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.

4. Abdullayev Z. S. Informatika va axborot texnologiyalari. Toshkent: Noshir, 2012.
5. Sattorov A. Informatika va axborot texnologiyalari. Toshkent: O‘qituvchi, 2008.
6. Qodirov F. E., O‘ktamov M. O‘., Musirmanov Sh. U. Kiberxavfsizlik asoslari. Samarqand, 2024.
7. Xaytullayeva N. S., Fayziyeva F. M., Sayfurov D. M. va boshq. Informatika va axborot texnologiyalari. Toshkent, 2021.

BIOMETRIK XAVFSIZLIKDA DEEPFAKE TAHDIDLARI. SUN’IY INTELLEKT ASOSIDAGI ANIQLASH VA HIMOYA TEXNOLOGIYALARI

Mamarimov Abror Kamalidin o‘g‘li, Mixliyeva Ulug‘oy Rabbim qizi
O‘zbekiston Milliy universitetining Jizzax filiali, Amaliy matematika fakulteti, Axborot tizimlari va texnologiyasi kafedrasi o‘qituvchi
mamaroimovabror@gmail.com, mixliyevau@gmail.com
Adirboyeva Shahnoza Amir qizi , Abduramonova Aziza Akram qizi
O‘zbekiston Milliy universitetining Jizzax filiali, talabasi

Annotatsiya. Ushbu maqolada sun'iy intellekt texnologiyalarining biometrik xavfsizlik tizimlariga ta'siri, xususan, generativ sun'iy intellekt asosida yaratilgan deepfake tahdidlari va ularga qarshi qo'llanilayotgan zamonaviy himoya mexanizmlari tahlil qilinadi. Maqolada "jonlilik testi" (liveness detection)ning faol va passiv turlari, ko'p qatlamli (multi-modal) biometrik tizimlar, maxfiylikni saqlovchi "bilim-nol" (zero-knowledge) tekshiruv usullari, shuningdek sohani xalqaro miqyosda tartibga solish tendentsiyalari ko'rib chiqiladi

Kalit so'zlar: sun'iy intellekt, biometrik xavfsizlik, deepfake, jonlilik testi (liveness detection), raqamli shaxs, autentifikatsiya, ma'lumotlar maxfiyligi.Sun’iy intellekt texnologiyalarining jadal rivojlanishi shaxsni identifikatsiya qilish va autentifikatsiya tizimlariga ham katta ta’sir ko‘rsatmoqda. Ayniqsa, generativ sun’iy intellekt yordamida yaratiladigan deepfake texnologiyalari biometrik xavfsizlik uchun yangi tahdidlarni yuzaga keltirmoqda. Soxta video, ovoz va tasvirlarning real ko‘rinishga ega bo‘lishi biometrik tizimlarni aldash imkoniyatini oshirmoqda. Shu sababli zamonaviy autentifikatsiya tizimlarida shaxsni aniqlash bilan birga, biometrik namunaning haqiqiyligini tekshirish ham muhim ahamiyat kasb etmoqda.Biometrik autentifikatsiya insonning fiziologik va xulq-atvor xususiyatlari asosida amalga oshiriladi. Yuz, barmoq izi, ko‘z tuzilishi kabi fiziologik belgilar bilan bir qatorda ovoz, klaviaturadan foydalanish va boshqa xulq-atvor xususiyatlaridan ham foydalaniladi. Hozirgi tizimlarda bir nechta biometrik belgilarni birgalikda qo‘llash orqali himoyaning qo‘shimcha qatlamlari yaratilmoqda. Bunday yondashuv biometrik ma’lumotni soxtalashtirishni murakkablashtiradi va autentifikatsiya ishonchliligini oshiradi.Biometrik ma’lumotlarning muhim jihati shundaki, ularni

parol kabi oddiy tarzda almashtirish imkoniyati mavjud emas. Shu sababli biometrik ma’lumotlarni saqlash va qayta ishlashda maxfiylik hamda xavfsizlik talablariga qat’iy rioya qilish zarur.

