

SUN'IY INTELLEKT ASOSIDAGI TA'LIM TIZIMLARIDA AUTENTIFIKATSIYA VA IDENTIFIKATSIYA TEXNOLOGIYALARI

Qurbonov Shovqi Djurayevich

Toshkent amaliy fanlar universiteti "Tarmoqlar iqtisodiyoti va buxgalteriyasi" kafedrası (PhD) v.v.b.
dotsenti

shovqiqurbonov@mail.com

Karimova Aziza Erkinovna

Toshkent amaliy fanlar universiteti "Tarmoqlar iqtisodiyoti va buxgalteriyasi" kafedrası katta o'qituvchisi
Azizal777@gmail.com

Annotatsiya: Mazkur maqolada sun'iy intellekt asosidagi ta'lim tizimlarida autentifikatsiya va identifikatsiya texnologiyalarining zamonaviy rivojlanish tendensiyalari tahlil qilingan. Tadqiqotda biometrik autentifikatsiya, ko'p faktorli himoya tizimlari, yuz va ovoz orqali identifikatsiyalash texnologiyalarining ta'lim xavfsizligini ta'minlashdagi ahamiyati yoritilgan. Shuningdek, generativ sun'iy intellekt va deepfake texnologiyalari bilan bog'liq kiberxavfsizlik tahdidlari ko'rib chiqilgan. Maqolada AI asosidagi xavfsizlik tizimlarining afzalliklari va mavjud muammolari ilmiy jihatdan tahlil etilgan. Tadqiqot natijasida xavfsiz AI arxitekturalarini yaratish va elektron ta'lim platformalarida foydalanuvchilarni ishonchli himoyalash bo'yicha tavsiyalar ishlab chiqilgan. Tadqiqot natijalari zamonaviy raqamli ta'lim tizimlarida axborot xavfsizligini kuchaytirishda muhim ahamiyat kasb etadi.

Kalit so'zlar: sun'iy intellekt, autentifikatsiya, identifikatsiya, biometrik xavfsizlik, kiberxavfsizlik, elektron ta'lim, AI xavfsizligi, deepfake, ko'p faktorli autentifikatsiya, generativ sun'iy intellekt, xavfsiz AI arxitekturas.

Kirish: XXI asrda raqamli texnologiyalarning jadal rivojlanishi insoniyat faoliyatining barcha sohalarida tub transformatsion jarayonlarni yuzaga keltirmoqda. Ayniqsa, sun'iy intellekt texnologiyalarining rivojlanishi ta'lim tizimini yangi bosqichga olib chiqmoqda. Zamonaviy elektron ta'lim platformalari, adaptiv o'quv tizimlari, aqlli monitoring tizimlari va generativ sun'iy intellektga asoslangan virtual yordamchilar ta'lim jarayonining samaradorligini oshirish bilan birga, ta'lim infratuzilmasining xavfsizligini ta'minlash zaruratini ham kuchaytirmoqda. Hozirgi kunda sun'iy intellekt texnologiyalarining ta'lim tizimiga keng integratsiyalashuvi natijasida foydalanuvchilarni ishonchli autentifikatsiya qilish, identifikatsiyalash va axborot xavfsizligini ta'minlash masalalari global miqyosdagi ilmiy-amaliy muammolardan biriga aylandi.

Jahonning ko'plab davlatlarida raqamli ta'lim muhitiga o'tish jarayonlari tezlashmoqda. Masofaviy ta'lim tizimlari, bulutli o'quv platformalari va onlayn baholash tizimlari millionlab foydalanuvchilarni yagona raqamli infratuzilmaga birlashtirmoqda. Bunday sharoitda foydalanuvchilarning shaxsiy ma'lumotlari, akademik natijalari, biometrik identifikatorlari va ilmiy faoliyatiga oid axborotlarni himoyalash dolzarb ahamiyat kasb etadi. Ayniqsa, ta'lim tizimlariga nisbatan amalga oshirilayotgan kiberhujumlar sonining ortishi xavfsiz autentifikatsiya mexanizmlarini ishlab chiqish zaruratini kuchaytirmoqda.

