MUHANDISLIK & IQTISODIYOT

№3

ijtimoiy-iqtisodiy, innovatsion texnik, fan va ta'limga oid ilmiy-amaliy jurnal

2026 MART

Milliy nashrlar

OAK: https://oak.uz/pages/4802

05.00.00 - Texnika fanlari
08.00.00 - Iqtisodiyot fanlar

ISSN: 3060-463X

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Elektron nashr, 2026-yil, mart

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

05.01.00 – Axborot texnologiyalari, boshqaruv va kompyuter grafikasi
05.01.01 – Muhandislik geometriyasi va kompyuter grafikasi. Audio va video texnologiyalari
05.01.02 – Tizimli tahlil, boshqaruv va axborotni qayta ishlash
05.01.03 – Informatikaning nazariy asoslari
05.01.04 – Hisoblash mashinalari, majmualari va kompyuter tarmoqlarining matematik va dasturiy ta'minoti
05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi
05.01.06 – Hisoblash texnikasi va boshqaruv tizimlarining elementlari va qurilmalari
05.01.07 – Matematik modellashtirish
05.01.11 – Raqamli texnologiyalar va sun'iy intellekt
05.02.00 – Mashinasozlik va mashinashunoslik
05.02.08 – Yer usti majmualari va uchish apparatlari
05.03.02 – Metrologiya va metrologiya ta'minoti
05.04.01 – Telekommunikasiya va kompyuter tizimlari, telekommunikasiya tarmoqlari va qurilmalari. Axborotlarni taqsimlash
05.05.03 – Yorug'lik texnikasi. Maxsus yoritish texnologiyasi
05.05.05 – Issiqlik texnikasining nazariy asoslari
05.05.06 – Qayta tiklanadigan energiya turlari asosidagi energiya qurilmalari
05.06.01 – To'qimachilik va yengil sanoat ishlab chiqarishlari materialshunosligi
05.08.03 – Temir yo'l transportini ishlatish
05.09.01 – Qurilish konstruksiyalari, bino va inshootlar
05.09.04 – Suv ta'minoti. Kanalizatsiya. Suv havzalarini muhofazalovchi qurilish tizimlari
10.00.06 – Qiyosiy adabiyotshunoslik, chog'ishtirma tilshunoslik va tarjimashunoslik
10.00.04 – Yevropa, Amerika va Avstraliya xalqlari tili va adabiyoti
08.00.01 – Iqtisodiyot nazariyasi
08.00.02 – Makroiqtisodiyot
08.00.03 – Sanoat iqtisodiyoti
08.00.04 – Qishloq xo'jaligi iqtisodiyoti
08.00.05 – Xizmat ko'rsatish tarmoqlari iqtisodiyoti
08.00.06 – Ekonometrika va statistika
08.00.07 – Moliya, pul muomalasi va kredit
08.00.08 – Buxgalteriya hisobi, iqtisodiy tahlil va audit
08.00.09 – Jahon iqtisodiyoti
08.00.10 – Demografiya. Mehnat iqtisodiyoti
08.00.11 – Marketing
08.00.12 – Mintaqaviy iqtisodiyot
08.00.13 – Menejment
08.00.14 – Iqtisodiyotda axborot tizimlari va texnologiyalari
08.00.15 – Tadbirkorlik va kichik biznes iqtisodiyoti
08.00.16 – Raqamli iqtisodiyot va xalqaro raqamli integratsiya
08.00.17 – Turizm va mehmonxona faoliyati

Ma'lumot uchun, OAK Rayosatining 2024-yil 28-avgustdagi 360/5-son qarori bilan "Dissertatsiyalar asosiy ilmiy natijalarini chop etishga tavsiya etilgan milliy ilmiy nashrlar ro'yxati"ga texnika va iqtisodiyot fanlari bo'yicha "Muhandislik va iqtisodiyot" jurnali ro'yxatga kiritilgan.