Ma’lumotlarni shifrlash, xavfsiz saqlash, ulardan foydalanish huquqlarini cheklash va foydalanuvchi roziligini nazorat qilish biometrik tizimlarning muhim talablaridan hisoblanadi.Deepfake tahdidlariga qarshi kurashishda asosiy texnologiyalardan biri jonlilik testi (liveness detection) hisoblanadi. Uning vazifasi biometrik namunaning haqiqiy insondan olinganligini aniqlash va sun’iy ravishda yaratilgan tasvir yoki videoni ajratishdan iborat. Jonlilik testi faol va passiv usullarga bo‘linadi. Faol usulda foydalanuvchidan ko‘z qisish, boshni burish yoki berilgan ko‘rsatmani bajarish talab qilinadi. Passiv usul esa foydalanuvchi harakatini talab qilmasdan, tasvirdagi mikroharakatlar, yorug‘lik aks etishi, teri tuzilishi kabi belgilarni avtomatik tahlil qiladi.Deepfake texnologiyalarining rivojlanishi biometrik himoyada faqat bitta tekshiruv usulidan foydalanish yetarli emasligini ko‘rsatmoqda. Shu sababli yuzni tanish, jonlilik testi, hujjatlarni tekshirish va xulq-atvor biometrikasini birlashtirgan ko‘p bosqichli autentifikatsiya tizimlariga ehtiyoj ortmoqda. Bunday tizimda foydalanuvchining nafaqat tashqi ko‘rinishi, balki uning harakati va taqdim etayotgan ma’lumotlari ham tahlil qilinadi.Biometrik xavfsizlikda ma’lumotlarning maxfiyligini ta’minlash ham muhim masalalardan biridir.

Biometrik ma’lumot shaxs bilan bevosita bog‘liq bo‘lganligi sababli uning yo‘qolishi yoki ruxsatsiz foydalanilishi jiddiy xavf tug‘dirishi mumkin. Shu bois zamonaviy tizimlarda shifrlash, xavfsiz saqlash va kirish huquqlarini nazorat qilish bilan bir qatorda, biometrik ma’lumotni imkon qadar kam miqdorda saqlash va qayta ishlashga asoslangan yondashuvlar ham qo‘llanilmoqda.Biometrik autentifikatsiya texnologiyalari moliya, elektron hukumat, masofaviy ish va ta’lim kabi ko‘plab sohalarda qo‘llanmoqda. Ayniqsa, masofadan turib shaxsni tasdiqlash zarur bo‘lgan xizmatlarda biometrik tekshiruv muhim vositaga aylanmoqda. Biroq bunday tizimlardan foydalanishda texnik samaradorlik bilan bir qatorda ma’lumotlar maxfiyligi va huquqiy talablarni ham hisobga olish zarur.Shunday qilib, sun’iy intellekt biometrik xavfsizlikka ikki tomonlama ta’sir ko‘rsatmoqda. Bir tomondan, deepfake texnologiyalari mavjud autentifikatsiya tizimlariga yangi tahdidlar yaratmoqda, ikkinchi tomondan esa sun’iy intellekt ushbu tahdidlarni aniqlash va ularga qarshi kurashish imkonini beruvchi yangi vositalarni shakllantirmoqda. Shu sababli biometrik xavfsizlikning kelajakdagi rivojida deepfake’ni aniqlash, jonlilik testi, ko‘p bosqichli autentifikatsiya va biometrik ma’lumotlarning maxfiyligini ta’minlash masalalari muhim o‘rin tutadi.Sun’iy intellekt asosida yaratiladigan deepfake tahdidlarining biometrik autentifikatsiya tizimlariga ta’sirini tahlil qilish hamda ularga qarshi qo‘llanilayotgan zamonaviy himoya usullarini ko‘rib chiqishdan iborat.

