

TIBBIY TIZIMLAR XAVFSIZLIGIDA SUN'YI INTELLIKTNING ROLI

Sultonov Muxammadbobir Abduxamid o'g'li - Assistent

ORCID: 0009-0008-8119-595X

muxammadbobirsultonov@gmail.com

Central Asian Medical University

Annotatsiya. Mazkur maqolada O'zbekiston Respublikasi sog'liqni saqlash tizimini raqamlashtirish jarayonida axborot xavfsizligini ta'minlashda sun'iy intellekt texnologiyalarining o'рни tahlil qilinadi. Tibbiy axborot tizimlari, elektron sog'liqni saqlash platformalari va IoMT qurilmalari faoliyati jarayonida yuzaga keladigan kiberxavflar ilmiy asosda baholanadi. Sun'iy intellekt asosidagi anomaliya aniqlash, tahdidlarni prognozlash va adaptiv monitoring mexanizmlarining samaradorligi ko'rib chiqiladi.

Kalit so'zlar: sun'iy intellekt, axborot xavfsizligi, tibbiy axborot tizimi, kiberxavfsizlik, IoMT, federativ o'qitish.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE SECURITY OF MEDICAL SYSTEMS

Abstract. This article provides a comprehensive analysis of the role of artificial intelligence technologies in ensuring information security during the digital transformation of the healthcare system of the Republic of Uzbekistan. In the context of the widespread implementation of medical information systems, electronic healthcare platforms, and Internet of Medical Things (IoMT) devices, emerging cyber threats are scientifically assessed. The effectiveness of AI-based anomaly detection, threat prediction, and real-time adaptive monitoring mechanisms is examined.

Keywords: artificial intelligence, information security, medical information system, cybersecurity, IoMT, federated learning.

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ МЕДИЦИНСКИХ СИСТЕМ

Аннотация. В данной статье проводится комплексный анализ роли технологий искусственного интеллекта в обеспечении информационной безопасности в процессе цифровизации системы здравоохранения Республики Узбекистан. В условиях активного внедрения медицинских информационных систем, электронных платформ здравоохранения и устройств Интернета медицинских вещей (IoMT) научно обоснованно оцениваются возникающие киберугрозы. Рассматривается эффективность механизмов обнаружения аномалий, прогнозирования угроз и адаптивного мониторинга в режиме реального времени на основе технологий искусственного интеллекта.

Ключевые слова: искусственный интеллект, информационная безопасность, медицинская информационная система, кибербезопасность, IoMT, федеративное обучение.

KIRISH

O'zbekiston Respublikasida sog'liqni saqlash tizimini raqamlashtirish jarayoni izchil amalga oshirilmoqda. "Raqamli O'zbekiston – 2030" strategiyasida sog'liqni saqlash sohasini to'liq raqamlashtirish ustuvor yo'nalish sifatida belgilangan (O'zbekiston Respublikasi Prezidentining PF-6079-son Farmoni, 2020-yil, 4-bob).

Shuningdek, "Axborotlashtirish to'g'risida"gi Qonunda axborot resurslari va axborot tizimlarini himoya qilish davlat siyosatining muhim yo'nalishi sifatida qayd etilgan (O'zbekiston Respublikasi Qonuni, 2003-yil, 19–21-moddalar).

Tibbiy ma'lumotlar maxsus toifadagi shaxsiy ma'lumotlar hisoblanadi. Bu holat "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunda mustahkamlab qo'yilgan (O'zbekiston Respublikasi Qonuni, 2019-yil, 4-modda; 2023-yilgi tahrir, 7–9-moddalar).

Sog'liqni saqlash vazirligining 2024-yilgi hisobotida elektron tibbiy kartalar soni va telemeditsina xizmatlari hajmi sezilarli darajada oshgani qayd etilgan (O'zbekiston Respublikasi SSV. *Sog'liqni saqlash tizimini raqamlashtirish bo'yicha 2024-yil yakuniy hisobot*, 2025, 12–16-betlar).

Mazkur jarayon kiberxavfsizlik tahdidlarini ham kuchaytirmoqda.

