ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-3

RAQAMLI TRANSFORMASIYA SHAROITIDA SUN'IY INTELLEKTGA ASOSLANGAN AXBOROT TIZIMLARI XAVFSIZLIGINI TA'MINLASHNING ZAMONAVIY MODELLARI

Termiz davlat pedagogika instituti. Maktabgacha ta'lim sirtqi 23-04 guruhi talabasi Nurmamatova Nodira Abdumalikovnaning A.K.T.fanidan yozgan mustaqil ta'lim ishi.

Annotasiya. Ushbu maqolada raqamli iqtisodiyot va elektron boshqaruv muhitida sun'iy intellektga asoslangan axborot tizimlarining xavfsizligini ta'minlash masalasi ilmiy-nazariy va amaliy jihatdan tahlil qilindi. Tadqiqotda kiberxavfsizlikning klassik tamoyillarining 2025 yilgi veb-ilovalar va LLM ilovalari uchun xavflar tasnifi, shuningdek, O'zbekistonda qabul qilingan yangi strategik va huquqiy hujjatlar bir-biriga bog'liq holda ko'rib chiqildi. Maqolada global miqyosda kiberxavflar moliyaviy, tashkiliy va institusional yo'qotishlarga olib kelayotgani, sun'iy intellekt esa bir vaqtning o'zida ham himoya vositasi, ham yangi xavflar manbai sifatida namoyon bo'layotgani asoslanadi. Muallif tomonidan **"ma'lumot-model-infratuzilma-inson-boshqaruv"** besh qatlamli integrasion xavfsizlik modeli taklif qilingan. Tadqiqot natijalari shuni ko'rsatadiki, O'zbekistonda sun'iy intellektni joriy etish sur'ati ortib borayotgan bir sharoitda xavfsizlikni faqat texnik muammo sifatida emas, balki huquqiy, tashkiliy, kadrlar siyosati va standartlashtirish bilan bog'liq kompleks masala sifatida ko'rish talab etiladi. Maqola axborot texnologiyalari, kiberxavfsizlik, raqamli boshqaruv sohalarida tadqiqot olib borayotgan olimlar, doktorantlar va amaliyotchilar uchun mo'ljallangan.

Kalit so'zlar: raqamli transformasiya, sun'iy intellekt, kiberxavfsizlik, Zero Trust, AI RMF, OWASP, LLM xavflari, axborot xavfsizligi, raqamli iqtisodiyot, O'zbekiston.

KIRISH.

XXI asrning ikkinchi choragiga kelib axborot texnologiyalari rivoji oddiy avtomatlashtirish bosqichidan chiqib, qaror qabul qilish, katta ma'lumotlarni tahlil qilish, davlat xizmatlarini optimallashtirish, moliyaviy monitoring, tibbiy diagnostika va sanoat boshqaruvi kabi sohalarga chuqur kirib bordi. Bu jarayonda sun'iy intellekt texnologiyalari strategik resurs maqomiga ko'tarildi. O'zbekistonda ham mazkur tendensiya davlat siyosati darajasiga olib chiqildi: 2024 yil 14 oktyabrdagi 2030 yilgacha sun'iy intellekt texnologiyalarini rivojlantirish strategiyasi mamlakatni AI'dan faol foydalanuvchi etakchi davlatlar qatoriga olib chiqishni maqsad qildi. Hujjatda 2030 yilga qadar sun'iy intellektga asoslangan dasturiy mahsulot va xizmatlar hajmini 1,5 mlrd AQSH dollariga etkazish, YAgona interaktiv davlat xizmatlari portalida AI-quvvatlangan xizmatlar ulushini 10 foizga oshirish kabi aniq maqsadli ko'rsatkichlar belgilangan.

