O‘ZBEKISTON RESPUBLIKASI

OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

FARG‘ONA DAVLAT UNIVERSITETI

FarDU.
ILMIY
XABARLAR

1995-yildan nashr etiladi
Yilda 6 marta chiqadi

4-2025

ANIQ FANLAR

НАУЧНЫЙ
ВЕСТНИК.
ФерГУ

Издаётся с 1995 года
Выходит 6 раз в год

MUNDARIJA

MATEMATIKA

FIZIKA-TEXNIKA

MATEMATIKA

FarDU. Ilmiy xabarlar – Scientific journal of the Fergana State University

Volume 31 Issue 4, 2025-yil DOI: 10.56292/SJFSU/vol31_iss4/a106

UO'K: 004.89:004.93'1

NEYRON TARMOQLAR YORDAMIDA ANOMALIYALARNI ANIQLASH TIZIMINI LOYIHALASHTIRISH

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

DESIGNING AN ANOMALIES DETECTION SYSTEM USING NEURAL NETWORKS

Umarov Shuxratjon Azizjonovich

Farg'ona davlat texnika universiteti "Dasturiy injiniring va kiberxavfizlik" kafedrasi dotsenti, fizika-matematika fanlari bo'yicha falsafa doktori (PhD)

Annotatsiya

Ushbu maqolada ma'lumotlar uzatish tarmoqlarida anomaliyalarni aniqlashning neyron tarmoqlari asosida aniqlash tizimini sxemasini ishlab chiqishning nazariy asoslari yoritilgan. Anomaliyalarni aniqlashning integrallashgan tizimi arxitekturasi taklif qilingan va real vaqtda anomaliyalarni aniqlash mexanizmlari tahlil qilingan. Nazariy tahlillar va amaliy tajribalar asosida neyron tarmoqli anomiyalarni aniqlash tizimlari IDS, Snort, Real Secure tizimlariga nisbatan yuqori samaradorligi aniqlangan.

Аннотация

В статье описаны теоретические основы разработки схемы системы обнаружения на основе нейронных сетей для обнаружения аномалий в сетях передачи данных. Предложена архитектура интегрированной системы обнаружения аномалий и проанализированы механизмы обнаружения аномалий в реальном времени. На основе теоретического анализа и практических экспериментов установлено, что системы обнаружения аномалий на основе нейронных сетей более эффективны, чем системы IDS, Snort и Real Secure.

Abstract

The article describes the theoretical basis for developing a detection system scheme based on neural networks for detecting anomalies in data transmission networks. The architecture of an integrated anomaly detection system is proposed and the mechanisms for detecting anomalies in real time are analyzed. Based on the theoretical analysis and practical experiments, it is established that anomaly detection systems based on neural networks are more effective than IDS, Snort and Real Secure systems.

Kalit so'zlar: *axborot xavfsizligi, anomaliyalarni aniqlash, neyron tarmoqlar, interaktiv model, seansli model, Counterpropagation, tarmoq trafigi, IDS.*

Ключевые слова: *информационная безопасность, обнаружение аномалий, нейронные сети, интерактивная модель, сеансовая модель, контрраспространение, сетевой трафик, IDS.*

Key words: *information security, anomaly detection, neural networks, interactive model, session model, counter-proliferation, network traffic, IDS.*

KIRISH

So'nggi yillarda anomaliyalarni aniqlash usullari va vositalari axborotni himoya qilish sohasidagi turli maqsadli dasturlarda muhim o'rin egallab kelmoqda. Ushbu usullar ilgari uchramagan noma'lum hujumlarni aniqlash imkonini beriganligi uchun soha mutaxassislari bu yo'nalishga katta e'tibor qaratmoqda. Bu esa, o'z navbatida, himoyaning oldini olish strategiyasini ishlab chiqarishda va amalga oshirishda asosiy talablardan biriga aylanmoqda. Anomaliya deganda ob'ektning normal, ruxsat etilgan modelidan tizim foydalanuvchisi ishtiroki yoki tarmoq faolligi asosida har qanday chetga chiqish harakati tushuniladi.