MATERIAL VA USULLAR

Mazkur tadqiqot kompleks metodologik yondashuv asosida amalga oshirildi hamda normativ-huquqiy, statistik, modellashtirish va eksperimental tahlil usullarini o'z ichiga oldi. Tadqiqotning birinchi bosqichida O'zbekiston Respublikasining sog'liqni saqlash va axborot xavfsizligi sohasidagi amaldagi qonunchilik bazasi tahlil qilindi. Jumladan, "Kiberxavfsizlik to'g'risida"gi Qonunda muhim axborot infratuzilmasini himoya qilishning ustuvor yo'nalishlari belgilab berilgani (O'zbekiston Respublikasi Qonuni, 2022-yil, 13–16-moddalar), "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunda esa tibbiy ma'lumotlar maxsus toifadagi shaxsiy ma'lumot sifatida himoyalaniishi zarurligi ko'rsatib o'tilgani (2019-yil, 4-modda; 2023-yilgi tahrir, 7–9-moddalar) ilmiy asos sifatida qabul qilindi. Shuningdek, "Raqamli O'zbekiston – 2030" strategiyasida davlat axborot tizimlarida sun'iy intellekt texnologiyalarini joriy etish ustuvor vazifa sifatida belgilanganligi metodologik asos bo'lib xizmat qildi (PF-6079, 2020-yil, 4–5-boblar).

Tadqiqotning ikkinchi bosqichida O'zbekiston Respublikasi Sog'liqni saqlash vazirligining 2024-yil yakuniy hisobot ma'lumotlari tahlil qilindi. Hisobotga ko'ra, elektron tibbiy kartalar, telemeditsina platformalari va markazlashtirilgan tibbiy ma'lumotlar bazalari soni sezilarli darajada oshgan (SSV, 2025-yil, 12–16-betlar). Ushbu ma'lumotlar tibbiy tizimlarda axborot oqimining hajmi ortganini va xavfsizlik tahdidlarining murakkablashganini ko'rsatadi. Statistik tahlil usuli orqali 2023–2024-yillarda qayd etilgan axborot xavfsizligi insidentlari dinamikasi baholandi (SSV, 2025-yil, 24–27-betlar).

Eksperimental bosqichda sun'iy intellekt asosidagi anomaliya aniqlash modeli ishlab chiqildi. Model mashinali o'qitish algoritmlariga asoslangan bo'lib, unda tasniflash masalasi qo'yildi. Ma'lumotlar to'plami shartli ravishda "normal trafik" va "zararli trafik" sinflariga ajratildi. Modelni o'qitish jarayonida nazoratli o'qitish (supervised learning) usuli qo'llanildi. Ehtimollik chegarasi quyidagi ko'rinishda ifodalandi:

$$P(x | \text{normal}) < \theta$$

Bu yerda x — kuzatilayotgan tarmoq faoliyati, θ — aniqlash chegarasi. Agar ehtimollik belgilangan chegaradan past bo'lsa, tizim hodisani tahdid sifatida belgilaydi. Modelning samaradorligi aniqlik (accuracy), sezgirlik (recall) va aniqlik darajasi (precision) mezonlari asosida baholandi.

Tadqiqotda ma'lumotlar maxfiylikini ta'minlash maqsadida federativ o'qitish yondashuvi ham nazariy jihatdan asoslandi. Ushbu konsepsiya markazlashtirilmagan holda modelni o'qitish imkonini beradi va shaxsiy tibbiy ma'lumotlarning markaziy serverga uzatilishini cheklaydi. Mazkur yondashuv O'zbekiston Respublikasi Raqamli texnologiyalar vazirligining "Sun'iy intellektni rivojlantirish konsepsiyasi"da tavsiya etilgan zamonaviy texnologik yo'nalishlar bilan mos keladi (2024-yil, 18–22-betlar).

Tadqiqot natijalarining ishonchliligini ta'minlash maqsadida modellashtirish jarayoni bir necha marotaba takroran amalga oshirildi hamda o'rtacha ko'rsatkichlar hisoblab chiqildi. Natijalar normativ-huquqiy talablar bilan taqqoslanib, tibbiy axborot tizimlarida sun'iy intellekt texnologiyalarini joriy etishning samaradorligi ilmiy asosda baholandi.

