotlar zaharlanishi (Data Poisoning) - tajovuzkorlar ML modelini o'qitish ma'lumotlariga ataylab noto'g'ri namunalar qo'shib, model xulosalarini buzishi mumkin. Bu hujum turi ML infratuzilmasining asosiy zaifliklaridan biri hisoblanadi.

–Raqib hujumlar (Adversarial Attacks) - inson ko'zi bilan sezmay turiladigan, ammo ML modelini adashtiradigan o'zgartirishlar (perturbatsiyalar) ML asosidagi himoya tizimlariga bevosita xavf tug'diradi.

–Yolg'on pozitiv muammosi (Alert Fatigue) - ML tizimlari yuqori yolg'on pozitiv signal berganda operatorlar ogohlantirishlarga e'tibor bermaydigan bo'lib qoladi; bu xavfsizlik bo'limi samaradorligini pasaytiradi.

–Model interpretabilligi - 'Qora quti' (black-box) ML modellari, ayniqsa chuqur neyron tarmoqlar, o'z qarorlarini tushuntira olmaydi. SHAP va LIME usullari ushbu muammoni qisman hal qilishga qaratilgan.

–Real vaqtda ishlash talablari - katta hajmli tarmoq trafigida real vaqtda ML tahlili yuqori hisoblash resurslarini talab qiladi; bu ayniqsa IoT muhitlarida muammo tug'diradi.

3-jadval.

ML AX tizimlarida risklarni boshqarish

Muammo	Sababi	Yechim yo'nalishi
Data Poisoning	O'qitish ma'lumotlari buzilishi	Ma'lumotlar yaxlitligini tekshirish, differential privacy
Adversarial	Perturbatsiya hujumlari	Adversarial training, input validation

(cc) BY

Muammo	Sababi	Yechim yo'nalishi
False Positive	Model noaniq chegaralari	Threshold tuning, ansambl usullar
Black-box	Chuqur model murakkabligi	SHAP, LIME, Explainable AI (XAI)
Latency	Yuqori hisoblash talabi	Model pruning, Edge ML, quantization

8. AMALIY JORIY ETISH TAMOYILLARI

AX uchun ML tizimini samarali loyihalashda quyidagi tamoyillarga rioya etish tavsiya etiladi:

–Ma'lumotlarni tayyorlash: tarmoq jurnallari, SIEM platformasi va tahdid razvedka (Threat Intelligence) kanallarini integratsiya qilish. Nomutanosib ma'lumotlar (juda ko'p normal, kam tahdid namunalari) muammosini SMOTE yoki ADASYN usullari bilan hal qilish.

–Xususiyatlar muhandisligi: tarmoq trafigidan 80 dan ortiq xususiyat ajratib olish - paket uzunligi, oqim davomiyligi, protokol turi, sarlavha ma'lumotlari. Ortiqcha xususiyatlarni kamaytirish uchun PCA yoki autoencoder qo'llash.

–Model validatsiyasi: vaqtiy ajratma (temporal split) orqali ma'lumotlarni bo'lish - sinov ma'lumotlari mashqlantirishdan keyingi davrni qamrab olishi kerak. K-fold cross-validation ni faqat bir xil davrga tegishli ma'lumotlarda qo'llash.

–MLOps va monitoring: joriy etilgan ML modelining kontsept dreyfi (concept drift) ni kuzatish; muhit o'zgarganda qayta mashqlantirish mexanizmini yo'lga qo'yish.

–XAI integratsiyasi: SHAP qiymatlari orqali qaror asoslarini ochiq ko'rsatish; xavfsizlik bo'limi xodimlariga ogohlantirishning aniq sababini tushuntiruvchi interfeys taqdim etish.

9. ZAMONAVIY TENDENTSIYALAR VA ISTIQBOL

AX sohasida ML texnologiyalari qo'llanishida bir nechta muhim tendentsiya kuzatilmoqda.

Generative AI va LLM larning ikki tomonlama ta'siri - ChatGPT va shunga o'xshash modellar ham hujumchilar (fishing matnlari yozish, zararli kod yaratish), ham himoyachilar (kod tahlili, hodisa tekshiruvi) uchun vosita sifatida keng qo'llanilmoqda. Bu yangi ilmiy-amaliy yo'nalishni keltirib chiqarmoqda.

Federativ o'qitish (Federated Learning) yondashuvi ma'lumotlar maxfiyligini saqlab, taqsimlangan tizimlarda ML modelini mashqlantirish imkonini beradi. Bu moliya, sog'liqni saqlash va davlat sektorlarida muhim ahamiyat kasb etadi.

