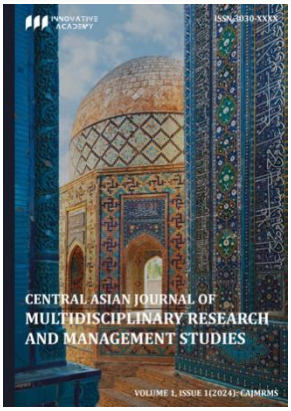


KIBERXAVFSIZLIK SOHASIDA SUN'IY INTELLEKT (SI)NING AHAMIYATI

Mirzayeva Shahlo Abduraxmonovna

Shahrisabz davlat pedagogika instituti katta o'qtuvchisi

Baxtiyorova Sevinch Faxriddin qizi

Ichki ishlar vazirligi akademiyasi kursanti

https://doi.org/10.5281/zenodo.15544689

ARTICLE INFO

Received: 15 th May 2025
Accepted: 19th May 2025
Published: 29th May 2025

KEYWORDS

Sun'iy intellekt (SI), kiberxavfsizlik , DDoS hujumlar, tahdid razvedkasi, Evristik tahlil (Heuristic Analysis) , Sandobox tahlili, Yadroviy (kernel-level) monitoring, SIEM — Security Information and Event Management , Darktrace, Honeytoken usullari va boshqalar .

ABSTRACT

Mazkur maqolada hozirgi rivojlanib kelayotgan axborot olami va kiberxavfsizlik sohasida Sun'iy intellekt (SI) qay darajada ahamiyatga ega ekanligi undan foydakanish jaroyonida maxsus usullarning mavjudligi shuningdek avtomatlashtirilgan qarorlar qabul qilish doirasi qay darajada ekanligi haqida keltirib o'tilgan. Qo'shimcha qilib aytib o'tish joizki, zararli dasturlar larnianiqlash usullar va tarmoqda yuzaga kelayotgan noodatiy faoliyatlarni aniqlashda Sun'iy intellekt (SI)ning o'rni atroflicha o'rganilgan.

Sun'iy intellekt (SI), kiberxavfsizlik , DDoS hujumlar, tahdid razvedkasi, Evristik tahlil (Heuristic Analysis) , Sandobox tahlili, Yadroviy (kernel-level) monitoring, SIEM — Security Information and Event Management , Darktrace, Honeytoken usullari va boshqalar .

Sun'iy intellekt (SI) kiberxavfsizlik sohasida tobora muhim rol o'ynamoqda. Uning asosiy afzalligi — katta miqdordagi ma'lumotlarni tezda tahlil qilish, tahdidlarni aniqlash va ularga avtomatik tarzda javob qaytarish imkoniyatidir. Sun'iy intellektning kiberxavfsizlikdagi asosiy o'rinlari va foydalarini bir necha yo'nalishlarda ko'rib chiqish mumkin.

Tahdidlarni aniqlash va oldini olish. SI tarmoqlardagi noodatiy faoliyatni aniqlay oladi (masalan, DDoS hujumlar, zararli dasturlar).An'anaviy tizimlarga qaraganda tezroq va aniqroq tahlil qiladi.Xulq-atvor tahlili.Foydalanuvchilarning odatdagi xatti-harakatlarini o'rganib, g'ayritabiiy harakatlarni (masalan, ma'lumotlarni katta hajmda yuklab olish) aniqlaydi.Ichki tahdidlarni (insider threat) aniqlashda foydali.Avtomatlashtirilgan qarorlar qabul qilish.Tahdid aniqlanganda, SI avtomatik tarzda xavfsizlik choralarini ko'radi (masalan, foydalanuvchini bloklash, tizimdan ajratish).Vaqtni tejaydi va inson omiliga bog'liqlikni kamaytiradi.Tahdid razvedkasi (Threat Intelligence).Turli manbalardan kelayotgan tahdidlar haqidagi ma'lumotlarni yig'ib, tahlil qiladi.Global va lokal xavf-xatarlar haqida oldindan ogohlantirish beradi. Zararli dasturlarni aniqlash. SI yangi, ilgari noma'lum bo'lgan zararli dasturlarni (zero-day attacks) tahlil qilishda foydali. Statik va dinamik tahlil orqali zararli kodlarni aniqlaydi. Ammo, noto'g'ri ma'lumotlarga asoslangan SI noto'g'ri xulosa chiqarishi mumkin.Kiberjinoyatchilar ham SI-dan foydalanishi mumkin (AI vs AI).Modelni o'rgatish uchun ko'p resurs talab qilinadi.

