MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

2-SON 1(2)
2023-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O’ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG’ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
Chop etish tili: O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2023 yil, Tom 1, №2
Vol.1, Iss.2, 2023 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O’zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro’yxatdan o’tgan.

Tahririyat manzili:
151100, Farg‘ona sh., Aeroport ko‘chasi 17-uy, 201A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz
Qo‘lyozmalar taqrizlanmaydi va qaytarilmaydi.

FARG’ONA - 2023 YIL

TAHRIR HAY'ATI

Jurnal quyidagi bazalarda indekslanadi:

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

KIBER TAHDIDLARNI BASHORAT QILISH VA XAVF-XATARLARDAN HIMOYALANISHDA SUN’IY INTELEKT IMKONIYATLARIDAN FOYDALANISH

D.X.Tojimatov,
katta o‘qituvchi, TATU Farg’ona filiali

Annotatsiya. Ushbu maqolada korxona tashkilotlarning axborot tizimlariga bo‘ladigan tahdidlarni erta aniqlashda sun’iy intelekt (AI) imkoniyatlaridan foydalanib vujudga kelishi yuqori bo‘lgan favqulotda holatlar va kiber hujumlarni oldini olish usullari taklif etilgan. Maqloda tabiiy va sun’iy tahdidlarni ehtimoliy kelib chiqishini tahlil qilish, tahdidni ajratib olish, darajasini aniqlash, qaror qabul qilish funksiyalarini qamrab olgan aqlliy himoya tizmini ishlab chiqish uchun muhum elementlar keltirilgan.

Kalit so‘zlar: kiber hujum, favqulotda vaziyat, geofizik hodisa, geologik hodisa, tahdid, kiberjinoyatchi, aqlliy himoya tizimi, Mashinani oqitish (ML), hacker, firewall.

Kirish. Ma’lumki tahdidlar tabiiy va sun’iy turlarga bo‘linadi. Axborot xavfsizligi sohasida tahdidlarni o‘rganish juda muhum hisoblanib, korxona va tashkilotlarga bo‘ladigan ehtimoliy zararlarni bartaraf etish aynan tahdidni aniqlash va uni darajasini to‘g‘ri baholagan holda ta’sirini kamaytirishga bog‘liq.

Tabiiy tahdid tabiat hodisalari tufayli vujudga kelishi ehtimolligi yuqori bo‘lgan favqulotda vaziyatni keltirib chiqaradigan jarayon hisoblanadi. Tabiiy xavf manbalari (tashuvchilari) litosfera, gidrosfera, atmosfera va kosmosning turli xil noqulay tabiiy jarayonlar sodir bo‘ladigan va xavfli tabiat hodisalarining yuzaga kelishi mumkin bo‘lgan qismlaridir.

Tabiiy favqulodda vaziyatlarning manbalari bo‘lgan xavfli tabiat hodisalarini quyidagilarga bo'lish mumkin:

- xavfli geofizik hodisalar (zilzilalar, vulqon otilishi);
- xavfli geologik hodisalar (ko‘chkilar, eroziya, qiyaliklarning yuvilishi, qurumlar);
- xavfli gidrometeorologik hodisalar, shu jumladan meteorologik (bo‘ronlar, dovullar, tornadolar, juda kuchli qor, jala, yomg‘ir, tumanlar, qattiq sovuq, issiqlik), agrometeorologik (ayozlar, quruq shamollar, tuproq va atmosfera qurg‘oqchiligi), gidrologik (suv toshqini, muzliklar, tirbandliklar, sellar), dengiz gidrologik va geliogeofizik xavflar (kuchli magnit bo‘ronlar, qisqa to'lqinli aloqaning uzilishi bilan ionosferada kuchli buzilish radiatsiyaviy vaziyat) va asteroid-kometa xavfi;
- tabiiy yong‘inlar[1].

Odatda tabiiy tahdidlar kiber tahdid hisoblanmaydi ammo favqulotda vaziyat sodir bo‘lganda uning korxona-tashkilotlarning axborot tizimlari uchun keltiradigan zarari kiber hujumnikidan ancha yuqori bo‘lishi mumkun.

Tabiiy tahdidlar axborot tizimlariga tog‘ridan-to‘g‘ri tasiri kam hisoblanib, asosan tizim o‘rnatilgan qurilmalarni vayron qilish orqali zarar keltiradi. Shu sababli xavfsizlik tizimlarini ishlab chiqishda tabiiy tahdidlarni aniqlash va favqulotda vaziyatni oldini olishga qaratilgan chora tadbirlar ko‘rilishi maqsadga muofiq hisoblanadi.

Sun’iy tahdidlar bevosita shaxsga bog‘liq bo‘lib, tasodifiy yoki qasddan uyushtirilgan tahdidlar turlariga bo‘linadi.

