TIBBIY AXBOROT TIZIMLARINING AXBOROT XAVFSIZLIGINI BOSHQARISH MODELLARI VA VOSITALARI: SO‘NGGI YILLARDAGI TENDENSIYALAR TAHLILI

INFORMATION SECURITY MANAGEMENT MODELS AND TOOLS OF MEDICAL INFORMATION SYSTEMS: ANALYSIS OF TRENDS IN RECENT YEARS

МОДЕЛИ И ИНСТРУМЕНТЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ: АНАЛИЗ ТРЕНДОВ ПОСЛЕДНИХ ЛЕТ

Muxtarov F.M. **– DSc**
Mukaramov T.T.
https://orcid.org/0009-0005-7429-4843
Central Asian Medical University

Muxtarov F.M., Mukaramov T.T. TIBBIY AXBOROT TIZIMLARINING AXBOROT XAVFSIZLIGINI BOSHQARISH MODELLARI VA VOSITALARI: SO'NGGI YILLARDAGI TENDENSIYALAR TAHLILI. In ActaCAMU (Vol. 11, Number 1, pp. 165–170). Zenodo. https://doi.org/10.5281/zenodo.17181749

Annotatsiya: *2020–2025 yillarda raqamli texnologiyalar jadal joriy etilishi tibbiy axborot tizimlarida (TAT) axborot xavfsizligini eng dolzarb masalaga aylantirdi. Telemeditsina, elektron tibbiy kartalar va bulutli bazalar samaradorlikni oshirgan bo‘lsada, yangi kiberxavf va tahdidlarni yuzaga chiqardi. JSST strategiyasi, NIS2 direktivasi, HICP va FDA ko‘rsatmalari tibbiy ma’lumotlar xavfsizligini majburiy boshqarishni belgilab berdi. Tadqiqotda nazariy, statistik va tizimli tahlil hamda STRIDE/DREAD risk baholash metodlari qo‘llanilib, xavfsizlikni ta’minlash texnik, huquqiy va tashkiliy choralar uyg‘unligi asosida ilmiy yoritildi.*

Kalit so‘zlar: *Tibbiy axborot tizimlari, raqamli sog‘liq, axborot xavfsizligi, telemeditsina, IoMT, Zero Trust, NIS2, HIPAA, GDPR, STRIDE, DREAD.*

Abstract: *Abstract: Between 2020 and 2025, the rapid adoption of digital technologies has made information security in health information systems (HIS) one of the most urgent issues. While telemedicine, electronic health records, and cloud databases have improved efficiency, they have also introduced new cyber risks and threats. International frameworks such as the WHO Global Strategy, the EU NIS2 Directive, HICP, and FDA guidelines have established mandatory requirements for safeguarding medical data. This study applies theoretical, statistical, and systemic analyses, together with STRIDE/DREAD risk assessment methods, demonstrating that effective HIS security requires an integrated set of technical, legal, and organizational measures.*

Keywords: *medical information systems, digital health, information security, telemedicine, IoMT, Zero Trust, NIS2, HIPAA, GDPR, STRIDE, DREAD.*

Аннотация: *В период 2020–2025 годов стремительное внедрение цифровых технологий сделало обеспечение информационной безопасности в медицинских информационных системах (МИС) одной из наиболее актуальных задач. Несмотря на то, что телемедицина, электронные медицинские карты и облачные базы повысили эффективность, они привели к возникновению новых киберугроз. Международные нормативные акты — Глобальная стратегия ВОЗ, директива ЕС NIS2, рекомендации HICP и FDA — закрепили обязательные требования по защите медицинских данных. В исследовании применены теоретический, статистический и системный анализы, а также методы оценки рисков STRIDE/DREAD, что показало необходимость комплексного сочетания технических, правовых и организационных мер для обеспечения безопасности МИС.*

Ключевые слова: *медицинские информационные системы, цифровое здравоохранение, информационная безопасность, телемедицина, IoMT, Zero Trust, NIS2, HIPAA, GDPR, STRIDE, DREAD.*

