# SUN’IY INTELLEKT ASOSIDA AXBOROT XAVFSIZLIGINI TA’MINLASH

***Suyunov Akmal Xo’shboq o’g’li***
*TerDU 1-bosqich magistranti*
*suyunovakmal27@gmail.com*

**Annotatsiya:** Ushbu maqolada sun’iy intellekt texnologiyalarining axborot xavfsizligini ta’minlashdagi o’rni tahlil qilingan. Jumladan, tahdidlarni oldindan aniqlash va real vaqt rejimida monitoring hamda mashinali o’rganish algoritmlarining axborot tizimlarida qo‘llanilishi yoritilgan. Shuningdek, ilg’or sun’iy intellektga asoslangan xavfsizlik tizimlari va ularning samaradorlik jihatlari ko’rib chiqilgan.

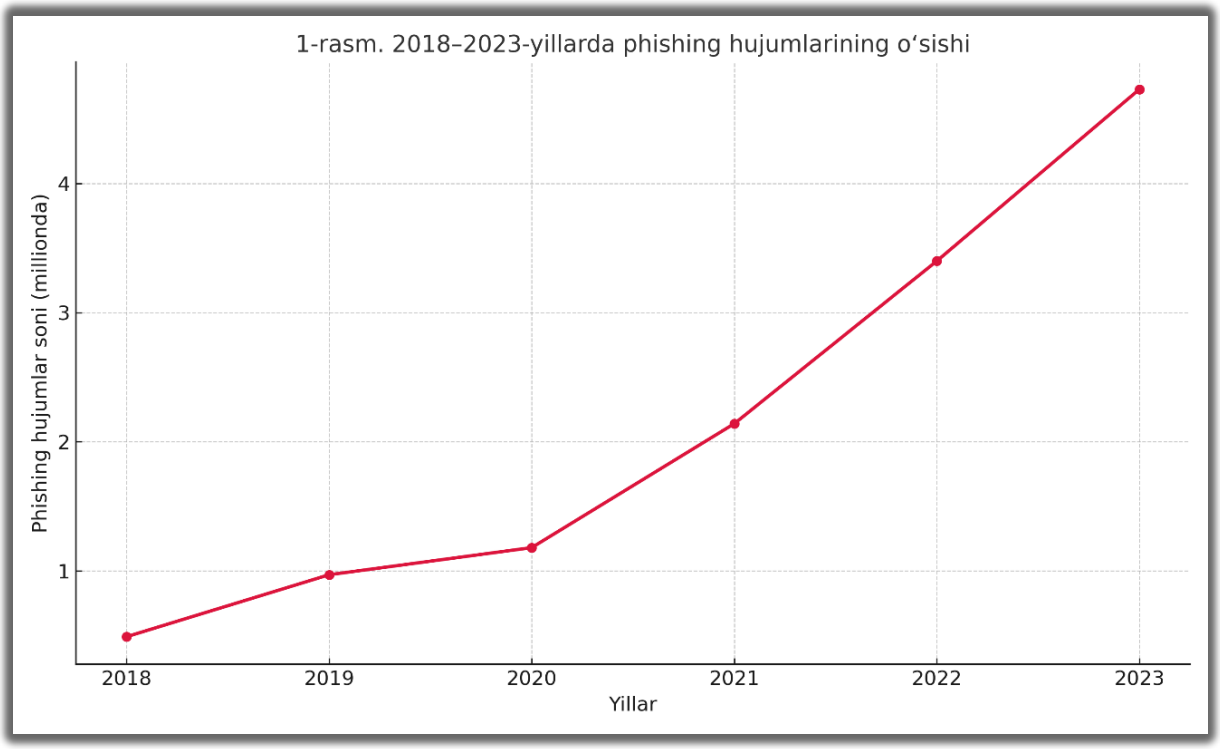
**Kalit so’zlar:** Axborot xavfsizligi, sun’iy intellekt, kiberxavfsizlik, mashinali o’rganish, neyron tarmoqlar, tahdidlarni aniqlash, foydalanuvchi xatti-harakatlarini tahlil qilish, AI asosidagi monitoring.

**Kirish.** Bugungi kunda raqamli texnologiyalar va sun’iy intellektning jadal rivojlanishi axborot xavfsizligini ta’minlashda dolzarb muammolardan biri sifatida ko’rilmoqda. Hozirda yangi kiberhujumlar, ma’lumotlarni o’g’irlash yoki tizimlarning buzilish holatlari sodir bo’lmoqda. Shu boisdan axborot xavfsizligini ta’minlashda sun’iy intellektning o’rni va uning samaradorligini oshirish masalalari va muammolarini hal etish, butun dunyo bo’ylab muhim ahamiyatga ega bo’lib bormoqda. AI asosidagi xavfsizlik texnologiyalari, ayniqsa, tahdidlarni aniqlash, foydalanuvchi xatti-harakatlarini tahlil qilish va real vaqt rejimida monitoring qilish kabi sohalarda yangi imkoniyatlar yaratmoqda. Hozirgi vaqtda kiberxavfsizlikni avtomatlashtirish va sun’iy intellektni joriy etish yo’nalishlari muntazam ravishda mukammallashib bormoqda.