Tasodifiy tahdidlar ehtiyotsizlik, beparvolik, bilimsizlik, sinalmagan hodimni ishga qabul qilish, texnik va dasturiy tizimlardagi xatolik tufayli vujudga keladi. Bunday tahdidlar maqsadsiz hisoblanib korxona-tashkilot uchun keltiradigan zararini oldindan aniqlash qiyin hisoblanadi[2].

Qasddan uyushtirilgan tahdidlar aniq maqsadga qaratilgan bo‘lib, ichki va tashqi tahdid turlariga bo‘linadi. Ichki tahdidlarga asosan yollanma josuslar, qasd olish maqsadidagi hodim havflari kiradi. Tashqi tahdidlarga esa ehtimoliy kiber hujumlar va kompyuter viruslari havfi kiradi. Qasddan uyushtirilgan tahdidlar korxona-tashkilot axborot tizimlarini yo‘q qilish, barqaror ishlashini izdan chiqarish, ma’lumotlarni o‘girlash, nusxa ko‘chirish, o‘zgartirish kabi maqsadlarga qaratilgan bo‘ladi[5].

Tahdidlarni erta aniqlash va ta’sirini kamaytirish usullarini quyidagicha bayon qilishimiz mumkun. Har qanday qimmatli aktivga ega korxona tashkilorlar axborot tizimlarini potensial tahdidlardan

https://doi.org/10.5281/zenodo.7979307

https://journals.indexcopernicus.com/search/article?articleId=3609129

himoyalashda turli fizik va apparat-dasturiy vositalardan foydalangan holda xavfsizlik usullaridan foydalanishadi. Fizik himoya usullari va vositalariga misol tariqasida qo‘riqlanadigan (sim to‘siq, balan beton devor) hudud, bardoshli obekt (bino), qo‘riqlash hizmati (qorovul, xavfsizlik hodimi), kuzatuv kameralari, signalizatsiya vositalari, axborot tizimi uchun alohida ajratilgan himoyalangan xona, eshik qulflari, o‘t o‘chirish vositalari, vintelatsiya vositalari, isitish yoki sovitish tizimlari kiradi. Apparat-dasturiy vositalar bevosita axborot tizimlari va u o‘rnatilgan kompyuterlarga bog‘lanadi. Bularga tarmoqlararo ekran vositalari, tarmoq marshrutizatorlari, komutatorlar, antivirus dasturlari, tarmoq analizatorlari, ddos hujumlariga qarshi vositalar va axborot tizimida foydalaniladigan kriptografik usullar, autentifikatsiya usullari, rollarga asoslangan usullarni misol sifatida keltirishimiz mumkun[3].

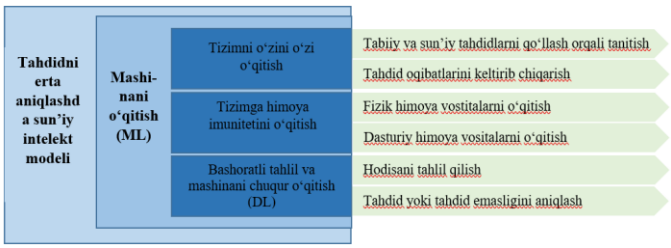
Axborotni tizimlarini himoyalashga qaratilgan barcha mavjud usullar hozirda bardoshli hisoblansada, ular tahdidlar avvaldan mavjud bo‘lgan hollarda yoki tahdid yuzaga kelganda uni aniqalash imkoniyatiga ega. Qolaversaga bunday vositalarni boshqarish inson omiliga bog‘liq bo‘lib qolmoqda. Bu esa axborot tizimlariga qaratilgan tahdid turlarini ajratib olish va himoya uchun usullarini tanlashda qaror qabul qilish vaqt yo‘qotilishiga olib keladi. Bazida to‘g‘ri himoya tizimlari tahdid ro‘y bergandan keyin o‘rnatiladi. Bungacha esa tahdidlar axborot tizimlariga zarar yetkazgan bo‘ladi. Hozirda hackerlar ko‘plab hujumlarda sun’iy intelektni keng qo‘llab kelmoqdalar. Bu mavjud tizimlarni bardoshlilik darajasini zaif holga keltirmoqda. Mashinani o‘qitish tizimlari orqali neyron tarmoqlar himoya tizimlarini mukkammal o‘rganadi va ularni zaif tamonlarini ochib beradi. Ayrim hollarda sohta tahdid yaratib himoya tizimlarini chalg‘itishga harakat qiladi[4].