Muassis: "Tadbirkor va ishbilarmon" MChJ

Hamkorlarimiz:

1. Toshkent shahridagi G.V.Plexanov nomidagi Rossiya iqtisodiyot universiteti
2. Toshkent davlat iqtisodiyot universiteti
3. Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti" milliy tadqiqot universiteti
4. Islom Karimov nomidagi Toshkent davlat texnika universiteti
5. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
6. Toshkent davlat transport universiteti
7. Toshkent arxitektura-qurilish universiteti
8. Toshkent kimyo-texnologiya universiteti
9. Jizzax politexnika instituti

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

MUNDARIJA

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

EXPLAINABLE AI YORDAMIDA SOC UCHUN TUSHUNTIRILADIGAN KIBERXAVF ANIQLASH TIZIMINI ISHLAB CHIQISH

N.N. Jo‘rayev
O‘zbekiston Respublikasi Harbiy xavfsizlik va mudofaa universiteti,
Toshkent harbiy okrugi fakulteti, Istiqbolli harbiy texnologiyalar kafedrasi boshlig‘i podpolkovnik

A.Sh. Juraboyev
O‘zbekiston Respublikasi Harbiy xavfsizlik va mudofaa universiteti,
Toshkent harbiy okrugi fakulteti, katta o‘qituvchisi podpolkovnik

Annotatsiya. So‘nggi yillarda kiberxavfsizlik sohasida sun’iy intellekt va mashinaviy o‘rganish texnologiyalaridan foydalanish sezilarli darajada kengayib bormoqda. Biroq ko‘plab algoritmlar “qora quti” tamoyiliga asoslanganligi sababli, ularning qaror qabul qilish jarayonini izohlash murakkab bo‘lishi mumkin. Bu holat xavfsizlik operatsiyalari markazlari (Security Operations Center – SOC) faoliyatida muhim ahamiyat kasb etadi, chunki xavfsizlik mutaxassislari aniqlangan tahdidlarning sabablarini ham tushunishi zarur. Mazkur tadqiqotda Explainable Artificial Intelligence (XAI) yondashuvi asosida tushuntiriladigan kiberxavf aniqlash tizimi modeli taklif etiladi. Tizim mashinaviy o‘rganish algoritmlaridan foydalangan holda tarmoq trafigini tahlil qiladi hamda aniqlangan tahdidlar uchun SHAP yoki LIME kabi tushuntirish mexanizmlarini qo‘llaydi. Natijada SOC mutaxassislari hujumlarning kelib chiqish sabablari va ta’sir etuvchi omillarni tezkor aniqlash imkoniyatiga ega bo‘ladi. Tadqiqot natijalari Explainable AI texnologiyalari kiberxavfsizlik tizimlarining ishonchliligi, shaffofligi va samaradorligini oshirishda muhim rol o‘ynashini ko‘rsatadi.

Kalit so‘zlar: kiberxavfsizlik, Explainable AI, XAI, SOC, kiberhujumlarni aniqlash, mashinaviy o‘rganish, tarmoq trafigi tahlili, SHAP, LIME.

Abstract. In recent years, the application of artificial intelligence and machine learning technologies in the field of cybersecurity has significantly expanded. However, many algorithms operate based on the “black-box” principle, which makes it difficult to interpret their decision-making processes. This issue is particularly important for Security Operations Centers (SOC), where security specialists need to understand the underlying causes of detected threats. This study proposes an explainable cyber-threat detection system model based on the Explainable Artificial Intelligence (XAI) approach. The system analyzes network traffic using machine learning algorithms and applies explanation mechanisms such as SHAP and LIME to interpret detected threats. As a result, SOC analysts can quickly identify the key factors and causes of cyberattacks. The findings demonstrate that Explainable AI technologies play an important role in improving the reliability, transparency, and effectiveness of cybersecurity systems.

Keywords: cybersecurity, Explainable AI, XAI, SOC, cyber-attack detection, machine learning, network traffic analysis, SHAP, LIME.

Аннотация. В последние годы применение технологий искусственного интеллекта и машинного обучения в сфере кибербезопасности значительно расширяется. Однако многие алгоритмы функционируют по принципу «чёрного ящика», что затрудняет интерпретацию процесса принятия решений. Данный аспект имеет особое значение для центров операций безопасности (Security Operations Center – SOC), поскольку специалистам по безопасности важно понимать причины выявленных угроз. В рамках данного исследования предлагается модель системы обнаружения киберугроз на основе подхода Explainable Artificial Intelligence (XAI). Система анализирует сетевой трафик с использованием алгоритмов машинного обучения и применяет механизмы объяснения, такие как SHAP и LIME, для интерпретации выявленных угроз. В результате специалисты SOC получают возможность оперативно определять ключевые факторы и причины кибератак. Результаты исследования показывают, что технологии Explainable AI играют важную роль в повышении надёжности, прозрачности и эффективности систем кибербезопасности.

