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.

7. Tekin, N., Acar, A., Aris, A., Uluagac, A. S., & Gungor, V. C. (2023). Energy consumption of on-device machine learning models for IoT intrusion detection. Internet of Things, 21, 100670.
8. 3GPP. (2021). 3GPP security standards for 5G networks. 3rd Generation Partnership Project. https://www.3gpp.org

SUN'IY INTELLEKT ASOSIDA AXBOROT TIZIMLARIDA KIBERHUJUMLARNI ANIQLASH VA OLDINI OLISH USULLARINI TAKOMILLASHTIRISH

Choryorqulov G'iyos Husan o'g'li
O'zbekiston Milliy universiteti Jizzax filiali
Axborot tizimlari va texnologiyalari kafedrasi assistenti
Xasanov Yorqinbek Aktam o'g'li
Shomirzayev Abdulaziz Sayfullo o'g'li
O'zbekiston Milliy universiteti Jizzax filiali
Axborot tizimlari va texnologiyalari yo'nalishi talabalari
Email: yorqinxasanov80@gmail.com
Email:shomirzayevabdulaziz990@gmail.com

Annotatsiya. Ushbu maqolada zamonaviy axborot tizimlarida kiberhujumlarni aniqlash va ularning oldini olishda sun'iy intellekt hamda mashinali o'qitish texnologiyalaridan foydalanish masalasi ko'rib chiqiladi. Axborot tizimlarida ma'lumotlar hajmining ortishi, tarmoq infratuzilmasining murakkablashuvi va kiberhujumlarning yangi ko'rinishlari an'anaviy xavfsizlik mexanizmlarini takomillashtirish zaruratini yuzaga keltirmoqda. Tadqiqotda tarmoq trafigini tahlil qilish orqali normal va anomal faoliyatni avtomatik aniqlashga asoslangan yondashuv taklif etiladi. Bunda Decision Tree, Random Forest va Support Vector Machine kabi mashinali o'qitish algoritmlaridan foydalanish imkoniyatlari ko'rib chiqiladi. Model samaradorligini baholash uchun Accuracy, Precision, Recall va F1-score ko'rsatkichlaridan foydalanish taklif etiladi. Tadqiqotning amaliy qismida ochiq tarmoq xavfsizligi datasetlaridan foydalanish orqali kiberhujumlarni aniqlash modelini sinovdan o'tkazish ko'zda tutiladi. Taklif etilayotgan yondashuv axborot tizimlarida xavfsizlik monitoringini avtomatlashtirish va shubhali faoliyat haqida tizim administratorini tezkor xabardor qilish imkonini berishi mumkin.

Kalit so'zlar: axborot tizimi, kiberxavfsizlik, kiberhujum, sun'iy intellekt, mashinali o'qitish, tarmoq trafigi, anomaliya aniqlash, intrusion detection system, Random Forest, Decision Tree, SVM.

1. KIRISH

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi natijasida davlat tashkilotlari, ta'lim muassasalari, banklar, korxonalar va boshqa tashkilotlarning faoliyatida axborot tizimlaridan keng foydalanilmoqda. Bunday tizimlarda katta hajmdagi ma'lumotlarning saqlanishi va qayta ishlanishi ularning xavfsizligini ta'minlash masalasini muhim vazifalardan biriga aylantirmoqda.

Axborot tizimlariga qarshi amalga oshiriladigan kiberhujumlar ma’lumotlarning yo‘qolishi, o‘g‘irlanishi, o‘zgartirilishi yoki tizim faoliyatining buzilishiga olib kelishi mumkin. Shu sababli axborot tizimlarida tarmoq faoliyatini monitoring qilish va shubhali harakatlarni o‘z vaqtida aniqlash muhim ahamiyatga ega.

Kiberhujumlarni aniqlashda Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) kabi texnologiyalardan foydalaniladi. IDS tizimdagi yoki tarmoqdagi shubhali faoliyatni aniqlash va bu haqda xabar berishga yo‘naltirilgan bo‘lsa, IPS aniqlangan tahdidga nisbatan avtomatik himoya choralarini amalga oshirish imkoniyatiga ega.

