SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

SUN’IY INTELLEKT YORDAMIDA KIBERHUJUMLARNI ANIQLASH VA OLDINI OLISHNING ZAMONAVIY USULLARI

Kurbonova Firuza Zaripovna

Texnika fanlari bo‘yicha falsafa doktori (PhD), dotsent.

Ichki ishlar vazirligi akademiyasi, Toshkent shahri, O‘zbekiston Respublikasi.

https://doi.org/10.5281/zenodo.20957351

Annotatsiya. Mazkur maqolada sun’iy intellekt texnologiyalarining kiberxavfsizlik tizimlaridagi o‘rni, kiberhujumlarni erta aniqlash va ularga qarshi kurashishdagi ilmiy yondashuvlar tahlil qilinadi. Mashinali o‘qitish va chuqur o‘qitish algoritmlarining tarmoq trafigini tahlil qilish, anomaliyalarni aniqlash hamda tahdidlarni prognozlashdagi imkoniyatlari ko‘rib chiqiladi. Shuningdek, sun’iy intellekt asosidagi xavfsizlik tizimlarini joriy etishning afzalliklari, cheklovlari va istiqbollari yoritiladi.

Kalit so‘zlar: sun’iy intellekt, kiberxavfsizlik, mashinali o‘qitish, chuqur o‘qitish, anomaliyalarni aniqlash, kiberhujum, raqamli xavfsizlik.

Аннотация. В данной статье анализируется роль технологий искусственного интеллекта в системах кибербезопасности, а также научные подходы к раннему выявлению кибератак и противодействию им. Рассматриваются возможности алгоритмов машинного обучения и глубокого обучения при анализе сетевого трафика, обнаружении аномалий и прогнозировании киберугроз. Кроме того, освещаются преимущества, ограничения и перспективы внедрения систем кибербезопасности, основанных на технологиях искусственного интеллекта.

Ключевые слова: искусственный интеллект, кибербезопасность, машинное обучение, глубокое обучение, обнаружение аномалий, кибератака, цифровая безопасность.

Abstract. This article analyzes the role of artificial intelligence technologies in cybersecurity systems and examines scientific approaches to the early detection and prevention of cyberattacks. It explores the capabilities of machine learning and deep learning algorithms in network traffic analysis, anomaly detection, and cyber threat prediction. Furthermore, the paper discusses the advantages, limitations, and future prospects of implementing artificial intelligence-based cybersecurity systems.

Keywords: artificial intelligence, cybersecurity, machine learning, deep learning, anomaly detection, cyberattack, digital security.

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida davlat boshqaruvi, bank-moliya tizimi, sog‘liqni saqlash, transport va sanoat tarmoqlari tobora ko‘proq raqamli infratuzilmaga tayanmoqda. Ushbu jarayonlar bilan bir qatorda kiberjinoyatchilikning yangi shakllari ham rivojlanmoqda. Kiberhujumlar endilikda nafaqat iqtisodiy zarar, balki davlat xavfsizligi, shaxsiy ma’lumotlarning daxlsizligi va muhim infratuzilmalarning uzluksiz faoliyatiga ham tahdid solmoqda.

An’anaviy himoya vositalari, jumladan signatura (imzo) asosida ishlovchi antiviruslar va oddiy xavfsizlik devorlari ilgari ma’lum bo‘lgan tahdidlarni aniqlashda samarali bo‘lsa-da, yangi va murakkab hujumlar, xususan Zero-Day ekspluatatsiyalari, polimorfik zararli dasturlar hamda maqsadli hujumlarni aniqlashda yetarli natija bermaydi. Shu sababli sun’iy intellekt va mashinali o‘qitish texnologiyalaridan foydalanish zamonaviy kiberxavfsizlikning muhim yo‘nalishiga aylandi.

Sun’iy intellekt (Artificial Intelligence — AI) insonning fikrlash, o‘rganish va qaror qabul qilish faoliyatini modellashtiruvchi algoritmlar va dasturiy tizimlar majmuasidir. Kiberxavfsizlikda AI katta hajmdagi ma’lumotlarni tahlil qilish, tarmoqdagi odatiy va g‘ayrioddiy faoliyatni farqlash hamda tahdidlarni real vaqt rejimida aniqlash imkonini beradi [1].

AI asosidagi tizimlarning ustunligi shundaki, ular doimiy ravishda yangi ma’lumotlardan o‘rganib boradi. Natijada tizim ilgari uchramagan tahdidlarni ham statistik va xulq-atvor tahlili orqali aniqlashi mumkin [2].

Mashinali o‘qitish (Machine Learning) sun’iy intellektning asosiy yo‘nalishlaridan biri bo‘lib, algoritmlarga ma’lumotlardan qonuniyatlarni mustaqil o‘rganish imkonini beradi[3].