Ключевые слова: кибербезопасность, Explainable AI, XAI, SOC, обнаружение кибератак, машинное обучение, анализ сетевого трафика, SHAP, LIME.

KIRISH

Zamonaviy jamiyatda raqamli texnologiyalar va global axborot tarmoqlarining jadal rivojlanishi natijasida kiberxavfsizlik masalalari tobora muhim ahamiyat kasb etmoqda. Internet tarmog‘i, bulutli xizmatlar, IoT qurilmalari hamda korporativ axborot tizimlarining keng qo‘llanilishi kiberhujumlar sonining ortishiga olib kelmoqda. Bugungi kunda kiberjinoyatchilar tomonidan amalga oshirilayotgan hujumlar tobora murakkablashib, avtomatlashtirilgan hamda yashirin shaklga ega bo‘lib bormoqda. Shu sababli tarmoq infratuzilmasini himoya qilish uchun zamonaviy, aqlli va moslashuvchan himoya tizimlarini yaratish dolzarb ilmiy-amaliy masalalardan biri hisoblanadi.

Kiberxavfsizlikni ta’minlash jarayonida muhim rol o‘ynaydigan tizimlardan biri bu Security Operations Center (SOC) hisoblanadi. SOC – bu tashkilotning axborot tizimlari va tarmoq infratuzilmasini real vaqt rejimida monitoring qilish, kiberhujumlarni aniqlash hamda ularga tezkor javob qaytarish bilan shug‘ullanuvchi markazdir. SOC mutaxassislari turli xil xavfsizlik vositalari, jumladan intrusion detection system (IDS), security information and event management (SIEM) hamda tarmoq monitoring platformalari orqali katta hajmdagi ma’lumotlarni tahlil qiladi. Biroq zamonaviy tarmoqlarda hosil bo‘ladigan ma’lumotlar hajmining katta bo‘lishi xavfsizlik tahlilchilariga qo‘shimcha yuklama keltirib chiqaradi va an’anaviy usullar yordamida barcha tahdidlarni tezkor aniqlash jarayonini murakkablashtiradi.

So‘nggi yillarda kiberxavfsizlik sohasida sun’iy intellekt va mashinaviy o‘rganish texnologiyalaridan foydalanish keng tarqalmoqda. Ushbu yondashuvlar katta hajmdagi tarmoq trafigini avtomatik ravishda tahlil qilish, anomaliyalarni aniqlash hamda potensial kiberhujumlarni prognoz qilish imkonini beradi. Biroq ko‘plab mashinaviy o‘rganish algoritmlari “qora quti” (black-box) tamoyiliga asoslangan bo‘lib, ular tomonidan qabul qilingan qarorlarning sabablarini tushuntirish murakkab bo‘lishi mumkin. Bu holat ayniqsa SOC muhitida muhim ahamiyat kasb etadi, chunki xavfsizlik mutaxassislari nafaqat tahdid aniqlanganligini bilishi, balki ushbu qarorning asosiy omillarini ham tushunishi zarur.

Mazkur muammoni samarali hal etish maqsadida so‘nggi yillarda Explainable Artificial Intelligence (EAI), ya’ni tushuntiriladigan sun’iy intellekt konsepsiyasi jadal rivojlanmoqda. EAI yondashuvlari mashinaviy o‘rganish modellari tomonidan qabul qilingan qarorlarni izohlash, muhim xususiyatlarni aniqlash hamda model ishlash jarayonining shaffofligini ta’minlashga xizmat qiladi. Xususan, SHAP (Shapley Additive Explanations) va LIME (Local Interpretable Model-agnostic Explanations) kabi metodlar model qarorlariga ta’sir etuvchi xususiyatlarni aniqlash orqali kiberxavfsizlik tizimlarida tushunarli va ishonchli tahlil imkoniyatini yaratadi.

Shu nuqtai nazardan, SOC muhitida qo‘llanilishi mumkin bo‘lgan tushuntiriladigan kiberxavf aniqlash tizimlarini ishlab chiqish muhim ilmiy va amaliy vazifa hisoblanadi. Explainable AI yondashuvlari nafaqat tahdidlarni aniqlash aniqligini oshiradi, balki xavfsizlik mutaxassislariga tahdid sabablarini tez va aniq tushunish imkonini ham beradi. Natijada xavfsizlik hodisalariga javob berish jarayoni tezlashadi va kiberxavfsizlik tizimining umumiy samaradorligi ortadi.

