SUN’IY INTELLEKT ASOSIDAGI TIBBIY TIZIMLARDA AXBOROT XAVFSIZLIGINI TA’MINLASHNING DOLZARBLIGI

Sadirova Xursanoy Xusanboy qizi
Farg‘ona davlat texnika universiteti “Dasturiy injiniring va kiberxavfsizlik” kafedrasi assistenti

Annotatsiya: *Ushbu maqolaning maqsadi – tibbiyotda sun’iy intellekt (SI) texnologiyalaridan foydalanishda axborot xavfsizligini ta’minlashning ahamiyatini yoritishdir.*

Kalit so‘zlar: *Sun’iy intellekt, diagnostika, davolash, identifikatsiya, RSA, SHA-256.*

Annotation: *The purpose of this article is to highlight the importance of ensuring information security when using artificial intelligence (AI) technologies in the field of medicine.*

Keywords: *Artificial intelligence, diagnostics, treatment, identification, RSA, SHA-256.*

KIRISH

Hozirgi davrda tibbiyot sohasi raqamlashtirish va sun’iy intellekt (SI) texnologiyalarini keng joriy etish bosqichiga kirgan. Diagnostika, kasalliklarni bashorat qilish, davolash jarayonlarini avtomatlashtirish va bemor ma’lumotlarini tahlil qilishda sun’iy intellekt vositalari muhim rol o‘ynamoqda. Biroq, tibbiy ma’lumotlarning maxfiyligi va ularni himoya qilish masalalari dolzarb muammo bo‘lib qolmoqda. Shuning uchun tibbiyotda sun’iy intellektdan foydalanishda axborot xavfsizligini ta’minlash nafaqat texnik, balki huquqiy va axloqiy jihatdan ham muhim ahamiyat kasb etadi [1].

Sun’iy intellektning tibbiyotdagi roli. Sun’iy intellekt texnologiyalari tibbiyotda rentgen va MRT tasvirlarini tahlil qilish, kasalliklarni erta aniqlash, dori vositalarini ishlab chiqish, shuningdek, klinik qarorlarni qo‘llab-quvvatlashda keng qo‘llanilmoqda. Bu jarayonlarda katta hajmdagi tibbiy ma’lumotlar — bemorlar tarixlari, genetik ma’lumotlar, laboratoriya natijalari — qayta ishlanadi.

ASOSIY QISM

Hozirgi kunda tibbiyot sohasida sun’iy intellekt (SI) texnologiyalari inson salomatligini saqlash, kasalliklarni erta aniqlash va davolash jarayonlarini takomillashtirishda muhim ahamiyat kasb etmoqda. SI tizimlari katta hajmdagi tibbiy ma’lumotlarni (Big Data) tahlil qilish, ularni qayta ishlash hamda natijalar asosida tibbiy qarorlar qabul qilish jarayonini soddalashtiradi. Bu esa shifokorlarga bemorlarni aniq tashxislash, individual davolash usullarini tanlash va xatoliklarni kamaytirish imkonini beradi [2].

Sun’iy intellekt tibbiyotda quyidagi yo‘nalishlarda keng qo‘llanilmoqda:

Diagnostika va tahlil tizimlari. SI algoritmlari rentgen, MRT va KT tasvirlarini aniqlik bilan tahlil qiladi, o‘sma, yallig‘lanish yoki boshqa patologiyalarni erta bosqichda

aniqlashga yordam beradi. Masalan, neyron tarmoqlar asosidagi tizimlar inson ko‘zi ilg‘ay olmagan mikroskopik o‘zgarishlarni aniqlashi mumkin [3].

Prognozlash va kasalliklarni oldindan bashorat qilish. Bemorlarning klinik ma’lumotlari, genetik tahlillar va hayot tarzi omillarini tahlil qilib, sun’iy intellekt turli kasalliklarning rivojlanish xavfini oldindan baholaydi. Bu esa profilaktika choralarini o‘z vaqtida ko‘rish imkonini beradi.

Davolash jarayonlarini optimallashtirish. SI tizimlari dori vositalarining o‘zaro ta’sirini, dozalarini va bemorning holatini hisobga olib, individual davolash rejasini shakllantiradi. Bundan tashqari, robototexnika asosidagi jarrohlik tizimlari (masalan, Da Vinci roboti) operatsiyalarni yuqori aniqlikda bajaradi.