Kirish. So‘nggi besh yillikda (2020–2025) raqamli sog‘liqni saqlash tizimlarining rivojlanishi bilan birga, tibbiy axborot tizimlari (TAT)da axborot xavfsizligini ta’minlash dolzarb masalaga aylandi. Telemeditsina, elektron tibbiy kartalar, bulutli ma’lumotlar bazalari va IoT asosidagi tibbiy qurilmalarning keng qo‘llanilishi sog‘liq sohasida samaradorlikni oshirdi, biroq shu bilan birga yangi kiberxavflarni ham yuzaga keltirdi. Jahon sog‘liqni saqlash tashkiloti (JSST), Yevropa Ittifoqi, AQSh Sog‘liqni saqlash vazirligi (HHS), hamda xalqaro standartlashtirish tashkilotlari tomonidan ishlab chiqilgan yondashuvlar ushbu muammolarni hal etishga qaratilgan.

Dolzarbligi. 2020–2025 yillar davomida sog‘liq sohasiga qaratilgan ransomware hujumlari, API xavfsizligi zaifliklari, IoMT (Internet of Medical Things) qurilmalaridagi xatoliklar mislsiz darajada ko‘paydi. 2024 yilda AQShda sog‘liqni saqlashga oid 700 dan ortiq ma’lumot buzilishlari qayd etildi, Change Healthcare hodisasi esa 190 milliondan ortiq shaxsiy ma’lumotlarning oshkor bo‘lishiga sabab bo‘ldi. Shu sababli TAT xavfsizligini boshqarish bo‘yicha yangilangan modellarga ehtiyoj keskin ortdi.

Tibbiy axborot tizimlarining axborot xavfsizligini boshqarish masalasi so‘nggi yillarda sog‘liqni saqlash sohasidagi eng dolzarb mavzulardan biriga aylandi. Raqamli transformatsiya jarayoni natijasida elektron tibbiy kartalar, telemeditsina xizmatlari, katta hajmdagi ma’lumotlar bazalari va IoT qurilmalariga asoslangan tibbiy jihozlarning keng joriy etilishi sog‘liqni saqlash tizimining samaradorligini oshirgan bo‘lsa-da, shu bilan birga, yangi kiberxavf va tahdidlarni yuzaga chiqarmoqda. Jahon sog‘liqni saqlash tashkilotining *Global Strategy on Digital Health 2020–2025* hujjatida raqamli sog‘liq infratuzilmasida axborot xavfsizligi strategik ustuvor yo‘nalish sifatida belgilangan bo‘lib, bu nafaqat texnologik, balki tashkiliy va huquqiy choralarni uyg‘unlashtirish zarurligini ko‘rsatadi.

Abouelmehdi va hamkorlari (2018) tomonidan olib borilgan tadqiqotlarda katta hajmdagi tibbiy ma’lumotlarni himoyalashda kriptografiya, anonimlashtirish va kirish nazorati usullarining samaradorligi asoslab berilgan. Ularning fikricha, shaxsiy sog‘liq ma’lumotlarini himoya qilish ko‘p qatlamli yondashuvni talab qiladi. Shojaei va boshqalar (2024) esa tibbiy axborot tizimlarida xavfsizlikni ta’minlashda intellektual tizimlar va avtomatlashtirilgan tahdid monitoringi muhim o‘rin tutishini ta’kidlagan. Ularning tadqiqoti sun’iy intellekt asosidagi tizimlarning potentsial xatarlarni erta aniqlash va tezkor javob choralarini ishlab chiqishda yuqori samaradorlikka ega ekanini ko‘rsatadi.

Xalqaro miqyosda ham so‘nggi yillarda muhim huquqiy va normativ hujjatlar qabul qilindi. 2023 yilda Yevropa Ittifoqi tomonidan tasdiqlangan NIS2 direktivasi sog‘liq sohasida majburiy xavfsizlik choralarini kuchaytirib, kiberhujumlar haqida xabar berish tartibini qat’iylashtirdi. AQShda esa HICP 2023 hujjatida sog‘liq sektoridagi eng muhim beshta kiberxavf aniqlanib, ularni kamaytirishga qaratilgan amaliy boshqaruv choralarini ishlab chiqish bo‘yicha tavsiyalar berildi. Shu bilan birga, FDA 2023–2025 yillarda tibbiy qurilmalar xavfsizligi bo‘yicha yangi qo‘llanmalar ishlab chiqdi. Unda qurilmalarning dasturiy ta’minotiga oid SBOM (Software Bill of Materials), zaifliklarni boshqarish va hayotiy sikl davomida xavfsizlikni ta’minlash kabi yangi talablar belgilandi.