Anomaliyalarni aniqlash vazifasini formal qo'yilishi quyidagicha bo'ladi: axborot tizimi tomonidan ma'lum cheklangan T vaqt davomida qayta ishlanadigan kirish ma'lumotlari D to'plami orqali belgilanadi. Bu T vaqt chekli bo'lganligi sababli, D to'plam ham chegaralangan bo'ladi. D to'plamni ikkita A va B qism to'plamdan iborat deb qaraladi: A to'plam - anomaliya yoki hujum

deb hisoblanadigan ma'lumotlar, B to'plam esa tizim uchun xavfsiz deb hisoblanadigan ma'lumotlar bo'lsin. Demak,

$$A \subset D, B \subset D,\ A \cap B = \varnothing, A \cup B = D.$$

B to'plamining barcha elementlari anomaliyalarni tahlil qiluvchi tizimlarning bilimlar bazasiga kiritilgan bo'lishi kerak. Turli hujumlar haqidagi ma'lumotlarni o'z ichiga olgan A to'plamining elementlari avvaldan bilimlar bazasida bo'lmaydi. O'z navbatida, B to'plamni ob'ektning xarakteristkasini, ya'ni foydalanuvchi harakatlari, tarmoq faolligini tavsiflovchi $B_1,...,B_n$ turli kichik to'plamlarga ajratish mumkin, ular ruxsat etilgan modelning shablonlari deb ham yuritiladi.

$$B = \bigcup_{i=1}^{n} B_i$$

Agar ob'ektning foydalanuvchi harakatlari, tarmoq faolligi ruxsat etilgan modeli aniq formallashtirilgan va hujumning aniqlash tizimining bilimlar bazasida to'liq mavjud bo'lsa, u holda nazariy jihatdan 1- va 2-tur xatolarini paydo bo'lish ehtimoli nolga teng bo'ladi. Lekin, zamonaviy axborot tizimlarining murakkabligiga bog'liq bo'lgan real cheklanishlar paydo bo'ladi, bu esa B to'plam elementlarining yetarlicha to'liq va aniq formallashtirilmasligiga olib keladi.

MATERIALLAR VA USULLAR

Amalda turli foydalanuvchilarning tarmoq faolligining ruxsat etilgan faoliyatining barcha mumkin bo'lgan variantlarini hisobga oladigan bunday universal anomaliyalarni aniqlash tizimini yaratish imkonsiz bo'lganligi sababli, vazifa quyidagi yo'llar bilan hal qilinishi mumkin:

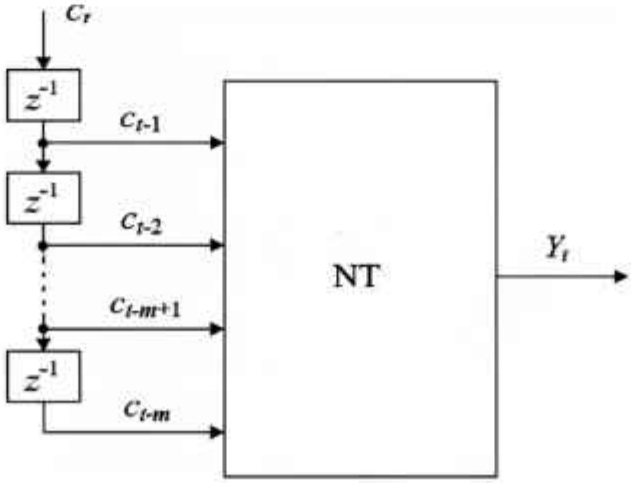
1) Ko'p sonli foydalanuvchilarning tarmoq trafiklarining ruxsat etilgan harakatlarini tahlil qilish o'rniga, muayyan tizimdagi individual foydalanuvchilarning tarmoq trafigining harakatlarini modellashtirish orqali.