Asosan Sun'iy intellekt (SI) kiberxavfsizlikning eng muhim yo'nalishlaridan biri bo'lgan zararli dasturlarni aniqlashda bir necha usullar orqali yordam berishi mumkin .imzo asosidaaniqlash

bu usul eng keng tarqalganlaridan biri hisoblanib uning prinsipi , zararli dastur kodining yoki uning faoliyatining oldindan ma’lum imzosiga (pattern) asoslanadi. Juda aniq va tez ishlaydi, kam resurs sarflaydi. Faqat ilgari aniqlangan (ma’lum) malware’larni ushlaydi, yangi turlar (zero-day)ni aniqlay olmaydi. Evristik tahlil (Heuristic Analysis) usulidan foydalanganimizda ular Zararli dastur xatti-harakatiga o‘xshash funksiyalarni izlaydi.Yangi yoki o‘zgartirilgan zararli dasturlarni aniqlash imkonini beradi.Ba'zida "false positive" (noto‘g‘ri ogohlantirish) bo‘lishi mumkin. Xulq-atvor (davranish) tahlili (Behavior-based Detection orqali dastur tizimda qanday harakat qilayotganiga qarab baho beradi (masalan, faylni shifrlasa — bu ransomware bo‘lishi mumkin).Yangi va noma’lum malware’larni ham aniqlaydi. Resurs talab qiladi, real vaqtda monitoring qilish kerak bo’ladi. Sandobox tahlili (Sandboxing) shubhali dastur virtual muhitda (izolyatsiyalangan tizimda) ishga tushiriladi va uning harakati kuzatiladi.Tashqi tizimga zarar yetkazmasdan dastur tahlil qilinadi. Sekin ishlashi mumkin, ba’zi ilg‘or malware’lar sandbox muhitini aniqlab, faoliyatini yashiradi.Sun’iy intellekt (AI) va Mashinali o‘rganish (ML) asosida aniqlash asosan katta miqdordagi zararli va normal dastur xatti-harakatlarini o‘rgatib, yangi tahdidlarni avtomatik ravishda aniqlaydi. yangi, o‘zgartirilgan yoki murakkab malware turlariga qarshi samarali.Modelni tayyorlash uchun ko‘p ma’lumot va resurs kerak bo‘ladi, noto‘g‘ri aniqlash holatlari bo‘lishi mumkin.Yadroviy (kernel-level) monitoring prinsiplariga to’xtalsak, Operatsion tizim yadrosida (kernel) yuz berayotgan faoliyatlar tahlil qilinadi. Rootkit kabi chuqur yashiringan malware’larni aniqlashga imkon beradi. Murakkab va tizim barqarorligiga ta’sir qilishi mumkin.

