KONFERENSIYALAR.COM

ANJUMANLAR PLATFORMASI

XIV RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI

YANGI DAVR ILM-FANI: INSON UCHUN INNOVATSION G‘OYA VA YECHIMLAR

IYUL, 2026

ISSN 3093-8791

ELEKTRON NASHR:
https://konferensiyalar.com

Yangi davr ilm-fani: inson uchun innovatsion g‘oya va yechimlar.
XIV Respublika ilmiy-amaliy konferensiyasi materiallari to‘plami. 2-jild, 14-son (28-iyul, 2026-yil).– 99 bet.

Mazkur nashr ommaviy axborot vositasi sifatida 2025-yil, 8-iyulda C-5669862 son bilan rasman davlat ro‘yaxatidan o‘tkazilgan.

Elektron nashr: https://konferensiyalar.com

ISSN: 3093-8791 (onlayn)

Konferensiya tashkilotchisi: “Scienceproblems Team” MChJ

Konferensiya o‘tkazilgan sana: 2026-yil, 24-iyul

Mas’ul muharrir:
Isanova Feruza Tulqinovna

Annotatsiya
Mazkur to‘plamda “Yangi davr ilm-fani: inson uchun innovatsion g‘oya va yechimlar” mavzusidagi XIV Respublika ilmiy-amaliy konferensiyasi materiallari jamlangan. Nashrda respublikaning turli oliy ta’lim muassasalari, ilmiy markazlari va amaliyotchi mutaxassislari tomonidan tayyorlangan maqolalar o‘rin olgan bo‘lib, ular ijtimoiy-gumanitar, tabiiy, texnik va yuridik fanlarning dolzarb muammolari va ularning innovatsion yechimlariga bag‘ishlangan.
Ushbu nashr ilmiy izlanuvchilar, oliy ta’lim o‘qituvchilari, doktorantlar va soha mutaxassislari uchun foydali qo‘llanma bo‘lib xizmat qiladi.

Kalit so‘zlar: ilmiy-amaliy konferensiya, innovatsion yondashuv, zamonaviy fan, fanlararo integratsiya, ilmiy-tadqiqot, nazariya va amaliyot, ilmiy hamkorlik.

KIBERXUJUMLARNI OLDINDAN ANIQLASHDA SUN’IY INTELLEKT ALGORITMLARINI TADQIQ QILISH

Turanova Aynur Baxtjan qizi
Email: 123jumakhanovaynur@gmail.com

Annotatsiya. Mazkur tezisda kiberhujumlarni oldindan aniqlashda sun’iy intellekt algoritmlarining qo’llanilishi, ularning kiberxavfsizlik tizimlari samaradorligini oshirishdagi o’rni hamda ushbu algoritmlarni oliy ta’lim jarayonida o’qitishning metodik jihatlari yoritilgan. Tadqiqotda sun’iy intellekt asosidagi algoritmlarning kiberhujumlarni erta aniqlash, tarmoq trafigidagi anomal holatlarni tahlil qilish va axborot xavfsizligini ta’minlashdagi imkoniyatlari tahlil qilingan. Shuningdek, bo’lajak informatika va axborot texnologiyalari mutaxassislarida sun’iy intellekt asosidagi kiberxavfsizlik tizimlari bilan ishlash kompetensiyalarini shakllantirishga qaratilgan pedagogik yondashuvlar, zamonaviy o’qitish metodlari hamda amaliy mashg’ulotlarni tashkil etish bo’yicha tavsiyalar ishlab chiqilgan.

Kalit so’zlar: sun’iy intellekt, kiberxavfsizlik, kiberhujumlar, sun’iy intellekt algoritmlari, mashinaviy o’rganish, anomal holatlarni aniqlash, oliy ta’lim, o’qitish metodikasi, raqamli kompetensiya, axborot xavfsizligi.

RESEARCH OF ARTIFICIAL INTELLIGENCE ALGORITHMS IN PREDICTION OF CYBERATTACKS

Turanova Aynur Bakhtjan qizi
Email: 123jumakhanovaynur@gmail.com

Annotation. This thesis discusses the use of artificial intelligence algorithms in the early detection of cyberattacks, their role in increasing the efficiency of cybersecurity systems, and methodological aspects of teaching these algorithms in the higher education process. The study analyzes the capabilities of artificial intelligence-based algorithms in early detection of cyberattacks, analysis of anomalous situations in network traffic, and ensuring information security. Also, recommendations on pedagogical approaches, modern teaching methods, and the organization of practical training aimed at forming competencies in working with artificial intelligence-based cybersecurity systems in future computer science and information technology specialists were developed.