An’anaviy kiberxavfsizlik tizimlarida keng qo‘llaniladigan imzo asosidagi aniqlash usuli avvaldan ma’lum bo‘lgan hujumlar belgilarini aniqlashga asoslanadi. Biroq yangi yoki ilgari noma’lum bo‘lgan hujumlarni aniqlashda bunday yondashuvning imkoniyatlari cheklanishi mumkin. Shu sababli tarmoqdagi faoliyatni ma’lumotlar asosida tahlil qila oladigan mashinali o‘qitish algoritmlaridan foydalanish dolzarb yo‘nalishlardan biri hisoblanadi.

Sun’iy intellekt va mashinali o‘qitish texnologiyalari katta hajmdagi tarmoq ma’lumotlarini tahlil qilish, normal faoliyatdan farq qiluvchi xatti-harakatlarni aniqlash va kiberhujumlarni tasniflash imkonini beradi. Shu nuqtayi nazardan, mazkur maqolada sun’iy intellekt asosida kiberhujumlarni aniqlash modelini ishlab chiqish va uni axborot tizimlarida qo‘llash imkoniyatlari o‘rganiladi.

2. TADQIQOTNING MAQSADI VA VAZIFALARI

2.1. Tadqiqot maqsadi

Tadqiqotning asosiy maqsadi — sun’iy intellekt va mashinali o‘qitish algoritmlaridan foydalanib, axborot tizimlaridagi normal va anomal tarmoq faoliyatini avtomatik aniqlash hamda kiberhujumlar to‘g‘risida tizim administratorini xabardor qilishga mo‘ljallangan yondashuvni ishlab chiqish.

2.2. Tadqiqot vazifalari

Belgilangan maqsadga erishish uchun quyidagi vazifalar amalga oshiriladi:

1. Axborot tizimlarida uchraydigan asosiy kiberxavfsizlik tahdidlarini o‘rganish.
2. Kiberhujumlarni aniqlashning an’anaviy usullarini tahlil qilish.
3. IDS va IPS tizimlarining ishlash tamoyillarini o‘rganish.
4. Sun’iy intellekt va mashinali o‘qitishning kiberxavfsizlikdagi imkoniyatlarini tahlil qilish.
5. Kiberhujumlarni aniqlash uchun mos mashinali o‘qitish algoritmlarini tanlash.
6. Tarmoq trafigiga oid ma’lumotlarni oldindan qayta ishlash usullarini aniqlash.
7. Tanlangan algoritmlarning samaradorligini tegishli mezonlar asosida baholash.
8. Axborot tizimlarida kiberhujumlarni aniqlashning taklif etilayotgan modelini ishlab chiqish.

3. TADQIQOT OBYEKTI VA PREDMETI

Tadqiqot obyekti — axborot tizimlarida yuzaga keladigan tarmoq faoliyati va kiberxavfsizlik jarayonlari.

Tadqiqot predmeti — sun’iy intellekt va mashinali o‘qitish algoritmlari yordamida tarmoq trafigidagi anomal faoliyatni aniqlash usullari.

4. TADQIQOT METODOLOGIYASI

Tadqiqotda tahlil, taqqoslash, klassifikatsiya, ma’lumotlarni oldindan qayta ishlash va mashinali o‘qitish usullaridan foydalanish ko‘zda tutiladi.

Amaliy tadqiqot uchun ochiq tarmoq xavfsizligi datasetlaridan foydalanish mumkin. Jumladan, CIC-IDS2017 datasetida normal tarmoq faoliyati bilan bir qatorda turli kiberhujumlarga tegishli trafik ma’lumotlari mavjud. UNSW-NB15 datasetida ham normal trafik va turli hujum turlariga tegishli ma’lumotlar keltirilgan.

Tadqiqotning umumiy algoritmi quyidagi ketma-ketlikda amalga oshiriladi:

Ma’lumotlarni olish → Ma’lumotlarni tozalash → Xususiyatlarni tanlash → Ma’lumotlarni o‘qitish va test qismlariga ajratish → ML modelini o‘qitish → Natijani baholash → Anomal trafikni aniqlash.

5. AXBOROT TIZIMLARIDA KIBERHUJUMLARNI ANIQLASH

Kiberhujumlarni aniqlash tizimlari axborot tizimlarining xavfsizligini monitoring qilishda muhim vositalardan biridir.