SI Tarmoqdagi Qanday Noodatiy Faoliyatlarni Aniqlaydi? Bu albatta o’rinli savol mavjud, DDoS hujumi, ma’lumotlar sizishi (data exfiltration), virus tarqatilishi bularningbarchasi ehtimoliy havflar hisoblanadi aytaylik tarmoq orqaliodatdagidan 110 baravar ko’p ma’lumot yuborilishi natijasida u trafk hajmining keskin o’zgarishinisezadi bunoodatiy holat haqida signal beradi.keyingi holatda esa Tashqi hujum, port scanning, brute-force urinishlari xavfi yuzaga kelib Ichki serverga ilgari hech qanday aloqa bo‘lmagan xorijiy IP’dan bog‘lanish orqali Noan’anaviy IP-manzillardan murojaatlarni aniqlab beradi. Tunda yoki dam olish kunlari katta hajmli fayllar ko‘chirilishi Ehtimoliy xavf ya’ni Ichki xodim tomonidan ma’lumot o‘g‘irlanishi yoki avtomatlashtirilgan hujumlar sababli odatdagi ish vaqtlaridan tashqari faoliyatlarni aniqlab kerakli signallarni adminga yetkazadi. Foydalanuvchi xatti-harakatidagi g‘ayritabiiyliklarni esa oddiy xodim birdaniga ma’muriy (admin) darajadagi amallarni bajara boshlasa, Credential hijacking (login va parollar o‘g‘irlanib, foydalanilmoqda) ehtimoli xavf orqali ma’lumot yetkazadi.Fayllarga bo‘lgan noodatiy murojaatlarni o’rganish jaroyanida katta hajmdagi muhim fayllar tez-tez ochilmoqda yoki shifrlanmoqda holati yuz berib Ransomware (shifrlovchi zararli dastur), data leak xavfini yuzaga keltiradi . Shubhali portlar yoki protokollardan foydalanish Ichki tarmoqda Tor, VPN yoki noma’lum protokollarning ishlatilishi qaysidir tarmoq bilan maxfiy aloqa kanallari orqali ma’lumot uzatish, xavfsizlik devoridan aylanib o‘tish bilan kuzatiladi.Qurilmalarning bir-biri bilan g‘alati aloqasi oddiy printer birdaniga ko‘p tarmoq faoliyati bilan band bo‘lib qoladinatijada IoT qurilmalari orqali hujum (botnet, lateral movement)xavfi kuzatiladi. Login va autentifikatsiyadagi g‘alati urinishlarni esa bitta foydalanuvchi nomi bilan bir vaqtning o‘zida bir nechta joydan login qilish jaroyonida Ehtimoliy xavf: Hisob buzilishi (account compromise), credential stuffingxavfi orqali aniqlab beradi.

Login va autentifikatsiya jarayonidagi g‘alati yoki shubhali urinishlarni aniqlash kiberxavfsizlikda juda muhim, chunki bu foydalanuvchi hisoblariga hujum qilishning eng keng tarqalgan usullaridan biri.

SI va ML asosida xulq-atvor (davranish) tahlili. Har bir foydalanuvchining odatdagi login va ishlash soatlari, qurilmalari, IP-manzillari, joylashuvi va boshqa xatti-harakatlari asosida profil yaratiladi.

- Noodatiy vaqt (masalan, kechasi soat 3:00 da login qilish)
- Yangi qurilma yoki IP-manzildan kirishga urinish

- Kichik vaqt ichida bir nechta login urinishlari
- Geografik imkonsiz joylar (masalan, bir daqiqa ichida Toshkentdan va London'dan login qilish)

Brute-force va credential stuffing hujumlarini aniqlaydi . Bitta login uchun ko'p parol urinishlari bo'lsa, tizim buni avtomatik aniqlaydi.

- Ko'p marta noto'g'ri parol kiritish
- IP-manzil bir necha loginlarga bir vaqtning o'zida murojaat qilsa
- Qisqa vaqt ichida minglab login urinishlari

SIEM tizimlari orqali monitoring. (SIEM — Security Information and Event Management)Tizimdagi barcha login va autentifikatsiya loglarini yig'ib, ularni real vaqtda tahlil qiladi.

- Noan'anaviy faoliyatlar
- Muayyan IP yoki foydalanuvchidan kelayotgan shubhali holatlar
- Tarmoq bo'ylab bir nechta nuqtalardan kelayotgan login harakatlari

GeoIP va joylashuv tahlili. Foydalanuvchi doimiy kiradigan joydan boshqa hududda login qilmoqchi bo'lsa, ogohlantirish beradi yoki kirishni cheklaydi.

- VPN, proxy orqali yashirin login
- IP-manzil geografik jihatdan mos kelmaydi

CAPTCHA va ko'p faktorli autentifikatsiya (MFA) orqali himoya. Shubhali harakat aniqlanganda, foydalanuvchidan qo'shimcha tasdiq so'raladi (SMS, email, biometrik tasdiq).