Mazkur tadqiqotning maqsadi – Explainable AI asosida SOC uchun tushuntiriladigan kiberxavf aniqlash tizimi modelini ishlab chiqish hamda uning samaradorligini tahlil qilishdan iborat. Tadqiqot doirasida mashinaviy o‘rganish algoritmlari yordamida tarmoq trafigi tahlil qilinadi hamda SHAP yoki LIME kabi tushuntirish metodlari orqali model qarorlarining interpretatsiya qilinadi. Ushbu yondashuv kiberxavfsizlik monitoring tizimlarining shaffofligi, ishonchliligi va samaradorligini oshirishga xizmat qiladi.

MAVZUGA OID ADABIYOTLAR SHARHI

Kiberxavfsizlik sohasida tarmoq tahdidlarini aniqlash va ularga qarshi kurashish maqsadida turli texnologiyalar hamda metodlar ishlab chiqilgan. Dastlabki intrusion detection system (IDS) tizimlari asosan signatura (signature-based) yoki qoidaga asoslangan yondashuvlardan foydalangan. Bunday tizimlar ma’lum hujum naqshlarini aniqlashda samarali bo‘lsa-da, yangi yoki ilgari noma’lum tahdidlarni aniqlash imkoniyatlari cheklangan edi. Shu sababli so‘nggi yillarda kiberxavfsizlik sohasida mashinaviy o‘rganish (Machine Learning) va chuqur o‘rganish (Deep Learning) texnologiyalaridan foydalanish jadal rivojlanmoqda.

Ko‘plab ilmiy tadqiqotlarda mashinaviy o‘rganish algoritmlarining tarmoq hujumlarini aniqlash samaradorligi o‘rganilgan. Masalan, Sommer va Paxson tarmoq xavfsizligi tizimlarida mashinaviy o‘rganish usullaridan foydalanish imkoniyatlarini tahlil qilib, bunday yondashuvlar katta hajmdagi tarmoq trafigini avtomatik tarzda tahlil qilishda samarali ekanligini ko‘rsatgan. Shuningdek, Chen va Guestrin tomonidan taklif etilgan XGBoost algoritmi ham kiberxavfsizlik sohasida keng qo‘llanilib, yuqori aniqlik va samaradorlikka ega bo‘lgan gradient boosting asosidagi tasniflash modeli sifatida e’tirof etiladi.

Tarmoq hujumlarini aniqlash jarayonida chuqur o‘rganish metodlari ham muhim o‘rin egallaydi. Hinton va Salakhutdinov tomonidan ishlab chiqilgan Autoencoder arxitekturasi ma’lumotlarni siqish va rekonstruksiya qilish asosida anomaliyalarni aniqlash imkonini beradi. Ushbu yondashuv ayniqsa nazoratsiz o‘rganish

(unsupervised learning) muhitida samarali bo‘lib, normal trafik modelini o‘rganish va undan og‘ishlarni aniqlash imkonini yaratadi. Shu bilan birga, zamonaviy tadqiqotlarda CIC-IDS2017 va UNSW-NB15 kabi datasetlar asosida mashinaviy o‘rganish modellari samaradorligi keng o‘rganilmoqda.

Biroq mashinaviy o‘rganish va chuqur o‘rganish modellari ko‘pincha “black-box” (qora quti) sifatida qaraladi, ya’ni ular tomonidan qabul qilingan qarorlarning ichki mexanizmini izohlash murakkab bo‘lishi mumkin. Bu holat ayniqsa Security Operations Center (SOC) muhitida muhim ahamiyat kasb etadi, chunki xavfsizlik tahlilchilari aniqlangan tahdidlarning sabablarini ham tushunishi zarur. Shu sababli so‘nggi yillarda Explainable Artificial Intelligence (XAI) konsepsiyasi faol rivojlanmoqda.

