SUN’IY INTELLEKT YORDAMIDA KIBERJINOYAT TAHDIDLARINI ANIQLASH VA ULARNING OLDINI OLISH IMKONIYATLARI

Murodjon Abdullayev
O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti, tadqiqotchisi. Toshkent, O‘zbekiston
imronkamron17@gmail.com
ORCID: 0009-0001-9832-7575
Axmadjon Eshmatov
Osiyo xalqaro universiteti, magistranti Buxoro, O‘zbekiston
axmadibroximovich@gmail.com
ORCID: 0009-0007-0467-3252

ANNOTATSIYA

Ushbu maqolada sun’iy intellekt (SI) texnologiyalarining kiberjinoyatlar tahdidlarini aniqlash va ularning oldini olishdagi o‘rni tahlil qilinadi. Maqolada kiberjinoyatlar turlari, sun’iy intellekt modellari, tahdidlarni aniqlash usullari va O‘zbekiston uchun amaliy yo‘nalishlar keng yoritilgan. Sun’iy intellekt asosida ishlovchi amaliy tizimlar, ularning ustunlik va kamchilik jihatlari, shuningdek, axloqiy va huquqiy masalalar ham yoritilgan. Ushbu maqolada sun’iy intellekt vositasida kiberjinoyatlarga qarshi kurashishning nazariy va amaliy jihatlari tahlil qilinadi.

Kalit so'zlar: Kiberjinoyatlar, sun’iy intellekt, mashinali o‘rganish, xavfsizlik tizimlari, anomaly detection, tahdid tahlili, Deep Learning, fishing, zararli dastur, DDoS hujum.

АННОТАЦИЯ

В данной статье анализируется роль технологий искусственного интеллекта (ИИ) в выявлении киберпреступных угроз и предотвращении их совершения. В статье подробно рассматриваются виды киберпреступлений, модели искусственного интеллекта, методы обнаружения угроз, а также практические направления их применения в условиях Республики Узбекистан. Освещаются практические системы, функционирующие на основе искусственного интеллекта, их преимущества и недостатки, а также этические и правовые аспекты использования данных технологий. В работе анализируются теоретические и практические аспекты противодействия киберпреступности с использованием средств искусственного интеллекта.

Ключевые слова: Киберпреступления, искусственный интеллект, машинное обучение, системы безопасности, обнаружение аномалий, анализ угроз, глубокое обучение (Deep Learning), фишинг, вредоносное программное обеспечение, DDoS-атаки.

ABSTRACT

This article analyzes the role of Artificial Intelligence (AI) technologies in detecting and preventing cybercrime threats. The paper comprehensively examines the types of cybercrimes, artificial intelligence models, threat detection methods, and practical application directions for the Republic of Uzbekistan. It also discusses AI-based practical systems, their advantages and limitations, as well as ethical and legal issues related to the use of these technologies. The study analyzes both theoretical and practical aspects of combating cybercrime using artificial intelligence tools.

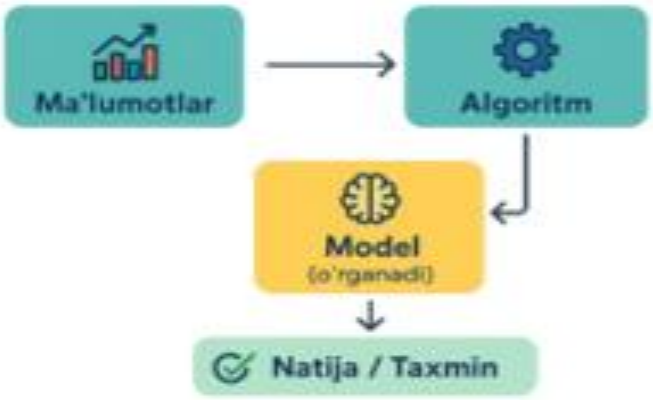
Keywords: Cybercrime, Artificial Intelligence, Machine Learning, Security Systems, Anomaly Detection, Threat Analysis, Deep Learning, Phishing, Malware, DDoS Attacks.

