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.

6. **Axmedov J.R.** Dasturlash asoslari. O‘quv q‘llanma //“Kreativ fikrlash nashriyot matbaa uyi” UO‘K: 689(086 D-18). ISBN: 978-9910-8173-8-0. 2025-yil. 180 bet

7. **Axmedov J.R., D.I.Kulmuradov, B.B.Toshpulatov.** “Kompyuterli loyihalash (CAD, CAM, CAE). (1-qism)” O`quv qo`llanma. UDK 21474.23 ISBN: 978-9943-9585-7-9. Jizzax. JizPI tipografiyasi. -2023. 166 bet.

8. **Ясницкий Л.Н.** *Введение в искусственный интеллект: учебное пособие для студентов вузов.* — Москва: Academia, 2005. — 175 с. ISBN: 5-7695-1958-4.

9. **Божич В.И. и др.; под ред. А.И. Галушкина, С.Д. Кулика.** *Нейрокомпьютеры в информационных и экспертных системах.* — Москва: Радиотехника, 2007. — 120 с. ISBN: 5-88070-134-4.

SUN'IY INTELLEKT ASOSIDAGI FISHING VA IJTIMOIY MUHANDISLIK HUJUMLARINI ANIQLASH TIZIMLARI: ZAMONAVIY YONDASHUVLAR TAHLILI

O‘zbekiston Milliy universiteti Jizzax filiali o‘qituvchisi
Yusupov Begzod Ismoil o‘g‘li
begzody231@gmail.com
O‘zbekiston Milliy Universiteti Jizzax filliali talabalari
Butunboyev Azizbek O’tkirbek o’g’li
butunboyevazizbek267@gmail.com
Ergashev Po‘latbek Nuriddin o‘g’li
ergashevpolatbek79@gmail.com
Kazakova Shahnoz Janatbek qizi
shahnozkazakova2@gmail.com

Annotatsiya: Ushbu maqolada sun'iy intellekt (SI) texnologiyalari asosida fishing va ijtimoiy muhandislik hujumlarini aniqlash tizimlari ilmiy-tahliliy nuqtai nazardan yoritilgan. Avvalo, generativ sun'iy intellektning kiberjinoyatchilar tomonidan qanday tarzda hujumlarni murakkablashtirish uchun qo‘llanilayotgani statistik ma'lumotlar asosida ko‘rsatib o‘tilgan. So‘ngra fishingga qarshi kurashda qo‘llaniladigan asosiy mashinaviy o‘qitish (Random Forest, Gradient Boosting, gibrid ansambl modellari), chuqur o‘qitish va tabiiy tilni qayta ishlash (NLP) usullari, shuningdek xulq-atvor tahliliga asoslangan anomaliyalarni aniqlash tizimlari ilmiy manbalar asosida tahlil qilingan. Turli tadqiqotlarda qo‘lga kiritilgan aniqlik ko‘rsatkichlari (93–99% oralig‘ida) taqqoslangan va ularning amaliy qo‘llanilish sohalari misollar bilan izohlangan.

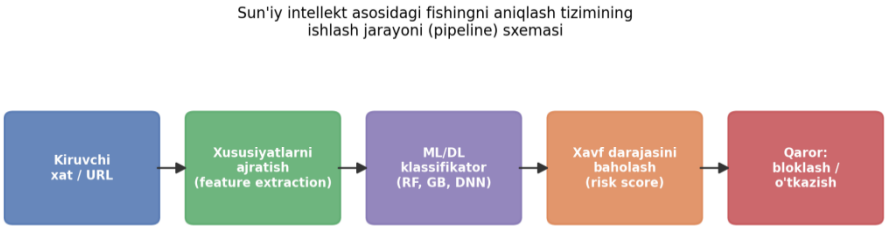
Kalit so‘zlar: sun'iy intellekt, fishing, ijtimoiy muhandislik, mashinaviy o‘qitish, chuqur o‘qitish, kiberxavfsizlik, deepfake, anomaliyalarni aniqlash, biznes elektron pochtasining buzilishi (BEC).