Mazkur tahlillar shuni ko‘rsatadiki, tibbiy axborot tizimlarida axborot xavfsizligini ta’minlash masalasi faqat texnologik choralar bilan chegaralanib qolmaydi. Bu jarayon ko‘p qirrali bo‘lib, texnik vositalar bilan bir qatorda riskga asoslangan boshqaruv tizimlari, xalqaro va milliy standartlarga muvofiqlik, hamda intellektual texnologiyalarni qo‘llashni talab etadi. Zero Trust arxitekturasi, API xavfsizligi protokollari va IoMT qurilmalari uchun ishlab chiqilgan maxsus yo‘riqnomalar amaliyotda keng tatbiq etilayotgani ham aynan shu tendensiyalarning dalilidir.

Shunday qilib, JSST strategik hujjatlari, Yevropadagi NIS2 direktivasi, AQShda qabul qilingan HICP va FDA yo‘riqnomalari sog‘liq sohasida xavfsizlikni ta’minlash bo‘yicha yagona boshqaruv mexanizmlarini shakllantirishda muhim o‘rin tutmoqda. Ilmiy tadqiqotlar esa kriptografik va anonimlashtirish usullari bilan bir qatorda, intellektual tizimlar va avtomatlashtirilgan monitoring

mexanizmlarini ham kengroq qo‘llash zarurligini ko‘rsatmoqda. Demak, tibbiy axborot tizimlarida axborot xavfsizligini boshqarish kelajakda ham ko‘p tarmoqli yondashuv asosida rivojlantirilishi zarur bo‘lib, bu sog‘liqni saqlash tizimining samaradorligi va barqarorligini ta’minlashda hal qiluvchi omil bo‘lib qoladi.

Normativ-huquqiy yondashuvlar. So‘nggi yillarda xalqaro miqyosda tibbiy axborot tizimlari (TAT) xavfsizligini boshqarish bo‘yicha bir qator yangi normativ hujjatlar va qo‘llanmalar ishlab chiqildi. Ularning har biri sog‘liq sohasida axborot xavfsizligini huquqiy va tashkiliy darajada mustahkamlash bilan birga, amaliy qo‘llanish doiralarini ham belgilab berdi.

Yevropa Ittifoqi – NIS2 direktivasi (2023). Ushbu hujjat Yevropa Ittifoqi miqyosida sog‘liqni saqlash sohasida kiberxavfsizlikni majburiy tartibda boshqarish talablarini joriy etdi. NIS2 direktivasi orqali sog‘liqni saqlash muassasalari hodisalar haqida xabar berish mexanizmlarini qat’iylashtirishi, riskga asoslangan boshqaruvni yo‘lga qo‘yishi va ta’minot zanjiri xavfsizligini ta’minlashi shart qilib qo‘yildi. Qo‘llanilish sohasi, avvalo, yirik kasalxonalar, milliy sog‘liqni saqlash tizimlari va tibbiy ma’lumotlarni qayta ishlovchi barcha tashkilotlarni qamrab oladi. Bu yondashuv orqali Yevropada sog‘liq sohasida xavfsizlikni boshqarish madaniyati yangi bosqichga ko‘tarildi va sog‘liqni saqlash infratuzilmasi milliy hamda transchegaraviy tahdidlarga nisbatan barqarorroq bo‘ldi.

AQSh sog‘liqni saqlash tizimi – HICP (Health Industry Cybersecurity Practices) 2023. AQSh sog‘liqni saqlash va ijtimoiy xizmatlar vazirligi (HHS) tomonidan ishlab chiqilgan ushbu hujjatda sog‘liq sohasidagi eng muhim beshta kiberxavf: **ransomware hujumlari, fishing (soxta havolalar orqali hujumlar), IoT/IoMT qurilmalardagi zaifliklar, ta’minot zanjiri xatarlarini ekspluatatsiya qilish hamda ichki foydalanuvchi xatolari** aniq belgilangan. HICP hujjati amaliy qo‘llanilishi bo‘yicha sog‘liqni saqlash tashkilotlarini uch guruhga – kichik, o‘rta va yirik muassasalarga ajratadi hamda har biriga xavfsizlik choralarini bosqichma-bosqich joriy qilish bo‘yicha tavsiyalar beradi. Masalan, kichik klinikalar uchun minimal xavfsizlik protokollari, yirik shifoxonalar uchun esa keng qamrovli SIEM, IDS/IPS tizimlari va xavfsizlik auditi choralarini joriy etish zaruriyati ko‘rsatib berilgan.