Raqamli rivojlanish shiddat bilan kechayotgan davrda kiberjinoyatlar nafaqat jismoniy shaxslarga, balki davlat tashkilotlari va yurik korxonalar xavfsizligiga ham jiddiy tahdid solib kelmoqda. Hozirgi kunda kiberxavfsizlik tizimlari murakkab tahdidlarni aniqlash va tezkor qarorlar qabul qilish jarayonlarida ko‘plab xato va kamchiliklarga yo’l qo’ymoqda. Shu sababli, xato, kamchiliklarni kamaytirish maqsadida sun’iy intellekt texnologiyalaridan foydalanish zarurati kundan-kunga oshib bormoqda.

Sun’iy intellekt nima va undan nima maqsadlarda foydalaniladi, kiberjinoyat tahdidlarini oldini olish va aniqlashda sun’iy intellektdan qanday foydalanish haqida so’z yuritiladi.

Sun’iy intellekt (SI) — bu kompyuterlar va dasturlar tomonidan inson aqliga xos funksiyalarni (masalan, o‘rganish, fikrlash, muammolarni hal qilish, qaror qabul qilish) bajarishga qodir texnologiyalar tizimidir [1]. Shu bilan bir qatorda Sun’iy intellekt tahdidlarni real vaqt rejimida kuzatish, ma’lumotlar oqimidan anomal xatti-harakatlarni ajratib olish, hamda avtomatlashtirilgan himoya tizimlarini yaratish imkonini beradi.

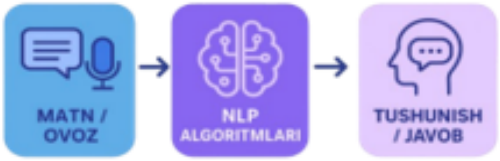
Statistik ma’lumotlarga ko‘ra, 2024-yilda dunyo bo‘ylab 33 milliarddan ortiq zararli kiberfaoliyatlar aniqlangan. Bu kabi zararli kiberjinoyatlarni amalga oshirishda, quyidagi zamonaviy texnologiyalardan foydalangan holda amalga oshirilgan. Masalan, *Phishing* – qalbaki xabarlar orqali shaxsiy ma’lumotlarni o‘g‘irlash, *Ransomware*– qurilmalarni bloklab, foydalanuvchidan to‘lov talab qilish, *DDoS* – serverlarni ishdan chiqarish, *Kriptovalyutaga oid jinoyatlar* – virtual valyutalardan noqonuniy foydalanish, Deepfake texnologiyalari orqali shaxsga tajovuz.



So‘nggi yillarda kiber tahdidlarni aniqlash va fosh etishda sun’iy intellekt (SI) modellari juda katta ahamiyat kasb etib kelmoqda, chunki zamonaviy kiberjinoyatlar juda murakkab, dinamik va yashirin shakllarda bo‘ladi. Quyida keltirilgan zamonaviy asosiy sun’iy intellekt (SI) modellarini ko‘rib ularni tahlil qilib chiqamiz. 1. Mashinali o‘rganish (Machine Learning), 2. Chuqur o‘rganish (Deep Learning), 3. NLP (Natural Language Processing), 4. Kompyuter ko‘rishi (Computer Vision). 5. Xulq-atvor (Behavioral)

Mashinali o‘rganish (Machine Learning): Bu kompyuter tizimlarining dasturda aniq ko‘rsatmalar berilmasdan, ma’lumotlar asosida o‘z faoliyatini avtomatik ravishda yaxshilashga imkon beruvchi sun’iy intellekt modeli [2]. Mashinali o’rganish modeli (Machine Learning) asosan Spamfilr-Elektron pochta xizmatiga kelgan xatlarning matni, jo‘natuvchi manzili va boshqa belgilarini tahlil qilib, ular spam (keraksiz) yoki normal xat ekanini avtomatik aniqlab beradi, shuningdek banklardagi firibgarliklarni ham aniqlashda yordam beradi.