Explainable AI texnologiyalarining asosiy maqsadi mashinaviy o‘rganish modellari tomonidan qabul qilingan qarorlarni tushuntirish hamda ularning ishlash jarayonini shaffof qilishdan iborat. Lundberg va Lee tomonidan ishlab chiqilgan SHAP (Shapley Additive Explanations) usuli model qaroriga ta’sir qiluvchi xususiyatlarning ahamiyatini matematik jihatdan aniqlash imkonini beradi. Xuddi shuningdek, Ribeiro va hamkorlari tomonidan taklif etilgan LIME (Local Interpretable Model-agnostic Explanations) metodi har bir alohida bashorat uchun lokal interpretatsiyani taqdim etadi. Ushbu metodlar kiberxavfsizlik tizimlarida aniqlangan tahdidlarning sabablarini tushuntirish va xavfsizlik mutaxassislariga qaror qabul qilish jarayonida yordam berish imkonini yaratadi.

So‘nggi ilmiy tadqiqotlarda XAI yondashuvlari kiberxavfsizlik sohasida tobora keng qo‘llanilmoqda. Masalan, SHAP asosida tarmoq hujumlarini aniqlash modellari natijalarini tahlil qilish orqali qaysi xususiyatlar hujumni aniqlashda muhim rol o‘ynashini aniqlash mumkin. Bunday yondashuv SOC mutaxassislariga hujumlarning xatti-harakatlarini chuqurroq tushunish hamda xavfsizlik siyosatini takomillashtirish imkonini beradi.

Shunday qilib, mavjud ilmiy tadqiqotlar shuni ko‘rsatadiki, mashinaviy o‘rganish modellari kiberhujumlarni aniqlashda yuqori samaradorlikni ta’minlashi mumkin, biroq ularning interpretatsiyasi alohida ilmiy e’tiborni talab etadi. Shu sababli Explainable AI texnologiyalarini kiberxavfsizlik tizimlariga integratsiya qilish SOC faoliyatining samaradorligini oshirish va aniqlangan tahdidlarning sabablarini tushuntirishda muhim ilmiy yo‘nalishlardan biri hisoblanadi. Mazkur tadqiqot aynan ushbu masalani o‘rganishga qaratilgan bo‘lib, unda SOC uchun tushuntiriladigan kiberxavf aniqlash tizimi modeli taklif etiladi.

TADQIQOT METODOLOGIYASI

Mazkur tadqiqotda SOC (Security Operations Center) muhitida kiberxavflarni aniqlash hamda ularning sabablarini tushuntirish imkonini beruvchi Explainable Artificial Intelligence (XAI) ga asoslangan model taklif etiladi. Taklif etilayotgan tizim ikki asosiy komponentdan iborat. Birinchi bosqichda mashinaviy o‘rganish algoritmlari yordamida kiberhujumlar aniqlanadi, ikkinchi bosqichda esa Explainable AI metodlari orqali model qarorlari interpretatsiya qilinadi.

Mazkur yondashuv kiberxavfsizlik tizimlarining nafaqat aniqlik darajasini oshirishga, balki ularning ishlash jarayonini yanada tushunarli va shaffof tarzda namoyon etishga xizmat qiladi. Natijada xavfsizlik mutaxassislari aniqlangan tahdidlarning sabablarini tezkor va aniq tahlil qilish imkoniyatiga ega bo‘ladilar.

TAHLIL VA NATIJALAR

Taklif etilayotgan Explainable Artificial Intelligence (XAI) tizimi SOC (Security Operations Center) muhitida kiberxavflarni aniqlash hamda ularning sabablarini tushuntirish imkonini beruvchi kompleks arxitekturaga asoslanadi. Mazkur tizim tarmoq trafigi, xavfsizlik loglari va SIEM platformalaridan kelib tushadigan ma’lumotlarni qabul qilish jarayonidan boshlanadi. Ushbu ma’lumotlar odatda IP manzillar, portlar, paketlar soni, trafik hajmi, ulanish davomiyligi kabi muhim xususiyatlardan iborat bo‘lib, ular tarmoq faoliyatining umumiy holatini tavsiflaydi.

Keyingi bosqichda ma’lumotlar oldindan qayta ishlash jarayonidan o‘tkaziladi. Ushbu jarayonda ma’lumotlar tozalanadi, yetishmayotgan qiymatlar to‘ldiriladi hamda xususiyatlar normalizatsiya qilinadi. Shuningdek, kategorik atributlar kodlanadi va modelni o‘qitish uchun mos formatga keltiriladi. Bunday yondashuv ma’lumotlarning sifatini oshirish va model ishlashining barqarorligini ta’minlashga xizmat qiladi.