An’anaviy aniqlash usullarini shartli ravishda quyidagi ikki asosiy guruhga ajratish mumkin:

Imzo asosidagi aniqlash. Bunda avvaldan ma’lum bo‘lgan kiberhujumlarning o‘ziga xos belgilari ma’lumotlar bazasida saqlanadi. Tizim yangi trafikni ushbu belgilar bilan taqqoslaydi.

Anomaliyaga asoslangan aniqlash. Bunda tizim avvalo normal faoliyatning xususiyatlarini o‘rganadi. Keyinchalik normal holatdan sezilarli farq qiluvchi faoliyat anomal deb belgilanadi. Anomaliyaga asoslangan yondashuv mashinali o‘qitish algoritmlaridan foydalanish uchun qulay hisoblanadi. Chunki model tarmoq faoliyatidagi ma’lum xususiyatlar asosida normal va anomal holatlarni farqlashni o‘rganishi mumkin.

6. SUN’IY INTELLEKT VA MASHINALI O‘QITISHNING KIBERXAVFSIZLIKDAGI O‘RNI

Sun’iy intellekt kiberxavfsizlikda katta hajmdagi ma’lumotlarni tahlil qilish va ulardan muhim qonuniyatlarni aniqlash uchun qo‘llanilishi mumkin.

Mashinali o‘qitish modeli tarmoq trafigining turli xususiyatlarini o‘rganadi. Bunday xususiyatlarga ulanish davomiyligi, paketlar soni, paketlar hajmi, protokol turi, portlar, yuborilgan va qabul qilingan ma’lumotlar miqdori kabi ko‘rsatkichlar kirishi mumkin.

Modelning ishlash jarayoni quyidagicha ifodalanadi:

Tarmoq trafigi → Ma’lumotlarni yig‘ish → Oldindan qayta ishlash → Xususiyatlarni ajratish → Mashinali o‘qitish modeli → Klassifikatsiya → Natija.

Natijada tarmoq faoliyati normal yoki anomal sifatida tasniflanadi.

7. TANLANGAN MASHINALI O‘QITISH ALGORITMLARI

Tadqiqotda uchta mashinali o‘qitish algoritmini taqqoslash taklif etiladi.

7.1. Decision Tree

Decision Tree — qarorlar daraxti asosida ishlaydigan klassifikatsiya algoritmi. Unda ma’lumotlar ketma-ket shartlar asosida guruhlarga ajratiladi. Uning afzalliklaridan biri natijani tushuntirish nisbatan osonligidir. Kiberxavfsizlikda tarmoq trafiklarini turli sinflarga ajratishda foydalanish mumkin.

7.2. Random Forest

Random Forest bir nechta Decision Tree modellaridan foydalanib, ularning natijalarini birlashtiradi. Bu yondashuv ayrim holatlarda bitta qaror daraxtiga nisbatan barqarorroq klassifikatsiya natijasini berishi mumkin. Random Forest tarmoq trafigidagi ko‘plab xususiyatlar bilan ishlash uchun qo‘llanilishi mumkin.

7.3. Support Vector Machine

Support Vector Machine ma’lumotlarni turli sinflarga ajratish uchun optimal ajratuvchi chegarani aniqlashga asoslangan algoritmdir.

8. MODEL SAMARADORLIGINI BAHOLASH

Mashinali o‘qitish modelining samaradorligini baholashda bir nechta statistik ko‘rsatkichlardan foydalanish maqsadga muvofiq.

Accuracy — barcha namunalar ichida to‘g‘ri klassifikatsiya qilingan namunalar ulushini ifodalaydi.

Precision — model tomonidan hujum deb aniqlangan namunalar ichida haqiqatan hujumga tegishli namunalar ulushini ko‘rsatadi.

Recall — mavjud haqiqiy hujumlarning qancha qismi model tomonidan aniqlanganini ko‘rsatadi.

F1-score — Precision va Recall qiymatlarining muvozanatli ko‘rsatkichidir.

9. KIBERHUJUMLARNI ANIQLASH VA OGOHLANTIRISH MEKANIZMI

Taklif qilinayotgan tizimning asosiy vazifasi kiberhujumni mustaqil ravishda amalga oshirish emas, balki tarmoq faoliyatidagi xavfli yoki anomal holatlarni aniqlash va administratorga o‘z vaqtida xabar berishdan iborat.

