O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI

mavzusidagi Xalqaro ilmiy-texnik anjuman materiallari to‘plami

2026-yil 25-26-sentabr

(2-qism)

JIZZAX-2026

Kompyuter ilmlari va muhandislik texnologiyalari. Xalqaro ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2026-yil 25-26-sentabr. 315-bet.

Xalqaro miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy kompyuter ilmlari va muhandislik texnologiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globallashuv sharoitida davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish bo‘yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e’tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma’ruza tezislari to‘plamida mamlakatimiz va xorijlik turli yo‘nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o‘qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mas’ul muharrirlar: DSc.prof. Turakulov O.X., t.f.n., dots. Baboyev A.M.

Tahrir hay’ati a’zolari: p.f.d.(DSc), prof. Turakulov O.X., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), prof. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Aliqulov S.T., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dots. Alibayev S.X., т.f.f.d.(PhD), dots. Abdumalikov A.A, p.f.f.d.(PhD) Hafizov E.A., f.f.f.d.(PhD) dots., Norbekova B.Sh. p.f.f.d.(PhD) dots. Sindorov L.K., t.f.f.d.(PhD), dots. Nasirov B.U., b.f.f.d. (PhD) O‘ralov A.I., p.f.n., dots. Aliqulov S.T., t.f.f.d.(PhD) Kuvandikov J.T., i.f.n., dots. Tsoy M.P., Sharipova S.F., Jo‘rayev M.M.

Mazkur to‘plamga kiritilgan ma’ruza tezislarining mazmuni, undagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o‘zlari mas’uldirlar.

2. Miura J., Uozumi H., Shirai Y. *Mobile Robot Motion Planning Considering the Motion Uncertainty of Moving Obstacles*. IEEE International Conference on Systems, Man, and Cybernetics, 1999.

3. Welch G., Bishop G. *An Introduction to the Kalman Filter*. University of North Carolina at Chapel Hill, 1995.

4. Thrun S., Burgard W., Fox D. *Probabilistic Robotics*. MIT Press, 2005.

5. Lütkepohl H. *New Introduction to Multiple Time Series Analysis*. Springer, 2005.

6. Du Toit N. E., Burdick J. W. *Robot Motion Planning in Dynamic, Uncertain Environments*. IEEE Transactions on Robotics, 2012.

7. Nair S. H., Tseng E. H., Borrelli F. *Collision Avoidance for Dynamic Obstacles with Uncertain Predictions using Model Predictive Control*. IEEE Conference on Decision and Control, 2022.

8. Macenski S., Foote T., Gerkey B., Lalancette C., Woodall W. *Robot Operating System 2: Design, Architecture, and Uses in the Wild*. Science Robotics, 2022.

9. Fox D., Burgard W., Thrun S. *The Dynamic Window Approach to Collision Avoidance*. IEEE Robotics & Automation Magazine, 1997.

10. van den Berg J., Lin M., Manocha D. *Reciprocal Velocity Obstacles for Real-Time Multi-Agent Navigation*. IEEE International Conference on Robotics and Automation, 2008.

11. Khatib O. *Real-Time Obstacle Avoidance for Manipulators and Mobile Robots*. The International Journal of Robotics Research, 1986.

KORPORATIV TARMOQLARDA HUJUM INSIDENTLARINI ANIQLASH USULLARI VA VOSITALARI

Choryorqulov G‘iyos Husan o‘g‘li
O‘zbekiston Milliy universiteti Jizzax filiali
“Axborot tizimlari va texnalogiyalari” kafedrasi assistenti
Aliqulova Gulsanam Farxod qizi
Saydullayeva Shaxzoda Anvar qizi
O‘zbekiston Milliy universiteti Jizzax filiali
“Axborot tizimlari va texnalogiyalari” yo‘nalishi talabalari

Annotatsiya. Ushbu maqolada korporativ tarmoqlarda yuzaga keladigan kiberhujum insidentlarini aniqlash usullari va zamonaviy vositalari atroflicha tahlil qilinadi. Axborot xavfsizligini ta’minlashda an’anaviy va zamonaviy yondashuvlar, jumladan, signatura asosidagi, anomaliyaga asoslangan va sun’iy intellektga asoslangan aniqlash usullari o‘rganiladi. Shuningdek, IDS/IPS tizimlari, SIEM platformalari hamda mashinali o‘qitish algoritmlarining amaliy qo‘llanilishi ko‘rib chiqiladi. Maqolada korporativ tarmoqlarda xavfsizlikni oshirish bo‘yicha tavsiyalar berilib, O‘zbekiston sharoitida ushbu texnologiyalarni joriy etish istiqbollari yoritiladi.