- Aniqlaydi va oldini oladi:
  - Botlar orqali login urinishlari
  - Parol o'g'irlangan bo'lsa ham, autentifikatsiyani to'liq bajara olmaydi

Honeytoken (tuzoq login) usullari. Maxsus "soxta" loginlar yaratiladi. Ularni ishlatishga urinish bo'lsa — bu hujum belgisi.Tizimda noma'lum aktor mavjudligini.Maxfiy login ma'lumotlari tarqalganini

Vizualizatsiya qilish uchun SI yordamida grafikalar

- Noodatiy IP'dan kirish
- Kirish vaqtidagi o'zgarishlar
- Xavfli joylashuvlar xaritada ko'rsatiladi

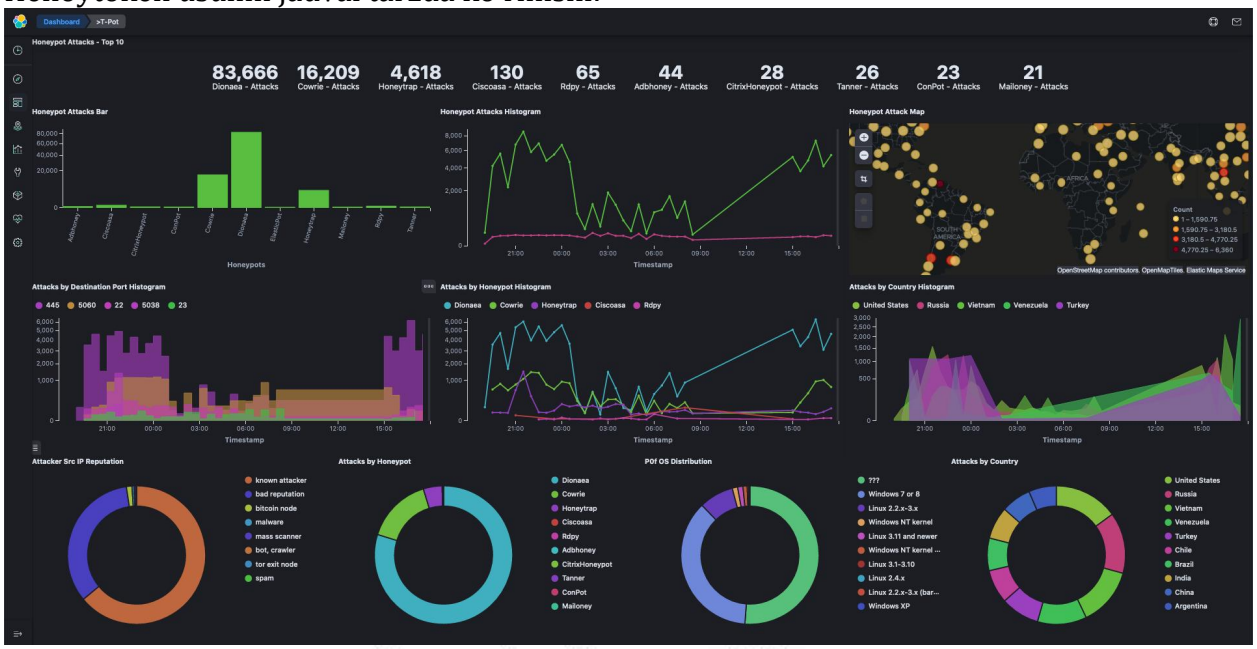
Agar raqam bilan aytadigan bo'lsak — tadqiqotlar va sanoat hisobotlariga ko'ra, sun'iy intellekt va mashinali o'rganish texnologiyalari kiberxavfsizlikda tahdidlarni aniqlash aniqligini 85–95% gacha oshirishi mumkin. IBM Security: SI asosidagi xavfsizlik tizimlari ma'lumotlarni buzilish holatlariga javob berish vaqtini 60% gacha qisqartirgan.Capgemini Research Institute: Kiberxavfsizlik sohasidagi tashkilotlarning 69% SI tahdidlarni aniqlashda zarur vosita deb hisoblaydi.Darktrace (SI asosidagi xavfsizlik kompaniyasi): Ularning texnologiyasi yordamida 99% real vaqtli tahdidlar avtomatik aniqlanadi.