Jarayon quyidagi ketma-ketlikda ishlaydi:

1. Tarmoq trafigi monitoring qilinadi.

2. Trafikdan tegishli xususiyatlar ajratib olinadi.

3. Ma’lumotlar mashinali o‘qitish modeliga uzatiladi.

4. Model faoliyatni normal yoki anomal sifatida tasniflaydi.

5. Anomal holat aniqlansa, tizim administratorga ogohlantirish yuboradi.

6. Administrator xavfsizlik siyosatiga muvofiq tegishli chorani belgilaydi.

Bunday yondashuv inson administratorining qaror qabul qilish jarayonini qo‘llab-quvvatlashga xizmat qilishi mumkin.

10. TAJRIBA NATIJALARINI OLISH USULI

Tadqiqotning amaliy bosqichida Python dasturlash muhiti va mashinali o‘qitish kutubxonalaridan foydalanish mumkin.

Tajriba quyidagi bosqichlardan tashkil topadi:

1. Datasetni yuklash.
2. Ma’lumotlarni tekshirish.
3. Keraksiz va takroriy ma’lumotlarni qayta ishlash.
4. Kategorik ma’lumotlarni raqamlashtirish.

5. Xususiyatlarni tanlash.
6. Ma’lumotlarni o‘qitish va test qismlariga ajratish.
7. Decision Tree modelini o‘qitish.
8. Random Forest modelini o‘qitish.
9. SVM modelini o‘qitish.
10. Har bir model natijasini baholash.
11. Natijalarni jadval va grafik yordamida taqqoslash.

Shu tariqa maqolaning amaliy qismida nazariy fikrlar emas, **tajriba orqali olingan ma’lumotlar** asosida xulosa chiqarish imkoniyati yaratiladi.

11. MUHOKAMA

Sun’iy intellekt asosidagi kiberxavfsizlik tizimlari tarmoq trafigini avtomatik tahlil qilish imkoniyatini kengaytiradi. Ayniqsa, katta hajmdagi ma’lumotlarni inson tomonidan qo‘lda tahlil qilish qiyin bo‘lgan sharoitlarda mashinali o‘qitish algoritmlaridan foydalanish amaliy ahamiyatga ega.

Biroq mashinali o‘qitish modelining samaradorligi foydalanilgan datasetning sifati, ma’lumotlarning muvozanati, tanlangan xususiyatlar va algoritm parametrlariga bog‘liq. Bundan tashqari, kiberxavfsizlik tizimlarida noto‘g‘ri aniqlash holatlari ham muhim masala hisoblanadi.

Shu sababli faqat Accuracy ko‘rsatkichiga tayanish yetarli emas. Precision, Recall va F1-score kabi qo‘shimcha ko‘rsatkichlarni ham hisobga olish zarur.

12.XULOSA

Tadqiqotda sun’iy intellekt va mashinali o‘qitish texnologiyalaridan foydalanib, axborot tizimlarida kiberhujumlarni aniqlash masalasi ko‘rib chiqildi. Tarmoq trafigini tahlil qilish asosida normal va anomal faoliyatni avtomatik ajratish imkoniyati tahlil qilindi.

Kiberhujumlarni aniqlash uchun Decision Tree, Random Forest va Support Vector Machine algoritmlaridan foydalanish taklif etildi. Ushbu algoritmlarning samaradorligini Accuracy, Precision, Recall va F1-score ko‘rsatkichlari orqali baholash mumkin.

Taklif etilgan model tarmoq trafigini yig‘ish, ma’lumotlarni qayta ishlash, xususiyatlarni ajratish, mashinali o‘qitish modeli yordamida klassifikatsiya qilish va anomal holat aniqlanganda administratorni ogohlantirish bosqichlaridan iborat.

Tadqiqotning keyingi bosqichida tanlangan dataset asosida amaliy tajriba o‘tkazish va turli algoritmlarning natijalarini taqqoslash maqolaning ilmiy-amaliy qiymatini oshiradi. Olingan real natijalar asosida axborot tizimlarida kiberhujumlarni aniqlashning samarali modelini shakllantirish imkoniyati paydo bo‘ladi.