Ma’lumotlarni boshqarish va tahlil qilish. Elektron tibbiy kartalar, laboratoriya ma’lumotlari va tibbiy tadqiqotlar SI yordamida markazlashtirilgan tizimlarda saqlanadi va tahlil qilinadi. Bu ma’lumotlar sog‘liqni saqlash tizimida qaror qabul qilishni tezlashtiradi.

Axborot xavfsizligini mustahkamlash. Tibbiyotda SI faqat tahlil vositasi emas, balki axborot xavfsizligini ta’minlovchi mexanizm sifatida ham xizmat qilishi mumkin. Masalan, SI asosida ishlovchi xavfsizlik tizimlari ruxsatsiz kirish, ma’lumotlar sizib chiqishi yoki g‘ayritabiiy tarmoq faolligini aniqlash orqali himoya darajasini oshiradi. Shu bilan birga, tibbiyotda SI tizimlaridan foydalanishda maxfiy ma’lumotlarni himoya qilish masalasi dolzarb bo‘lib qolmoqda. Sun’iy intellekt modellarini o‘qitishda ishlatiladigan bemor ma’lumotlari shifrlangan holda saqlanishi, uzatilishi va qayta ishlanishi zarur. Aks holda, shaxsiy ma’lumotlarning oshkor bo‘lishi axborot xavfsizligiga putur yetkazadi [5].

Tibbiyotda sun’iy intellekt texnologiyalaridan foydalanish jarayonida eng muhim masalalardan biri — axborot xavfsizligini ta’minlashdir. Chunki bu tizimlar bemorlar, shifokorlar va tibbiy muassasalarga oid maxfiy ma’lumotlarni to‘plash, saqlash va qayta ishlash bilan bevosita bog‘liqdir. Tibbiyotdagi axborotlar orasida shaxsiy identifikatsiya ma’lumotlari, genetik ma’lumotlar, tibbiy tarix, tashxis va davolash natijalari mavjud bo‘lib, ularning oshkor bo‘lishi jiddiy oqibatlarga olib keladi.

Ma’lumotlarning maxfiyligi va ruxsatsiz kirish xavfi. Tibbiy axborotlar yuqori qiymatga ega bo‘lgani sababli kiberjinoyatchilar uchun eng qimmatli nishonlardan biridir. Sun’iy intellekt tizimlariga ulanadigan serverlar, bulutli saqlash tizimlari yoki tarmoq orqali ma’lumot uzatish jarayonida ruxsatsiz kirish, parolni buzish, fishing (soxta havola) hujumlari kuzatilishi mumkin. Agar bunday tizimlar yetarli darajada himoyalanmagan bo‘lsa, bemorlarning shaxsiy ma’lumotlari uchinchi shaxslarga sizib chiqadi, bu esa tibbiy muassasalarga nisbatan ishonchni kamaytiradi.

Sun’iy intellekt modellarining zaifligi va ma’lumotlar manipulyatsiyasi. Sun’iy intellekt tizimlari o‘qitish uchun katta hajmdagi ma’lumotlar to‘plamiga tayanadi. Agar ushbu ma’lumotlar noto‘g‘ri, soxtalashtirilgan yoki buzilgan bo‘lsa, tizimning ishlashi ham ishonchsiz bo‘ladi. Bunday holatda AI noto‘g‘ri tashxis qo‘yishi yoki noaniq natija berishi mumkin. Shuningdek, “data poisoning” (ma’lumotlarni zaharlash) deb ataluvchi hujum turi orqali yovuz niyatli shaxslar o‘quv ma’lumotlariga zararli ma’lumotlar kiritib, butun tahlil jarayonini izdan chiqarishlari mumkin.

Ko‘plab axborot xavfsizligi buzilishlari texnik kamchilikdan emas, balki inson omili tufayli sodir bo‘ladi. Shifokorlar, hamshiralarning parollarni himoyasiz saqlashi, noma’lum havolalarni bosishi yoki tibbiy tizimga USB qurilma ulashi kabi holatlar tizim xavfsizligiga zarar yetkazadi. Bu esa axborot xavfsizligini ta’minlashda kadrlarning raqamli savodxonligini oshirish zarurligini ko‘rsatadi [7].