Kiberxavfsizlikda quyidagi usullar keng qo‘llaniladi:

Nazorat ostida o‘qitish (Supervised Learning): Bu usulda model oldindan belgilangan (yorliqlangan) ma’lumotlar asosida o‘qitiladi. Masalan, zararli va xavfsiz fayllar to‘plami yordamida algoritm yangi faylni tasniflaydi.

Ko‘p qo‘llaniladigan algoritmlar: **Decision Tree; Random Forest; Support Vector Machine (SVM); Logistic Regression.**

Nazoratsiz o‘qitish (Unsupervised Learning): Mazkur usul oldindan belgilangan javoblarsiz ishlaydi. Asosiy vazifasi — odatiy faoliyatdan chetga chiqadigan holatlarni aniqlash. Masalan: tarmoq trafigidagi g‘ayrioddiy faollik; noma’lum zararli dasturlar; ichki tahdidlar.

Asosiy algoritmlar: K-Means; DBSCAN; Isolation Forest. Chuqur o‘qitish (Deep Learning). Deep Learning sun’iy neyron tarmoqlariga asoslanadi va murakkab ma’lumotlar bilan ishlash imkonini beradi.

Kiberxavfsizlikda quyidagilar qo‘llaniladi: **CNN** – zararli dasturlarni aniqlash; **RNN va LSTM** – tarmoq trafigini vaqt bo‘yicha tahlil qilish;

Autoencoder – anomaliyalarni aniqlash. Sun’iy intellekt yordamida aniqlanadigan kiberhujumlar; AI quyidagi tahdidlarni samarali aniqlaydi[1],[2]:

DDoS hujumlari - Tarmoq trafikidagi keskin o‘zgarishlarni tahlil qilib hujumni boshlanish bosqichidayoq aniqlaydi.

Malware - Faylning xatti-harakatlarini kuzatib, ilgari noma’lum bo‘lgan zararli dasturlarni aniqlaydi.

Fishing - Elektron pochta matni, jo‘natuvchi manzili va havolalarni NLP algoritmlari yordamida tekshiradi.

Botnet - Qurilmalarning bir xil xatti-harakatlarini aniqlab, bot tarmoqlarini topadi.

Zero-Day hujumlari - Signaturasi mavjud bo‘lmagan yangi ekspluatatsiyalarni xulq-atvor tahlili orqali aniqlaydi.

Sun’iy intellekt asosidagi IDS va IPS tizimlari - Zamonaviy axborot xavfsizligida AI quyidagi tizimlar bilan integratsiyalashmoqda:

Intrusion Detection System (IDS) – tarmoqdagi shubhali faoliyatni aniqlaydi.

Intrusion Prevention System (IPS) – aniqlangan hujumni avtomatik ravishda bloklaydi.

AI integratsiyasi natijasida:

- noto‘g‘ri ogohlantirishlar kamayadi;
- aniqlash tezligi oshadi;
- real vaqt monitoringi yo‘lga qo‘yiladi.
- Sun’iy intellektning afzalliklari
- millionlab hodisalarni soniyalar ichida tahlil qiladi;
- real vaqt rejimida ishlaydi;
- inson omilidan kelib chiqadigan xatolarni kamaytiradi;
- yangi tahdidlarga moslashadi;
- xavfsizlik markazlari (SOC) ishini avtomatlashtiradi.

AI texnologiyalarini qo‘llash bilan bog‘liq ayrim cheklovlar mavjud: sifatli o‘quv ma’lumotlarining yetishmasligi; noto‘g‘ri ijobiy (False Positive) va noto‘g‘ri salbiy (False Negative) natijalar; katta hisoblash resurslariga ehtiyoj; AI modellariga qarshi adversarial hujumlar.

O‘zbekistonda davlat axborot tizimlari va muhim axborot infratuzilmalarini

himoya qilishda AI texnologiyalarini joriy etish dolzarb vazifalardan biridir. Bank tizimi, elektron hukumat, telekommunikatsiya va huquqni muhofaza qiluvchi organlarda AI asosidagi xavfsizlik yechimlarini bosqichma-bosqich joriy etish kiberhujumlarni erta aniqlash va ularga tezkor javob berish imkonini oshiradi [3],[4].

Shuningdek, mahalliy mutaxassislarni tayyorlash, ilmiy tadqiqotlarni rivojlantirish va milliy ma’lumotlar to‘plamlarini yaratish ushbu yo‘nalishning samaradorligini oshiradi.

Xulosa

Tadqiqot natijalari shuni ko‘rsatadiki, raqamli texnologiyalar jadal rivojlanayotgan bugungi sharoitda kiberxavfsizlikni ta’minlash davlat organlari, xususiy sektor va jamiyat oldidagi ustuvor vazifalardan biriga aylangan. Kiberhujumlarning murakkablashuvi, ularning avtomatlashtirilgan va sun’iy intellekt elementlaridan foydalangan holda amalga oshirilishi an’anaviy himoya vositalarining imkoniyatlarini cheklab qo‘ymoqda. Shu sababli sun’iy intellekt texnologiyalarini axborot xavfsizligi tizimlariga integratsiya qilish zamonaviy kiberxavfsizlikning eng istiqbolli yo‘nalishlaridan biri hisoblanadi.