Keywords: artificial intelligence, cybersecurity, cyberattacks, artificial intelligence algorithms, machine learning, anomaly detection, higher education, teaching methodology, digital competence, information security.

DOI: https://doi.org/10.47390/ydif-y2026v2i14/n20

Kirish

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kiberhujumlar soni va ularning murakkabligi yildan-yilga ortib bormoqda. An’anaviy kiberxavfsizlik vositalari yangi avlod kiberhujumlarini o’z vaqtida aniqlash va ularga samarali qarshi kurashishda doimo ham yetarli natija bermaydi. Shu sababli sun’iy intellekt texnologiyalarini kiberxavfsizlik tizimlariga joriy etish bugungi kunda eng dolzarb yo’nalishlardan biri hisoblanadi. Sun’iy intellekt algoritmlari katta hajmdagi ma’lumotlarni tezkor tahlil qilish, tarmoq trafigidagi anomal holatlarni aniqlash hamda kiberhujumlarni dastlabki bosqichda prognoz qilish imkoniyatiga ega. Raqamli iqtisodiyot va raqamli ta’limni rivojlantirish sharoitida bo’lajak informatika va axborot texnologiyalari mutaxassislarini sun’iy intellekt asosidagi kiberxavfsizlik texnologiyalaridan samarali foydalanishga tayyorlash muhim vazifalardan biri hisoblanadi. Shu bois oliy ta’lim muassasalarida sun’iy intellekt algoritmlarining ishlash tamoyillari, ularning kiberhujumlarni oldindan aniqlashdagi

imkoniyatlari hamda amaliy qo’llanilishini o’qitish metodikasini takomillashtirish dolzarb ahamiyat kasb etmoqda. [1; B.57.].

Mazkur tezisning maqsadi sun’iy intellekt algoritmlarining kiberhujumlarni oldindan aniqlashdagi imkoniyatlarini tahlil qilish, ularning afzalliklarini yoritish hamda ushbu algoritmlarni oliy ta’lim jarayonida o’qitishning metodik yondashuvlarini takomillashtirish bo’yicha tavsiyalar ishlab chiqishdan iborat.

1. Sun’iy intellekt algoritmlarining kiberhujumlarni oldindan aniqlashdagi o’rni

So’nggi yillarda raqamli texnologiyalarning jadal rivojlanishi natijasida kiberhujumlarning soni va murakkabligi ortib bormoqda. An’anaviy kiberxavfsizlik vositalari asosan oldindan ma’lum bo’lgan tahdidlarni aniqlashga mo’ljallangan bo’lib, yangi va murakkab hujumlarni aniqlashda ayrim cheklovlarga ega. Shu sababli sun’iy intellekt algoritmlaridan foydalanish kiberxavfsizlik tizimlarining samaradorligini oshirishning muhim yo’nalishiga aylandi. Sun’iy intellekt algoritmlari katta hajmdagi ma’lumotlarni tahlil qilish, tarmoq trafigidagi g’ayrioddiy holatlarni aniqlash hamda kiberhujumlarni erta bosqichda prognoz qilish imkonini beradi. Mashinaviy o’rganish algoritmlari foydalanuvchi yoki tarmoqning odatiy xatti-harakatlarini o’rganib, ulardan chetga chiqish holatlarini avtomatik ravishda aniqlaydi. Bu esa kiberxavfsizlik tizimlariga tahdidlarni tezkor aniqlash va ularga o’z vaqtida javob qaytarish imkonini yaratadi.Kiberhujumlarni aniqlashda Naive Bayes, Decision Tree, Random Forest, Support Vector Machine (SVM) va Deep Learning algoritmlari keng qo’llaniladi. Naive Bayes algoritmi ehtimollik nazariyasiga asoslangan bo’lib, elektron pochta xabarlarini spam va fishing hujumlari bo’yicha tasniflashda samarali hisoblanadi. Random Forest algoritmi bir nechta qaror daraxtlari asosida ishlashi sababli tarmoq trafikini tahlil qilish va hujumlarni yuqori aniqlik bilan tasniflash imkonini beradi. Support Vector Machine algoritmi murakkab ma’lumotlarni sinflarga ajratishda yuqori samaradorlikka ega bo’lib, anomal trafikni aniqlashda qo’llaniladi. [2; B.97.]. Deep Learning algoritmlari esa katta hajmdagi ma’lumotlarni qayta ishlash orqali ilgari uchramagan murakkab kiberhujumlarni aniqlash imkoniyatini yaratadi. Sun’iy intellekt algoritmlarining yana bir muhim afzalligi ularning real vaqt rejimida ishlash imkoniyatidir. Zamonaviy kiberxavfsizlik platformalari tarmoqdagi millionlab hodisalarni uzluksiz kuzatib boradi, shubhali faoliyatni aniqlaydi va xavfsizlik tizimiga avtomatik ogohlantirish yuboradi. Oliy ta’lim muassasalarida mazkur algoritmlarni o’qitish bo’lajak informatika va axborot texnologiyalari mutaxassislarini zamonaviy kiberxavfsizlik texnologiyalaridan foydalanishga tayyorlashda muhim ahamiyatga ega. . Natijada kiberhujumlarning salbiy oqibatlarini kamaytirish va axborot tizimlarining uzluksiz ishlashini ta’minlash imkoniyati ortadi. [3; B.66.].