Shundan so‘ng tarmoq trafigi mashinaviy o‘rganish algoritmlari yordamida tahlil qilinadi. Ushbu bosqichda Gradient Boosting, Random Forest yoki neyron tarmoqlarga asoslangan modellardan foydalanish mumkin. Mazkur modellar tarmoqdagi normal faoliyatni potentsial hujumlardan farqlash orqali kiberxavflarni aniqlash imkonini beradi.

Model tomonidan qabul qilingan qarorlarning tushunarli bo‘lishini ta’minlash maqsadida Explainable AI moduli qo‘llaniladi. Ushbu bosqichda SHAP yoki LIME algoritmlari yordamida qaysi xususiyatlar model qaroriga ko‘proq ta’sir ko‘rsatgani aniqlanadi. Natijada SOC mutaxassislari aniqlangan tahdidlarning sabablarini aniq ko‘rish va tahlil qilish imkoniyatiga ega bo‘ladi.

Tizim tomonidan olingan natijalar SOC monitoring panelida vizual grafiklar, risk darajasi ko‘rsatkichlari hamda tushuntirish diagrammalari orqali aks ettiriladi. Bunday vizualizatsiya xavfsizlik tahlilchilariga tahdidlar

haqida tezkor va tushunarli ma’lumot olish imkonini yaratadi hamda qaror qabul qilish jarayonini samarali qo‘llab-quvvatlaydi.

Tadqiqot doirasida model qarorlarini interpretatsiya qilish uchun Explainable AI metodlaridan foydalaniladi. Xususan, SHAP (Shapley Additive Explanations) usuli kooperativ o‘yin nazariyasiga asoslanib, model qaroriga har bir xususiyatning ta’sir darajasini aniqlash imkonini beradi. Mazkur usul yordamida model tomonidan qabul qilingan qarorlar qanday omillar asosida shakllanganini matematik jihatdan tushuntirish mumkin. Natijada kiberxavfsizlik tizimlarining shaffofligi va ishonchliligi yanada ortadi.

$$\phi_i = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(|N| - |S| - 1)!}{|N|!} [f(S \cup \{i\}) - f(S)]$$

Bu yerda:

- φ_i—xususiyatning model qaroriga qo‘shgan hissasi,
- S — xususiyatlar to‘plami,
- F(x) — model bashorati.

SHAP yordamida qaysi tarmoq xususiyatlari hujumni aniqlashda eng muhim rol o‘ynayotgani aniqlanadi.

LIME (Local Interpretable Model-agnostic Explanations)

LIME metodi har bir alohida bashorat uchun lokal interpretatsiyani taqdim etadi. Bu usul modelning murakkab qarorini soddalashtirilgan chiziqli model yordamida yaqinlashtiradi:

$$\xi(x) = \arg\min_{g \in G} L(f, g, \pi_x) + \Omega(g)$$

Bu yerda:

- f— asl model,
- g — tushuntiruvchi model,
- L — yo‘qotish funksiyasi,
- π_x — lokal og‘irlik funksiyasi.

LIME (Local Interpretable Model-agnostic Explanations) metodidan foydalanish orqali SOC mutaxassislari har bir aniqlangan tahdid bo‘yicha model tomonidan qabul qilingan qarorning asosiy sabablarini aniq ko‘rish va tahlil qilish imkoniyatiga ega bo‘ladilar. Ushbu yondashuv model bashoratining lokal interpretatsiyasini taqdim etib, qaror qabul qilish jarayonining tushunarli va shaffof bo‘lishini ta’minlaydi. Natijada xavfsizlik tahlilchilari aniqlangan tahdidlarning shakllanishiga ta’sir etuvchi muhim xususiyatlarni tezkor aniqlash hamda ularning kiberxavfsizlik tizimiga ta’sirini chuqurroq baholash imkoniyatiga ega bo‘ladilar.

Taklif etilgan modelning samaradorligini aniqlash maqsadida uning ishlash natijalari bir qator muhim baholash mezonlari asosida tahlil qilinadi. Ushbu mezonlar modelning kiberhujumlarni aniqlash aniqligi, barqarorligi hamda amaliy qo‘llash jarayonidagi samaradorligini kompleks baholash imkonini beradi.