Tibbiyotda sun’iy intellekt tizimlaridan foydalanish samaradorligini oshirish bilan bir qatorda, axborot xavfsizligini ta’minlash masalasi ham eng muhim ustuvor yo‘nalishlardan biridir. Tibbiy ma’lumotlarning maxfiyligi, butunligi va mavjudligini saqlash bemor huquqlarini himoya qilish, tibbiy tashkilotlar obro‘sini mustahkamlash hamda sun’iy intellekt tizimlarining ishonchliligini kafolatlashda muhim rol o‘ynaydi.

Quyida tibbiyotda axborot xavfsizligini ta’minlashda qo‘llaniladigan asosiy texnik va tashkiliy chora-tadbirlar keltirilgan:

Kriptografiya va ma’lumotlarni shifrlash Tibbiyotda ma’lumotlar doimiy ravishda yig‘iladi, saqlanadi va tarmoqlar orqali uzatiladi. Shu sababli ularni kriptografik algoritmlar yordamida shifrlash zarur. Shifrlash texnologiyalari bemor ma’lumotlarini ruxsatsiz kirishdan himoya qiladi, ularning tarmoq orqali uzatilish jarayonida o‘zgarmasligini ta’minlaydi. Masalan, AES (Advanced Encryption Standard), RSA, SHA-256 kabi algoritmlar tibbiy axborot tizimlarida keng qo‘llaniladi. Bulutli saqlashda esa end-to-end encryption texnologiyasi yordamida faqat ruxsat etilgan foydalanuvchilar ma’lumotlarga kira oladi.

Autentifikatsiya va identifikatsiya tizimlari. Autentifikatsiya — bu foydalanuvchi yoki qurilmaning haqiqiyligini aniqlash jarayoni. Tibbiy axborot tizimlarida ikki bosqichli autentifikatsiya (2FA), biometrik autentifikatsiya (barmoq izi, yuzni aniqlash) yoki raqamli sertifikatlar orqali kirish huquqini tekshirish zarur.

Identifikatsiya esa foydalanuvchining kimligini aniqlash imkonini beradi. Bu mexanizmlar yordamida har bir foydalanuvchining tizimdagi harakati nazorat ostida bo‘ladi va ruxsatsiz kirish ehtimoli keskin kamayadi [8].

Xavfsiz tarmoq protokollaridan foydalanish. Ma’lumotlar tarmoq orqali uzatilayotganda ularning xavfsizligini ta’minlash uchun HTTPS, SSL/TLS, VPN kabi xavfsiz aloqa protokollaridan foydalanish zarur.

Bundan tashqari, tibbiy muassasalarda ichki tarmoqlarni tashqi internetdan ajratish, xavfsizlik devorlari (firewall), kirish nazorati tizimlari va tarmoq trafikini monitoring qilish dasturlarini o‘rnatish tavsiya etiladi. Bu orqali ma’lumotlar oqimida g‘ayritabiiy faollik yoki kiberhujum belgilarini erta aniqlash mumkin.

Sun’iy intellekt algoritmlarining ishonchliligi va shaffofligini ta’minlash. Tibbiy ma’lumotlarga asoslangan SI tizimlarining qarorlari inson hayotiga bevosita ta’sir qilgani sababli, ularning ishonchliligi, shaffofligi va izohlanishi muhim ahamiyatga ega. Tizimda “qora quti” (black box) mexanizmlarini kamaytirish, ya’ni har bir qarorning qanday shakllangani haqida izohli axborot beruvchi Explainable AI (XAI) yondashuvlarini joriy etish zarur. Bundan tashqari, sun’iy intellekt modellarini muntazam audit qilish, ularning natijalarini tekshirish va yangilab borish orqali noto‘g‘ri tahlil yoki manipulyatsiya xavfi kamaytiriladi.

Foydalanuvchi ruxsatlari va nazorat tizimlarini kuchaytirish. Tibbiy muassasalarda har bir foydalanuvchiga u bajaradigan vazifasiga mos darajada kirish huquqi berilishi kerak. Masalan, shifokor, hamshira va laboratoriya xodimi bir xil darajadagi ma’lumotlarga kira olmasligi lozim. Buning uchun rolga asoslangan kirish nazorati (Role-Based Access Control, RBAC) mexanizmini joriy etish samarali yechim hisoblanadi. Bu usul orqali faqat tegishli ruxsatga ega shaxslar tibbiy ma’lumotlarni ko‘rish yoki tahrirlash imkoniga ega bo‘ladi [9].