Tahdidlarni erta aniqlash bizga tahdid turini hususiyatlarini o‘rganish, u keltirib chiqaradigan oqibatini baxolash va unga qarshi zaruriy choralarni ko‘rish imkoniyatini taqdim etadi. Lekin axborot tizimiga bo‘ladigan kiber tahdidlar sodir bo‘lishiga nisbatan ancha yuqori tezlikda amalga oshadi[6]. Chunki kompyuterda axborot almashuv va hisoblash tezligi inson omilidan yuqori hisoblanadi. Shu sababdan sun’iy intelekt orqali tahdidlarni erta aniqlash tahdidlarni turini tez va to‘g‘ri baholashga va ularga qarshi himoya vositalarini to‘g‘ri tanlashga yordam berishi mumkun. Bu albatta sun’iy intelekt imkoniyatlaridan foydalangan holda alohida aqlliy xavfsizlik tizimini ishlab chiqishni va bu tizimga korxona-tashkilotlarni axborot tizimlarini integratsiya qilishni talab qiladi.

Adabiyotlar tahlili va metodologiya. Maqolani yozishda kiber tahdidlarni bashorat qilish usullarini S.V.Gorbunov, E.S.Ermakovlarning “Методические подходы к прогнозированию тенденций угроз природного характера на долгосрочную перспективу” mavzusidagi va Nik Botsromning “Superintelligence Paths, Dangers, Strategies” mavzusidagi hamda D.Tojimatovning “Kiberxavfsizlik: tahdilar, muammolar, yechimlar” mavzusidagi maqolalaridan, kiberxavfsizlikda sun’iy intelektni qo‘llash prinsiplarini va yechimlarini S.A.Petronko, D.N.Biryukov, A.S.Petronkolarning “Умная кибербезопасность”, “Технологии больших данных Big Data в области информационной безопасности и ИИ” mavzularidagi va D.Tojimatovning “Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems” mavzusidagi maqolalari o‘rganib chiqilib, tahlil qilingan. Yuqorida nomi keltirilgan olimarni ilmiy maqolalaridan foydalanib iqtiboslar keltirilgan.

Natijalar. Masalani yechilishi

Yuqoridagi tahdid turlari va ularga qarshi himoya vositalaridan kelib chiqib tahdidlarni erta aniqlashda quyidagi sun’iy intelekt modeli taklif etiladi.



1-rasm. Tahdidni erta aniqlashda va unga qarshi qaror qabul qilishda sun’iy intelekt modeli.

Yuqoridagi model orqali sun’iy intelektdan foydalangan holda aqlliy himoya tizimini ishlab chiqilishi mumkun. Modelda quyidagi ketma-ketlikda ishlarni amalga oshirishga mo‘ljallangan.

1. Ishlab chiqiladigan himoya tizimini sinov axborot tizimiga integratsiya qilgan holda turli tabiiy va sun’iy tahdilar amalga oshiriladi. Sun’iy intelektni neyron tarmog‘i mashinani o‘qitish (ML) orqali barcha tahdidlarni tanib oladi. (Sinov jarayoni qancha uzoq muddatga

https://doi.org/10.5281/zenodo.7979307

https://journals.indexcopernicus.com/search/article?articleId=3609129

cho‘zilsa tizim shuncha ko‘p tahdidni tanib oladi).

2. Tahdidlarni tanib olish bilan bir paytda tahdid keltirib chiqaradigan oqibatlarni yozib boradi. (Bunda sinov axborot tizimiga turli ta’sirlar bo‘lishi mumkun: tizim o‘chib ketishi, zararlanishi vhkz. Bunday hollarda aqlliy himoya tizimini boshqa sinov axborot tizimi bilan integratsiya qilib borish tavsiya etiladi).
3. Aqlliy himoya tizimiga tahdidlarni bartaraf etishda fizik usullarni va vositalarni tanitish. (qulflar, signalizatsiya vositalari, o‘t o‘chiruvchi vositalar vhkzlar)
4. Aqlliy himoya tizimiga tahdidlarni bartaraf etishda dasturiy usullarni va vositalarni tanitish. (tarmoqlararo ekran, antiviruslar, ddos hujumidan himoya vositalari vhkzlar)
5. Axborot tizimi atrofida bo‘layotgan jarayon va hodisalarni tahli qilish (to‘plangan katta ma’lumotlarga bazasiga asoslanib).
6. Hodisa va jarayonlarni tahdid yoki tahdid emasligini aniqlash (to‘plangan katta ma’lumotlar bazasiga asoslanib).
7. Hodisa va jarayonlarni tahdid sifatida baxolanganda chora ko‘rish uchun tizim egasini ogoxlantirish.
8. Tahdid yuzaga kelish xavfi yuqori bo‘lganda yoki bevosita axborot tizimiga jiddiy zarar yetkazilishi aniqlanganda mustaqil himoya vositalarini qo‘llash.

Muxokama. Axborot tizimlariga bo‘ladigan tahdidlarni erta aniqlashda sun’iy intelekt imkoniyatlaridan foydalanib aqlliy himoya tizimini ishlab chiqishda quyidagi apparat-dasturiy vositalar va dasturlash tilidan foydalanish tavsiya etiladi.