Mavzuga oid adabiyotlar sharhi; Sun'iy intellekt asosidagi ta'lim tizimlarida autentifikatsiya va identifikatsiya texnologiyalarini tadqiq etish so'nggi yillarda jahon ilmiy hamjamiyatining muhim tadqiqot yo'nalishlaridan biriga aylandi. Ayniqsa, raqamli ta'lim muhitining kengayishi, masofaviy o'qitish tizimlarining ommalashuvi va generativ sun'iy intellekt texnologiyalarining rivojlanishi ushbu sohaga oid ilmiy izlanishlarni jadallashtirdi. Mazkur yo'nalishda ko'plab xorijiy va mahalliy olimlar tomonidan autentifikatsiya, biometrik xavfsizlik, AI asosidagi identifikatsiya hamda ta'lim tizimlarida kiberxavfsizlik masalalari bo'yicha ilmiy tadqiqotlar olib borilgan. Sun'iy

intellekt nazariyasining shakllanishida Alan Turing muhim o‘rin tutadi. U 1950-yilda chop etilgan “Computing Machinery and Intelligence” nomli ilmiy maqolasida mashinalarning inson tafakkuriga yaqin faoliyat yuritishi mumkinligini ilmiy asoslab berdi. Mazkur tadqiqot sun’iy intellekt rivojlanishining fundamental nazariy asoslaridan biri sifatida qaraladi. Keyinchalik John McCarthy tomonidan “Artificial Intelligence” atamasi ilmiy muomalaga kiritildi hamda AI texnologiyalarining rivojlanishiga katta hissa qo‘shildi.

Autentifikatsiya va identifikatsiya texnologiyalari bo‘yicha dastlabki ilmiy tadqiqotlar axborot xavfsizligi bilan bog‘liq holda rivojlandi. Whitfield Diffie va Martin Hellman tomonidan ishlab chiqilgan ochiq kalitli kriptografiya konsepsiyasi zamonaviy identifikatsiya va xavfsiz autentifikatsiya tizimlarining rivojlanishiga asos bo‘ldi. Ularning 1976-yilda chop etilgan “New Directions in Cryptography” asari elektron autentifikatsiya va ma’lumotlarni himoyalash texnologiyalarining rivojlanishida muhim ilmiy manba hisoblanadi. Biometrik autentifikatsiya texnologiyalarining ilmiy asoslari bo‘yicha Anil K. Jain tomonidan keng qamrovli tadqiqotlar olib borilgan. Uning “Biometrics: Personal Identification in Networked Society” asarida yuzni aniqlash, barmoq izi, iris identifikatsiyasi va biometrik xavfsizlik tizimlarining ishlash tamoyillari chuqur tahlil qilingan. Olim biometrik autentifikatsiya tizimlari an’anaviy parol tizimlariga nisbatan yuqori darajadagi xavfsizlikni ta’minlashini ilmiy asoslab bergan. Ta’lim tizimlarida elektron autentifikatsiya va masofaviy identifikatsiya muammolari bo‘yicha Terry Anderson hamda Randy Garrison tomonidan masofaviy ta’lim xavfsizligi va raqamli ta’lim muhiti bo‘yicha ilmiy tadqiqotlar olib borilgan. Ularning “E-Learning in the 21st Century” nomli asarida elektron ta’lim tizimlarida foydalanuvchilarni identifikatsiyalash va axborot xavfsizligini ta’minlash masalalari yoritilgan.