Kalit so‘zlar: kiberxavfsizlik, korporativ tarmoq, hujum insidenti, IDS, IPS, SIEM, sun’iy intellekt, mashinali o‘qitish.

Kirish.

Hozirgi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida korporativ tarmoqlarning ahamiyati keskin ortib bormoqda. Raqamli transformatsiya jarayonlari barcha sohalarga kirib borar ekan, tashkilotlar o‘z faoliyatini samarali yuritish uchun keng ko‘lamli tarmoq infratuzilmalariga tayanmoqda. Shu bilan birga, kiberxavfsizlik muammolari ham dolzarb masalalardan biriga aylanib, korporativ tarmoqlarda yuzaga keladigan hujum insidentlarini o‘z vaqtida aniqlash va bartaraf etish zarurati ortmoqda.

Bugungi kunda dunyo miqyosida kiberhujumlar soni va murakkabligi oshib borayotganligi sababli an’anaviy himoya usullari yetarli darajada samarali bo‘lmay qolmoqda. Xususan, zararli dasturlar, tarmoq hujumlari, ichki tahdidlar va ijtimoiy muhandislik usullari orqali amalga oshiriladigan hujumlar korporativ tizimlar xavfsizligiga jiddiy xavf tug‘dirmoqda. Shu bois, hujum insidentlarini aniqlashning zamonaviy, tezkor va intellektual usullarini ishlab chiqish muhim ahamiyat kasb etadi.

Korporativ tarmoqlarda hujum insidentlarini aniqlash — bu axborot tizimlarining maxfiyligi, yaxlitligi va mavjudligini ta’minlashga qaratilgan muhim jarayon hisoblanadi. Mazkur jarayonda tarmoq trafigini monitoring qilish, shubhali faoliyatni aniqlash hamda tahdidlarga nisbatan tezkor choralar ko‘rish asosiy vazifalardan biri hisoblanadi.

Shu bilan birga, sun’iy intellekt va mashinali o‘qitish texnologiyalarining rivojlanishi hujumlarni aniqlash tizimlarini yangi bosqichga olib chiqmoqda. Ushbu texnologiyalar katta hajmdagi ma’lumotlarni tahlil qilish, yashirin tahdidlarni aniqlash va real vaqt rejimida qaror qabul qilish imkonini beradi. Natijada, korporativ tarmoqlarda xavfsizlikni ta’minlash yanada samarali va ishonchli bo‘lib bormoqda.

Mazkur maqolada korporativ tarmoqlarda hujum insidentlarini aniqlashning asosiy usullari, zamonaviy vositalari hamda sun’iy intellekt texnologiyalarining ushbu jarayondagi o‘rni atroflicha tahlil qilinadi.

Adabiyotlar tahlili

Bugungi kunda korporativ tarmoqlarda axborot xavfsizligini ta’minlash va kiberhujum insidentlarini aniqlash masalalari dunyo miqyosida dolzarb ilmiy yo‘nalishlardan biri hisoblanadi. So‘nggi yillarda olib borilgan tadqiqotlar shuni ko‘rsatadiki, an’anaviy himoya usullari zamonaviy, murakkab va yashirin kiberhujumlarni aniqlashda yetarli darajada samarali emas. Shu sababli, ilmiy adabiyotlarda sun’iy intellekt va mashinali o‘qitish asosida ishlovchi tizimlarga katta e’tibor qaratilmoqda.

Ko‘plab xorijiy va mahalliy tadqiqotchilar tomonidan Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) tizimlarining samaradorligi o‘rganilgan. Xususan, ushbu tizimlar tarmoq trafigini tahlil qilish orqali hujumlarni aniqlashda keng qo‘llanilmoqda. Biroq, signatura asosidagi aniqlash usullari faqat

oldindan ma’lum bo‘lgan hujumlarni aniqlay olishi, yangi tahdidlarni aniqlashda esa cheklanganligi ta’kidlab o‘tilgan.