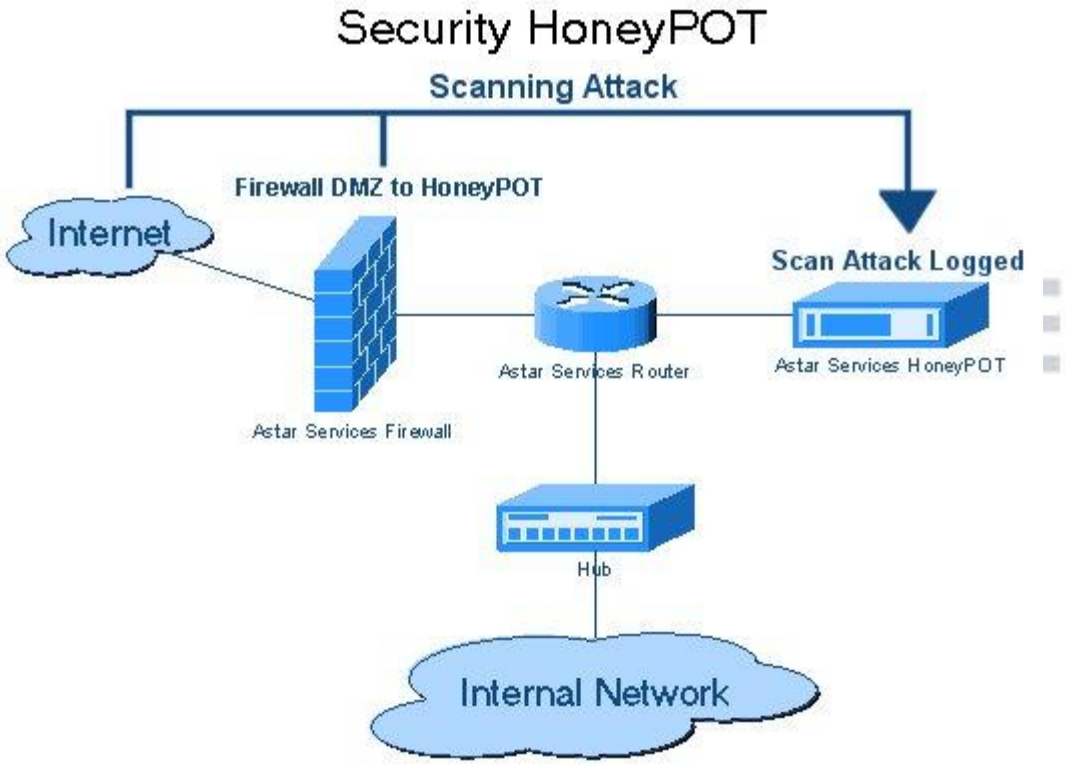
Darktrace — sun'iy intellekt (SI) asosida ishlaydigan kiberxavfsizlik kompaniyasi bo'lib, 2013-yilda Buyuk Britaniyaning Kembrij shahrida tashkil etilgan. Kompaniya sun'iy intellekt va mashinaviy o'rganish texnologiyalarini qo'llab, tizimlar va tarmoqlarda noma'lum tahdidlarga qarshi samarali himoya ta'minlaydi. **Asosiy** mahsulotlar va texnologiyalar:

- ActiveAI Security Platform™: Darktrace'ning asosiy platformasi bo'lib, u tashkilotning raqamli ekotizimini real vaqt rejimida o'rganib, tahdidlarni aniqlaydi va ularga avtomatik javob beradi.
- Antigena: Avtomatik javob berish texnologiyasi bo'lib, tahdidlar aniqlanganda tizimni izolyatsiya qilish yoki zararli faoliyatni to'xtatish kabi choralarni ko'radi.
- Threat Visualizer: Tarmoq faoliyatini vizual tarzda ko'rsatib, xavfli holatlarni aniqlashni osonlashtiradi.

Honeytoken — bu kiberxavfsizlikda sun'iy tuzoq (honeypot) texnologiyasining bir turi bo'lib, hujumchilarning tizimga noqonuniy kirishini aniqlash va oldini olish uchun ishlatiladi.

