# KOMPYUTER TARMOQ HUJUMLARI IZLARINI ANIQLASHDA MODELLAR VA ALGORITMLAR ASOSIDA O‘RGANISH IMKONIYATI

**Ramazonova Madina Shavkatovna**
*Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika” kafedrasi assistenti.*
*Email: abdujabbor.madina1989@gmail.com*
**Raxmanqulova Mashhura Ruziboyevna**
*“Kiberxavfsizlik markazi” davlat unitar korxonasi,hodimi.*
*Email:m.raxmanqulova@csec.uz*

**Annotatsiya.** Axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda tarmoqlarga bo‘ladigan kiberhujumlar soni ham ortib bormoqda. Bugungi kunda korxonalar, davlat muassasalari va shaxsiy foydalanuvchilarning tarmoq xavfsizligini ta’minlash dolzarb muammolardan biriga aylangan. Kompyuter tarmoq hujumlari izini erta aniqlash va oldini olish axborot texnologiyalari sohasida muhim masalalardan biridir.Ushbu maqolada sun’iy intellekt yordamida tarmoq hujumlarini aniqlash natijalari, AI va an’anaviy IDS/IPS tizimlarining solishtirma tahlili, hamda LSTM, CNN va Transformer modellarining qo‘llanilishi bo‘yicha tajribalar va natijalar tahlil qilinadi.Taqdim etilgan natijalar tarmoq xavfsizligini mustahkamlash, hujumlarni erta aniqlash va ularning oldini olish bo‘yicha amaliy tavsiyalarni o‘z ichiga oladi. Tadqiqot natijalari kiberxavfsizlik sohasi mutaxassislari, IT xavfsizlik muhandislari va tadqiqotchilar uchun foydali bo‘lishi mumkin.

**Kalit so‘zlar:** trafik tahlili, hujumlar izlarini aniqlash algoritmlari, transformator modeli, sun'iy intellektga asoslangan tahlil usullari

**Аннотация**: В современную технологическую эпоху, наряду с быстрым развитием информационных технологий, наблюдается рост числа кибератак на компьютерные сети. В настоящее время обеспечение сетевой безопасности для предприятий, государственных учреждений и отдельных пользователей стало одной из актуальных проблем. Раннее выявление и предотвращение следов атак на компьютерные сети является важной задачей в сфере информационных технологий. Цель данной статьи — анализ результатов обнаружения сетевых атак с использованием искусственного интеллекта, сравнительный анализ систем ИИ с традиционными IDS/IPS-системами, а также проведение экспериментов и представление результатов применения моделей LSTM, CNN и Transformer. Для эффективного внедрения представленных результатов предлагаются практические рекомендации по усилению сетевой безопасности, раннему обнаружению и



ISSN 3030-3907

предотвращению атак. Полученные в ходе исследования результаты могут быть полезны специалистам по кибербезопасности, инженерам ИБ и научным работникам.

**Ключевые слова:** анализ трафика, алгоритмы обнаружения следов атак, модель преобразователя, методы анализа на основе искусственного интеллекта.

**Abstract:**In today's modern technological age, along with the rapid development of information technology, the number of cyberattacks on networks is also increasing. Today, ensuring network security for enterprises, government institutions and individual users has become one of the pressing problems. Early detection and prevention of traces of computer network attacks is one of the important issues in the field of information technology. The aim of the article is analyzing the results of detecting network attacks using artificial intelligence, a comparative analysis of AI and traditional IDS/IPS systems, as well as experiments and results on the use of LSTM, CNN and Transformer models. In order to effectively implement the presented results, include practical recommendations for strengthening network security, early detection and prevention of attacks. While doing research, the results of the study may be useful for cybersecurity specialists, IT security engineers and scientific users.

**Keywords:** traffic analysis, algorithms for detecting traces of attacks,transformer model, artificial intelligence-based analysis methods

**Kirish**

Bugungi kunda kompyuter tarmoqlari hujumlari soni kun sayin oshib bormoqda bu esa xavfsizlikni ta’minlovchi hodimlarda qiyinchiliklarni yuzaga keltiradi. Eng ommaviy hujumlar DDoS (Distributed Denial-of-Service), Man-in-the-Middle, SQL Injection, ransomware va shu kabi boshqa turli xil hujumlar ma’lumotlar xavfsizligini buzishi, tizimlarning ishdan chiqishiga sabab bo‘lishi va iqtisodiy yo‘qotishlarga olib kelishi mumkin. Shu sababli, hujumlarni erta aniqlash va ularga samarali javob berish kiberxavfsizlik strategiyasining muhim tarkibiy qismidir.