Fizik tahdidlarni aniqlashda:

- issiqlik teplovisorlari;
- kuzatuv kameralari;
- xarakat datchiklari;
- ovozli signalizatsiya vositalari;
- namlik datchiklari;
- havo datchiklari;
- issiqlik datchiklari;
- elektron qulflar;
- lazer qurilmalari;
- ultrabinafsha nurli fonarlar;
- o‘rgatilgan jonivorlar;
- teleskop;
- o‘lchov vositalari.

Sun’iy tahdidlarni aniqlashda:

- 1-faktorli autentifikatsiya usullari (parollar, pin kodlar, kalit so‘zlar);
- 2-faktorli autentifikatsiya vositalari (uniklal hisoblangan jixozlar);
- 3-faktorli autentifikatsiya usullari (biometrik unikal a‘zolar);
- ekspert dasturlar;
- anitviruslar;
- firewallar (tarmoqlararo ekran);
- rezerv nusxalovchi dasturlar;
- xizmat ko‘rsatuvchi dasturlar;
- tarmoq analizatorlar;
- tarmoq skanerlari;
- tarmoq qurilmalari;
- kuzatuv kameralari;
- radio to‘lqin kuchaytiruvchi, so‘ndiruvchi vositalar.

Dasturlash tillari: Python, C++, Java.

Tavsiya etilgan vositalar korxona-tashkilot axborot tizimlariga bo‘ladigan tahdidlarni aniqlash va ularga qarshi choralarni qo‘llash uchun xizmat qiladi. Vosita va usullar axborot tizimlarini hususiyatlaridan kelib chiqib boyitilishi mumkun.

Xulosa. Izlanishlar natijasida shunday qarorga kelindi, hozirda axborot tizimlarini himoya qilishda mukammal aqlliy himoya tizimi mavjud emas. Ishlab chiqilgan tizimlar tahdid turlarini ortib borishi natijasida bardoshsiz bo‘lib qolmoqda. Yangi tahdidlarni inson omili tomonidan o‘rganib, tahlil qilinib, unga qarshi himoya vositalarini ishlab chiqilgunicha tahdid oqibatlari korxona-tashkilotlarning axborot tizimlariga ancha zarar yetkazmoqda. Taklif etilayotgan aqlliy himoya tizimi tahdidlarni maqolada keltirilgan sun’iy intelekt modeli yordamida o‘rganib o‘zida katta ma’lumotlar bazasini muntazam shakillantirib boradi va uning yordamida yangi tahdidlarni mavjud tahdidlar bilan solishtirgan holda o‘xshash husisiyatlariga qarab mavjud himoya vositalarini taklif etadi. Himoya vositalarini yangi tahdidga bardoshliligini baholaydi va kamchiliklarini mutaxassislarga ochib beradi.

Agar taklif etilayotgan model yordamida aqlliy himoya tizimi ishlab chiqilsa axborot tizimlari yo‘q qilinishi, ma’lumotlarini o‘g‘irlanishini oldi olinishi va ruxsatsiz kirishlarni bartaraf etishi mumkun.

Adabiyotlar ro‘yxati

[1]. С.В. Горбунов, Е.С. Ермакова: Методические подходы к прогнозированию

https://doi.org/10.5281/zenodo.7979307

https://journals.indexcopernicus.com/search/article?articleId=3609129

https://al-fargoniy.uz/

[2]. тенденций угроз природного характера на долгосрочную перспективу, Вестник Воронежского института ГПС МЧС России, №2(19), 2016.

[3]. Nik Botsrom: Superintelligence Paths, Dangers, Strategies, 2014.

[4]. С.А.Петренко, Д.Н.Бирюков, А.С.Петронко: Умная кибербезопасность, III International Conference «The 2019 Symposium on Cybersecurity of the Digital Economy — CDE’19»

[5]. Петренко А. С., Петренко С. А. Технологии больших данных Big Data в области информационной безопасности и ИИ // Материалы Второй международной научно-технической конференции CDE18. – 2018. – СПб. – С. 248–2

[6]. D.X.Tojimatov: Kiberxavfsizlik: tahdilar, muammolar, yechimlar, “Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalari sohasida zamonaviy muammolar va yechimlar”Respublika Ilmiy-texnik anjumani TATU Farg‘ona filiali 2022 yil 15-16 aprel.

[6]. Dostonbek T., Jamshid M. Use of Artificial Intelligence Opportunities for Early Detection of Threats to Information Systems //Central Asian Journal of Theoretical and Applied Science. – 2023. – Т. 4. – №. 4. – С. 93-98.

https://doi.org/10.5281/zenodo.7979307

https://journals.indexcopernicus.com/search/article?articleId=3609129

https://al-fargoniy.uz/