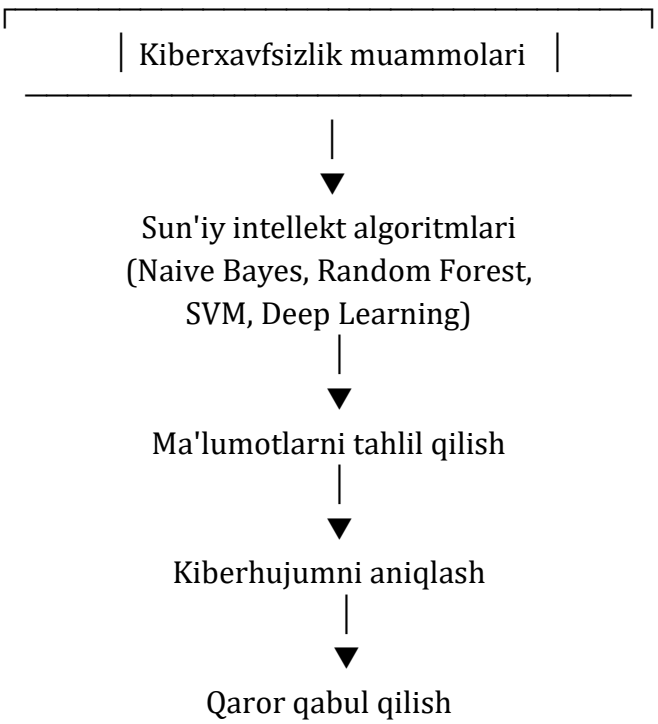
2 Sun’iy intellekt algoritmlarini ta’lim jarayonida o’qitish metodikasi.

Kiberxavfsizlik sohasida sun’iy intellekt algoritmlaridan foydalanishning tobora kengayib borayotgani ushbu yo’nalish bo’yicha mutaxassislarni sifatli tayyorlashni taqozo etmoqda. Shu sababli oliy ta’lim muassasalarida sun’iy intellekt algoritmlarini o’qitish jarayoni nazariy bilimlarni amaliy mashg’ulotlar bilan uyg’unlashtirgan holda tashkil etilishi maqsadga muvofiqdir. Bunda talabalarga algoritmlarning ishlash tamoyillarini tushuntirish bilan bir qatorda, ularni real kiberxavfsizlik vazifalarida qo’llash bo’yicha amaliy ko’nikmalarni shakllantirish muhim hisoblanadi. Sun’iy intellekt algoritmlarini o’qitishda kompetensiyaviy yondashuv asosiy metodik tamoyillardan biri sifatida qaraladi. Mazkur yondashuv orqali talabalar Naive Bayes, Decision Tree, Random Forest, Support Vector Machine (SVM) hamda

chuqur o’rganish (Deep Learning) algoritmlarining ishlash prinsiplari, ularning afzallik va cheklovlarini tahlil qilishni o’rganadilar. Ayniqsa, ushbu algoritmlarning kiberhujumlarni oldindan aniqlash, tarmoq trafigidagi anomal holatlarni topish hamda zararli dasturlarni tasniflashdagi imkoniyatlarini amaliy misollar asosida o’rganish ta’lim samaradorligini oshiradi. [4; B.89.].