Tarmoq xavfsizligini ta’minlashda Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) tizimlari keng qo‘llaniladi. IDS tizimlari hujumlarni aniqlash va tahlil qilishga mo‘ljallangan bo‘lsa, IPS tizimlari esa hujumning oldini olish va tarmoq xavfsizligini real vaqt rejimida ta’minlash uchun ishlatiladi. Biroq, an’anaviy IDS/IPS tizimlari hujumlarni qoida (rule-based) va signatura (signature-based) usullar asosida aniqlaydi. Ushbu yondashuv oldindan ma’lum bo‘lgan hujumlarni samarali topa oladi, biroq yangi, ilgari noma’lum bo‘lgan hujumlarni aniqlashda ojiz qolishi mumkin.



ISSN 3030-3907

So‘nggi yillarda sun’iy intellekt (AI) va mashinani o‘rganish (ML) texnologiyalaridan foydalangan holda tarmoq hujumlarini aniqlash va oldini olish bo‘yicha samarali yondashuvlar ishlab chiqilmoqda. Ushbu texnologiyalar ma’lumotlarni avtomatik tahlil qilish, anomaliyalarni aniqlash, oldindan bashorat qilish va noma’lum hujumlarni tanib olish imkoniyatiga ega. Ayniqsa, chuqur o‘rganish (Deep Learning) modellarining rivojlanishi natijasida IDS/IPS tizimlarining aniqligi sezilarli darajada oshdi. LSTM (Long Short-Term Memory), CNN (Convolutional Neural Network) va Transformer kabi modellar real vaqt rejimida ishlash va katta hajmdagi tarmoq trafiklarini samarali tahlil qilish imkonini beradi.

Shu bilan birga, sun’iy intellektga asoslangan hujum aniqlash tizimlarining ustunliklari va kamchiliklari ham ko‘rib chiqiladi.

**Experimental**

Tarmoq xavfsizligi - bu kompyuter tarmoqlari va ularning foydalanuvchilarini turli xil kiberxavflardan himoya qilishga qaratilgan chora-tadbirlar majmui hisoblanadi. U kompyuter tizimlari, serverlar, qurilmalar va tarmoq infrastrukturasining butunligini, maxfiyligini va mavjudligini (CIA - Confidentiality, Integrity, Availability) ta’minlashga xizmat qiladi [1].

Tarmoq xavfsizligi quyidagi asosiy yo‘nalishlarni o‘z ichiga oladi:

- **Axborotni shifrlash** – ma’lumotlarning ruxsatsiz foydalanilishining oldini olish.
- **Tarmoqni monitoring qilish** – IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlari yordamida hujumlarni oldindan aniqlash.
- **Autentifikatsiya va ruxsat nazorati** – foydalanuvchilarni tekshirish va ularga ruxsat darajalarini belgilash.
- **Zararli dasturlardan himoya qilish** – antivirus va firewall tizimlaridan foydalanish.

Tarmoq xavfsizligining ahamiyati hozirgi kunda tobora ortib bormoqda, chunki tashkilotlar va davlat idoralarining katta qismi o‘z faoliyatini raqamli muhitda olib boradi. Tarmoq hujumlarining zararli ta’siri katta bo‘lib, moliyaviy yo‘qotishlar, maxfiy ma’lumotlarning oshkor bo‘lishi va tizimlarning ishdan chiqishiga olib kelishi mumkin [2].

Tarmoq hujumlari odatda ikki asosiy turga bo‘linadi: **aktiv** va **passiv** hujumlar.

Aktiv hujumlar hujumchining tarmoqdagi ma’lumotlarga bevosita ta’sir o‘tkazishini anglatadi. Ushbu hujumlar quyidagi turlarga bo‘linadi:



ISSN 3030-3907

– DoS (Denial of Service) va DDoS (Distributed Denial of Service) hujumlari – tarmoq xizmatlarini haddan tashqari yuklash orqali ishlashiga to‘sqinlik qiladi [3].

– Man-in-the-Middle (MITM) hujumi – hujumchi tarmoq orqali o‘tuvchi ma’lumotlarni o‘zgartirishi yoki o‘g‘irlashi mumkin [4].

– SQL Injection – ma’lumotlar bazasiga kiritilayotgan so‘rovlarga zararli kodlarni joylashtirish orqali tizimni buzish [5].

– **Cross-Site Scripting (XSS)** – veb-brauzer orqali foydalanuvchilarga zararli kod yuborish.

Passiv hujumlar hujumchining tizimga ta’sir o‘tkazmagan holda ma’lumotlarni o‘g‘irlashini anglatadi. Ushbu hujumlar quyidagilarni o‘z ichiga oladi:

– **Sniffing** (Trafikni tinglash) – hujumchi tarmoq orqali uzatilayotgan paketlarni tahlil qilib, maxfiy ma’lumotlarni aniqlaydi.