Kirish: Zamonaviy kiberxavfsizlik sohasida fishing va ijtimoiy muhandislik hujumlari eng keng tarqalgan va eng samarali tahdid turlaridan biri bo‘lib qolmoqda. Jahon iqtisodiy forumining 2026-yilgi Global kiberxavfsizlik hisobotiga ko‘ra,

tashkilotlarning 73 foizi 2025-yilda kiberfiribgarlik hujumlariga duch kelgan, bunda sun'iy intellekt yordamida kuchaytirilgan fishing birinchi marta ransomware hujumlaridan oldinga chiqib, korxonalar uchun eng dolzarb xavf sifatida qayd etilgan. Generativ sun'iy intellektning ommalashuvi bu sohada tubdan burilish nuqtasini yaratdi. KnowBe4 kompaniyasining 2025-yilgi hisobotiga koʻra, fishing xatlarining 82,6 foizi hozirda sun'iy intellekt yordamida yaratilgan kontentga ega boʻlib, bu koʻrsatkich 2023-yildan buyon 1265 foizga oʻsgan. Bunday sharoitda an'anaviy himoya usullari — imlo xatolarini, noqulay iboralarni yoki umumiy murojaatlarni aniqlashga asoslangan yondashuvlar — oʻz samaradorligini yoʻqotmoqda. Ushbu vaziyat, oʻz navbatida, mudofaa tomonida ham sun'iy intellektdan foydalanishni ob'ektiv zaruratga aylantirdi.

Fishing va ijtimoiy muhandislikning zamonaviy shakllari : Ijtimoiy muhandislik — texnik zaifliklardan emas, balki inson psixologiyasidan (ishonch, shoshilinchlik, obroʻ-e'tibor hissi) foydalangan holda maxfiy ma'lumotlarni yoki moliyaviy resurslarni egallashga qaratilgan firibgarlik usulidir. Fishing esa ushbu usulning eng ommaviy koʻrinishi boʻlib, odatda soxta elektron xat yoki veb-sahifa orqali amalga oshiriladi. Sun'iy intellekt ushbu hujumlarning sifat jihatidan yangi bosqichga oʻtishiga sabab boʻldi. Xususan, Hoxhunt kompaniyasining global tahdidlarni kuzatish tarmogʻi (4 million foydalanuvchi ma'lumotlari asosida) SI yordamida yaratilgan fishing xatlarining ulushi 2025-yil noyabr oyida atigi 4 foizni tashkil etgan boʻlsa, dekabr oyida bu koʻrsatkich 56 foizga, ya'ni 14 baravar oshganini qayd etadi.Amaliy misol sifatida, Microsoft tomonidan oʻtkazilgan tadqiqotda sun'iy intellekt yordamida yaratilgan fishing xatlarining bosish (click) darajasi 54 foizni tashkil etgan, holbuki inson tomonidan qoʻlda tayyorlangan xatlarda bu koʻrsatkich atigi 12 foiz boʻlgan — ya'ni SI samaradorlikni 4,5 barobarga oshirgan [3]. Bundan tashqari, sun'iy intellekt orqali generativ ovoz taqlidi (vishing) hollari 2023–2024-yillar oralig'ida 442 foizga, deepfake video firibgarlik holatlari esa 2025-yilda yiliga 680 foizga oʻsgan (2-rasmga qarang). Alohida ta'kidlash joizki, biznes elektron pochtasining buzilishi (Business Email Compromise, BEC) — ijtimoiy muhandislikning eng qimmatga tushadigan turi hisoblanadi. AQSH Federal tergov byurosining Internet jinoyatlari shikoyatlar markazi (FBI IC3) ma'lumotlariga koʻra, 2024-yilda BEC hujumlari orqali 21 442 ta rasmiy shikoyat qayd etilgan boʻlib, umumiy zarar 2,77 milliard AQSH dollarini tashkil etgan.