Biroq raqamlashtirish tezlashgan sari himoya perimetri kengaymaydi, aksincha, parchalanadi. Ilgari tashkilotning "ichki tarmog'i" va "tashqi muhiti" o'rtasida nisbatan aniq chegara bor edi. Hozir esa bulutli xizmatlar, mobil ilovalar, API integrasiyalar, uchinchi tomon platformalari, generativ modellar va avtonom agentlar bu chegarani amalda yo'qqa chiqardi. SHu bois axborot tizimlari xavfsizligini eski "bir marta tekshirish va ishonish" usulida ta'minlash etarli emas. NIST Zero Trust Architecture yondashuviga ko'ra, himoya tarmoq perimetridan foydalanuvchi, aktiv va resurs darajasiga ko'chirilishi lozim. Bu esa sun'iy intellektni joriy etish jarayonida xavfsizlik arxitekturasini qayta ko'rib chiqishni talab qiladi.

Global hisobotlar vaziyatning jiddiyligini yanada ochiq ko'rsatmoqda. IBM'ning 2024 yilgi ma'lumotlar buzilishi bo'yicha hisobotiga ko'ra, bir hodisaning o'rtacha global qiymati 4,88 mln

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-3

AQSH dollariga etgan, moliya sektorida esa bu ko'rsatkich 6,08 mln dollarga chiqqan. Bundan tashqari, moliyaviy tashkilotlar bir buzilishni aniqlash uchun o'rtacha 168 kun, bartaraf etish uchun yana 51 kun sarflagan. World Economic Forum'ning 2025 yilgi hisobotida esa tashkilotlarning 66 foizi kelasi yilda kiberxavfsizlikka eng katta ta'sirni AI ko'rsatishini kutgani holda, faqat 37 foizi AI vositalari joriy etilishidan oldin ularning xavfsizligini baholash jarayonlariga ega ekani qayd etilgan. Yirik tashkilotlarning 54 foizi ta'minot zanjiri muammolarini kiberbarqarorlikka erishishdagi asosiy to'siq deb baholagan.

SHu nuqtai nazardan qaraganda, sun'iy intellektga asoslangan axborot tizimlari xavfsizligi axborot texnologiyalari fanining eng dolzarb yo'nalishlaridan biridir. Bu erda muammo faqat serverni himoya qilish yoki parol mustahkamligini oshirishda emas. Asosiy muammo - **AI tizimlarida ma'lumotlarning kelib chiqishi, modelning ishonchliligi, chiqish natijasining nazorat qilina olishi, inson omilining etukligi va huquqiy javobgarlik chegaralarini** kompleks tarzda boshqarishdadir.

Adabiyotlar tahlili. O'zbekistonlik tadqiqotchilarning ishlarida axborot xavfsizligi va kiberxavfsizlikning nazariy poydevori ancha oldin shakllangan. S.K. G'aniev, A.A. G'aniev, Z.T. Xudoyqulovning "Kiberxavfsizlik asoslari" o'quv qo'llanmasida kriptografik himoya, foydalanishni nazoratlash, tarmoq xavfsizligi, risklarni boshqarish, kiberjinoyatchilik va kiberetika masalalari tizimli bayon qilingan. S.K. G'aniev, M.M. Karimov, K.A. Tashevning "Axborot xavfsizligi" darsligi esa mazkur sohaning nazariy apparati va himoya mexanizmlarini mustahkamlashda muhim manba hisoblanadi. Bu ishlar klassik axborot xavfsizligi paradigmasi uchun mustahkam baza yaratgan.