**Adabiyotlar sharhi.** Axborot xavfsizligini ta’minlashda zamonaviy yondashuvlar borasida sun’iy intellekt (AI) va mashinaviy o’qitish (ML) texnologiyalari tobora muhim o’rin egallamoqda. So’nggi yillarda ushbu texnologiyalarga asoslangan xavfsizlik tizimlari kiberhujumlarning oldini olishda samarali vosita sifatida keng qo’llanilmoqda. Tadqiqotlar shuni ko’rsatmoqdaki, an’anaviy yondashuvlar — antiviruslar, xavfsizlik devorlari va statik tahlil vositalari — dinamik va murakkab tahdidlarga qarshi bundan-buyon har doim ham samarali bo’la olmaydi. Shu sababli, sun’iy intellekt asosidagi xavfsizlik yondashuvlari, global miqyosda joriy etilmoqda.

Adabiyotlarda sun’iy intellektning katta til modellari (LLM – Large Language Models) asosida kiberxavfsizlikni ta’minlashga oid ishlanmalar dolzarb mavzu sifatida bugungi kunda yuzaga kelmoqda. Shu boisdan Xitoylik bir guruh tadqiqiotchilar, Xu va boshqalar (2024-yil) tomonidan olib borilgan tizimli adabiyotlar sharhida 127 ta

asosiy ilmiy ish tahlil qilishgan, LLM’larning zaifliklarni aniqlash, zararli dasturlarni tahlil qilish, fishing hujumlarini oldindan ko‘rish va tarmoq xavfsizligini baholashdagi roli aniq ravshan ochib berilgan. Tadqiqotda LLM’larning kiber tahdidlarni aniqlashdagi samaradorligi ta’kidlangan bo’lsada, tushunarlilik, maxfiylik va domenlarga moslashtirish kabi muammolar ham keltirib o’tilgan. Quyidagi rasmda siz yaqinlar oralig’ida fishing hujumlari sonining ortishi keltirib o’tilgan.




1-rasm.

Shuningdek, Gaith Rjoub, Jamal Bentahar, Omar Abdel Wahab va boshqalarning ilmiy izlanishlaridan kelib chiqgan holda, sun’iy intellekt (AI) modellari, ayniqsa chuqur o’rganish (deep learning) asosidagi tizimlarning “qora quti” (black-box) xususiyatlari ustida izlanishlar qilingan. Mualliflar tushuntiriladigan sun’iy intellekt (XAI) yondashuvlarini kiberxavfsizlik sohasida qo’llash imkoniyatlarini o’rganib, mavjud metodologiyalarni tahlil qilganlar. Ular XAI yordamida kiber tahdidlarni yaxshiroq tushunish va samarali himoya qilish, choralarini ishlab chiqish imkoniyatlarini ko’rsatib o’tishganlar.

Hozirda birqancha amaliy ishlar ham olib borilmoqda bularga misol sifatida, Microsoft kompaniyasi tomonidan yaratilgan (2024-yil) Security Copilot – bu sun’iy intellekt asosidagi interaktiv yordamchi bo‘lib, u kiberxavfsizlik mutaxassislariga tahdidlar haqida tezkor va kontekstga asoslangan ma’lumotlarni taqdim etadi.

Yanabir amaliy izlanishlardan biri – bu Trend Micro AI Vositasi (2023-yil) AI asosida yaratilgan xavfsizlik platformasidir. U mashinaviy o‘qitish (ML) yordamida tahdidlarni aniqlaydi, xavf darajasini baholaydi va avtomatik tarzda inson omilisiz qarorlar qabul qilish imkoniyatiga ega.

Bundan tashqari, blokcheyn texnologiyasi ham ma’lumotlarni markazlashmagan tarzda saqlash va tranzaksiyalarni buzilmasligini kafolatlashda muhim rol o’ynaydi. Ralf Merkle tomonidan ilgari surilgan Merkle daraxtlari asosida qurilgan blokcheyn tizimlari ayniqsa moliyaviy sektorlarda keng qo‘llanilmoqda. Ammo blokcheyn texnologiyasida ham xesh funksiyalarining zaifliklari va ko’p resurslar talab qilishi, bu uning salbiy tarafi hisoblanadi. Bu muammolarni AI asosida tahlil qilish va optimallashtirish yo‘nalishidagi tadqiqotlar dolzarb bo’lib qolmoqda.