– **Eavesdropping** (Maxfiy ma’lumotlarni eshitish) – ruxsatsiz ravishda ma’lumotlarni olish va foydalanish.

– **Phishing** (Fishing hujumi) – foydalanuvchilarni firibgarlik yo‘li bilan o‘z ma’lumotlarini oshkor qilishga undash.

Tarmoq hujumlari texnologiyalar rivojlanishi bilan murakkablashib bormoqda. Ularning oldini olish uchun mustahkam xavfsizlik choralari va ilg‘or texnologiyalar talab qilinadi [6].

Tarmoq hujumlarini o‘z vaqtida aniqlash va oldini olish axborot xavfsizligini ta’minlashning eng muhim jihatlaridan biridir. Hujum izlarini aniqlash (Intrusion Detection) quyidagi sabablarga ko‘ra dolzarb hisoblanadi:

– Ma’lumotlarning maxfiyligini ta’minlash – ruxsatsiz kirishning oldini olish va ma’lumotlarning uchinchi shaxslarga tushib qolishining oldini olish [7].

– Tizimlarning butunligini saqlash – ma’lumotlarni buzish va manipulyatsiya qilishga qarshi kurash.

– Hujumlarni tahlil qilish va reaksiya berish – IDS va SIEM tizimlari hujumlarni aniqlash va ularga tezkor javob qaytarishga imkon beradi [8].

– Regulyator talablariga javob berish – ko‘plab kompaniyalar ISO 27001, GDPR va boshqa xalqaro standartlarga muvofiq hujumlarni kuzatib borishlari talab etiladi [9].

Hujum izlarini aniqlashning asosiy usullari quyidagilardan iborat:

1. Qoida asosida aniqlash (Rule-based detection) – ma’lum bir hujum imzolari asosida ishlaydi.

2. Xulq-atvor tahliliga asoslangan aniqlash (Behavior-based detection) – odatiy tarmoq trafikidan farqli holatlarni aniqlaydi.



ISSN 3030-3907

3. Sun’iy intellekt va mashinani o‘rganish usullari – anomal xatti-harakatlarni bashorat qilish uchun ishlatiladi.

Tahlillar shuni ko‘rsatadiki, an’anaviy IDS tizimlari hujumlarning faqat imzolari bo‘yicha aniqlashi sababli yangi turdagi hujumlarni oldindan ko‘ra olmaydi. Shu sababli, mashinani o‘rganish va chuqur o‘rganish texnologiyalariga asoslangan yangi yondashuvlar hozirgi vaqtda eng istiqbolli yo‘nalishlardan biri hisoblanadi [10].

**3.1.Hujum izlarini aniqlash usullari**

Hujum izlarini aniqlash texnologiyalari turli usullarga asoslanadi, jumladan, qoida asosidagi tahlil, imzo asosidagi usullar, xulq-atvor va anomaliya asosida aniqlash, sun’iy intellekt hamda mashinani o‘rganish modellari yordamida tahlil va SIEM tizimlari orqali monitoring.

*Qoida asosidagi tahlil (Rule-based detection, IDS - Intrusion Detection Systems)*

Qoida asosidagi hujum izlarini aniqlash tizimlari (7-jadval) oldindan belgilangan qoidalar va shablonlarga asoslanadi.Ushbu tizimlar tarmoq trafigini yoki tizim loglarini skanerlash orqali hujumlarni aniqlaydi [17].

**7-jadval.**

**Qoida asosidagi hujum izlarini aniqlash tizimlari**

| Vositalar | Tavsif | Afzalliklari | Kamchiliklari |
|---|---|---|---|
| Snort | Ochiq kodli IDS/IPS tizimi | Bepul va moslashuvchan | Yangi tahdidlarga nisbatan zaif |
| Suricata | Yuqori samarali tarmoq tahdidlarini aniqlash tizimi | Tezkor ishlash va ko‘p ipli (multi-threading) qo‘llab-quvvatlash | Murakkab sozlash talab etadi |
| Zeek (Bro) | Tarmoq xavfsizligini tahlil qilish va hujumlarni aniqlash vositasi | Tarmoqdagi hodisalarni keng qamrovli tahlil qilish | Katta hajmdagi loglarni qayta ishlash talab etadi |

**Imzo asosidagi usullar (Signature-based methods)**

Imzo asosidagi usullarda (8-jadval) ilgari ma’lum bo‘lgan hujumlarning imzolari (patterns) bazasi yaratiladi va tarmoq yoki tizimdagi harakatlar ushbu imzolar bilan solishtiriladi. IDS va IPS (Intrusion Prevention Systems) tizimlari ko‘pincha ushbu yondashuvga asoslanadi [18].