Keyingi bosqichda mahalliy adabiyotlarda raqamli kriminalistika, raqamli dalillar va ochiq manbali tahlil usullari alohida yo'nalish sifatida rivojlana boshladi. YUsupov, G'ulomov va Nasrullaev tomonidan tayyorlangan "Raqamli kriminalistika" o'quv qo'llanmasi ushbu yo'nalishning amaliyotdagi ahamiyatini ko'rsatsa, Abduraximov, Allanov, Turdibekov va Davlatov raqamli kriminalistika sohasidagi asosiy muammolarni dalillarni yig'ish, tahlil qilish va texnologik ko'pqirralilik nuqtai nazaridan tahlil qilgan. Normurodova esa raqamli ochiq manbalardan kriminalistik tadqiqotlarda foydalanish imkoniyatlarini yoritgan. Bu ishlardan ko'rinadiki, mahalliy ilmiy maktab kiberxavfsizlikni faqat abstrakt xavfsizlik tushunchasi sifatida emas, balki dalil, tekshiruv va profilaktika tizimi sifatida ham ko'ra boshlagan.

Sun'iy intellektga oid mahalliy tadqiqotlarda asosan uning funksional imkoniyatlari, ta'lim, iqtisodiyot va boshqaruvda qo'llanishi keng yoritilgan. Masalan, Usmonov AI tizimlarining inson faoliyatidagi o'rnini tarixiy va amaliy nuqtai nazardan tahlil qiladi. Lekin aksariyat ishlarda AI'ning xavfsizlikka bog'liq qirrasi - ya'ni model ustidan nazorat, ma'lumot manbalari ishonchliligi, prompt injection, training data poisoning, sensitive information disclosure kabi yangi xavflar - etarli darajada chuqurlashtirilmagan. Xalqaro adabiyotda esa aynan shu yo'nalish alohida sohaga aylanib ulgurdi. Demak, mahalliy va xalqaro ilmiy yondashuvlarni birlashtirish dolzarb vazifadir.

TADQIQOT METODOLOGIYASI.

Maqolada qiyosiy-huquqiy tahlil, tizimli yondashuv, risk-orientirlangan tahlil va konseptual modellashtirish usullaridan foydalanildi. Birinchi bosqichda O'zbekistondagi huquqiy va strategik hujjatlar: kiberxavfsizlik to'g'risidagi qonun, 2024 yilgi AI strategiyasi, 2025 yilgi axborot texnologiyalaridan foydalanib sodir etiladigan jinoyatlarga qarshi kurashni kuchaytirishga oid qaror hamda 2026 yil 10 martda qabul qilingan Kiberxavfsizlik strategiyasi tahlil qilindi. Ikkinchi bosqichda NIST AI RMF, NIST'ning Generative AI Profile hujjati, OWASP Top 10:2025 va OWASP

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

LLM Top 10 manbalari asosida xavflar tasnifi shakllantirildi. Uchinchi bosqichda milliy amaliyotga mos **integrasion besh qatlamli xavfsizlik modeli** ishlab chiqildi.

Metodologik jihatdan ushbu tadqiqotning asosiy nuqtasi shuki, AI xavfsizligi odatiy axborot xavfsizligiga qo'shimcha bob emas. U mustaqil tahlil birligi sifatida qaraldi. CHunki AI tizimlarida risk faqat infratuzilmada emas, balki ma'lumot tozaligida, model mantig'ida, chiqish natijasini tushuntirish imkoniyatida, inson nazoratida va regulyator mosligida ham yashirin bo'ladi. NIST'ning GAI profilida ham boshqaruv, kontent kelib chiqishi, joriy etishdan oldingi testlash va insidentni oshkor qilish asosiy to'rt yo'nalish sifatida ajratilgani bejiz emas.

NATIJALAR VA MUHOKAMA.