Bugungi kunda sun’iy intellekt va mashinaviy o’qitish texnologiyalari kiberxavfsizlik sohasida tahdidlarni oldindan prognoz qilish, foydalanuvchi va obyekt xatti-harakatlarini (ing.qisqartmasi – UEBA) aniqlash, g’ayritabiiy xarakatlarni avtomatik ravishda tanib olish imkonini bermoqda. Xususan, AI asosidagi tahlil algoritmlari kiberhujumlarning dinamikasini o’rganish va ularga qarshi samarali choralar ko’rishda katta afzallik bermoqda.

**Mavzuning o’rganilganlik darajasi:** Kiberxavfsizlik sohasida sun’iy intellekt texnologiyalarining qo’llanilishi axborot xavfsizligini ta’minlashda sezilarli ijobiy natijalar bermoqda. So’nggi yillarda olib borilgan ilmiy izlanishlar va texnologik yutuqlar, bu boradagi istiqbollarni yaqqol ko’rsatib bermoqda.

Masalan, 2020-yilda S. Buczak va E. Guven tomonidan olib borilgan “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection” nomli tadqiqotda mashinaviy o’qitish algoritmlaridan (Decision Trees, Random Forest, SVM, KNN, va Neural Networks) foydalanilgan holda tarmoqdagi g’ayritabiiy xarakatlarni aniqlash samaradorligi tahlil qilingan. Tadqiqot natijalari shuni ko’rsatdiki, AI asosidagi tahdidni aniqlash tizimlari an’anaviy qoida (rule-based) tizimlarga qaraganda ancha yuqori aniqlik va moslashuvchanlikka ega bo’lib, oldindan ogohlantirish, o’z-o’zini o’rganish qobiliyati, katta hajmdagi ma’lumotni qayta ishlash, avtomatik tahlil va xulosalar, hamda bundan tashqari, ba’zi kamchiliklar ham bor, noaniqlik va yolg’onning ijobiy holatlar, ma’lumotlar to’plamiga qaramlik, tushuntirishdagi murakkablik (explainability), xavfsizlikning o’ziga xos xatarlaridan iboratdir.

Sun’iy intellektni qo’llash bo’yicha bir juft olimlar, J. Sommer va J. Paxson (2010-yil) tomonidan olib borilgan “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection” nomli tadqiqotda sun’iy intellekt va mashinaviy o’qitish algoritmlarini tarmoqdagi kiberhujumlarni aniqlashda qo’llash imkoniyatlari chuqur tahlil qilingan. Ushbu ish mashinaviy o’qitish algoritmlarining haqiqiy (real-world) muhitda qo’llanilganda qanday natijalar berishini va qanday muammolarga duch kelinishini aniq ravshan yoritib bergan. Tadqiqotchilar real muhitdagi murakkabliklar, noto’g’ri xabarlar (false positives), va sun’iy test muhitlari bilan real tarmoq o’rtasidagi tafovutlarni chuqur va aniq o’rganishgan.

Yana bir muhim tadqiqotchi — Somya Ranjan Sahoo va uning hamkasblari tomonidan olib borilgan ishda (2022-yil) AI va ML texnologiyalarining kiberxavfsizlikdagi tadbiq qilinishi chuqur tahlil qilingan. Ular o'z maqolalarida mashinaviy o'qitish algoritmlaridan foydalangan holda zararli dasturlarni aniqlash va tahdidlarni tasniflash imkoniyatlarini ko'rib chiqqanlar. Shunga qaramasdan bu tadqiqotda ham kamchiliklarni ko'rishimiz mumkin, izohlanish muammosi, resursga talabchanlik, soxta ijobiy holatlar ba'zi holatlarda xakerlik faoliyati deb noto'g'ri signal berishi mumkin, bu esa noto'g'ri xavfni baholashga olib keladi.

Kelajakda kiberxavfsizlik sohasida sun'iy intellekt va mashinaviy o'qitish texnologiyalarining rivojlanishi davom etadi. Yangi algoritmlar va metodologiyalar ishlab chiqilish, tizimlarni yanada samarali va xavfsiz qilishga yordam beradi. Shuningdek, sohada boshqa innovatsion texnologiyalar ham kiberhujumlarni oldini olishda muhim o'rin egallaydi.

***Tahlil va natijalar:*** Axborot xavfsizligini ta'minlashda ko'plab ilmiy ishlar va dasturlar yaratilgan va yaratilmoqda, Mashhur sun'iy intellekt texnologiyalari va ularning qo'llanilishi va imkoniyatlari ortib bormoqda va davom etadi. Quyidagi jadvalda to'rta sun'iy intellektga asoslangan texnologiya keltirilgan.