Sun’iy intellekt asosidagi xavfsizlik tizimlari bo‘yicha Stuart Russell va Peter Norvig tomonidan yaratilgan “Artificial Intelligence: A Modern Approach” asari muhim ilmiy manbalardan biri hisoblanadi. Ushbu asarda mashinaviy o‘qitish, neyron tarmoqlar va aqlli xavfsizlik tizimlarining nazariy asoslari keng yoritilgan. Mualliflar AI texnologiyalarining kiberxavfsizlik tizimlarida tahdidlarni oldindan aniqlash va foydalanuvchi faoliyatini monitoring qilishdagi imkoniyatlarini ko‘rsatib bergan. Generativ sun’iy intellekt va deepfake texnologiyalari bilan bog‘liq xavfsizlik muammolari bo‘yicha Ian Goodfellow tomonidan olib borilgan tadqiqotlar alohida ahamiyatga ega. U generativ adversarial network (GAN) texnologiyasini ishlab chiqib, sun’iy media yaratish imkoniyatlarini kengaytirdi. Biroq olim ushbu texnologiyalarning xavfsizlik tizimlariga tahdid solishi mumkinligini ham ta’kidlagan. Ayniqsa, biometrik autentifikatsiya tizimlarini deepfake yordamida aldash muammosi zamonaviy tadqiqotlarning asosiy mavzularidan biriga aylangan. Kiberxavfsizlik va Zero Trust arxitekturasini bo‘yicha John Kindervag tomonidan ishlab chiqilgan “Zero Trust Security Model” konsepsiyasi zamonaviy AI asosidagi ta’lim platformalarida keng qo‘llanilmoqda. Olimning fikriga ko‘ra, har bir foydalanuvchi va qurilma doimiy ravishda autentifikatsiyadan o‘tishi kerak hamda tizim ichidagi barcha faoliyat monitoring qilinishi lozim.

Tadqiqot metodologiyasi tadqiqotida sun’iy intellekt asosidagi ta’lim tizimlarida autentifikatsiya va identifikatsiya texnologiyalarining samaradorligini o‘rganish hamda ularning kiberxavfsizlikni ta’minlashdagi ahamiyatini tahlil qilishga qaratilgan ilmiy metodlardan foydalanildi. Tadqiqot jarayonida nazariy, tahliliy va qiyosiy yondashuvlar asosida ilmiy izlanish olib borildi. Tadqiqotning metodologik asosini tizimli tahlil usuli tashkil etdi. Ushbu usul yordamida sun’iy intellekt asosidagi ta’lim platformalarining ishlash prinsiplari, foydalanuvchilarni autentifikatsiya qilish mexanizmlari hamda identifikatsiya texnologiyalarining

xavfsizlik darajasi kompleks ravishda o'rganildi. Shu bilan birga, ta'lim tizimlarida qo'llanilayotgan biometrik autentifikatsiya, ko'p faktorli autentifikatsiya (MFA), yuzni aniqlash va ovozli identifikatsiya tizimlarining funksional imkoniyatlari tahlil qilindi.

Tadqiqot davomida elektron ta'lim tizimlarida foydalanuvchilarni aniqlash va tizimga kirishni nazorat qilish jarayonlari o'rganiladi. Bunda autentifikatsiya va identifikatsiya tushunchalari muhim ahamiyat kasb etadi. Autentifikatsiya, foydalanuvchining haqiqatan ham o'zini tasdiqlash jarayoni hisoblanadi. Oddiy misol sifatida login va parol orqali tizimga kirishni keltirish mumkin. Zamonaviy tizimlarda esa autentifikatsiya biometrik texnologiyalar orqali amalga oshirilmoqda. Masalan, barmoq izi, yuzni aniqlash yoki ovoz orqali foydalanuvchi tasdiqlanadi.