2) Foydalanuvchining trafigining normal harakatini mumkin bo'lgan variantlarini normal shaklda tavsiflash va ruxsat etilgan faoliyatning bir qator misollar ko'rinishidagi harakat shablonlarini tahlil qilish orqali.

Keltirilgan holatlar aynan bir server yoki ish stansiyasida joylashgan va real yoki o'zgaruvchan kirish ma'lumotlari asosida individual foydalanuvchining tarmoq trafigining harakatlari xususiyatlariga moslashtiriladigan neyron tarmoqli anomaliyalarni aniqlash tizimlarini qurish uchun asos bo'ladi.

Quyida foydalanuvchi harakatlarining kompleks modelini qurishga asoslangan neyron tarmoqli anomaliyalarni aniqlash tizimini yaratishga loyihaviy yondashuv taklif etiladi. Ushbu yondashuvdagi model mos ravishda foydalanuvchi harakatining dinamik va statistik xossalarini hisobga oluvchi interaktiv va seansli qismlardan iborat.

Interaktiv model – foydalanuvchi ish vaqtidagi anomal faoliyatni aniqlash uchun ishlatiladi. Axborot tizimining har bir foydalanuvchisi uchun avvalgi harakatlari (buyruqlari) asosida uning keyingi harakatlarini (buyruqlarini) bashoratlash uchun neyron tarmoq quriladi va bazasi boyitiladi (o'qitiladi) (1-rasm).



1-rasm. Foydalanuvchi harakatlarining interaktiv modeli

Bunda neyron tarmoq ko'p qatlamli perseptron sifatida ishlatiladi, bunda t vaqt momentidagi ish natijasi quyidagi ifoda bilan aniqlanadi:

$$Y_t = F(X_t),\ X_t = (c_{t-1}, c_{t-2}, \ldots, c_{t-m})^T,$$

bu yerda $F(\ )$ - neyron tarmoq tomonidan amalga oshiriladigan nochiziqli o'zgartirish, c_i - seansning i-buyrug'i; m - avvalgi buyruqlar soni.

Seansli model esa butun seans davomidagi foydalanuvchining noodatiy faoliyatini aniqlash uchun mo'ljallangan bo'lib, buning uchun statistik ma'lumotlar to'plamidan foydalanadi. O'qitilgan neyron tarmoq bu holatda foydalanuvchining faolligi uning avval qurilgan harakatlari modeliga qanchalik mos kelishini aniqlaydi. Seansli modelni amalga oshirishda neyron tarmoqning kirish ma'lumotlari sifatida quyidagilar olinadi:

c_i - i-seansdagi buyruqlar soni;

o_i - interaktiv modelning prognoz qilingan buyruqlari foiz nisbati;

h_i - kompyuter raqami;

d_i - i-seansning davomiyligi;

s_i - i-seansning boshlanish vaqti ($i = 1,2,\ldots,N$).

Seansli model uchun neyron tarmoqning chiqishi quyidagi funksiya bilan hisoblanadi:

$$Y_t = F(X_t),\ X_t = (c_i, o_i, h_i, d_i, s_i)^T$$

bu yerda $F(\ )$ - yuqorida ko'rsatilgan c_i, o_i, h_i, d_i, s_i o'zgaruvchilarga nisbatan nochiziqli o'zgartirish funksiyasi.