1-jadval

| Texnologiya | Vazifasi | Afzalliklari |
|---|---|---|
| Machine Learning | Tahdidlarni aniqlash | Moslashuvchanlik, tezlik |
| Deep Learning | Noaniqlikni tahlil qilish | Kengaytirilgan aniqlik |
| LLM (ChatGPT kabi) | Xavfsizlik so‘rovlari tahlili | Keng bilim bazasi |
| XAI | Izohlanadigan qarorlar | Ishonchni oshiradi |

Quyidagi jadvalda uchta mashhur sun'iy intellekt modelining phishing e-maillarini aniqlashdagi samaradorligi ko‘rsatilgan. Bu modellar real vaqtda ishlovchi kichik dataset asosida sinovdan o'tkazilgan. Statistik ma'lumotlar asosida Random Forest modeli eng yuqori aniqlikni ko'rsatgan bo'lsa ham, resurslarga talab yuqoriligi sabab uni kichik tizimlarda to‘liq ishlatish cheklanishi mumkin.

2-jadval

| **Model** | **Aniqlik (%)** | **Afzalliklari** | **Kamchiliklari** |
|---|---|---|---|
| **Decision Tree** | 85 | Soddalik, izohlanish | Overfittingka moyil |
| **Random Forest** | 91 | Yuqori aniqlik, barqarorlik | Resurs talabchan |

| | | | |
|---|---|---|---|
| **Naive Bayes** | 78 | Tezlik, kam resursga ehtiyoj | Past aniqlik, murakkab holatlarda zaif |

Sun’iy intellekt modellari bugungi kunda bir qancha yirik kompaniya va tashkilotlar tomonidan keng miqyosda qo’llanilmoqda. Masalan, Google va Microsoft o’zlarining email xizmatlarida AI asosida fishing e-maillarni filtrlaydi. Statista (2024) ma’lumotlariga ko’ra, 2023-yilda butun dunyo bo’ylab aniqlangan fishing hujumlarining soni 4,7 milliondan oshgan. Bu ko’rsatkich 2020-yilga nisbatan qariyb ikki baravarga oshganini ko’rsatadi. Bunday tahdidlarning ko’payishi AI yordamida avtomatik tahlil va filtr tizimlarining ahamiyatini yanada oshiradi.

**Xulosa va takliflar.** Ushbu maqolada sun’iy intellekt texnologiyalarining axborot xavfsizligini ta’minlashdagi o’rni va ahamiyati tahlil qilindi. AI va ML algoritmlari yordamida tahdidlarni oldindan aniqlash, tahlil qilish va oldini olish imkoniyatlari ko’rib o’tildi. LLM (katta til modellari) va XAI (izohlanadigan sun’iy intellekt) texnologiyalari esa nafaqat tahdidlarni aniqlashda, balki ularning sabablarini tushuntirishda muhim o’rin egallaydi.

Shuningdek, yuqorida taqdim qilinganidek, yirik texnologik kompaniyalar (masalan, Google va Microsoft) AI texnologiyalaridan phishing hujumlariga qarshi kurashishda faol foydalanmoqda. 2023-yilda butun dunyo bo’ylab aniqlangan fishing hujumlar soni 4,7 millionga yetgani (Statista, 2024) bu texnologiyalarning dolzarbligini yana bir bor isbotlaydi.

## Adabiyotlar ro’yhati

1. Russell, Stuart J., and Peter Norvig. *Artificial intelligence: a modern approach*. pearson, 2016.
2. Goodfellow, Ian, et al. *Deep learning*. Vol. 1. No. 2. Cambridge: MIT press, 2016.
3. Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2003.
4. Shukla, Sameer. "Synergizing Machine Learning and Cybersecurity for Robust Digital Protection." (2023).
5. Abawajy, Jemal, and Andrei Kelarev. "A multi-tier ensemble construction of classifiers for phishing email detection and filtering." *Cyberspace Safety and Security: 4th International Symposium, CSS 2012, Melbourne, Australia, December 12-13, 2012. Proceedings 4*. Springer Berlin Heidelberg, 2012.
6. Doshi, Rohan, Noah Apthorpe, and Nick Feamster. "Machine learning ddos detection for consumer internet of things devices." *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018.

7. Ribeiro, Marco Tulio, Sameer Singh, and Carlos Guestrin. "" Why should i trust you?" Explaining the predictions of any classifier." *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*. 2016.
8. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
9. Toyirov, A. X., M. J. Zaripova, and F. T. Jumaev. "The use of virtual computers in teaching of information disciplines." *World science* 1.3 (3) (2015): 13-16.

**Web manbalar**

1. https://apwg.org/trendsreports/
2. https://www.statista.com/statistics/1493550/phishing-attacks-global-number/
3. https://www.statista.com/statistics/266155/number-of-phishing-attacks-worldwide/