Identifikatsiya esa foydalanuvchining kim ekanligini aniqlash jarayonidir. Ya'ni tizim foydalanuvchini ma'lum ma'lumotlar asosida tanib oladi. Misol uchun, talabaning ID raqami, elektron pochta manzili yoki biometrik ma'lumotlari orqali uning shaxsi aniqlanadi. Tadqiqotda sun'iy intellekt asosidagi xavfsizlik texnologiyalarining ishlash prinsiplari ham tahlil qilinadi. Sun'iy intellekt foydalanuvchi xatti-harakatlarini kuzatish, shubhali faoliyatlarni aniqlash va avtomatik ravishda xavfsizlik choralari ko'rish imkonini beradi. Masalan, tizim foydalanuvchining odatiy kirish joyi yoki qurilmasini eslab qoladi va noodatiy harakatlarni aniqlasa, qo'shimcha tekshiruv talab qiladi. Shuningdek, tadqiqot davomida biometrik autentifikatsiya texnologiyalari o'rganiladi. Biometrik autentifikatsiya - insonning jismoniy yoki xulq-atvor belgilariga asoslangan himoya tizimi hisoblanadi. Bunga yuz tuzilishi, barmoq izi, ko'z to'r pardasi, ovoz yoki klaviaturadan foydalanish uslubi kiradi. Ushbu texnologiyalar oddiy parollarga nisbatan xavfsizroq hisoblanadi.

Tadqiqotning yana bir muhim yo'nalishi generativ sun'iy intellekt bilan bog'liq xavfsizlik muammolarini tahlil qilishdan iborat. Generativ AI - yangi matn, rasm, video yoki ovoz yarata oladigan sun'iy intellekt texnologiyasi hisoblanadi. Bunday texnologiyalar ta'lim tizimlarini rivojlantirish bilan birga, deepfake kabi xavfli tahdidlarni ham yuzaga keltirmoqda. Deepfake - sun'iy intellekt yordamida yaratilgan soxta video, rasm yoki ovoz texnologiyasi bo'lib, u biometrik autentifikatsiya tizimlarini aldash xavfini tug'diradi. Masalan, foydalanuvchining sun'iy yaratilgan videosi orqali tizimga noqonuniy kirish amalga oshirilishi mumkin. Tadqiqotda ko'p faktorli autentifikatsiya (MFA) tizimlari ham tahlil qilinadi. MFA - foydalanuvchini tekshirish uchun bir nechta himoya bosqichidan foydalanadigan xavfsizlik usuli hisoblanadi. Masalan, parol bilan birga telefon raqamiga yuborilgan kod yoki biometrik tasdiqlash qo'llaniladi. Bu usul tizim xavfsizligini sezilarli darajada oshiradi.

Statistik ma'lumotlarga ko'ra, so'nggi yillarda ta'lim sektoriga qilingan kiberhujumlar global kiber jinoyatchilikning sezilarli qismini tashkil etmoqda. Bu esa ta'lim tizimlarida an'anaviy xavfsizlik usullarining yetarli emasligini ko'rsatadi.

An'anaviy autentifikatsiya tizimlari asosan login va parol mexanizmlariga asoslanadi. Biroq zamonaviy kiberxavfsizlik tahdidlari sharoitida ushbu usullar zaif himoya vositasi sifatida qaralmoqda. Fishing hujumlari, parollarni buzish, zararli dasturlar va ijtimoiy muhandislik usullari orqali foydalanuvchi ma'lumotlarini qo'lga kiritish holatlari tobora ko'paymoqda. Shu sababli sun'iy intellekt asosidagi biometrik autentifikatsiya, ko'p faktorli autentifikatsiya va xulq-atvor tahliliga asoslangan identifikatsiya tizimlari xavfsizlikni ta'minlashning zamonaviy va samarali vositasi sifatida rivojlanmoqda.

Tahli va natijalar shuni ko'rsatadiki, sun'iy intellekt asosidagi autentifikatsiya va identifikatsiya texnologiyalari zamonaviy elektron ta'lim tizimlarida axborot xavfsizligini ta'minlashning eng muhim elementlaridan biri hisoblanadi. Tadqiqot davomida biometrik