Zaxira nusxalarini yaratish va avariya holatlarida tiklash. Axborot xavfsizligini ta’minlash faqat kiberhujumlardan himoya bilan cheklanmaydi. Texnik nosozliklar, tabiiy ofatlar yoki tizimdagi xatoliklar sababli ma’lumotlar yo‘qolishi mumkin. Shuning uchun tibbiy axborotlar muntazam zaxira (backup) qilinishi, zaxira nusxalar esa alohida xavfsiz joyda yoki himoyalangan serverlarda saqlanishi kerak. Avariya holatlarida tiklash (disaster recovery) rejasi ishlab chiqilishi ham zarur.

Xodimlarning axborot xavfsizligi bo‘yicha malakasini oshirish. Eng ilg‘or texnik vositalar ham inson omili sababli yuzaga keladigan xatoliklarni to‘liq oldini ololmaydi. Shu sababli tibbiyot xodimlari uchun axborot xavfsizligi madaniyati, kiberhujumlardan himoyalanish, fishing havolalarni aniqlash kabi mavzularda doimiy o‘quv-seminarlar tashkil etish lozim. Bu yondashuv tibbiy tashkilotlarda xavfsizlikka nisbatan mas’uliyatni oshiradi va real xavflarni kamaytiradi.

XULOSA

Tibbiyotda sun’iy intellektdan foydalanishning samarasi bevosita axborot xavfsizligiga bog‘liq. Tibbiy ma’lumotlar himoyalanmagan bo‘lsa, hatto eng ilg‘or SI tizimlari ham ishonchli bo‘la olmaydi. Shu sababli har bir tibbiy tashkilotda ma’lumotlarni shifrlash, ikki bosqichli autentifikatsiya, foydalanuvchi ruxsatlarini nazorat qilish, xavfsizlik siyosatini yangilab borish kabi chora-tadbirlarni amalga oshirish zarur.

FOYDALANILGAN ADABIYOTLAR:

1. Sadirova Xursanoy Xusanboy Qizi, & Raxmatov Rasuljon Ravshanjon O‘G‘Li (2025). KOMPYUTER TARMOQLARIDA HUJUM IZLARINI ANIQLASH VA ULARNI TURLARI BO‘YICHA TIZIMLI TASNIFLASH. Al-Farg’oniy avlodlari, 1 (2), 40-44. doi: 10.5281/zenodo.15541367

2. Садирова, Х. (2023). МЕТОДЫ ОЦЕНКИ ВЕРОЯТНОСТИ НАРУШЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ. Universum: технические науки, (12-1 (117)), 65-66.

3. Mirzayevich, T. M., & Qizi, S. X. X. (2023). AXBOROTNI HIMOYALASHDA CHETLAB O’TISHNING MUMKIN BO ‘LGAN EHTIMOLLIK XOLATINI BAHOLASH USULLARI. Al-Farg’oniy avlodlari, 1(4), 189-193.

4. Xusanova Moxiraxon Qurbonaliyevna (2025). KORXONA VA TASHKILOTLARNING AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA VPN TARMOQ QURISHNING ZAMONAVIY YECHIMLARI. Al-Farg’oniy avlodlari, 1 (2), 122-125. doi: 10.5281/zenodo.15581004

5. Ганиева, Ш. Н., & Жабборов, Х. И. (2017). ESSENTIAL METHODS AND PRINCIPLES OF INFORMATION SECURITY IN THE FIELD OF CONTROL. Теория и практика современной науки, (1 (19)), 1063-1066.

6. Xusanova Moxiraxon Qurbonaliyevna (2025). KORXONA VA TASHKILOTLARNING AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA VPN TARMOQ QURISHNING ZAMONAVIY YECHIMLARI. Al-Farg’oniy avlodlari, 1 (2), 122-125. doi: 10.5281/zenodo.15581004

7. Muminov Kamolkhon Ziyodjon O’G’Li (2024). Social Engineering, Human Factor in Cybersecurity. Al-Farg’oniy avlodlari, (3), 149-152. doi: 10.5281/zenodo.13954935

8. Ганиева, Ш. Н., & Жабборов, Х. И. (2017). ESSENTIAL METHODS AND PRINCIPLES OF INFORMATION SECURITY IN THE FIELD OF CONTROL. Теория и практика современной науки, (1 (19)), 1063-1066.

9. Umarov, Sh. A., Rakhmonov, O. Sh. (2024). Assessment of the level of security available in 4G and 5G mobile communication networks. Al-Farg‘oniy avlodlari, 1(4), 294–297.