ISSN 3030-3907

**8-jadval.**

**Imzo asosidagi usullarga asoslangan tizimlar**

| Vositalar | Tavsif | Afzalliklari | Kamchiliklari |
|---|---|---|---|
| Snort | Imzo asosidagi IDS tizimi | Yuqori aniqlik | Zero-day hujumlarni aniqlay olmaydi |
| Kaspersky IDS/IPS | Imzo asosida tahdidlarni aniqlash | Yangi tahdidlar bazasini tez yangilash | Tijorat mahsuloti, bepul versiyasi yo‘q |
| Cisco Firepower | Integratsiyalashgan IPS tizimi | Tarmoq va endpoint xavfsizligini ta’minlaydi | Murakkab sozlash va yuqori narx |

**Xulq-atvor va anomaliya asosida aniqlash (Behavior-based and Anomaly Detection)**

Xulq-atvor va anomaliya asosida aniqlashga asoslangan usullarda (9-jadval) tizim yoki foydalanuvchilarning odatiy harakatlari kuzatilib, odatdagidan farqli xatti-harakatlar aniqlanganda tahdid sifatida belgilanadi [19].

**9-jadval.**

**Xulq-atvor va anomaliya asosida aniqlashga asoslangan tizimlar**

| Vositalar | Tavsif | Afzalliklari | Kamchiliklari |
|---|---|---|---|
| Darktrace | Sun’iy intellekt asosida anomaliyalarni aniqlash | O‘z-o‘zidan o‘rganish va moslashuvchanlik | Yuqori narx va katta hisoblash resurslari talab etadi |
| Vectra AI | Tarmoqdagi zararli harakatlarni kuzatish | Real vaqt rejimida monitoring va tahdidlarni aniqlash | Barcha turdagi hujumlarni 100% aniqlash kafolatlanmagan |
| IBM QRadar | Xulq-atvor asosida tahlil qilish | Ilg‘or analitika va integratsiya | Katta hajmdagi loglar bilan ishlashda resurs talabchan |

**Sun’iy intellekt va mashinani o‘rganish modellari yordamida tahlil**

Sun’iy intellekt (AI) va mashinani o‘rganish (ML) asosidagi tizimlar (10-jadval) hujumlarni oldindan bashorat qilish va aniqlash uchun ishlatiladi. Ushbu yondashuv katta hajmdagi ma’lumotlarni tahlil qilish va anomaliyalarni aniqlashda samarali hisoblanadi [20].



ISSN 3030-3907

**10-jadval.**

**Sun’iy intellekt va mashinani o‘rganish asosidagi tizimlar**

| Vositalar | Tavsif | Afzalliklari | Kamchiliklari |
|---|---|---|---|
| Splunk | SIEM va AI asosida tahlil qilish | Keng qamrovli log tahlili va vizualizatsiya | Yuqori narx va katta resurs sarfi |
| IBM Watson | AI yordamida kiberxavfsizlik tahlili | Mashinani o‘rganish orqali tahdidlarni avtomatik aniqlash | Modelni o‘qitish va sozlash uchun katta vaqt talab etadi |
| Elastic Security | Ma'lumotlar oqimini tahlil qilish | Bepul va ochiq kodli, kengaytiriladigan | Katta hajmdagi ma’lumotlarni qayta ishlash resurs talab etadi |

### 3.2.Hujum izlarini aniqlash algoritmlari

Tarmoq hujumlarini aniqlash algoritmlari turli yondashuvlar asosida ishlab chiqilgan bo‘lib, ularning har biri ma’lum afzalliklarga va kamchiliklarga ega. Quyida ushbu algoritmlar haqida batafsil ma’lumot beriladi (12-jadval).

Hujumlarni aniqlashning probabilistik yondashuvlaridan biri Bayes tarmoqlari hisoblanadi. Ushbu yondashuv hujum ehtimolini hisoblash va voqealar orasidagi bog‘liqlikni tahlil qilish uchun qo‘llaniladi [23]. Klassifikatsiya asosida hujumlarni aniqlash uchun esa KNN, SVM va Random Forest algoritmlari qo‘llaniladi [24,25]. Ushbu usullar katta hajmdagi ma’lumotlarni qayta ishlash va tahlil qilishga moslashtirilgan.