Tadqiqot natijalariga ko'ra, sun'iy intellektga asoslangan axborot tizimlari uchun xavflar kamida beshta yirik guruhga bo'linadi. Birinchi guruh - **ma'lumot xavflari**. Bunda ma'lumot manbasining ishonchli emasligi, datasetdagi og'ishlar, maxfiy ma'lumotning o'quv ma'lumotiga kirib ketishi, sintetik va real ma'lumotlar aralashuvidan kelib chiqadigan aniqlik muammolari muhim o'rin tutadi. Ikkinchi guruh - **model xavflari**. Bu erda adversarial manipulation, hallucination, training data poisoning, model theft, overreliance va explainability muammolari markazda turadi. Uchinchi guruh - **ilova va infratuzilma xavflari** bo'lib, veb-ilovalar darajasida 2025 yilda ham Broken Access Control, Security Misconfiguration, Software Supply Chain Failures kabi muammolar dolzarbligicha qolayotgani qayd etilgan. To'rtinchi guruh - **inson omili**. Bu sohada foydalanuvchining prompt bilan modelni yo'ldan ozdirishi, natijaga asossiz ishonishi, maxfiy ma'lumotni noo'rin kiritishi kabi holatlar ustuvor xavf manbai hisoblanadi. Beshinchi guruh - **boshqaruv va huquqiy risklar** bo'lib, javobgarlik, audit izi, regulyator talablarga moslik va insident haqida o'z vaqtida xabar berish muammolarini o'z ichiga oladi.

SHu asosda maqolada **"ma'lumot-model-infratuzilma-inson-boshqaruv"** degan besh qatlamli integrasion xavfsizlik modeli taklif etiladi. Unga ko'ra, AI tizimining xavfsizligi eng zaif bo'g'inga bog'liq. Masalan, infratuzilma juda kuchli himoyalangan bo'lishi mumkin, lekin o'quv ma'lumoti ifloslangan bo'lsa, butun tizim ishonchsiz natija beradi. YOki model texnik jihatdan yaxshi qurilgan bo'lishi mumkin, lekin inson nazorati yo'qligi sababli uning natijalari noto'g'ri qarorlarga asos bo'ladi. Demak, AI xavfsizligida "bir nuqtali himoya" emas, **qatlamli ishonch arxitekturasi** zarur. Zero Trust'ning mohiyati ham aynan shunda: hech bir foydalanuvchi, qurilma yoki servis avvaldan ishonchli deb qabul qilinmaydi, har bir murojaat kontekst, rol, qurilma holati va risk darajasi asosida qayta baholanadi.

NIST AI RMF'ning amaliy qiymati shundaki, u riskni texnik muammodan tashqari, boshqaruv kategoriyasi sifatida ham ko'radi. Uning asosiy funksiyalari **Govern, Map, Measure, Manage** deb belgilangan. Bu mantiqni O'zbekiston amaliyotiga moslashtirsak, "Govern" bosqichida AI bo'yicha ichki siyosat, mas'ul shaxs, huquqiy moslik va etik standartlar, "Map" bosqichida ma'lumot manbalari, model limitlari, foydalanish konteksti va tashqi ta'minot zanjiri, "Measure" bosqichida bias, privacy, robustness, accuracy va red-teaming natijalari, "Manage" bosqichida esa insidentlarga javob, doimiy monitoring, versiya nazorati va audit trail tashkil etilishi kerak. Bu yondashuvni joriy etmasdan turib, AI'ni davlat xizmatlari, banklar, ta'lim yoki tibbiyotga ommaviy tatbiq etish strategik xato bo'lishi mumkin.

OWASP'ning LLM ilovalari uchun xavflar tasnifi esa AI xavfsizligi muammosini yanada aniqlashtiradi. Unda prompt injection, insecure output handling, training data poisoning, model denial of service, supply chain vulnerabilities, sensitive information disclosure kabi xavflar sanab o'tilgan.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

VOLUME-6, ISSUE-3

Bu xavflarning har biri O'zbekistonda endi-endi rivojlanayotgan generativ AI servislari uchun ham to'liq dolzarb. Masalan, davlat yoki ta'lim tashkiloti ichki hujjatlar bilan ishlaydigan LLM'ni joriy etsa, maxfiy ma'lumot ochilishi xavfi birinchi darajali masalaga aylanadi. YOki moliyaviy xizmatda chat-bot tavsiyalari avtomatik amalga ulangan bo'lsa, insecure output handling orqali biznes jarayoniga zarar etkazish mumkin. SHu sababli generativ AI'ni "foydali yordamchi" deb emas, **xavfsizlik profiliga ega alohida raqamli sub'ekt** deb baholash to'g'riroq.