Maqolada tahlil qilingan ilmiy manbalar va zamonaviy amaliyot shuni ko‘rsatadiki, mashinali o‘qitish (Machine Learning) hamda chuqur o‘qitish (Deep Learning) algoritmlari tarmoq trafigini real vaqt rejimida tahlil qilish, foydalanuvchilar xatti-harakatlarini o‘rganish, anomaliyalarni aniqlash, zararli dasturlarni tasniflash va ilgari uchramagan tahdidlarni prognozlashda yuqori samaradorlikka ega[1]. Ayniqsa, signaturaga asoslangan an’anaviy himoya vositalari aniqlay olmaydigan Zero-Day hujumlari, murakkab maqsadli hujumlar (APT), botnetlar va polimorfik zararli dasturlarni aniqlashda sun’iy intellektning afzalliklari yaqqol namoyon bo‘ladi.

Shu bilan birga, sun’iy intellektni kiberxavfsizlik sohasida qo‘llash ayrim muammolarni ham yuzaga keltiradi. Jumladan, algoritmlarni o‘qitish uchun katta

hajmdagi ishonchli ma’lumotlar bazasining zarurligi, noto‘g‘ri ijobiy va noto‘g‘ri salbiy natijalar ehtimoli, hisoblash resurslariga bo‘lgan yuqori talab hamda sun’iy intellekt modellariga qarshi adversarial hujumlar ushbu texnologiyalarni yanada takomillashtirish zarurligini ko‘rsatadi. Shu sababli AI tizimlarini joriy etishda texnik yechimlar bilan bir qatorda axborot xavfsizligi standartlari, xavflarni boshqarish metodologiyasi va malakali mutaxassislarni tayyorlash masalalariga ham alohida e’tibor qaratilishi lozim [5], [6],[7].

O‘zbekiston Respublikasida raqamli transformatsiya jarayonlari jadallashib borayotgan bir paytda davlat axborot tizimlari, bank-moliya sektori, telekommunikatsiya tarmoqlari va muhim axborot infratuzilmalarida sun’iy intellekt asosidagi xavfsizlik tizimlarini bosqichma-bosqich joriy etish dolzarb vazifa hisoblanadi. Bunday yondashuv kiberhujumlarni erta aniqlash, xavfsizlik hodisalariga tezkor javob qaytarish, inson omili bilan bog‘liq xatolarni kamaytirish hamda axborot tizimlarining barqaror ishlashini ta’minlashga xizmat qiladi.

Kelgusidagi ilmiy tadqiqotlarda milliy ma’lumotlar to‘plamlari asosida mashinali o‘qitish modellarini ishlab chiqish, sun’iy intellektning izohlanadigan (Explainable AI) usullarini kiberxavfsizlik tizimlariga tatbiq etish, avtomatlashtirilgan tahdidlarni tahlil qilish platformalarini yaratish hamda sun’iy intellekt asosidagi himoya vositalarining samaradorligini amaliy tajribalar orqali baholash muhim ilmiy yo‘nalishlardan biri bo‘lib qoladi.

Xulosa qilib aytganda, sun’iy intellekt nafaqat zamonaviy kiberhujumlarni aniqlash va ularga qarshi kurashishning samarali vositasi, balki kelajakdagi raqamli xavfsizlik tizimlarining asosiy tarkibiy elementi hisoblanadi. Uni ilmiy asoslangan yondashuvlar, xalqaro standartlar va milliy kiberxavfsizlik siyosati bilan uyg‘un holda rivojlantirish O‘zbekistonning axborot makonida barqaror va ishonchli kiberxavfsizlik muhitini shakllantirishga xizmat qiladi.

REFERENCES

1. Artificial Intelligence: A Modern Approach / Stuart Russell, Peter Norvig. – 4th Edition. – Pearson, 2021.
2. Deep Learning / Ian Goodfellow, Yoshua Bengio, Aaron Courville. – MIT Press, 2016.
3. Machine Learning for Cybersecurity / Akhil Kumar. – Springer, 2020.
4. National Institute of Standards and Technology (NIST). *Cybersecurity Framework (CSF).* – Gaithersburg, USA, 2018.
5. International Organization for Standardization. *ISO/IEC 27001: Information Security Management Systems – Requirements.* – 2022.
6. Cybersecurity and Cyberwar: What Everyone Needs to Know / P. W. Singer, Allan Friedman. – Oxford University Press, 2014.
7. Hacking: The Art of Exploitation / Jon Erickson. – No Starch Press, 2008.