Ilmiy manbalarda anomaliyaga asoslangan yondashuvlar ham keng yoritilgan bo‘lib, ular tizimning normal faoliyatidan chetga chiqishlarni aniqlash orqali yangi turdagi hujumlarni topish imkonini beradi. Shu bilan birga, bunday usullarda noto‘g‘ri ogohlantirishlar sonining yuqoriligi muammosi mavjudligi qayd etilgan.

Zamonaviy tadqiqotlarda esa sun’iy intellekt texnologiyalariga alohida urg‘u berilmoqda. Mashinali o‘qitish algoritmlari (Decision Tree, Random Forest, Neural Networks) asosida yaratilgan tizimlar katta hajmdagi ma’lumotlarni tahlil qilish orqali murakkab va yashirin hujumlarni aniqlashda yuqori samaradorlik ko‘rsatmoqda. Ayrim tadqiqotlarda SIEM (Security Information and Event Management) tizimlari bilan integratsiyalashgan AI modellarining real vaqt rejimida tahdidlarni aniqlash imkoniyati yuqori ekani ta’kidlangan.

Shuningdek, so‘nggi ilmiy ishlarda foydalanuvchi xatti-harakatlarini tahlil qilish (User Behavior Analytics – UBA) orqali ichki tahdidlarni aniqlash masalalari ham keng o‘rganilmoqda. Bu esa korporativ tarmoqlarda xavfsizlikni kompleks tarzda ta’minlash imkonini beradi.

Metodologiya

Korporativ tarmoqlarda hujum insidentlarini aniqlash metodikasi — bu zamonaviy texnologiyalar, xususan sun’iy intellekt va tarmoq monitoringi vositalari yordamida tahdidlarni aniqlash, tahlil qilish va oldini olish usullari majmuasidir.

Mazkur metodika quyidagi bosqichlardan iborat:

1-bosqich: Tarmoq infratuzilmasini tahlil qilish

Ushbu bosqichda korporativ tarmoqning mavjud holati baholanadi. Tarmoq qurilmalari, serverlar, trafik hajmi va xavfsizlik darajasi o‘rganiladi. Shuningdek, zaif nuqtalar aniqlanadi.

2-bosqich: Mos aniqlash vositalarini tanlash

Bu bosqichda tashkilot ehtiyojlariga mos xavfsizlik vositalari tanlanadi. Jumladan:

- IDS va IPS tizimlari
- SIEM platformalari
- Tarmoq monitoring dasturlari

3-bosqich: Sun’iy intellekt asosida model yaratish

Ushbu bosqichda mashinali o‘qitish algoritmlari yordamida hujumlarni aniqlash modeli ishlab chiqiladi. Model tarmoq trafigi asosida o‘qitilib, normal va shubhali faoliyatni ajrata oladi.

4-bosqich: Sinov va baholash (pilot loyiha)

Yangi tizim dastlab kichik miqyosda sinovdan o‘tkaziladi. Aniqlik darajasi, noto‘g‘ri ogohlantirishlar soni va umumiy samaradorlik baholanadi.

5-bosqich: To‘liq joriy etish va monitoring

Sinov muvaffaqiyatli yakunlangach, tizim korporativ tarmoqda to‘liq joriy etiladi. Doimiy monitoring va yangilanishlar orqali tizim samaradorligi oshirib boriladi.

Korporativ tarmoqlarda sun’iy intellekt texnologiyalaridan foydalanish kiberxavfsizlikni ta’minlashda muhim ahamiyat kasb etmoqda. Zamonaviy SI vositalari yordamida tarmoqdagi trafikni real vaqt rejimida tahlil qilish, shubhali faoliyatlarni aniqlash hamda tahdidlarga tezkor javob berish imkoniyati yaratiladi.

Sun’iy intellekt asosidagi tizimlar katta hajmdagi ma’lumotlarni qayta ishlash orqali hujumlarni aniqlash aniqligini oshiradi va xavfsizlik tizimlarini avtomatlashtirishga xizmat qiladi. Bu esa korporativ tarmoqlarning barqarorligi va ishonchliligini ta’minlashda muhim omil hisoblanadi.

Shuningdek, SI texnologiyalari yordamida tarmoq faoliyatini chuqur tahlil qilish, foydalanuvchi xatti-harakatlarini kuzatish va potentsial tahdidlarni oldindan prognoz qilish mumkin. Natijada, hujumlarning oldini olish imkoniyati sezilarli darajada oshadi.