FDA – tibbiy qurilmalar kiberxavfsizligi bo‘yicha qo‘llanmalar (2023–2025). AQSh oziq-ovqat va farmatsevtika idorasi (FDA) tomonidan ishlab chiqilgan ushbu qo‘llanmalarda IoMT qurilmalarining xavfsizligi alohida e’tiborga olingan. Unga ko‘ra, ishlab chiqaruvchilar qurilmalarning dasturiy ta’minotiga oid **SBOM (Software Bill of Materials)** hujjatini majburiy taqdim etishi, zaifliklarni muntazam ravishda kuzatib borishi va hayotiy sikl davomida xavfsizlikni ta’minlash choralarini ko‘rishi lozim. Ushbu talablardan amaliy foydalanish sohasi tibbiy qurilmalarni ishlab chiqaruvchi kompaniyalar, klinikalarda qo‘llanilayotgan diagnostika va monitoring uskunalari, shuningdek, bemorlar tomonidan uy sharoitida ishlatiladigan tibbiy qurilmalarni qamrab oladi. Natijada, qurilmalar nafaqat ishlab chiqarish bosqichida, balki ekspluatatsiya jarayonida ham kiberxavflarga qarshi himoyalangan bo‘lishi ta’minlanadi.

Umuman olganda, NIS2, HICP 2023 va FDA qo‘llanmalari global sog‘liq sohasida normativ-huquqiy muhitni takomillashtirish bilan birga, tibbiy axborot tizimlari xavfsizligini boshqarishda majburiy me’yorlarni belgilab berdi. Bu hujjatlarning qo‘llanilishi sog‘liqni saqlash tizimining barcha qatlamlarini qamrab olib, **yirik shifoxonalardan tortib kichik klinikalargacha, ishlab chiqaruvchilardan tortib yakuniy foydalanuvchilargacha bo‘lgan keng ko‘lamda** xavfsizlikni mustahkamlash imkonini bermoqda. Shu orqali axborot xavfsizligi nafaqat texnik jihatdan, balki tashkiliy va huquqiy asosda ham keng miqyosda boshqarilmoqda.

Metodlar. Ushbu tahliliy tadqiqot tibbiy axborot tizimlarining axborot xavfsizligini boshqarish bo‘yicha so‘nggi yillarda qo‘llanilayotgan ilmiy, texnik va huquqiy yondashuvlarni chuqur o‘rganishga qaratildi. Tadqiqot jarayonida ko‘p tarmoqli metodlar majmuasidan foydalanildi.

Birinchidan, **nazariy tahlil** metodlari qo‘llanilib, xalqaro miqyosda keng qabul qilingan axborot xavfsizligi standartlari chuqur o‘rganildi. Xususan, **ISO/IEC 27001** axborot xavfsizligi boshqaruv tizimlari uchun umumiy ramka, **ISO 27799** esa aynan sog‘liq sohasida shaxsiy tibbiy ma’lumotlarni himoya qilish bo‘yicha maxsus qo‘llanma sifatida tahlil qilindi. Bundan tashqari, AQShda amal qiluvchi **HIPAA (Health Insurance Portability and Accountability Act)** qonuni,

ActaCAMU
№ 11 2025
ISSN: 2181-4155

Yevropa Ittifoqidagi **GDPR (General Data Protection Regulation)** reglamenti va 2023 yilda qabul qilingan **NIS2 direktivasi** normativ-huquqiy jihatdan tahlil qilinib, ular orqali tibbiy axborot tizimlarida axborot xavfsizligini ta’minlashning majburiy talablari aniqlab chiqildi. Bu yondashuv tadqiqotning nazariy asoslarini mustahkamlab berdi.