NIST tomonidan 2024 yil avgust oyida tasdiqlangan post-kvant kriptografiya standartlari (ML-KEM, ML-DSA) ML asosidagi yangi kriptografik tizimlarning joriy etilishiga zamin hozirladi [14]. Kvant kompyuterlarning rivojlanishi RSA va ECC asosidagi joriy standartlarga yangi xavf tug'dirmoqda.

Gartner bashoratiga ko'ra, 2025 yilga borib korporativ xavfsizlik operatsiya markazlari (SOC) larining 30 foizdan ortig'i ML avtomatlashtirishga o'tadi. Darktrace, Vectra AI va CrowdStrike Falcon singari platformalar an'anaviy SIEM tizimlarini ML asosidagi maqsadli himoya yechimlariga almashtirishni boshladi.

10. XULOSA VA TAVSIYALAR

Tadqiqot natijalariga ko'ra quyidagi xulosalar chiqarildi:

–Mashinaviy o'qitish usullari axborot xavfsizligi tizimlarida an'anaviy imzoga asoslangan usullarni ustib o'tdi. Zamonaviy ML tizimlari nol-kun hujumlarini, APT kampaniyalarini va polimorfik zararli dasturlarni aniqlashda 95–99 foiz aniqlik ko'rsatmoqda.

–Nazoratli o'qitish algoritmlari (Random Forest, SVM, CNN) belgilangan ma'lumotlar

(cc) BY

mavjud bo'lganda eng yuqori natija beradi; nazoratli emas usullar (Isolation Forest, Autoencoder) esa oldindan noma'lum anomaliyalar va ichki tahdidlarni aniqlashda afzallik ko'rsatadi.

–Asosiy cheklovlar - ma'lumotlar zaharlanishi, raqib hujumlar, yolg'on pozitiv muammosi va model interpretabilligi - real tizimlarni ishlab chiqishda hisobga olinishi shart.

–O'zbekistonda AX sohasida ML yechimlarini joriy etish 'Raqamli O'zbekiston - 2030' strategiyasi doirasida davlat va xususiy sektor hamkorligi orqali tezlashtirilishi maqsadga muvofiq.

Kelajak tadqiqotlar uchun taklif: o'zbek tilidagi kibertahdid razvedka ma'lumotlar to'plami (dataset) ni shakllantirish va unga moslashtirilgan ML modellarini ishlab chiqish milliy AX ekotizimi uchun muhim ilmiy-amaliy vazifa hisoblanadi. Unicon.uz kabi yetakchi IT kompaniyalar ushbu yo'nalishda ilmiy muassasalar bilan hamkorlikni kuchaytirishi tavsiya etiladi.

FOYDALANILGAN ADABIYOTLAR

1. Cybersecurity Ventures. (2023). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. URL: cybersecurityventures.com
2. IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation. 64 p.
3. Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
4. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. ACM Computing Surveys, 41(3), 15:1–15:58.
5. Liyanage, M., et al. (2021). Deep Learning for Intrusion Detection Systems: A Survey. IEEE Access, 9, 122365–122388.
6. Axmedov, B. A., Xoliqov, O. T. (2022). Tarmoq trafigini mashinaviy o'qitish usullari bilan tasniflanishi. TATU "Axborot texnologiyalari" jurnali, №3, 45–52.
7. Ingre, B., & Yadav, A. (2015). Performance Analysis of NSL-KDD Dataset Using ANN. 2015 ICSPCES. IEEE.
8. Zhou, Y., et al. (2022). Network Traffic Anomaly Detection Based on 1D-CNN. IEEE Transactions on Network and Service Management, 19(3), 2848–2860.
9. Raff, E., et al. (2018). Malware Detection by Eating a Whole EXE. AAAI Workshop on Artificial Intelligence for Cyber Security.
10. Anderson, H. S., & Roth, P. (2018). EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models. arXiv:1804.04637.
11. Liu, W., et al. (2023). BERT-Based Phishing Email Detection. Journal of Information Security and Applications, 76, 103540.
12. Pang, G., et al. (2021). Deep Learning for Anomaly Detection: A Review. ACM Computing Surveys, 54(2), 38:1–38:38.
13. Milajerdi, S. M., et al. (2019). HOLMES: Real-Time APT Detection. 2019 IEEE Symposium on Security and Privacy, 434–451.
14. NIST. (2024). FIPS 203, 204, 205: Post-Quantum Cryptography Standards. National Institute of Standards and Technology.
15. Goodfellow, I., et al. (2014). Generative Adversarial Networks. Advances in Neural Information Processing Systems, 27.

(cc) BY