Bunda neyron tarmoq chiqishi ikkita qiymatni qabul qilishi mumkin: 1 - foydalanuvchining normal harakati uchun va 0 - anomal harakat uchun. Bashorat bo'yicha, foydalanuvchining har bir ish seansi uchun alohida audit fayli yaratiladi: unda quyidagi ma'lumotlar yozib boriladi: buyruqni ishga tushirish vaqti / buyruq identifikatori / buyruq nomi / boshlanish yoki tugash belgisi. Buyruqlarni kodlashda bir xil buyruqlarga bir xil qiymatlar mos kelishini ta'minlash muhimdir. Shu maqsadda kompleks modelning interaktiv qismi uchun har bir foydalanuvchi bo'yicha yig'ilgan ma'lumotlar asosida ko'rsatilgan vaqt davomida foydalanuvchi tomonidan kiritilgan buyruqlar to'plami tuziladi. So'ngra har bir buyruqqa tegishli o'nlik son beriladi, bu son keyinchalik audit fayllarini buyruqlar ketma-ketligiga aylantirishda ishlatiladi. Natijada har bir foydalanuvchi uchun quyidagi ma'lumotlar to'plami tuziladi:

$$\{c_j^i\},\quad i = 1,2,\ldots,N;\quad j = 1,2,\ldots,N_i,$$

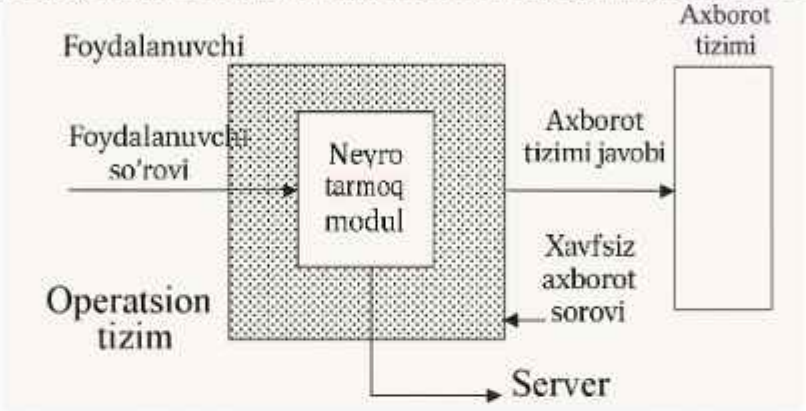
bu yerda c_j^i - i-seansda kiritilgan j-buyruq raqami; N_i - i-seansdagi umumiy buyruqlar soni; N - seanslar soni.

Neyron tarmoqlaridan tarmoq trafigidagi anomaliyalarni aniqlash uchun tizimi quyidagi vazifalarni hal qilishga imkon beradi:

1. Ethernet tarmog'i segmentining tarmoq trafigini ushlab olish;
2. TCP/IP protokollar steklari paketlarining mazmunini dekodlash;
3. Dekodlangan paket asosida statistik ko'rsatkichlarni shakllantirish;
4. ART2M adaptiv neyron tarmoqlarini qo'llash va vektorlarni klasterlash yo'li bilan tarmoq trafigi profillarini shakllantirish;
5. O'qitish jarayonida shakllangan klasterlardan ko'rsatkichlar vektorlarining chiqishi asosida anomal tarmoq faolligini aniqlash;
6. Modelning dasturiy komponentlari faoliyati to'g'risida statistik ma'lumotlarni yig'ish.