Milliy kontekstda bu masalaning ahamiyati ortib bormoqda. ITU'ning 2024 yilgi Global Cybersecurity Index hisobotida O'zbekiston 89,2 ball bilan Tier 2 (Advancing) guruhiga kiritildi, 2020 yilda esa mamlakat ko'rsatkichi 71,11 bo'lgan. Bu o'sish huquqiy, tashkiliy va texnik salohiyat ortganini ko'rsatadi. Biroq 2025 yilgi ayrim rasmiy sharhlarda kiberjinoyatlar yil boshidan sodir etilgan jinoyatlarning 42 foizini tashkil etgani ham ta'kidlangan. Demak, reyting oshgani bilan xavf yuklamasi ham kamaymagan, aksincha, raqamli faollik oshib borgan sari hujum sathi kengaygan. 2026 yil 10 martda Kiberxavfsizlik strategiyasi bo'yicha yangi farmon qabul qilingani ham shuning institusional tasdig'idir.

O'zbekistonning 2030 yilgacha AI strategiyasida 2025-2026 yillarda AI sohasida milliy standartlarni ishlab chiqish, to'qqizta milliy standartni xalqaro standartlar bilan uyg'unlashtirish, GPU'larga asoslangan yuqori unumli hisoblash klasteri va "big data" server uskunalarini ishga tushirish, shuningdek, dunyoning etakchi universitetlariga maqsadli o'rinlar ajratish kabi vazifalar belgilangan. Bu maqsadlar juda to'g'ri, lekin ular **standartlashtirish + xavfsizlik + kadrlar tayyorlash** birgalikda olib borilsagina samara beradi. Infratuzilma bor, lekin model auditi yo'q, kadr bor, lekin huquqiy protokol yo'q, servis bor, lekin loglash va insidentni ochiqlash tizimi yo'q - bunday holatda texnologik taraqqiyot emas, texnologik zaiflik yuzaga keladi.

Maqolada amaliyot uchun quyidagi shartli baholash formulasi taklif etiladi: **AI-KX = (E × T × O) / N**, bu erda **E** - hodisa ehtimoli, **T** - ta'sir og'irligi, **O** - ochiqlik darajasi, **N** - nazorat mexanizmlari etukligi. Agar ushbu indeks yuqori chiqsa, tashkilot AI tizimini joriy etishdan oldin qo'shimcha test, red-teaming, data lineage audit va access segmentation choralarini ko'rishi kerak bo'ladi. Formula universal standart emas, balki tahliliy amaliyot uchun taklif etilayotgan lokal indikatordir. Uning afzalligi shundaki, AI xavfini oddiy "bor-yo'q" shaklida emas, balki boshqaruv qarorlari uchun miqdoriy ko'rinishda ifodalashga yordam beradi. IBM hisobotlarida AI va avtomatlashtirish xavflarni barvaqt aniqlash va yo'qotishlarda xarajatni sezilarli kamaytirishi mumkinligi ta'kidlangani ham shunday yondashuvning amaliy qiymatini tasdiqlaydi.

SHu bilan birga, kadrlar siyosati masalasi etarlicha baholanmayapti. World Economic Forum'ga ko'ra, jamoat sektoridagi tashkilotlarning 49 foizi kiberxavfsizlik maqsadlariga erishish uchun zarur kadrlarga ega emas. Bu raqam O'zbekiston uchun ham jiddiy signal sifatida qabul qilinishi kerak. CHunki AI tizimlarini sotib olish oson, ammo ularni xavfsiz tarzda joriy qilish, baholash, loglash, monitoring qilish va huquqiy jihatdan muhofaza qilish uchun mutaxassislar maktabi kerak. SHu sababli IT yo'nalishidagi oliy ta'lim dasturlariga **AI security engineering, model auditing, prompt safety, digital forensics, privacy engineering** kabi modullarni tizimli kiritish zarur.