Sun'iy intellekt asosidagi aniqlash tizimlarining ishlash tamoyillari: Fishing va ijtimoiy muhandislik hujumlarini aniqlashda qoʻllaniladigan sun'iy intellekt tizimlari, odatda, bir necha bosqichli jarayon (pipeline) asosida ishlaydi: dastlab kiruvchi xat yoki havoladan xususiyatlar ajratib olinadi, soʻngra ular mashinaviy yoki chuqur oʻqitish klassifikatori orqali tahlil qilinadi, natijada xavf darajasi (risk score) hisoblanadi va, nihoyat, xatni bloklash yoki foydalanuvchiga yetkazish haqida avtomatik qaror qabul qilinadi (1-rasmga qarang).



1-rasm. Sun'iy intellekt asosidagi fishingni aniqlash tizimining ishlash jarayoni (pipeline) sxemasi

Statistik xususiyatlarga asoslangan mashinaviy o‘qitish usullari: Fishingni aniqlashning eng keng tarqalgan yondashuvlaridan biri — veb-manzil (URL) va veb-sahifaning statistik xususiyatlarini (domen uzunligi, maxsus belgilar soni, SSL sertifikat holati va boshqalar) tahlil qiluvchi klassifikatorlardan foydalanishdir. Tadqiqotlar shuni ko‘rsatadiki, Tasodifiy o‘rmon (Random Forest) algoritmi ushbu vazifada 93–96 foiz aniqlikka erishadi, Auto-WEKA optimallashtiruvi bilan esa aniqlik 99 foizgacha, soxta ijobiy signallar darajasi esa atigi 1 foizgacha kamayadi. Yanada yuqori natijalarga gibrid (ansambl) modellar orqali erishilmoqda. Xususan, qaror daraxtlari, tasodifiy o‘rmon va gradientli kuchaytirish (Gradient Boosting) klassifikatorlarini birlashtirgan gibrid model 98,4 foizgacha aniqlikni ta'minlagan. Shu bilan birga, Gradient Boosting klassifikatoriga asoslangan alohida model URL xususiyatlarini tahlil qilish orqali 97,6 foiz aniqlik, 96,5 foiz aniqlik ko‘rsatkichi (precision) va 98,1 foiz sezuvchanlik (recall) darajasiga erishgan . Turli tadqiqotlarda qo‘lga kiritilgan ushbu ko‘rsatkichlar. (1-jadvalda umumlashtirilgan).

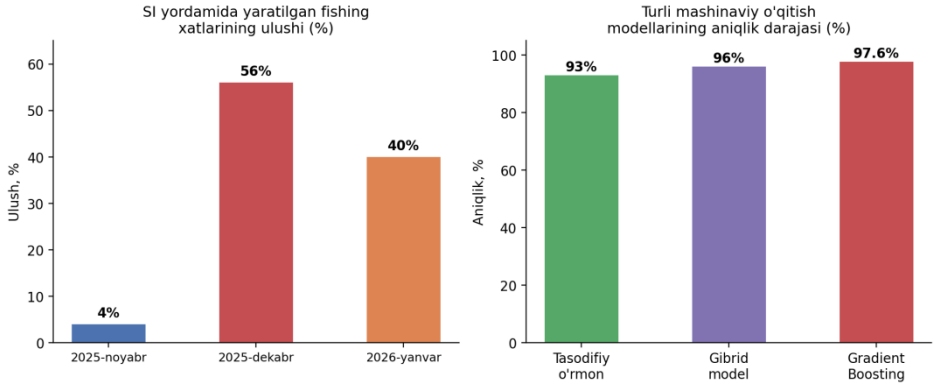
Fishingni aniqlashda qo'llaniladigan mashinaviy o'qitish
modellarining samaradorlik ko'rsatkichlari solishtirmasi

Model / usul	Aniqlik (Accuracy)	Aniqlik darajasi (Precision)	Sezuvchanlik (Recall)	Manba
Tasodifiy o'rmon (Random Forest)	93–96%	—	—	[6]
Random Forest + Auto-WEKA	99%	—	—	[6]
Gibrid ansambl model (DT + RF + GB)	98,4%	—	—	[7]
Gradient Boosting Classifier	97,6%	96,5%	98,1%	[8]
Chuqur neyron tarmoq (DNN), 14 ta xususiyat asosida	94,46%	—	—	[9]