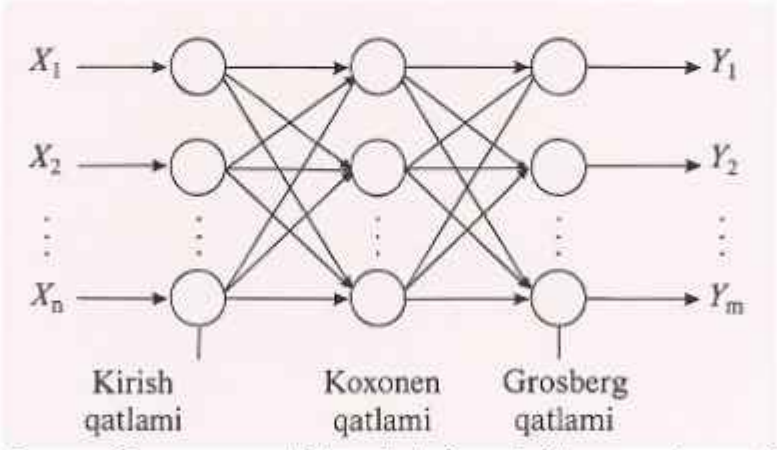
Paketlarni ushlab olish uchun LIBPCAP kutubxonasi funksiyalaridan foydalaniladi. Har bir kadr sana, vaqt va kadr uzunligini ifodalovchi sarlavha bilan birga qayd qilinadi. Dekodlash moduli ko'rsatkichlar vektorini shakllantiradi. Parametrlar sifatida qaysi tarmoq osti paketlarini tahlil qilish manzili, MAC va IP manzillarining ruxsat etilgan TCP va UDP port raqamlaridan foydalaniladi. Hosil bo'lgan vektorning koordinatlari paketlar nuqtasi va berilgan vaqt oralig'idagi paket parametrlari qiymatlarining o'rta arifmetigidan iborat. Jami statistik

ko'rsatkichlar vektori 20 ta koordinatani o'z ichiga oldi: 1-3. Vaqt birligidagi kiruvchi va chiquvchi IP-paketlar soni. 4-6. Vaqt birligidagi kiruvchi va chiquvchi TCP-paketlar soni. 7-9. Vaqt birligidagi kiruvchi va chiquvchi UDP-paketlar soni. 10. Vaqt birligidagi hal etilmagan UDP portlariga so'rovlar soni. 11-12. Vaqt birligidagi tugallangan va tugamagan UDP protokoli bo'yicha so'rovlar soni. 13. Vaqt birligidagi javob vaqti tugagan va tugamagan UDP protokoli bo'yicha so'rovlar soni. 14-15. Vaqt birligidagi portlarga TCP so'rovlari soni. 16-18. Vaqt birligidagi o'rnatish holatidagi SYN SEND bo'lgan TCP ulanishlari soni, bunda ochiq holat - ESTABLISHED, yopiq holat -FINWAIT. 19. TCP protokolining ruxsat etilgan portlariga so'rovlar sonining ushbu protokolning barcha portlariga so'rovlar soniga nisbati. 20. TCP ulanishlari sonining umumiy ulanishlar soniga nisbati. Keltirilgan tahlil asosida istiqbolli integratsiyalashgan anomayalarni aniqlash tizimi arxitekturasi quyidagicha bo'ladi (2-rasm).



2-rasm. Integratsiyalashgan anomayalarni aniqlash tizimi

Ko'rib chiqilayotgan kombinatsiyalashgan hujumlarni aniqlash usulining o'ziga xosligi shundaki, neyron tarmoqga kirish ma'lumotlarini tanish va ularni $n = K + 1$ ta mumkin bo'lgan sinflardan biriga ajratish vazifasi yuklatiladi. Bular hujumlar sinflari yoki xavfsiz ma'lumotlar sinfi bo'lishi mumkin.



3-rasm. Qarama-qarshi tarqalishning gibrid neyron tarmog'i

Turli xildagi neyron tarmoqlarning xususiyatlarini qiyosiy tahlil qilish shuni ko'rsatdiki, ma'lumotlarni qayta ishlashning eng yaxshi natijalari qarshi tarqalishning gibrid neyron tarmog'i (Counterpropagation network) yordamida olinishi mumkin. Ushbu tarmoq kirish qatlamidan tashqari 2 ta qatlamning ketma-ket ulanishidan iborat: Koxonen qatlami va Grossberg qatlami (3-rasm).