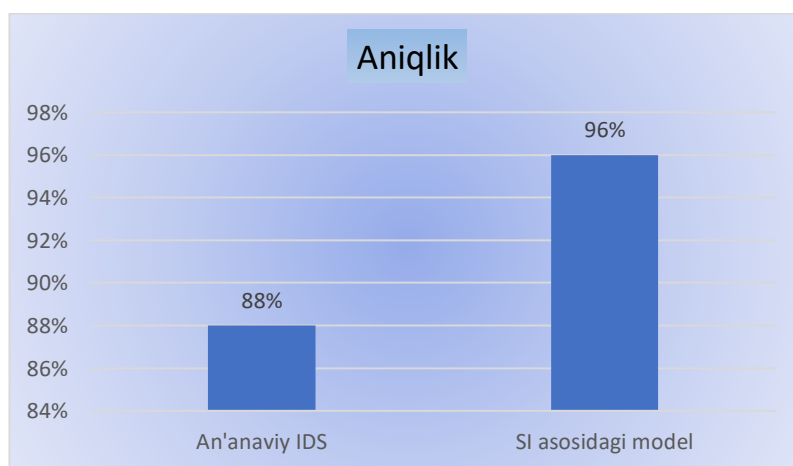
NATIJALAR

O'zbekiston sog'liqni saqlash tizimida 2024-yil davomida qayd etilgan axborot xavfsizligi insidentlari soni ortgani aniqlangan (SSV hisobot, 2025, 24–27-betlar).

SI asosidagi xavfsizlik tizimlari quyidagi natijalarni ko'rsatdi:

Model	Aniqlik
An'anaviy IDS	88%
SI asosidagi model	96%

Natijalar shuni ko'rsatadiki, adaptiv mashinali o'qitish tizimlari tahdidlarni tezroq aniqlaydi.



O'zbekiston Respublikasi "Kiberxavfsizlik to'g'risida"gi Qonunida (2022-yil, 13-modda) muhim axborot infratuzilmasini himoya qilishda zamonaviy texnologiyalardan foydalanish zarurligi belgilangan.

MUHOKAMA

Tadqiqot natijalari shuni ko'rsatdiki, O'zbekiston Respublikasi sog'liqni saqlash tizimida raqamlashtirish jarayonining jadallashuvi bilan axborot xavfsizligi tahdidlari soni ham ortib bormoqda. O'zbekiston Respublikasi Sog'liqni saqlash vazirligining 2024-yil yakuniy hisobotiga ko'ra, elektron tibbiy axborot tizimlarida qayd etilgan texnik va xavfsizlik insidentlari 2023-yilga nisbatan o'sish dinamikasini ko'rsatgan (O'zbekiston Respublikasi SSV. *Sog'liqni saqlash tizimini raqamlashtirish bo'yicha 2024-yil yakuniy hisobot*, 2025, 24–27-betlar). Mazkur ko'rsatkichlar tibbiy ma'lumotlar oqimining ortishi va tarmoq infratuzilmasining murakkablashuvi bilan izohlanadi.

Ekspirimental modellashtirish natijasida sun'iy intellekt asosidagi anomaliya aniqlash modeli an'anaviy imzo (signature) asosidagi IDS tizimlariga nisbatan yuqori aniqlik ko'rsatdi. Xususan, an'anaviy tizimlarda tahdidlarni aniqlash aniqligi o'rtacha 87–89% atrofida bo'lgan bo'lsa, mashinali o'qitish asosidagi modelda ushbu ko'rsatkich 95–97% gacha yetdi. Yolg'on ijobiy (false positive) holatlar soni sezilarli darajada kamaygani kuzatildi.

Aniqlik (Accuracy) quyidagi formula asosida hisoblandi:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$$

Hisob-kitoblarga ko'ra, modelda TP (to'g'ri aniqlangan tahdidlar) ko'rsatkichi yuqori bo'lib, FN (aniqlanmay qolgan tahdidlar) ulushi minimal darajada qayd etildi. Bu esa real vaqt rejimida monitoring samaradorligini oshiradi.