Honeytokenlar, asosan, tizimda mavjud bo'lmagan yoki foydalanuvchilar tomonidan ishlatilmaydigan ma'lumotlar, fayllar yoki resurslar sifatida yaratiladi.
Henoytoken usulini jadval tarzda ko'rinishi:





KIBERXAVFSIZLIKDA FOYDALANILADIGAN SUN'IY INTELLEKT TURLARI

1. Mashinali o'rganish (Machine Learning - ML).Tahdidlarni aniqlashda tarixiy ma'lumotlardan o'rganadi. Antivirualar, anomaliya aniqlash tizimlari, SIEM tizimlarida keng qo'llanilib kelinmoqda.
2. Chuquroq o'rganish (Deep Learning).Katta hajmdagi loglar va trafiklarni tahlil qilishda ishlatiladi.Soxta foydalanuvchilarni aniqlash, phishingni tahlil qilish jarayonlarida qo'llaniladi.
3. NLP (Natural Language Processing).Email, chat va hujjatlarda phishing, zararli linklar yoki tahdidli tilni aniqlaydi.Email xavfsizligi, chatbot hujumlariga qarshi faol dasturiy ta'minotlardan biri.

4. Xatti-harakat (Behavioral Analysis) modellar. Har bir foydalanuvchi, qurilma yoki tizimning odatiy xatti-harakatini o‘rganadi. Insider threat detection, noan’anaviy login harakatlarini aniqlashda qo‘llaniladi.
5. Avtomatlashtirilgan qaror qabul qilish (Automated Decision-Making).Tahdid aniqlanganda avtomatik javob choralarini ko‘radi (izolyatsiya, bloklash). SOAR tizimlarida (Security Orchestration, Automation and Response) qo‘llaniladi.

Xulosa sifatida asosan Sun’iy intellekt kiberxavfsizlikda mavjud tahdidlarni:

- aniqlaydi (detection),
- tahlil qiladi (analysis),
- oldini oladi (prevention),
- va reaksiya bildiradi (response).

Hozirda deyarli har bir zamonaviy xavfsizlik tizimi AI yoki ML komponentiga ega, ayniqsa katta tashkilotlar va davlat agentliklarida bu jaroyan jadallik bilan rivojlanishiga o’z hissasini qo’shib kelmoqda.

FOYDALANILGAN ADABIYOTLAR:

1. Raxmatov, Sherqo‘Zi Olimovich. "masofaviy ta’lim dasturlarining ta’lim tizimida afzalliklari va amaliy ahamiyati (moodle, scorm, tutor dasturlari misolida)." Oriental renaissance: Innovative, educational, natural and social sciences 1.11 (2021): 1263-1270.
2. Berdiyeva, Gulnoza. "O’ZBEKISTON ELEKTRON SAVDO TIZIMIDA MUAMMOLAR VA TAKLIFLAR." Science and innovation in the education system 3 (2024): 16-22.
3. Berdiyeva, Gulnoza. "RAQAMLI IQTISODIYOTNING MAQSAD VA VAZIFALARI VA UNING O'ZBEKISTONDA RIVOJLANISHI." Педагогика и психология в современном мире: теоретические и практические исследования 3 (2024): 11-14.
4. Gulnoza Raxmatov Sherqo'zi Olimovich, Berdiyeva, Raimbek Muzaffarov. ELEKTRON TIJORATNING AN'ANAVIY SAVDO TURLARI BILAN XARAKTERLI XUSUSIYATLARI. Инновационные исследования в современном мире: теория и практика. 2024/4/8. ст 14-18
5. Raxmatov Sherqo'zi Akbar Kodirov. Ta'lim jarayonida bulutli texnalogiyalardan foydalanishning samaradorligi. Pedagogis Internatsianal researcg. 2023/5/15. ISSN:281-4027_SJIF:4.995. ст-69
6. Berdiqulov, Bektosh, and Shohboz Musirmanov. "WEB SAHIFA BO ‘LIMINI O ‘QITISH METODIKASI." Молодые ученые 3.6 (2025): 42-45.
7. Abdinazarov, Asadbek, and Shohboz Musirmanov. "EHTIMOLLAR NAZARIYASI VA TASODIFIY HODISALAR." Молодые ученые 3.6 (2025): 29-31.
8. Usmon o‘g‘li, Musirmanov Shohboz. "IJTIMOIY TARMOQLAR ORQALI TURISTIK JOYLARNI REKLAMA QILISH VA MIJOZLAR BILAN SAMARALI ALOQA O ‘RNATISH." Scientific Journal of Actuarial Finance and Accounting 4.10 (2024): 369-374.
9. Jo’rayeva, Feruza, and Aziza Normataova. "KATTA MA’LUMOTLAR (BIG DATA) UCHUN DBMS TIZIMLARI." Инновационные исследования в современном мире: теория и практика 3.14 (2024): 31-35. Feruza Jo’rayeva. TA’LIM JARAYONIDA AQL XARITALARIDAN FOYDALANISH VA ULARNING AHAMIYATI. Молодые ученые. 2024/4/8. ст-159-166
10. Feruza Jo‘rayeva, Shahrizoda Pardayeva. KOMPYUTER O ‘YINLARI-MANQURTLIK VOSITASI. Current approaches and new research in modern sciences. 2024/4/5. ст-12-18
11. Feruza Jo‘rayeva, Gulhayo Hamdamova. MEDIA SAVODXONLIK TUSHUNCHASI VA UNING JAMIYATIMIZ HAYOTIDAGI AHAMIYATI. Педагогика и психология в современном мире: теоретические и практические исследования. 2024/3/31. ст-31-35
12. Sevinch Maslaitdinova Jo'rayeva Feruza. VIRTUAL LABORATORIYALAR VA ULARNING O ‘QITISH JARAYONIDAGI AHAMIYATI. PEDAGOGS. Ст-196-200