1-jadval. Fishingni aniqlashda qo‘llaniladigan mashinaviy o‘qitish modellarining samaradorlik ko‘rsatkichlari solishtirmasi [6; 7; 8; 9]

Chuqur o‘qitish va tabiiy tilni qayta ishlash (NLP) asosidagi tizimlar Zamonaviy fishing xatlari endi grammatik xatolarsiz, kontekstga mos va shaxsiylashtirilgan tarzda yaratilayotgani sababli, faqat statistik xususiyatlarga tayanish yetarli emas. Shu sababli chuqur o‘qitish tarmoqlari — jumladan chuqur neyron tarmoqlar (DNN), Wide & Deep va TabNet arxitekturalari — matn mazmuni va yashirin semantik bog‘lanishlarni tahlil qilish uchun qo‘llanilmoqda. Amaliy tadqiqotda 58 645 ta URL manzili va 111 ta xususiyatni o‘z ichiga olgan ma'lumotlar to‘plami asosida ishlab chiqilgan forward-feed neyron tarmog‘i, atigi 14 ta asosiy xususiyatdan foydalangan holda 94,46 foiz aniqlikka erishgan, bu esa hisoblash resurslarini tejagan holda yuqori samaradorlikni ta'minlash mumkinligini isbotlaydi.

Xulq-atvor tahliliga asoslangan anomaliyalarni aniqlash: Matn yoki URL tahlilidan farqli o‘laroq, xulq-atvorga asoslangan tizimlar foydalanuvchi yoki tashkilot ichidagi odatiy faoliyat naqshlarini (login vaqti, IP manzil, xat yozish uslubi, moliyaviy operatsiyalar chastotasi) o‘rganib, ulardan chetlanishlarni real vaqt rejimida aniqlaydi. Bunday tizimlar, ayniqsa, BEC hujumlarini — ya'ni rahbariyat nomidan yuborilgan, ammo odatiy til uslubi yoki so‘rov turidan farq qiluvchi xatlarni — aniqlashda samarali hisoblanadi.



2-rasm. SI yordamida yaratilgan fishing xatlarining ulushi dinamikasi va turli mashinaviy o‘qitish modellarining aniqlik ko‘rsatkichlari solishtirmasi [2; 6; 7; 8]

SI asosidagi aniqlash tizimlarining amaliy ahamiyati

Sun'iy intellekt asosidagi aniqlash tizimlarining amaliy ahamiyati bir necha yo‘nalishda namoyon bo‘ladi. Birinchidan, ular real vaqt rejimida ishlash imkoniyatiga ega bo‘lib, xat yoki veb-sahifa foydalanuvchiga yetib borishidan oldin uni bloklash imkonini beradi. Ikkinchidan, ushbu tizimlar doimiy o‘z-o‘zini takomillashtirish (continuous learning) xususiyatiga ega bo‘lib, yangi hujum naqshlarini avtomatik ravishda o‘rganib boradi. Amaliy misol tariqasida, korporativ elektron pochta xavfsizligi platformalari xat matni, jo‘natuvchi manzili, havolalar va ilova fayllarini bir vaqtning o‘zida tahlil qilib, xavf darajasini foizlarda baholaydi va yuqori xavfli xatlarni avtomatik ravishda karantinga joylashtiradi.

Muammolar va cheklovlar : Sun'iy intellekt asosidagi aniqlash tizimlari yuqori samaradorlikka qaramay, bir qator jiddiy muammolarga ham duch kelmoqda. Birinchi muammo — bu 'raqobatbardosh sun'iy intellekt' (AI vs AI) holati bo‘lib, hujumchilar tomonidan qo‘llanilayotgan SI texnologiyalari doimiy ravishda takomillashib bormoqda. Xususan, hozirgi kunda polimorf fishing hujumlarining 92 foizdan ortig‘i sun'iy intellekt yordamida bir kampaniya doirasida yuzlab kontekstual jihatdan noyob xat variantlarini yaratadi, bu esa an'anaviy naqshga asoslangan filtrlarni samarasiz qilib qo‘yadi. Ikkinchi muammo — model eskirishi (concept drift) hodisasi bo‘lib, bu vaqt o‘tishi bilan hujum naqshlarining o‘zgarishi natijasida ilgari yuqori aniqlikka ega bo‘lgan modellarning samaradorligi pasayib borishini anglatadi. Shu sababli aniqlash tizimlarini muntazam ravishda yangi ma'lumotlar bilan qayta o‘qitib turish zarurati yuzaga keladi. Uchinchi muammo — deepfake ovozli va videofiribgarlikka qarshi kurashning murakkabligi. Tadqiqotlar shuni ko‘rsatadiki, inson yuqori sifatli deepfake videolarni atigi 24,5 foiz aniqlik bilan