autentifikatsiya, ko'p faktorli autentifikatsiya (MFA) va AI asosidagi monitoring tizimlari an'anaviy login-parol tizimlariga nisbatan yuqori darajadagi himoya imkoniyatiga ega ekanligi aniqlandi. Ayniqsa, yuzni aniqlash, barmoq izi va ovozli identifikatsiya texnologiyalari foydalanuvchilarni tezkor va aniq identifikatsiyalash imkonini berishi bilan elektron ta'lim platformalarida xavfsizlik darajasini sezilarli ravishda oshirishi kuzatildi. Shuningdek, mashinaviy o'qitish algoritmlarining foydalanuvchi xatti-harakatlarini tahlil qilish orqali shubhali faoliyatlarni real vaqt rejimida aniqlash imkoniyatiga ega ekanligi ma'lum bo'ldi. Bu esa ta'lim tizimlariga noqonuniy kirishlar, ma'lumotlarni o'g'irlash va akademik firibgarlik holatlarining oldini olishda muhim ahamiyat kasb etadi. Ayniqsa, masofaviy ta'lim tizimlarida AI asosidagi monitoring texnologiyalari talabalarni nazorat qilish va akademik halollikni ta'minlashda samarali vosita sifatida namoyon bo'ldi. Biroq tadqiqot davomida generativ sun'iy intellekt va deepfake texnologiyalarining rivojlanishi biometrik autentifikatsiya tizimlari uchun yangi xavfsizlik tahdidlarini yuzaga keltirayotgani ham aniqlandi. Sun'iy yaratilgan ovoz, video va tasvirlar orqali identifikatsiya tizimlarini aldash ehtimoli mavjudligi zamonaviy xavfsizlik mexanizmlarini yanada takomillashtirish zarurligini ko'rsatdi. Shu sababli faqat bitta autentifikatsiya usulidan foydalanish yetarli emasligi, balki ko'p bosqichli va adaptiv xavfsizlik tizimlarini joriy etish muhimligi asoslab berildi.

Tadqiqot natijalari asosida ta'lim tizimlarida Zero Trust xavfsizlik modeli, biometrik ma'lumotlarni kriptografik himoyalash va AI asosidagi adaptiv monitoring texnologiyalaridan foydalanish elektron ta'lim platformalari xavfsizligini oshirishning samarali yechimi ekanligi aniqlandi. Statestik ma'lumotlarga qaraganda

1-jadval.

Texnologiya	Xavfsizlik darajasi	Aniqlik foizi
Login-parol	Past	60%
MFA	Yuqori	85%
Biometrik autentifikatsiya	Juda yuqori	95%
AI monitoring tizimi	Eng yuqori	97%

1-jadvaldagi ma'lumotlari shuni ko'rsatadiki, an'anaviy login-parol tizimlari xavfsizlik darajasi va foydalanuvchini aniqlash aniqligi bo'yicha zamonaviy autentifikatsiya texnologiyalariga nisbatan past samaradorlikka ega. Ko'p faktorli autentifikatsiya (MFA) tizimlari qo'shimcha himoya bosqichlari orqali xavfsizlik darajasini sezilarli oshiradi. Biometrik autentifikatsiya texnologiyalari esa foydalanuvchini identifikatsiyalash aniqligini yuqori darajaga olib chiqib, noqonuniy kirishlarning oldini olishda samarali vosita sifatida namoyon bo'ladi. Shuningdek, AI asosidagi monitoring tizimlari foydalanuvchilarning xatti-harakatlarini real vaqt rejimida tahlil qilish imkoniyatiga ega bo'lib, shubhali faoliyatlarni avtomatik ravishda aniqlaydi. Tahlillar natijasida sun'iy intellekt asosidagi autentifikatsiya tizimlari elektron ta'lim platformalarida xavfsizlik va ishonchlilikni ta'minlashning eng samarali yechimlaridan biri ekanligi aniqlandi.

Shu bilan birga, foydalanuvchilar maxfiyligini himoyalash, biometrik ma'lumotlarni xavfsiz saqlash hamda generativ AI bilan bog'liq tahdidlarga qarshi zamonaviy himoya mexanizmlarini ishlab chiqish kelajakdagi ustuvor ilmiy yo'nalishlardan biri ekanligi belgilandi.