Foydalanilgan adabiyotlar

1. G‘aniyev S. K., Karimov M. M., Tashev K. A. Axborot xavfsizligi. Toshkent: Fan va texnologiya, 2017.
2. G‘aniyev S. K., G‘aniyev A. A., Xudoyqulov Z. T. Kiberxavfsizlik asoslari. Toshkent: Aloqachi, 2020.
3. G‘ulomov S. S., Begalov B. A. Informatika va axborot texnologiyalari. Toshkent: Fan, 2010.

4. Abdullayev Z. S. Informatika va axborot texnologiyalari. Toshkent: Noshir, 2012.
5. Sattorov A. Informatika va axborot texnologiyalari. Toshkent: O‘qituvchi, 2008.
6. Qodirov F. E., O‘ktamov M. O‘., Musirmanov Sh. U. Kiberxavfsizlik asoslari. Samarqand, 2024.
7. Xaytullayeva N. S., Fayziyeva F. M., Sayfurov D. M. va boshq. Informatika va axborot texnologiyalari. Toshkent, 2021.

BIOMETRIK XAVFSIZLIKDA DEEPFAKE TAHDIDLARI. SUN’IY INTELLEKT ASOSIDAGI ANIQLASH VA HIMOYA TEXNOLOGIYALARI

Mamarimov Abror Kamalidin o‘g‘li, Mixliyeva Ulug‘oy Rabbim qizi
O‘zbekiston Milliy universitetining Jizzax filiali, Amaliy matematika fakulteti, Axborot tizimlari va texnologiyasi kafedrasi o‘qituvchi
mamaroimovabror@gmail.com, mixliyevau@gmail.com
Adirboyeva Shahnoza Amir qizi , Abduramonova Aziza Akram qizi
O‘zbekiston Milliy universitetining Jizzax filiali, talabasi

Annotatsiya. Ushbu maqolada sun'iy intellekt texnologiyalarining biometrik xavfsizlik tizimlariga ta'siri, xususan, generativ sun'iy intellekt asosida yaratilgan deepfake tahdidlari va ularga qarshi qo'llanilayotgan zamonaviy himoya mexanizmlari tahlil qilinadi. Maqolada "jonlilik testi" (liveness detection)ning faol va passiv turlari, ko'p qatlamli (multi-modal) biometrik tizimlar, maxfiylikni saqlovchi "bilim-nol" (zero-knowledge) tekshiruv usullari, shuningdek sohani xalqaro miqyosda tartibga solish tendentsiyalari ko'rib chiqiladi

Kalit so'zlar: sun'iy intellekt, biometrik xavfsizlik, deepfake, jonlilik testi (liveness detection), raqamli shaxs, autentifikatsiya, ma'lumotlar maxfiyligi.Sun’iy intellekt texnologiyalarining jadal rivojlanishi shaxsni identifikatsiya qilish va autentifikatsiya tizimlariga ham katta ta’sir ko‘rsatmoqda. Ayniqsa, generativ sun’iy intellekt yordamida yaratiladigan deepfake texnologiyalari biometrik xavfsizlik uchun yangi tahdidlarni yuzaga keltirmoqda. Soxta video, ovoz va tasvirlarning real ko‘rinishga ega bo‘lishi biometrik tizimlarni aldash imkoniyatini oshirmoqda. Shu sababli zamonaviy autentifikatsiya tizimlarida shaxsni aniqlash bilan birga, biometrik namunaning haqiqiyligini tekshirish ham muhim ahamiyat kasb etmoqda.Biometrik autentifikatsiya insonning fiziologik va xulq-atvor xususiyatlari asosida amalga oshiriladi. Yuz, barmoq izi, ko‘z tuzilishi kabi fiziologik belgilar bilan bir qatorda ovoz, klaviaturadan foydalanish va boshqa xulq-atvor xususiyatlaridan ham foydalaniladi. Hozirgi tizimlarda bir nechta biometrik belgilarni birgalikda qo‘llash orqali himoyaning qo‘shimcha qatlamlari yaratilmoqda. Bunday yondashuv biometrik ma’lumotni soxtalashtirishni murakkablashtiradi va autentifikatsiya ishonchliligini oshiradi.Biometrik ma’lumotlarning muhim jihati shundaki, ularni