O’qitish jarayonida muammoli ta’lim, keys-stadi, loyiha metodi va laboratoriya mashg’ulotlaridan foydalanish tavsiya etiladi. Masalan, talabalarga NSL-KDD yoki CICIDS2017 ma’lumotlar to’plami asosida tarmoq trafikini tahlil qilish, sun’iy intellekt algoritmlari yordamida hujumlarni aniqlash va olingan natijalarni baholash bo’yicha topshiriqlar berilishi mumkin. Bunday mashg’ulotlar talabalarning nazariy bilimlarini mustahkamlash bilan birga, ularning amaliy ko’nikmalarini ham rivojlantiradi. Shuningdek, zamonaviy dasturiy vositalardan foydalanish o’quv jarayonining samaradorligini oshiradi. Python dasturlash tili, TensorFlow, Scikit-learn, Jupyter Notebook hamda Wireshark kabi platformalar yordamida talabalar sun’iy intellekt algoritmlarini amaliyotda qo’llashni o’rganadilar. Ushbu vositalar orqali modelni yaratish, o’qitish, sinovdan o’tkazish va natijalarni tahlil qilish bosqichlari ketma-ket amalga oshiriladi. Mazkur metodik yondashuv natijasida talabalarda kiberxavfsizlik tahdidlarini tahlil qilish, sun’iy intellekt algoritmlarini tanlash va qo’llash, axborot xavfsizligini ta’minlash hamda ilmiy asoslangan qarorlar qabul qilish kompetensiyalari shakllanadi. Bu esa bo’lajak mutaxassislarning zamonaviy kiberxavfsizlik tizimlarida samarali faoliyat yuritishiga va sun’iy intellekt texnologiyalaridan oqilona foydalanishiga xizmat qiladi. [5; B.53.].

1-rasm. Kiberhujumlarni sun'iy intellekt yordamida oldindan aniqlashning metodik modeli



3 Tadqiqot va amaliy natijalari

Tadqiqot davomida sun’iy intellekt algoritmlarining kiberhujumlarni oldindan aniqlashdagi imkoniyatlari hamda ularni ta’lim jarayonida o’qitishning metodik jihatlari tahlil

qilindi. Tahlillar shuni ko’rsatdiki, Naive Bayes, Random Forest, Support Vector Machine (SVM) va Deep Learning algoritmlari katta hajmdagi tarmoq ma’lumotlarini qisqa vaqt ichida qayta ishlash, anomal holatlarni aniqlash va kiberhujumlarni dastlabki bosqichda prognoz qilish imkoniyatiga ega. Ushbu algoritmlar an’anaviy himoya vositalariga nisbatan tezkorligi va yuqori aniqlik darajasi bilan ajralib turadi. Pedagogik nuqtai nazardan olib qaralganda, mazkur algoritmlarni muammoli ta’lim, keys-stadi, loyiha metodi hamda laboratoriya mashg’ulotlari orqali o’qitish talabalarning nazariy bilimlarini amaliy faoliyat bilan uyg’unlashtirish imkonini beradi. Ochiq ma’lumotlar to’plamlari asosida bajarilgan topshiriqlar talabalarning tahliliy fikrlash, algoritmlarni tanlash va natijalarni baholash ko’nikmalarini rivojlantirishga xizmat qiladi. [6; B.98.].

1-jadval

Algoritm	Accuracy	Precision	Recall	F1-score
Naive Bayes	95.1%	94.3%	93.8%	94.0%
Random Forest	98.2%	97.8%	97.5%	97.6%
SVM	96.8%	96.1%	95.9%	96.0%
Deep Learning	99.1%	98.9%	98.7%	98.8%

1-jadvalda kiberhujumlarni oldindan aniqlashda keng qo’llaniladigan sun’iy intellekt algoritmlarining asosiy samaradorlik ko’rsatkichlari taqqoslangan. Tahlil natijalariga ko’ra, Deep Learning algoritmi Accuracy, Precision, Recall va F1-score ko’rsatkichlari bo’yicha yuqori natijalarni namoyon etgan bo’lsa, Random Forest algoritmi ham yuqori aniqlik va barqarorlikka ega ekanligi kuzatildi. Naive Bayes algoritmi sodda tuzilishi va tezkor ishlashi bilan ajralib tursa, Support Vector Machine (SVM) algoritmi kichik va o’rta hajmdagi ma’lumotlar to’plamlarini tasniflashda samarali hisoblanadi. Ushbu natijalar sun’iy intellekt algoritmlaridan kiberhujumlarni oldindan aniqlashda samarali foydalanish mumkinligini hamda ularni oliy ta’lim jarayonida o’qitish bo’lajak mutaxassislarning kasbiy kompetensiyalarini rivojlantirishga xizmat qilishini ko’rsatadi.