Chuqur o‘rganish (Deep Learning) - bu mashinali o‘rganish (Machine Learning) modelining bir turi bo‘lib, ko‘p qatlamli sun’iy neyron tarmoqlar yordamida murakkab ma’lumotlarni avtomatik ravishda tahlil qilish va ulardan xulosa chiqarishni ta’minlaydi [3]. Chuqur o‘rganish modeli (Deep Learning) kibertahdidlar bilan bevosita aloqaga ega, chunki u ko‘plab xavfsizlik tizimlaridagi tahdidlarni avtomatik aniqlash va oldini olishda ishlatiladi. Misol uchun katta miqdordagi dasturiy kodlar



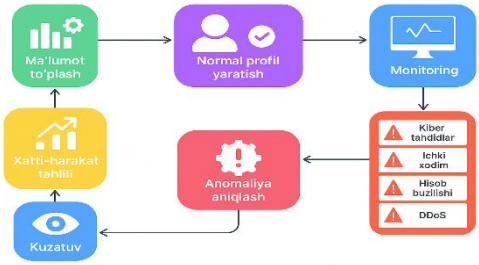
yoki fayl xususiyatlarini tahlil qilib, zararli dastur signallarini topish, tarmoq trafigidagi odatiy bo‘lmagan harakatlarni (anomaliyalarni) topib, DDoS yoki port skanerlash kabi hujumlarni erta aniqlash, shaxsga doir ma’lumotlar yush, ovoz yoki barmoq izlarini haqiqiyligini tekshiradi va noqonuniy kirishlarni to‘xtatish, oldingi hujumlar va xakerlik faoliyatlari haqidagi ma’lumotlardan foydalanib, kelajakda sodir bo‘lishi mumkin bo’lgan tahdidlarni oldidan bashorat qilishga yordam beradi. *NLP (Natural Language Processing)* - sun’iy intellektning modeli bo‘lib, kompyuterlarning inson tilini tushunishi, tahlil qilishi va yaratishini ta’minlab beradi [4].

Kibertahdidlarning katta qismi matnli ma’lumotlar orqali amalga oshirilishini inobatga olsak, NLP (Natural Language Processing) texnologiyasi ushbu tahdidlarni aniqlashda asosiy vosita hisoblanadi. Masalan, NLP algoritmlari elektron pochta yoki xabar matnlari ustida tahlil olib borib, foydalanuvchini aldashga yoki zararli havolalarga yo‘naltirishga urinish belgilarini aniqlashga yordam beradi, bundan tashqari NLP foydalanuvchi yozgan matnda zararli buyruqlar yoki kod injeksiyalarini aniqlashga yordam beradi. Ijtimoiy muhandislik hujumlarida, kiberjinoyatchilar til manipulyatsiyasi orqali foydalanuvchidan maxfiy ma’lumotlar olishga harakat qiladi, NLP bu manipulyativ til uslublarini aniqlashda yordam beradi. NLP avtomatik ravishda soxta xabarlar (fake) va yolg‘on ma’lumotlar (dezinformatsiya) ni tarqatuvchi matnlarni aniqlaydi, bu esa axborot xavsizligining bir qismi hisoblanadi. Xullas, NLP (Natural Language Processing) kiberxavfsizlik sohasida matn orqali amalga oshiriladigan tahdidlarni aniqlash va ularni avtomatik ravishda filtrlash uchun ishlatiladi.

Kompyuter ko‘rishi (Computer Vision) — bu sun’iy intellektning bir sohasi bo‘lib, kompyuter va tizimlarga rasmlar va video orqali olgan vizual ma’lumotlarni tahlil qilish, aniqlash va ulardan xulosa olishga imkon beradi [5]. Kompyuter ko‘rishi (Computer Vision) kibertahdidlar va kiberjiyatchiliklarni aniqlashda bir necha yo‘llar bilan aniqlashda yordam beradi. Misol uchun, Davlat tashkilotlari, o‘quv muassasalari va boshqa korxonalarga yuzni aniqlash orqali ruxsat etilmagan shaxslarga kirishni avtomat to‘xtatadi ya’ni ma’lumot markaziga noqonuniy kirishga uringan shaxslarni kameralar real vaqt rejimida aniqlaydi. Bundan tashqari xavfsizlik kameralaridagi anomal xatti-harakatlarni aniqlashga yordam beradi, ya’ni oddiy harakatlar bilan solishtirganda noodatiy yoki shubhali harakatlarni tahlil qiladi. Bu ma’lumot o‘g‘irlashga urinishlarni erta aniqlashga yordam beradi. Computer Vision yordamida raqamli firibgarlikni ham aniqlash imkoniyatlari ham mavjud, ya’ni ekran tasvirlari orqali qalbaki hujjat, soxta shaxsiy guvohnoma yoki bank kartalarini aniqlashda

yordam beradi. Jinoiy hodisa yuz berganda, kamera yozuvlarini avtomatik tahlil qilib, jinoyatchining harakatlarini vaqt bo‘yicha rekanstruksiya qiladi. Bu politsiya va kiberxavfsizlik bo‘limlariga tezkor dalil taqdim qiladi.