So‘nggi yillarda Deep Learning asosida ishlovchi model va neyron tarmoqlarga asoslangan yondashuvlar keng qo‘llanilmoqda. Ushbu usullar hujum naqshlarini o‘rganish va ularga mos javoblarni ishlab chiqish imkoniyatini beradi ([27]. Shuningdek, anomaliyalarni aniqlash usullari, masalan, K-means va DBSCAN algoritmlari, ma’lumotlar orasidagi kutilmagan o‘zgarishlarni aniqlashga yordam beradi [28].

**12-jadval.**

**Hujum izlarini aniqlash algoritmlari tahliliy jadvali**

| Algoritm | Tavsifi | Afzalliklari | Kamchiliklari |
|---|---|---|---|
| **Bayes tarmoqlari va ehtimollik modellari** | Hujum ehtimolini hisoblash va voqealar orasidagi bog‘liqlikni tahlil qilish uchun qo‘llaniladi. | O‘z-o‘zini moslashtirish imkoniyati, statistik asosga ega. | Ma’lumotlar yetarli bo‘lmasa, noto‘g‘ri natija berishi mumkin [23]. |



ISSN 3030-3907

| | | | |
|---|---|---|---|
| **KNN (K-Eng yaqin qo‘shnilar)** | Har bir yangi kiruvchi ma’lumotni eng yaqin qo‘shnilar bilan taqqoslab hujumni aniqlaydi. | Oddiy va samarali usul, turli hujum turlariga moslashuvchan. | Katta hajmdagi ma’lumotlarda sekin ishlashi mumkin [24]. |
| **SVM (Support Vector Machine)** | Ma’lumotlarni chiziqli yoki chiziqli bo‘lmagan chegaralar bo‘yicha ajratib, hujumlarni aniqlaydi. | Yuqori aniqlik darajasi, kichik ma’lumotlar to‘plami uchun samarali. | Katta hajmdagi ma’lumotlarda sekin ishlaydi, parametrlarni sozlash muhim [26]. |
| **Random Forest** | Bir nechta qaror daraxtlari asosida hujumlarni tasniflaydi. | Yaxshi umumlashtirish qobiliyati, yuqori aniqlik. | Model murakkabligi va interpretatsiya qilish qiyinligi [25]. |
| **Deep Learning va neyron tarmoqlar** | Hujum naqshlarini o‘rganish uchun chuqur neyron tarmoqlardan foydalanadi. | O‘z-o‘zini o‘rganish imkoniyati, yuqori aniqlik. | Katta hisoblash resurslari talab qiladi, tushuntirish murakkab [27]. |
| **K-means va DBSCAN asosida anomaliyalarni aniqlash** | Ma’lumotlar orasidagi anomaliyalarni guruhlash orqali hujumlarni aniqlaydi. | Belgilangan modelga bog‘liq bo‘lmasdan ishlaydi. | To‘g‘ri klasterlash parametrlari tanlanmasa, natija noto‘g‘ri bo‘lishi mumkin [28]. |

### 3.2.1 IDS/IPS tizimlarining natijalari va samaradorligi

Tarmoq hujumlarini aniqlash tizimlari (IDS) va oldini olish tizimlari (IPS) xavfsizlik infratuzilmasining muhim qismi hisoblanadi. Quyida **Suricata, Snort va Zeek** kabi IDS/IPS tizimlarining (13-jadval) real tarmoq muhitida ishlash samaradorligi, xatoliklar statistikasi va samaradorlikni oshirish uchun qo‘yilgan qadamlar keltirilgan.



ISSN 3030-3907

**13-jadval.**

**IDS/IPS tizimlarining samaradorligi**

| Tizim | Afzalliklari | Kamchiliklari |
|---|---|---|
| **Suricata** | Yuksak ishlash tezligi (multi-threaded ishlash), katta tarmoq trafikini real vaqtda tahlil qilish | Resurs talabchanligi yuqori, noto‘g‘ri ijobiy (False Positive) natijalar |
| **Snort** | Yengil va moslashuvchan, aniq qoida (rule-based) tizimga ega | Katta trafikda ishlashda samaradorlik pasayishi mumkin |
| **Zeek (Bro)** | Tarmoq faoliyatini chuqur tahlil qilish, tajovuzkor xatti-harakatlarni kontekst asosida aniqlash | Qoida yozish murakkabligi, real vaqtda oldini olish emas, balki kuzatuv uchun ishlatiladi |

IDS/IPS tizimlari ba’zan haqiqiy tahdid bo‘lmagan holatlarni hujum deb noto‘g‘ri aniqlaydi yoki aksincha, haqiqiy hujumlarni sezmay qolishi mumkin.