Sun’iy intellekt asosida hujum insidentlarini aniqlash tizimlarining asosiy afzalliklari va kamchiliklari keltirilgan:

Afzalliklari	**Kamchiliklari**
Tarmoq trafigini real vaqt rejimida monitoring qilish	Texnik infratuzilma talablarining yuqoriligi
Murakkab va yashirin hujumlarni aniqlash imkoniyati	Moliyaviy xarajatlarning kattaligi
Noto‘g‘ri harakatlarni avtomatik aniqlash	Noto‘g‘ri ogohlantirishlar (false positives)
Xavfsizlik jarayonlarini avtomatlashtirish	Malakali mutaxassislar yetishmasligi
Katta hajmdagi ma’lumotlarni tezkor tahlil qilish	Modelni o‘qitish uchun katta ma’lumot talab etilishi
Tahdidlarni oldindan prognoz qilish	Ma’lumotlar maxfiyligi va xavfsizlik muammolari

Yuqoridagi jadvaldan ko‘rinib turibdiki, sun’iy intellekt texnologiyalarining kiberxavfsizlik sohasida qo‘llanilishi bir qator muhim afzalliklarga ega. Xususan, hujumlarni tezkor aniqlash, tizimlarni avtomatlashtirish va real vaqt rejimida monitoring qilish imkoniyatlari korporativ tarmoqlar xavfsizligini sezilarli darajada oshiradi.

Shu bilan birga, ushbu texnologiyalarni joriy etishda ayrim muammolar ham mavjud. Jumladan, SI tizimlari ba’zan noto‘g‘ri yoki to‘liq bo‘lmagan xulosalar chiqarishi mumkin. Bu esa noto‘g‘ri ogohlantirishlar sonining oshishiga olib keladi. Bundan tashqari, bunday tizimlarni yaratish va joriy etish katta moliyaviy resurslar hamda yuqori malakali mutaxassislarni talab qiladi.

Shuning uchun sun’iy intellekt texnologiyalaridan foydalanishda ularni mustaqil qaror qabul qiluvchi tizim sifatida emas, balki mutaxassisga yordam beruvchi vosita sifatida qo‘llash maqsadga muvofiqdir. Yakuniy qaror esa inson tomonidan qabul qilinishi zarur.

Xulosa.

Xulosa qilib aytganda, korporativ tarmoqlarda hujum insidentlarini aniqlash zamonaviy axborot xavfsizligining eng muhim yo‘nalishlaridan biri hisoblanadi.

Raqamli texnologiyalar rivojlanib borayotgan hozirgi sharoitda kiberhujumlarning murakkablashuvi an’anaviy himoya vositalarining samaradorligini pasaytirib, yangi yondashuvlarni joriy etishni talab etmoqda.

Mazkur tadqiqot natijalari shuni ko‘rsatadiki, sun’iy intellekt va mashinali o‘qitish texnologiyalaridan foydalanish hujum insidentlarini aniqlash jarayonini sezilarli darajada takomillashtiradi. Ushbu texnologiyalar yordamida tarmoq trafigini real vaqt rejimida tahlil qilish, yashirin tahdidlarni aniqlash va xavfsizlik choralarini avtomatlashtirish imkoniyati kengayadi. Natijada, korporativ tarmoqlarning barqarorligi va ishonchliligi oshadi.

Shu bilan birga, bunday tizimlarni joriy etish jarayonida texnik infratuzilma, moliyaviy resurslar va malakali mutaxassislar yetishmasligi kabi muammolar mavjudligi ham aniqlandi. Bundan tashqari, sun’iy intellekt tizimlarining ba’zan noto‘g‘ri xulosalar chiqarishi ehtimoli mavjud bo‘lib, bu esa inson nazoratining muhimligini yana bir bor tasdiqlaydi.

O‘zbekiston sharoitida korporativ tarmoqlar xavfsizligini ta’minlashda zamonaviy texnologiyalarni joriy etish bosqichma-bosqich amalga oshirilmoqda. Kelajakda ushbu yo‘nalishda quyidagi strategik vazifalar dolzarb bo‘lib qoladi: kiberxavfsizlik sohasida malakali kadrlar tayyorlash, ilg‘or texnologiyalarni joriy etish, sun’iy intellekt tizimlarini milliy infratuzilmaga integratsiyalash hamda axborot xavfsizligi bo‘yicha huquqiy va etik me’yorlarni takomillashtirish.