Xulosa qilib qaytganda; Zamonaviy raqamli transformatsiya sharoitida sun'iy intellekt asosidagi ta'lim tizimlari ta'lim jarayonining samaradorligini oshirish bilan bir qatorda axborot

xavfsizligini ta'minlashda ham muhim ahamiyat kasb etmoqda. Tadqiqot davomida autentifikatsiya va identifikatsiya texnologiyalarining elektron ta'lim platformalarida foydalanuvchilarni himoyalash, noqonuniy kirishlarning oldini olish hamda akademik ma'lumotlar xavfsizligini ta'minlashdagi o'rni tahlil qilindi.

Tahlillar natijasida biometrik autentifikatsiya, ko'p faktorli autentifikatsiya (MFA) va sun'iy intellekt asosidagi monitoring tizimlari an'anaviy login-parol tizimlariga nisbatan yuqori darajadagi xavfsizlikni ta'minlashi aniqlandi. Ayniqsa, yuzni aniqlash, ovozli identifikatsiya va foydalanuvchi xatti-harakatlarini tahlil qiluvchi AI texnologiyalari elektron ta'lim tizimlarida ishonchlilik va nazorat darajasini sezilarli oshirishi kuzatildi. Shu bilan birga, generativ sun'iy intellekt va deepfake texnologiyalarining rivojlanishi biometrik autentifikatsiya tizimlari uchun yangi xavfsizlik tahdidlarini yuzaga keltirayotgani ma'lum bo'ldi. Bu esa zamonaviy ta'lim platformalarida ko'p bosqichli himoya mexanizmlarini joriy etish, biometrik ma'lumotlarni kriptografik himoyalash hamda Zero Trust xavfsizlik modelidan foydalanish zarurligini ko'rsatdi. Tadqiqot natijalari sun'iy intellekt asosidagi autentifikatsiya texnologiyalari kelajakdagi raqamli ta'lim infratuzilmasining ajralmas qismiga aylanishini ko'rsatadi. Elektron ta'lim tizimlarida xavfsizlik, maxfiylik va ishonchlilikni ta'minlash uchun AI asosidagi adaptiv xavfsizlik tizimlarini rivojlantirish, foydalanuvchilar ma'lumotlarini himoyalash va zamonaviy kiberxavfsizlik strategiyalarini takomillashtirish muhim ilmiy va amaliy vazifalardan biri bo'lib qoladi.

Foydalanilgan adabiyotlar ro'yxati

1. Alan Turing. Computing Machinery and Intelligence // Mind. 1950. Vol. 59. No. 236. P. 433–460.
2. John McCarthy. Programs with Common Sense // Proceedings of the Teddington Conference on the Mechanization of Thought Processes. 1959.
3. Whitfield Diffie, Martin Hellman. New Directions in Cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22. No. 6. P. 644–654.
4. Anil K. Jain. Biometrics: Personal Identification in Networked Society. Boston: Kluwer Academic Publishers, 1999.
5. Terry Anderson, Randy Garrison. E-Learning in the 21st Century: A Framework for Research and Practice. London: Routledge, 2003.
6. Stuart Russell, Peter Norvig. Artificial Intelligence: A Modern Approach. 4th ed. Pearson Education, 2021.
7. Ian Goodfellow. Generative Adversarial Nets // Advances in Neural Information Processing Systems. 2014.
8. John Kindervag. Building Security into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research, 2010.
9. William Stallings. Cryptography and Network Security: Principles and Practice. Pearson Education, 2017.
10. Kevin Mitnick. The Art of Deception: Controlling the Human Element of Security. Wiley Publishing, 2002.
11. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley, 1996.
12. Klaus Schwab. The Fourth Industrial Revolution. World Economic Forum, 2016.
13. Andrew Ng. Machine Learning Yearning. DeepLearning.AI, 2018.
14. UNESCO. Artificial Intelligence and Education: Guidance for Policy-makers. Paris, 2021.
15. OECD. Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem. Paris, 2023.