Quyidagi 14-jadvalda **real test natijalari** asosida Suricata, Snort va Zeek tizimlarining **FP (False Positive) va FN (False Negative) darajalari** ko‘rsatilgan.

| Tizim | Noto‘g‘ri ijobiy FP (%) | Noto‘g‘ri salbiy FN (%) |
|---|---|---|
| **Suricata** | 5-8% | 2-5% |
| **Snort** | 7-12% | 4-6% |
| **Zeek** | 3-6% | 1-4% |

**Yuqorida keltirilgan natijalardan olingan xulosalar:**

- **Zeek** kontekstual tahlil ishlatgani sababli hujumlarni aniqroq aniqlaydi va FP/FN darajasi nisbatan past.
- **Suricata** katta trafikni tahlil qilishda yaxshi ishlaydi, lekin noto‘g‘ri ijobiy natijalari Snortdan past.
- **Snort** tajribali foydalanuvchilar uchun moslashuvchan, lekin to‘g‘ri sozlanmasa, noto‘g‘ri natijalar soni ortishi mumkin.

IDS/IPS tizimlarining aniqlash aniqligini oshirish va xatolarni kamaytirish uchun quyidagi chora-tadbirlar qo‘llanildi:

***Qoida (rule) asosida optimallashtirish:***

- IDS tizimlarida haddan tashqari ko‘p qoidalar noto‘g‘ri ijobiy natijalarni ko‘paytirishi mumkin.
- IDS tizimlarining o‘ziga xos hujumlar uchun maxsus qoida bazalari yaratildi.

***Mashinali o‘rganish asosida tahlil:***



ISSN 3030-3907

– Suricata + AI: Sun’iy intellekt yordamida anomal trafikni yanada aniqroq aniqlash mexanizmi qo‘shildi.

– Zeek + ML: Zeek loglari asosida mashinali o‘rganish modeli ishlab chiqildi, natijada FN darajasi sezilarli kamaydi.

***Threshold (Chegaraviy qiymatlar) optimallashtirildi:***

– IDS tizimlari noto‘g‘ri ijobiy natijalarni kamaytirish uchun hujumlar intensivligiga qarab filtrlar qo‘shildi.

– Masalan, DDoS hujumlarini aniqlashda oddiy ping so‘rovlarini hujum deb qabul qilmaslik uchun cheklovlar belgilandi.

***Real vaqtli monitoring va avtomatlashtirilgan javob choralarini qo‘shish:***

– IDS tizimlari IPS tizimlariga ulanishi orqali avtomatik ravishda firewall qoidalarini o‘zgartirish imkoniyati yaratildi.

– Masalan, **Snort + IPTables** ishlatilib, xavfli IP-manzillar avtomatik ravishda bloklandi.

IDS/IPS tizimlari samaradorligini oshirish uchun qoida optimallashtirish, sun’iy intellekt qo‘llash, threshold sozlash va real vaqtli javob berish mexanizmlari muhim ahamiyat kasb etadi. Zeek va Suricata kabi tizimlar AI va avtomatlashtirish orqali yanada samarali bo‘lishi mumkin.

### 3.2.2 Sun’iy intellekt yordamida hujum izlarini aniqlash va optimallashtirish

Sun’iy intellekt (AI) va mashinani o‘rganish (ML) hujumlarni aniqlash tizimlarini (IDS/IPS) ancha samarali qiladi. Quyida **AI yordamida amalga oshirilgan tahlillar, an’anaviy IDS/IPS tizimlariga nisbatan AI yondashuvlarining ustunlik va kamchiliklari,** shuningdek**, LSTM, CNN va Transformer modellarining qo‘llanilishi bo‘yicha natijalar** keltirilgan.

Mashinani o‘rganish va chuqur o‘rganish modellaridan foydalanib, IDS/IPS tizimlarining samaradorligi oshirilmoqda. Quyidagi 15-jadvalda **KDD CUP 99, CIC-IDS-2017 va UNSW-NB15** kabi tarmoq hujumlarini aniqlash uchun mashhur datasetlar asosida AI modellarining natijalari keltirilgan.

**15-jadval.**

**Tarmoq hujumlarini aniqlovchi datasetlar asosidagi AI modellar**

| Model | Aniqlik (Accuracy %) | False Positive (%) | False Negative (%) | Qo‘llash sohasi |
|---|---|---|---|---|
| **Random Forest** | 93.5% | 4.2% | 6.3% | Kichik datasetlar uchun mos |
| **LSTM (Long Short-Term Memory)** | 96.8% | 3.5% | 2.7% | Sekin o‘zgaruvchi tarmoq hujumlari uchun yaxshi |



ISSN 3030-3907

| | | | | |
|---|---|---|---|---|
| **CNN (Convolutional Neural Network)** | 97.2% | 2.9% | 2.4% | Trafik oqimlarida naqshlarni aniqlash uchun samarali |
| **Transformer (BERT)** | 98.5% | 1.7% | 1.5% | Katta real vaqtli tarmoq ma'lumotlarini tahlil qilishda kuchli |

**15-jadvalda keltirilgan ma'lumotlardan olingan xulosalar:**

–Transformerlar (BERT, GPT asosidagi modellar) real vaqtli tahlil va katta hajmdagi tarmoq trafiklarini o'rganishda eng samarali natijani berdi.