Xulq-atvor (Behavioral) tahlil modeli — foydalanuvchi yoki tizimning odatiy xatti-harakatlarini o‘rganib, shu profilga mos kelmaydigan g‘ayrioddiy holatlarni aniqlashga mo‘ljallangan model [6].



Bu model odatda tizimdagi odatiy ishlash tartibidan farqli harakatlarni aniqlaydi. Masalan, Oddiy ish vaqtida va oddiy fayl ma’lumotlari bilan ishlaydigan xodim birdan katta hajmdagi fayllarni yuklab olsa - behavioral modeli buni o‘g‘irlash sifatida belgilaydi. Foydalanuvchi odatda O‘zbekiston Respublikasi hududidan tizimga kiradi, lekin birdan chet davlatdan kirish holati bo‘lsa, model kirishni shubhali deb topadi.

Umumiy aytganda Xulq-atvor (Behavioral) tahlil modeli, foydalanuvchilar tizimdan noodatiy vaqtlarda foydalanishi, katta hajmdagi ma’lumotlarni yuklab olishi va boshqa hududlardan tizimga kirishi shunga o‘xshash shubhali holatlarni aniqlashga yordam beradi. Xulq-atvor (Behavioral) modeli *User and Entity Behavior Analytics (UEBA)* tizimlarining asosiy komponenti hisoblanadi, UEBA esa kiberjinoyatlarni aniqlashda ishlatiladi.

Zamonaviy sun’iy intellekt modellari kiber tahdidlarni aniqlash va fosh etishda nafaqat reaktiv, balki proaktiv himoya darajasini ta’minlaydi. Klasik signaturaga asoslangan usullar faqat ma’lum tahdidlarni topa olgan bo‘lsa, SI modellarining kuchi ularning xatti-harakatlarni chuqur o‘rganish, ularni kontekstga bog‘lab tahlil qilish va ilgari noma’lum bo‘lgan hujum turlarini ham aniqlash imkoniyatida yotadi.

Bugungi kunda chuqur o‘rganish Mashinali o‘rganish (Machine Learning), Chuqur o‘rganish (Deep Learning), NLP (Natural Language Processing), Kompyuter ko‘rishi (Computer Vision), Xulq-atvor (Behavioral) kabi modellar, kiberxavfsizlik tizimlarini faqat himoya vositasi emas, balki faol razvedka va tahdidni oldindan bashorat qiluvchi mexanizmga aylantirmoqda.

Biroq, bu modellarning samaradorligi — to‘g‘ri ma’lumot to‘plash, uzluksiz o‘qitish va inson ekspertizasi bilan integratsiyalashgan holda ishlashga bog‘liq. Shunday ekan, kelajakdagi eng muvaffaqiyatli kiberxavfsizlik yondashuvi — bu sun’iy intellekt (SI) algoritmlarining tezkor tahlil kuchini, insonning strategik fikrlash qobiliyati bilan birlashtirgan gibrid model bo‘ladi.

Foydalanilgan adabiyotlar:

1. **Russell, S., & Norvig, P.** (2020). *Artificial Intelligence: A Modern Approach* (4th Edition). Pearson Education.
2. Tom M. Mitchell, "Machine Learning", McGraw Hill, 1997.
3. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
4. Jurafsky, D., & Martin, J. H. (2023). *Speech and Language Processing* (3rd ed.). Pearson.
5. https://www.forbes.com/sites/davidbalaban/2024/04/27/how-computer-vision-is-transforming-cybersecurity/?utm_source=chatgpt.com
6. Chandola, V., Banerjee, A., & Kumar, V. (2009) – *Anomaly Detection: A Survey*. CM Computing Surveys, 41(3).