MUHOKAMA VA NATIJALAR

Gibrid tarmoqni o'qitish ikki bosqichda amalga oshiriladi. Birinchi bosqichda Koxonen qatlami o'qitiladi. Bu holatda "o'qituvchisiz" o'qitish algoritmi va "G'olib hamma narsaga ega bo'ladi" tamoyili qo'llaniladi. Ushbu algoritmning mohiyati kirish vektorining $X_1,\ldots,X_m$ komponentlarini Koxonen qatlami neyronlari bilan bog'lovchi shunday sozlashdan iboratki, berilgan kirish vektori uchun ushbu qatlamning faqat bir neyroni chiqishda mantiqiy bir ("neyron-g'olib") bo'ladi, qolgan barcha neyronlar esa nolga teng bo'ladi. Yakunda, o'qitish jarayoni tugagandan so'ng, Koxonen

qatlami tanish funksiyasini bajaradi, ya'ni kirish vektori X ning hujum mavjudligi yoki yo'qligi belgilari bilan tavsiflanadigan u yoki bu klasterga tegishliligi haqida xulosa beradi.

Ikkinchi bosqichda Grossberg qatlamining bog'lanish vaznlari sozlanadi. Ushbu qatlam "o'qituvchi bilan" o'qitiladi va Koxonen qatlamining hosil bo'lgan tasodifiy chiqishini neyron tarmoqli klassifikator chiqishlariga aylantirish uchun xizmat qiladi. Bunda barcha qatlamlar emas, balki faqat Koxonen qatlamining neyron-g'oliblari bilan bog'langanlari o'zgartiriladi. Qarama-qarshi tarqalish tarmog'ining afzalligi uning umumlashtirish qobiliyatidir. Neyron tarmoqni o'qitish jarayonida kirish vektorlari tegishli chiqish vektorlari bilan bog'lanadi, bunda tarmoqning umumlashtirish qobiliyati hatto to'liq bo'lmagan yoki buzilgan kirish vektori holatida ham to'g'ri chiqishni olishga imkon beradi. Integratsiyalashgan neyron tarmoqli anomaliyalarni aniqlash tizimi dasturiy modulini amalga oshirish uchun asosiy platforma sifatida Apache 1.3 www-serveri tanlandi. Foydalanuvchi va www-server o'rtasidagi almashinuv HTTP 1.1 murakkab amaliy daraja protokoli orqali amalga oshirildi. Axborot tizimi xavfsizligini ta'minlash uchun CGI va Cookie o'zgaruvchilarining ruxsat etilgan qiymatlarini nazorat qilish zarur deb qabul qilindi.

Neyron tarmoqning kirishlar soni m×4=9×4=36 ga teng deb qabul qilinadi, ya'ni nazorat qilinadigan 9 ta o'zgaruvchining har biri 4 ta mumkin bo'lgan qiymatdan birini qabul qilishi mumkin. Tarmoq chiqishlari soni soddalashtirish uchun tarmoq chiqishida foydalanuvchining xavfsiz ishlashi uchun "1" va hujum holatida "0" olinadi. Aslida, tarmoqning ancha moslashuvchan ish logikasi qo'llanildi:

- Y≥0.7 - "hujum yo'q";
- Y≤0.3 - "hujum mavjud";
- 0.3<Y<0.7 - xato qaror (1- yoki 2-turdagi xatolar).

Taqqoslash uchun, neyron tarmoqli anomaliyalarni aniqlash tizimidan tashqari, keng tarqalgan hujumlarni aniqlash tizimlari Snort va Real Secure Network Sensor skanerlash usuli bilan testdan o'tkazildi (1-jadval).