–CNN va LSTM naqshlarni tahlil qilishda an'anaviy ML modellarga qaraganda samaraliroq.

–Random Forest oddiy IDS tizimlarida ishlatilishi mumkin, lekin katta datasetlarda samaradorligi pastroq.

**16-jadval.**

**AI yondashuvlarining an'anaviy IDS/IPS tizimlariga nisbatan ustunlik va kamchiliklari**

| Xususiyat | An'anaviy IDS/IPS | AI asosidagi IDS/IPS |
|---|---|---|
| **Aniqlash usuli** | Qoida (rule-based) | O'z-o'zidan o'rganish (self-learning) |
| **Moslashuvchanlik** | Hujumlar qo'llanma asosida aniqlanadi | Yangi, noma'lum hujumlarni aniqlay oladi |
| **Noto'g'ri ijobiy (FP) darajasi** | Yuqori (8-12%) | Past (1.5-5%) |
| **Hujumning oldini olish** | Faqat aniqlaydi, ba'zida kech javob beradi | Oldindan bashorat qilishi mumkin |
| **Real vaqtli ishlash** | Samarali, lekin murakkab hujumlarni e'tibordan chetda qoldirishi mumkin | Katta tarmoq hajmida ishlash uchun ko'proq hisoblash resurslarini talab qiladi |
| **Qo'llash qiyinligi** | IDS/IPS tizimlarini sozlash nisbatan oson | Modelni o'qitish va moslash oson emas |

**16-jadvaldagi AI yondashuvlarining an'anaviy IDS/IPS tizimlariga nisbatan ustunlik va kamchiliklari tahlilidan olingan xulosalar:**

**–AI asosidagi tizimlar yangi va noma'lum hujumlarni ham aniqlash qobiliyatiga ega, an'anaviy IDS/IPS esa faqat oldindan belgilangan hujumlarni topa oladi.**

**–AI tizimlari noto'g'ri ijobiy natijalarni kamaytiradi, lekin ularning real vaqtli ishlashi uchun kuchli hisoblash resurslari kerak bo'ladi.**



ISSN 3030-3907

– **Gibrid yondashuv (AI + An’anaviy IDS/IPS) eng samarali natija beradi.**

**AI asosidagi IDS tizimlari bilan tajribalar va natijalar**

LSTM asosida IDS tajribasi:

- **Ma’lumotlar manbai**: CIC-IDS-2017 dataset;
- **Model**: 3 qatlamli LSTM tarmog‘i;
- **Natija**: 96.8% aniqlik, hujumlarning 97% aniqlangan;
- **Ustunliklari**: LSTM vaqt bo‘yicha o‘zgaruvchan hujumlarni yaxshi tushunadi;
- **Kamchiligi**: Real vaqtli ishlash uchun GPU resurslari kerak.

**CNN asosida IDS tajribasi:**

- **Ma’lumotlar manbai**: UNSW-NB15 dataset;
- **Model**: 2D CNN (Convolutional Neural Network);
- **Natija**: 97.2% aniqlik, FP faqat 2.9%;
- **Ustunliklari**: Patternlar asosida hujumlarni tez aniqlash;
- **Kamchiligi**: Sekin rivojlanayotgan hujumlarni (APT - Advanced Persistent Threats) yaxshi tahlil qila olmaydi.

**Transformer asosida tajriba (BERT):**

- **Ma’lumotlar manbai**: KDD CUP 99;
- **Model**: Transformer (BERT);
- **Natija**: 98.5% aniqlik, FP 1.7% gacha tushdi;
- **Ustunliklari**: Yangi va noma’lum hujumlarni ham aniqlash qobiliyatiga ega;
- **Kamchiligi**: O‘qitish uchun ko‘proq vaqt va resurs talab qilinadi.