XULOSA.

Tadqiqot natijalari shuni ko'rsatadiki, sun'iy intellektga asoslangan axborot tizimlari xavfsizligi axborot texnologiyalari fanining yordamchi mavzusi emas, balki uning markaziy muammolaridan biriga aylandi. Bu sohadagi eng katta xato - AI'ni faqat innovasion qulaylik manbai deb baholashdir. Amalda esa AI har bir tashkilotda hujum yuzasini kengaytiruvchi, javobgarlik chegaralarini

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

murakkablashtiruvchi va boshqaruvni qayta qurishni talab qiluvchi yangi raqamli muhitni yaratadi. SHuning uchun **AI'ni joriy etish sur'ati uning xavfsizlik boshqaruvi sur'atidan yuqori bo'lmasligi kerak**.

O'zbekistonda mazkur yo'nalish uchun muhim institusional poydevor shakllanmoqda: kiberxavfsizlik to'g'risidagi qonun mavjud, 2024 yilda AI strategiyasi qabul qilindi, 2025-2026 yillarda esa kiberjinoyatchilikka qarshi kurash va kiberxavfsizlik strategiyasini mustahkamlashga oid yangi hujjatlar qabul qilindi. Lekin navbatdagi bosqich huquqiy hujjatlarni ko'paytirish emas, balki ularni **standartlar, audit amaliyoti, kadrlar tayyorlash, milliy data boshqaruvi va AI-xavflarni baholash infrastrukturasi** bilan to'ldirishdan iborat bo'lishi lozim.

Maqolada taklif etilgan **"ma'lumot-model-infratuzilma-inson-boshqaruv"** modeli va **AI-KX indeksi** tashkilotlarga AI tizimlarini joriy etishda nazariy emas, amaliy mantiq bera oladi. Ilmiy nuqtai nazardan esa bu yondashuv klassik axborot xavfsizligi maktabini generativ va intellektual tizimlar davriga moslashtirishga xizmat qiladi. **Xavfsiz AI - bu faqat texnik jihatdan mustahkam AI emas, u huquqiy jihatdan mas'ul, tashkiliy jihatdan boshqariluvchi, etik jihatdan izchil va inson nazoratidan chiqmaydigan AI'dir.** Ana shu tamoyil kelgusi yillarda axborot texnologiyalari sohasidagi ilmiy tadqiqotlar va amaliy islohotlar uchun bosh mezon bo'lishi kerak.

FOYDALANILGAN ADABIYOTLAR

1. G'aniev S.K., G'aniev A.A., Xudoyqulov Z.T. Kiberxavfsizlik asoslari: o'quv qo'llanma. - Toshkent: Aloqachi, 221 b., 2020.
2. G'aniev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. - Toshkent: Fan va texnologiya, 372 b., 2016.
3. YUsupov S.YU., G'ulomov SH.R., Nasrullaev N.B. Raqamli kriminalistika: o'quv qo'llanma. - Toshkent: Aloqachi, 240 b., 2020.
4. Abduraximov B., Allanov O., Turdibekov B., Davlatov M. Raqamli kriminalistika sohasidagi asosiy muammolar // Innovative Development in Educational Activities. - T. 2, № 18. - B. 240-255, 2023.
5. Normurodova B. Raqamli ochiq manbalar va ulardan raqamli kriminalistikada foydalanish // Actual Problems of Humanities and Social Sciences. - T. 4, № 5, 2024.
6. Usmonov M.T. o'g'li. Sun'iy intellekt tizimlarining insoniyat faoliyatida tutgan o'rni // Academic Research in Modern Science. - Xalqaro ilmiy onlayn konferensiya materiallari, 2023.