farqlay oladi, bu esa ushbu turdagi hujumlarga qarshi asosan texnik (SI asosidagi) himoya vositalariga tayanish zarurligini ko‘rsatadi.

Xulosa: O‘tkazilgan tahlil shuni ko‘rsatadiki, sun'iy intellekt zamonaviy fishing va ijtimoiy muhandislik hujumlariga qarshi kurashning ajralmas qismiga aylanib bormoqda. Mashinaviy o‘qitish, chuqur o‘qitish va xulq-atvor tahliliga asoslangan tizimlar 93 foizdan 99 foizgacha yuqori aniqlik ko‘rsatkichlarini namoyish etib, an'anaviy himoya usullariga nisbatan sezilarli ustunlikka ega ekanligini isbotladi. Shu bilan birga, hujumchilar tomonidan ham xuddi shu texnologiyalardan foydalanilayotgani sababli, kiberxavfsizlik sohasi tobora 'sun'iy intellektga qarshi sun'iy intellekt' xarakteriga ega bo‘lib bormoqda. Shu sababli, kelajakda samarali himoyani ta'minlash uchun aniqlash tizimlarini doimiy ravishda takomillashtirish, xodimlarni SI asosidagi simulyatsiyalar orqali o‘qitish hamda texnik va inson omilini uyg‘unlashtirgan kompleks yondashuvni qo‘llash zarur bo‘ladi.

Foydalanilgan adabiyotlar

1. AI phishing: How attackers achieve 54% click rates in 5 minutes. — Vectra AI, 2026. — URL: https://www.vectra.ai/topics/ai-phishing

2. Hoxhunt Phishing Trends Report 2026. — Hoxhunt, 2026. — URL: https://hoxhunt.com/blog/ai-phishing-attacks

3. AI Phishing Statistics 2026: The Inflection Point, the 14× Surge, and Why MFA No Longer Protects You. — Axis Intelligence, 2026. — URL: https://axis-intelligence.com/ai-phishing-statistics/

4. AI Spear Phishing in 2026: Statistics, Trends & CISO Action Guide. — Brightside AI, 2026. — URL: https://www.brside.com/blog/ai-spear-phishing-2026-ciso-guide

5. 2024 FBI IC3 Report: Business Email Compromise Remains a Multi-Billion Dollar Threat. — Abnormal AI, 2025. — URL: https://abnormal.ai/blog/2024-fbi-ic3-report

6. Kazi R. Evaluation of Machine Learning Classifiers for Phishing Detection. — University of Victoria, 2016. — URL: https://dspace.library.uvic.ca/items/4fa15a2c-e257-4440-9416-069bb839b06d

7. Hybrid machine learning model for phishing detection. Proceedings of 2024 IEEE 12th International Conference on Intelligent Systems (IS). — IEEE, 2024. — URL: https://researchportal.port.ac.uk/en/publications/hybrid-machine-learning-model-for-phishing-detection/

8. Gradient Boosting Classifier for Phishing Website Detection. — SLIIT Research & Development Archive, 2024. — URL: https://rda.sliit.lk/handle/123456789/4068

9. Enhancing Phishing Detection: A Machine Learning Approach With Feature Selection and Deep Learning Models. — IEEE Access, 2025. — URL: https://impressions.manipal.edu/open-access-archive/14154

10. Cost of a Data Breach Report 2025. — IBM, 2025. — URL: https://www.stingrai.io/blog/phishing-statistics-2026 (IBM 2025 hisoboti asosida keltirilgan ma'lumotlar).