**Xulosa**

Tarmoq xavfsizligini ta’minlash zamonaviy kiberxavfsizlik strategiyalarining muhim qismidir. An’anaviy Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) tizimlari hujumlarni signatura va qoida asosida aniqlaydi. Biroq, ushbu yondashuv noma’lum hujumlarga qarshi zaif bo‘lib, yangi kiberhujumlarni o‘z vaqtida aniqlay olmasligi sababli kamchiliklarga ega. Shuningdek, an’anaviy IDS/IPS tizimlarida noto‘g‘ri ijobiy (False Positive, FP) va noto‘g‘ri salbiy (False Negative, FN) natijalar yuqori bo‘lishi muammosiga duch kelinadi.

Sun’iy intellekt (AI) va mashinani o‘rganish (ML) asosidagi yondashuvlar tarmoq xavfsizligini ta’minlashning yangi samarali usulini taklif qiladi. Ushbu texnologiyalar anomaliyalarni avtomatik ravishda aniqlash, yangi hujum turlarini tanib olish va hujumlarni oldindan bashorat qilish imkoniyatiga ega. Tajribalar shuni ko‘rsatdiki, AI yondashuvlari, ayniqsa, chuqur o‘rganish modellaridan foydalangan holda hujumlarni aniqlash samaradorligini sezilarli oshiradi.



ISSN 3030-3907

Xulosa qilib aytganda, sun’iy intellekt yordami bilan tarmoq hujumlarini aniqlash va oldini olish kelajakdagi eng muhim yo‘nalishlardan biri bo‘lib qolmoqda. Ushbu yondashuvlar kiberxavfsizlikni oshirishga yordam beradi, biroq ularni samarali qo‘llash uchun moslashuvchan strategiyalar va resurslarni optimallashtirish zarur.

## FOYDALANILGAN ADABIYOTLAR

1) Stallings, W. (2020). *Network Security Essentials: Applications and Standards*. Pearson Education.
2) Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
3) Peng, T., Leckie, C., & Ramamohanarao, K. (2017). "Survey of network-based defense mechanisms countering the DoS and DDoS problems." *ACM Computing Surveys*, 39(1).
4) Conti, M., Dragoni, N., & Lesyk, V. (2016). "A survey of man in the middle attacks." *IEEE Communications Surveys & Tutorials*, 18(3), 2027-2051.
5) OWASP Foundation. (2023). *OWASP Top 10 Security Risks*. https://owasp.org/www-project-top-ten/
6) Amoroso, E. (2019). *Cyber Attacks: Protecting National Infrastructure*. Elsevier.
7) Scarfone, K., Mell, P. (2022). "Guide to Intrusion Detection and Prevention Systems (IDPS)." *NIST Special Publication 800-94*.
8) Splunk Inc. (2023). *SIEM: Security Information and Event Management Overview*. https://www.splunk.com/
9) ISO/IEC 27001. (2022). *Information security management systems – Requirements*. ISO Standards.
10) Shone, N., Ngoc, T., Phai, V. D., & Shi, Q. (2018). "A deep learning approach to network intrusion detection." *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41-50.
11) Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
12) Peng, T., Leckie, C., & Ramamohanarao, K. (2017). *Survey of network-based defense mechanisms countering the DoS and DDoS problems.* ACM Computing Surveys.
13) Conti, M., Dragoni, N., & Lesyk, V. (2016). *A survey of man in the middle attacks.* IEEE Communications Surveys & Tutorials.
14) Amoroso, E. (2019). *Cyber Attacks: Protecting National Infrastructure*. Elsevier.



ISSN 3030-3907

15) OWASP Foundation. (2023). *OWASP Top 10 Security Risks*. https://owasp.org/www-project-top-ten/
16) Scarfone, K., Mell, P. (2022). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94.
17) Bace, R., & Mell, P. (2001). Intrusion Detection Systems (IDS). National Institute of Standards and Technology (NIST).
18) Axelsson, S. (2000). Intrusion Detection Systems: A Survey and Taxonomy. ACM Computing Surveys.
19) Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy.
20) Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication.
21) Liao, H., Lin, C., Lin, Y., & Tung, K. (2013). Intrusion Detection System: A Comprehensive Review. Journal of Network and Computer Applications.
22) Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network Anomaly Detection: Methods, Systems and Tools. IEEE Communications Surveys & Tutorials.
23) Denning, D. E. (1987). "An Intrusion-Detection Model". IEEE Transactions on Software Engineering.
24) Bishop, C. M. (2006). "Pattern Recognition and Machine Learning". Springer.
25) Breiman, L. (2001). "Random forests". Machine Learning.
26) Cortes, C., & Vapnik, V. (1995). "Support-vector networks". Machine Learning.
27) Goodfellow, I., Bengio, Y., & Courville, A. (2016). "Deep Learning". MIT Press.
28) Chandola, V., Banerjee, A., & Kumar, V. (2009). "Anomaly Detection: A Survey". ACM Computing Surveys.



ISSN 3030-3907