13. Tuxtanazarova N. A Davletov A. J. , Mavlanberdiyev S. F., Norqulova Z. N., Jurayeva F. B., Jurayeva D. Sh. STUDY RATIO OF MOISTURE AND BIOME FOR EXTREME SITUATION. ВЫСШАЯ ШКОЛА• №23 / 2021. 2021/12/23. ст-34-36

14. J.Toshpo‘lotova M.O‘ktamov, Sh.Aliqulov. Iqtidorli talabalarni fan, ta’lim va ishlab chiqarish korxonalari bilan integratsiya qilishning zamonaviy usullari. Fan va texnika taraqqiyotida intellektual yoshlarning o‘rn. 2024/4/29. ст-54-57

15. J.Toshpo‘lotova M.O‘ktamov, Sh.Aliqulov. Hozirgi globallashuv jarayonida intellektual yoshlarning ijtimoiy rivojlanish davridagi roli. Fan va texnika taraqqiyotida intellektual yoshlarning o‘rn. 2024/4/29. ст-40-43

16. Aliqulov Shukurullo Fayzullo o‘g‘li. TA ‘LIMDA MULTIMEDIYA TEXNOLOGIYALARINI QO ‘LLASH. PEDAGOGS. 2024/2/8. Ст-51-55

17. Shukurullo Fayzullo o‘g‘li. Aliqulov.". TA ‘LIMDA MULTIMEDIYA TEXNOLOGIYALARINI QO ‘LLASH." PEDAGOGS. 2024. ст-51-55

18. Shamsiddinov, G’iyosjon, Gulandom Raxmatova, and Zilola Rajapova. "KLIENT-SERVER ARXITEKTURALARI." *Наука и инновация* 3.6 (2025): 113-119.

19. Shamsiddinov, G’iyosjon, Gulandom Raxmatova, and Zilola Rajapova. "VIRTUAL BORLIQ VA UNING ASOSIY TUSHINCHALARI." *Наука и инновация* 3.6 (2025): 52-58.

20. Shamsiddinov, G‘iyosjon, Barchin Ro‘ziqulova, and Laziza Inatillayeva. "BOSHLANG ‘ICH TA’LIMDA AXBOROT TEXNOLOGIYALARIDAN FOYDALANISH USULLARI VA AFZALLIKLARI." *Педагогика и психология в современном мире: теоретические и практические исследования* 3.10 (2024): 39-41.

21. Shamsiddinov, G‘iyosjon, and Gulandom Raxmatova. "O ‘ZBEKISTONDA AXBOROT HAVFSIZLIGINI MA’NAVIY VA HUQUQIY ASOSLARI." *Решение социальных проблем в управлении и экономике* 3.4 (2024): 45-57.

INNOVATIVE ACADEMY