Tahlillar shuni ko‘rsatadiki, sun’iy intellekt biometrik xavfsizlikda ham xavf, ham himoya vositasi sifatida namoyon bo‘lmoqda. Deepfake texnologiyalari biometrik identifikatsiya tizimlariga tahdid tug‘dirayotgan bo‘lsa, sun’iy intellekt asosidagi jonlilik testi va deepfake’ni aniqlash usullari ushbu tahdidlarni kamaytirishga xizmat qilmoqda. Shu sababli kelajakdagi biometrik xavfsizlik

tizimlari ko‘p bosqichli himoya, biometrik ma’lumotlar maxfiyligi va xalqaro xavfsizlik standartlariga asoslanishi zarur. Ushbu yo‘nalishlarning uyg‘un rivojlanishi sun’iy intellekt davrida ishonchli va xavfsiz raqamli identifikatsiyani ta’minlash imkonini beradi.

Foydalanilgan adabiyotlar

1. ISO/IEC 30107-1:2023**.** *Information technology — Biometric presentation attack detection — Part 1: Framework.* International Organization for Standardization, 2023.

2. Ngan, M. L., Grother, P., Hom, A. *Face Analysis Technology Evaluation (FATE) Part 10: Performance of Passive, Software-based Presentation Attack Detection (PAD) Algorithms.* NISTIR 8491, National Institute of Standards and Technology, 2023.

3. Kotalwar, A., Joshi, R. R. *Adaptive multimodal liveness detection framework for biometric authentication against spoofing and deepfake attacks.* Discover Artificial Intelligence, 2026.

4. OLOID**.** *Liveness Detection Guide: Protecting Digital Identity 2026.* 2026. Ushbu manba liveness detection, deepfake, foto, video va boshqa spoofing hujumlaridan himoyalanish masalalarini yoritadi.

MA’LUMOTLAR ISHONCHLILIGINI OSHIRISHDA BIG DATANING O‘RNI VA VAZIFALARI

Ulug‘murodov Shoh Abbos Baxodir o‘g‘li
Axborot tizimlari va texnologiyalari kafedrasi, o‘qituvchisi
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali
shohabbosdev@gmail.com
Qodirov Zoxidjon Tohir o‘g‘li
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali
Magistratura bo‘limi “Dasturiy injiniring” yo‘nalishi magistranti
zokhidjonyuta@gmail.com

Annotatsiya. Zamonaviy axborot tizimlarida ma’lumotlar ishonchliligini ta’minlash muammosi Big Data texnologiyalari nuqtayi nazaridan ko‘rib chiqildi. Tizimga kirib kelayotgan ma’lumotning bir qismi noto‘g‘ri, to‘liq bo‘lmagan yoki qasddan o‘zgartirilgan bo‘lishi mumkin. An’anaviy relyatsion nazorat esa yuqori tezlikdagi oqimni to‘liq tekshirishga ulgurmaydi. Tadqiqotda o‘nta ilmiy manbaa qiyosiy tahlil qilindi va har biri bo‘yicha qaysi sifat mezoni, qanday nazorat mexanizmi va qanday o‘lchov ko‘rsatkichi qo‘llanilgani aniqlandi.

Natijada, Big Data ma’lumotlar ishonchliligini ta’minlashda beshta asosiy vazifani bajarishi aniqlandi: kirish validatsiyasi, triangulyatsiya, asosiy ma’lumotlarni boshqarish (MDM), anomaliyani aniqlash va ma’lumot kelib chiqishini kuzatish (Data Lineage). Bu beshta vazifa tekshiruv xarajati ortib boruvchi tartibda yagona qatlamga — ma’lumotlar ishonchliligi qatlamiga (Data Reliability Layer) birlashtirildi, har bir mezon uchun esa aniq o‘lchov ko‘rsatkichi belgilandi.