Shunday qilib, korporativ tarmoqlarda hujum insidentlarini aniqlashda sun’iy intellekt texnologiyalaridan samarali foydalanish orqali yuqori darajadagi xavfsizlikni ta’minlash va zamonaviy, barqaror axborot muhitini yaratish mumkin.

Foydalanilgan adabiyotlar

1. Норматов, Н., and А. Мамараимов. "Ta’lim tizimida baholash tizimini avtomatlashtirishni joriy etish jarayonlari va foydalanish metodlari." *Информатика и инженерные технологии* 1.2 (2023): 356-359.

2. Чорркулов Г., Норматов Н., Мамараимов А. Роль анализа текстовых связей в электронных документах в информационной безопасности //Информатика и инженерные технологии. – 2023. – Т. 1. – №. 1. – С. 67-71.

3. Мамараимов А., Чорёркулов Г., Норматов Н. Tanib olish modullarini dasturiy amalga oshirish //Информатика и инженерные технологии. – 2023. – Т. 1. – №. 2. – С. 38-44.

4. Nizomiddin N. et al. TA’LIMDA DASTURLASH JARAYONINI BAHOLASHGA ASOSLANGAN AVTOMATLASHTIRILGAN TIZIMNI TADBIQ ETISH //International Journal of Contemporary Scientific and Technical Research. – 2023. – С. 24-28.

5. Northcutt, S. & Novak, J. Network Intrusion Detection. New Riders Publishing, 2002.

6. Chuvakin, A., Schmidt, C. & Phillips, K. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngress, 2012.

7. Sommer, R. & Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 2010.
8. Stallings, W. Network Security Essentials: Applications and Standards. Pearson, 2020.

SUN'IY INTELLEKT YORDAMIDA MODELLASHTIRISH: ZAMONAVIY YONDASHUVLAR VA AMALIY QO'LLANILISH SOHALARI

Axmedov Juraboy Raxmonberdiyevich
O'zbekiston Milliy universitetining Jizzax filiali Axborot tizimlari va texnologiyalari kafedrasi professori v.b, pedagogika fanlari doktori (DSc)
E-mail: jaxmedov48@gmail.com
Mixliyeva Ulug'oy Rabbim qizi
O'zbekiston Milliy universitetining Jizzax filiali Axborot tizimlari va texnologiyalari kafedrasi assistenti

Annotatsiya: Ushbu maqolada sun'iy intellekt texnologiyalari yordamida modellashtirishning zamonaviy usullari, asosiy tamoyillari va amaliy qo'llanilish yo'nalishlari tahlil qilinadi. Sun'iy intellekt asosidagi modellar murakkab jarayonlarni matematik va statistik usullar bilan ifodalash, katta hajmdagi ma'lumotlarni qayta ishlash, mavjud qonuniyatlarni aniqlash hamda kelajakdagi holatlarni prognoz qilish imkonini beradi. Maqolada mashinaviy o'qitish, neyron tarmoqlar, chuqur o'rganish va gibrid modellashtirish yondashuvlarining xususiyatlari ko'rib chiqiladi. Shuningdek, ushbu texnologiyalardan iqtisodiyot, tibbiyot, sanoat, energetika va ta'lim sohalarida foydalanish imkoniyatlari yoritiladi.

Kalit so'zlar: sun'iy intellekt, modellashtirish, mashinaviy o'qitish, neyron tarmoq, chuqur o'rganish, prognozlash, ma'lumotlar tahlili, matematik model.

Моделирование с использованием искусственного интеллекта: современные подходы и области практического применения.

Аннотация: В статье анализируются современные методы, фундаментальные принципы и практические аспекты моделирования с использованием технологий искусственного интеллекта. Модели на базе ИИ позволяют описывать сложные процессы с помощью математических и статистических методов, обрабатывать большие массивы данных, выявлять скрытые закономерности и прогнозировать развитие событий. Рассматриваются особенности машинного обучения, нейронных сетей, глубокого обучения и гибридных подходов к моделированию. Также освещаются возможности применения данных технологий в таких сферах, как экономика, медицина, промышленность, энергетика и образование.

Ключевые слова: искусственный интеллект, моделирование, машинное обучение, нейронная сеть, глубокое обучение, прогнозирование, анализ данных, математическая модель.