- Accuracy – umumiy aniqlik darajasi
- Precision – aniqlangan tahdidlarning haqiqiyligi
- Recall – aniqlangan hujumlarning ulushi
- F1-score – precision va recall muvozanati
- ROC-AUC – modelning diskriminativ qobiliyati

Formulalar quyidagicha ifodalanadi:

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

Taklif etilgan Explainable Artificial Intelligence (XAI) asosidagi tizim bir qator muhim afzalliklarga ega. Mazkur yondashuv kiberhujumlarni yuqori aniqlik bilan aniqlash imkonini beradi, model tomonidan qabul qilingan qarorlarni tushuntirishni ta’minlaydi hamda SOC mutaxassislari uchun tezkor va samarali tahlil

o‘tkazish imkoniyatini yaratadi. Shuningdek, ushbu tizim kiberxavfsizlik monitoring jarayonining shaffofligini oshirishga xizmat qiladi. Shu tariqa, Explainable AI yondashuvi kiberxavfsizlik tizimlarida nafaqat hujumlarni aniqlash, balki ularning sabablarini tushuntirish orqali xavfsizlik mutaxassislariga yanada asosli va samarali qaror qabul qilish imkoniyatini yaratadi.

Tadqiqot doirasida Explainable Artificial Intelligence (XAI) asosidagi kiberxavf aniqlash modeli SOC muhitida tarmoq trafigini tahlil qilish orqali sinovdan o‘tkazildi. Mashinaviy o‘rganish algoritmlaridan foydalanish natijasida tarmoq faoliyatidagi anomaliyalarni aniqlash imkoniyati sezilarli darajada oshdi. Model yordamida normal trafik va potentsial kiberhujumlar o‘rtasidagi farqlar aniqlanib, xavfli faoliyatlarni avtomatik ravishda tasniflash imkoniyati yaratildi. Model samaradorligini baholash jarayonida accuracy, precision, recall hamda F1-score kabi ko‘rsatkichlardan foydalanildi va olingan natijalar modelning yuqori aniqlik bilan ishlashini ko‘rsatdi.

Shuningdek, SHAP va LIME kabi Explainable AI metodlari model qarorlarini interpretatsiya qilish imkonini berdi. Ushbu metodlar yordamida qaysi tarmoq xususiyatlari kiberhujumni aniqlashda muhim rol o‘ynashi aniqlanib, SOC mutaxassislari uchun tushunarli va asosli tahlil natijalari taqdim etildi. Natijada taklif etilgan model nafaqat kiberhujumlarni aniqlash jarayonini avtomatlashtirishga xizmat qiladi, balki xavfsizlik tahlilchilariga tahdidlarning sabablarini tez va aniq tushunish imkoniyatini ham yaratadi. Bu esa kiberxavfsizlik monitoring tizimlarining umumiy samaradorligini oshirishga xizmat qiladi.

XULOSA VA TAKLIFLAR

Mazkur tadqiqotda Security Operations Center (SOC) muhitida kiberxavflarni aniqlash hamda ularning sabablarini tushuntirish imkonini beruvchi Explainable Artificial Intelligence (XAI) ga asoslangan model taklif etildi. Tadqiqot natijalari shuni ko‘rsatadiki, mashinaviy o‘rganish algoritmlari kiberhujumlarni aniqlashda yuqori samaradorlikni ta’minlashi mumkin, biroq ularning qaror qabul qilish jarayoni ko‘pincha “qora quti” tamoyiliga asoslanadi. Shu sababli model qarorlarini tushuntirish imkoniyatini yaratish kiberxavfsizlik tizimlarining ishonchliligi hamda amaliy qo‘llanilishi uchun muhim ahamiyat kasb etadi.

Taklif etilgan tizim arxitekturasi mashinaviy o‘rganish modellari va Explainable AI metodlarini birlashtirish orqali kiberxavflarni aniqlash hamda ularning sabablarini tahlil qilish imkonini beradi. SHAP va LIME kabi interpretatsiya usullari model qaroriga ta’sir etuvchi xususiyatlarni aniqlashga yordam beradi va SOC mutaxassislariga tahdidlarning asosiy sabablarini chuqurroq tushunish imkonini yaratadi. Bu esa xavfsizlik hodisalariga tezkor javob qaytarish jarayonining samaradorligini oshiradi.

Tadqiqot natijalari Explainable AI texnologiyalarini kiberxavfsizlik monitoring tizimlariga integratsiya qilish SOC faoliyatining samaradorligini oshirishini ko‘rsatadi. Mazkur yondashuv tarmoq trafigidagi tahdidlarni aniqlash jarayonini nafaqat avtomatlashtiradi, balki xavfsizlik mutaxassislariga qaror qabul qilish uchun zarur bo‘lgan tushunarli va shaffof tahlil natijalarini ham taqdim etadi. Shu sababli Explainable AI asosidagi kiberxavf aniqlash tizimlari zamonaviy kiberxavfsizlik infratuzilmasining muhim komponentlaridan biri sifatida qaralishi mumkin.