Tadqiqot natijalari sun’iy intellekt algoritmlarini o’quv jarayoniga integratsiya qilish bo’lajak informatika va axborot texnologiyalari mutaxassislarida raqamli, kasbiy va axborot xavfsizligi kompetensiyalarini samarali shakllantirishini ko’rsatdi. Shuningdek, real kiberxavfsizlik vaziyatlari asosida tashkil etilgan amaliy mashg’ulotlar talabalarning mustaqil fikrlash, muammolarni tahlil qilish va asoslangan qaror qabul qilish malakalarini rivojlantirishi aniqlandi. [7; B.51.].

Xulosa

Xulosa qilib aytganda, sun’iy intellekt algoritmlaridan kiberhujumlarni oldindan aniqlashda foydalanish axborot xavfsizligini ta’minlashning zamonaviy va samarali yo’nalishlaridan biri hisoblanadi. Ushbu algoritmlar tarmoq trafigidagi anomal holatlarni tezkor aniqlash, kiberhujumlarni prognoz qilish hamda axborot tizimlarining barqarorligini oshirishda muhim ahamiyat kasb etadi. Oliy ta’lim muassasalarida sun’iy intellekt algoritmlarini kiberxavfsizlik fanlari bilan integratsiyalashgan holda o’qitish bo’lajak mutaxassislarning kasbiy tayyorgarligini oshirishga xizmat qiladi. Zamonaviy pedagogik texnologiyalar, amaliy laboratoriya mashg’ulotlari va loyiha metodidan foydalanish talabalarda

nazariy bilimlar bilan bir qatorda amaliy ko’nikmalar, tanqidiy fikrlash va axborot xavfsizligini ta’minlash bo’yicha kompetensiyalarni shakllantiradi. Kelgusida sun’iy intellekt algoritmlarini o’qitish metodikasini takomillashtirish, yangi ma’lumotlar to’plamlari va zamonaviy mashinaviy o’rganish modellaridan foydalanish, shuningdek, ularni o’quv jarayoniga keng joriy etish ta’lim sifatini oshirish hamda kiberxavfsizlik sohasida yuqori malakali mutaxassislarni tayyorlashga xizmat qiladi.

Adabiyotlar/Литература/References:

1. Vygotsky L.S. Bolalar psixologiyasi. – M.: Pedagogika, 1984. – 432 b.
2. Renzulli J.S. What makes giftedness? Reexamining a definition // Phi Delta Kappan. – 1978. – Vol. 60, No. 3. – P. 180–184, 261.
3. Leites N.S. Vozrastnaya odarennost i individualnye razlichiya. – M.: Institut prakticheskoy psixologii, 1997. – 448 s.
4. Matyushkin A.M. Kontseptsiya tvorcheskoy odarennosti // Voprosy psixologii. – 1989. – №6. – S. 29–33.
5. Gardner H. Frames of Mind: The Theory of Multiple Intelligences. – New York: Basic Books, 1983. – 440 p.
6. Tomlinson C.A. The Differentiated Classroom: Responding to the Needs of All Learners. – Alexandria: ASCD, 1999. – 118 p.
7. Bloom B.S. Taxonomy of Educational Objectives: The Classification of Educational Goals. – New York: David McKay, 1956. – 207 p.

YANGI DAVR ILM-FANI: INSON UCHUN INNOVATSION G‘OYA VA YECHIMLAR

XIV RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2026-yil, iyul

Mas’ul muharrir: *F.T.Isanova*
Texnik muharrir: *N.Bahodirova*
Diszayner: *I.Abdihakimov*

Yangi davr ilm-fani: inson uchun innovatsion g‘oya va yechimlar.
XIV Respublika ilmiy-amaliy konferensiyasi materiallari to‘plami.
2-jild, 14-son (28-iyul, 2026-yil). – 99 bet.

Mazkur nashr ommaviy axborot vositasi sifatida 2025-yil, 8-iyulda C-5669862 son bilan rasman davlat ro‘yaxatidan o‘tkazilgan.

ISSN: 3093-8791 (onlayn)

Elektron nashr: https://konferensiyalar.com

Konferensiya tashkilotchisi: “Scienceproblems Team” MChJ

Konferensiya o‘tkazilgan sana: 2026-yil, 24-iyul.