1-jadval

Anomaliyalarni aniqlash tizimini skanerlash natijalarining qiyosiy jadvali

Turi	Umumiy hujumlar soni	To'g'ri aniqlangan hujumlar soni	2-turdagi xato ehtimolligi	Umumiy xavfsiz so'rovlar soni	Soxta ishoralar soni	1-turdagi xato ehtimolligi
Nessus skanerlash						
Neyron tarmoqli AAT	1247	1149	0,08	132	7	0,05
Real Secure Network Sensor	1247	732	0,41	132	3	0,02
Snort	1247	821	0,34	132	24	0,18
Nikto skanerlash						
Neyron tarmoqli AAT	3125	2986	0,04	83	8	0,10
Real Secure Network Sensor	3125	1029	0,67	83	2	0,02
Snort	3125	936	0,70	83	13	0,16
XSpider skanerlash						
Neyron tarmoqli AAT	732	707	0,03	62	12	0,19
Real Secure Network Sensor	732	632	0,14	62	3	0,05
Snort	732	548	0,18	62	5	0,08

XULOSA

Jadvaldan ko'rinib turibdiki, hujumlarni aniqlashning kombinatsiyalashgan usulini qo'llagan neyron tarmoqli anomaliyalarni aniqlash tizimi klassik anomaliyalarni aniqlash tizimilarga nisbatan xato qarorlar qabul qilish ehtimolini 4-5 marta kamaytirishni ta'minlaydi.

Nazariy tajribalar natijalariga ko'ra neyron tarmoq signaturali analizatorga alternativa emas, balki tarmoq trafigining statistik xossalarini sezilarli darajada buzuvchi, vaqt bo'yicha taqsimlangan hujumlarni aniqlash uchun unga qo'shimcha sifatida qo'llanilishi kerak.

Bajarilgan nazariy tadqiqotlarning natijalari shuni ko'rsatadiki, signaturalarni qidirish usulidan asosiy usul sifatida foydalanilganda foydalanuvchining xavfsiz harakatlari shablonlari to'plamini qo'shish 2-turdagi xato ("hujumni o'tkazib yuborish") paydo bo'lish ehtimolligining o'zgarishiga olib kelmaydi. Shuningdek, hujumlarning "noaniq" tavsifi bilan signaturalarni qidirish usulidan foydalanilganda foydalanuvchining xavfsiz harakatlarining aniqlovchi shablonlari sonining oshishi 1-turdagi xato ("soxta hujum") paydo bo'lish ehtimolligining kamayishiga olib keladi.

ADABIYOTLAR RO'YXATI

1. Акбаров Д. Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши //Ўзбекистон маркаси. – 2009. – Т. 432.
2. Мухториддинов М., Акбаров Н., Умаров Ш. Machine learning for network security and anomaly detection //Conference on Digital Innovation:" Modern Problems and Solutions. – 2023.
3. Umarov Sh. A. Axborot xavfsizligining intellektual tizimlarini qurish asoslari. //Buxoro davlat universiteti ilmiy axboroti. – 2024. №2. 9-16-bet
4. Бурляев Г. И., Ляликова В. Г. Системы обнаружения вторжений с использованием iot-технологий //Вестник науки. – 2024. – Т. 4. – №. 12 (81). – С. 1558-1562.
5. Ghimire S. et al. Probabilistic-based electricity demand forecasting with hybrid convolutional neural network-extreme learning machine model //Engineering Applications of Artificial Intelligence. – 2024. – Т. 132. – С. 107918.
6. Саиег Т. Х. Анализ комплексного метода предотвращения обхода систем обнаружения вторжения (IDS) //Инновационная наука. – 2023. – №. 11-1. – С. 54-57.
7. Umarov Sh.A., Umarova M.I. Neyro-noravshan va modulli neyron tarmoq hujumlarini aniqlash tizimlarini qurish. // Buxoro davlat universiteti ilmiy axboroti. – 2025. №6. 292-297-bet
8. Chalapathy R., Chawla S. Deep learning for anomaly detection: A survey //arXiv preprint arXiv:1901.03407. – 2019.
9. Wang S. et al. Machine learning in network anomaly detection: A survey //IEEe Access. – 2021. – Т. 9. – С. 152379-152396.
10. Васильева К. В., Лаврова Д. С. Обнаружение аномалий в киберфизических системах с использованием графовых нейронных сетей //Проблемы информационной безопасности. Компьютерные системы. – 2021. – №. 1. – С. 117-130.