Kelgusida tadqiqotni rivojlantirish doirasida real vaqt rejimida ishlovchi kiberxavfsizlik monitoring tizimlarini yaratish, konsept drift muammosini hisobga olgan adaptiv modellardan foydalanish hamda federativ o‘rganish texnologiyalarini joriy etish istiqbolli yo‘nalishlardan biri hisoblanadi. Bundan tashqari, Explainable AI metodlarini SIEM va boshqa xavfsizlik platformalari bilan integratsiya qilish orqali kiberxavfsizlik tizimlarining samaradorligini yanada oshirish mumkin.

Umuman olganda, Explainable AI yondashuvi kiberxavfsizlik tizimlarining shaffofligi, ishonchliligi va samaradorligini oshirishga xizmat qiladi hamda SOC mutaxassislariga murakkab kiberxavf holatlarini chuqurroq tahlil qilish imkonini beradi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge: MIT Press, 2016. – 775 p.
2. Bishop C. M. Pattern Recognition and Machine Learning. – New York: Springer, 2006. – 738 p.
3. Géron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. – 2nd ed. – Sebastopol: O’Reilly Media, 2019. – 851 p.
4. Chollet F. Deep Learning with Python. – 2nd ed. – New York: Manning Publications, 2021. – 504 p.
5. Molnar C. Interpretable Machine Learning: A Guide for Making Black Box Models Explainable. – Munich: Leanpub, 2022. – 350 p.
6. Lundberg S. M., Lee S. I. A Unified Approach to Interpreting Model Predictions // Advances in Neural Information Processing Systems. – 2017. – Vol. 30. – P. 4765–4774.
7. Ribeiro M. T., Singh S., Guestrin C. “Why Should I Trust You?” Explaining the Predictions of Any Classifier // Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. – 2016. – P. 1135–1144.

8. Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System // Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. – 2016. – P. 785–794.
9. Ke G. et al. LightGBM: A Highly Efficient Gradient Boosting Decision Tree // Advances in Neural Information Processing Systems. – 2017. – P. 3146–3154.
10. Prokhorenkova L. et al. CatBoost: Unbiased Boosting with Categorical Features // Advances in Neural Information Processing Systems. – 2018. – P. 6638–6648.
11. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // IEEE Symposium on Security and Privacy. – 2010. – P. 305–316.
12. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization (CIC-IDS2017) // Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP). – 2018. – P. 108–116.
13. Moustafa N., Slay J. UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems // Military Communications and Information Systems Conference. – 2015. – P. 1–6.
14. Hinton G. E., Salakhutdinov R. R. Reducing the Dimensionality of Data with Neural Networks // Science. – 2006. – Vol. 313. – P. 504–507.
15. Saito T., Rehmsmeier M. The Precision–Recall Plot Is More Informative than the ROC Plot When Evaluating Binary Classifiers on Imbalanced Datasets // PLoS ONE. – 2015. – Vol. 10(3).
16. Fawcett T. An Introduction to ROC Analysis // Pattern Recognition Letters. – 2006. – Vol. 27. – P. 861–874.
17. Pedregosa F. et al. Scikit-learn: Machine Learning in Python // Journal of Machine Learning Research. – 2011. – Vol. 12. – P. 2825–2830.
18. McNemar Q. Note on the Sampling Error of the Difference Between Correlated Proportions or Percentages // Psychometrika. – 1947. – Vol. 12. – P. 153–157.

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Ingliz tili muharriri: Feruz Hakimov

Musahhih: Zokir Alibekov

Sahifalovchi va dizayner: Abdurahmon Qurbonov

2026. № 3

"Muhandislik va iqtisodiyot" jurnali 26.06.2023-yildan
O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi
Axborot va ommaviy kommunikatsiyalar agentligi tomonidan
№S–5669245 reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan.
Litsenziya raqami: №095310.

Manzilimiz: Toshkent shahri Yunusobod tumani 15-mavze 19-uy

+998 93 718 40 07 https://muhandislik-iqtisodiyot.uz/index.php/journal t.me/yait_2100