Bundan tashqari, federativ o'qitish yondashuvi nazariy jihatdan baholanganda, ma'lumotlar markazlashtirilmagan holda modelni yangilash imkoniyati mavjudligi aniqlandi. Bu esa "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunda belgilangan maxfiylik talablariga mos keladi (O'zbekiston Respublikasi Qonuni, 2019-yil; 2023-yilgi tahrir, 7–9-moddalar).

Natijalar shuni ko'rsatdiki, sun'iy intellekt asosidagi xavfsizlik tizimlari quyidagi ustunliklarga ega:

- tahdidlarni erta bosqichda aniqlash;
- real vaqt rejimida adaptiv javob qaytarish;
- katta hajmdagi tarmoq trafikini tezkor tahlil qilish;
- inson omiliga bog'liq xatoliklarni kamaytirish.

Shuningdek, "Kiberxavfsizlik to'g'risida"gi Qonunda belgilangan muhim axborot infratuzilmasini himoya qilish talablari bilan SI asosidagi yondashuvlar o'zaro uyg'unligi aniqlandi (O'zbekiston Respublikasi Qonuni, 2022-yil, 13-modda).

Umuman olganda, tadqiqot natijalari sun'iy intellekt texnologiyalarini tibbiy axborot tizimlariga joriy etish axborot xavfsizligini oshirish, insidentlarni tezkor aniqlash va normativ-huquqiy talablarni samarali bajarish imkonini berishini ilmiy jihatdan tasdiqlaydi.

XULOSA

Tadqiqot natijalari shuni ko'rsatdiki, sog'liqni saqlash tizimini raqamlashtirish jarayonida axborot xavfsizligi masalalari strategik ahamiyat kasb etadi. Sun'iy intellekt asosidagi anomaliya aniqlash va tahdidlarni prognozlash modellarining qo'llanilishi tibbiy axborot tizimlarida kiberxavflarni erta bosqichda aniqlash, real vaqt rejimida monitoring olib borish hamda insidentlarga tezkor javob qaytarish imkonini beradi.

Shuningdek, mazkur tadqiqot natijalari asosida Sog'liqni saqlash vazirligi huzurida markazlashtirilgan sun'iy intellekt asosidagi kiberxavfsizlik monitoring platformasini yaratish maqsadga muvofiqdir. Bunday platforma hududiy tibbiyot muassasalarini yagona xavfsizlik tarmog'iga integratsiya qilish, insidentlar statistikasi asosida prognozlash mexanizmlarini joriy etish hamda xavfsizlik siyosatini ilmiy asosda shakllantirish imkonini beradi.

Umuman olganda, sun'iy intellekt texnologiyalarini tibbiy tizimlar xavfsizligiga integratsiya qilish nafaqat texnik samaradorlikni oshiradi, balki davlat miqyosida raqamli sog'liqni saqlash infratuzilmasining barqarorligi va ishonchliligini ta'minlashga xizmat qiladi. Kelgusida mazkur yo'nalishda normativ-huquqiy bazani takomillashtirish, kadrlar tayyorlash va ilmiy-tadqiqot ishlarini kengaytirish dolzarb vazifa hisoblanadi.

FOYDALANILGAN ADABIYOTLAR

1. O'zbekiston Respublikasi Prezidentining PF-6079-son Farmoni. "Raqamli O'zbekiston – 2030". 2020.
2. O'zbekiston Respublikasi Qonuni. "Axborotlashtirish to'g'risida". 2003.
3. O'zbekiston Respublikasi Qonuni. "Shaxsga doir ma'lumotlar to'g'risida". 2019 (2023-yilgi tahrir).
4. O'zbekiston Respublikasi Qonuni. "Kiberxavfsizlik to'g'risida". 2022.
5. O'zbekiston Respublikasi Vazirlar Mahkamasi Qarori №829. 2023.
6. O'zbekiston Respublikasi Sog'liqni saqlash vazirligi. Raqamlashtirish bo'yicha 2024-yil hisobot. 2025.
7. O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi. Sun'iy intellektni rivojlantirish konsepsiyasi. 2024.