Ikkinchidan, **statistik tahlil** metodlari qo‘llanildi. So‘nggi yillarda turli mamlakatlarda qayd etilgan ma’lumot buzilishlari, xususan **ransomware hujumlari**, ma’lumotlar sizib chiqishi va tibbiy qurilmalar zaifliklari haqidagi hisobotlar solishtirildi. AQSh sog‘liqni saqlash vazirligi huzuridagi HHS OCR tomonidan e’lon qilingan yillik hisobotlar, Emsisoft va JAMA Network Open kabi tashkilotlarning tahlillari asosida xavfsizlik buzilishlarining dinamikasi va ularning oqibatlari o‘rganildi. Bu usul orqali axborot xavfsizligi muammolarining real ko‘rinishlari statistik ma’lumotlar bilan asoslandi.

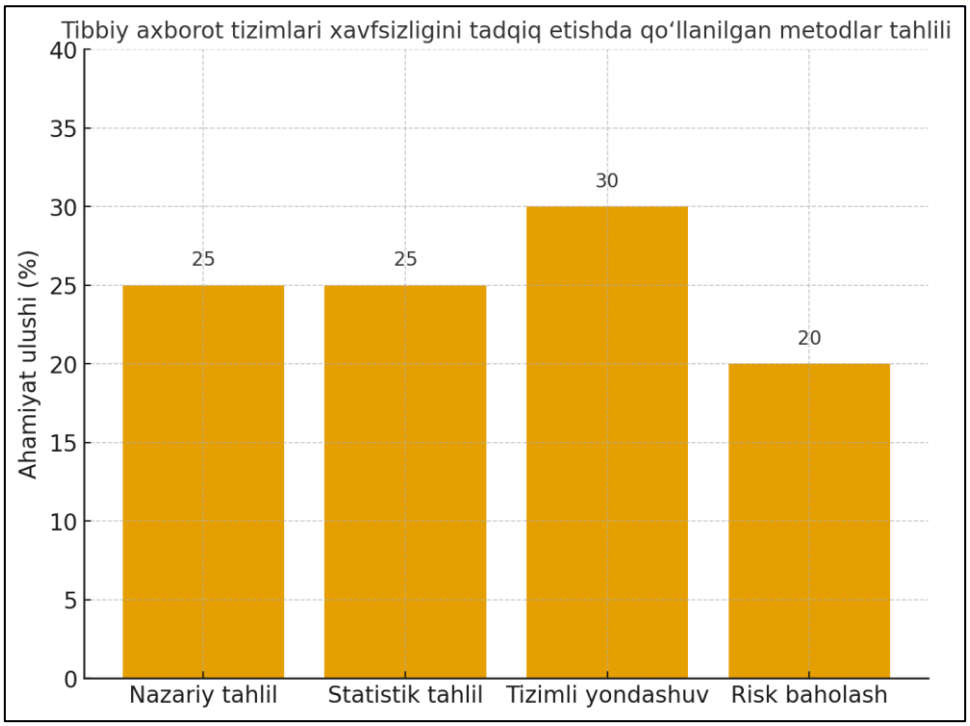
Uchinchidan, **tizimli yondashuv**dan foydalanildi. Tibbiy axborot tizimlarining zamonaviy arxitekturasi va ulardagi xavfsizlik mexanizmlari modellashtirildi. Xususan, **Zero Trust** arxitekturasi tamoyillari, ya’ni doimiy autentifikatsiya, mikrosegmentatsiya va uzluksiz monitoringning amaliyotda qo‘llanishi tahlil qilindi. Bundan tashqari, **API xavfsizligi**ni ta’minlovchi HL7 FHIR va SMART on FHIR protokollari, OAuth 2.0 va OpenID Connect asosidagi autentifikatsiya va avtorizatsiya mexanizmlari o‘rganildi. Shuningdek, **IoMT (Internet of Medical Things)** qurilmalarida xavfsizlikni ta’minlashga doir FDA va ENISA yo‘riqnomalari modellashtirilib, ular asosida amaliy integratsiya imkoniyatlari baholandi.

To‘rtinchidan, **risk baholash metodlari** sifatida STRIDE va DREAD modellari qo‘llanildi. STRIDE modeli orqali tahdidlar oltita asosiy toifaga (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege) ajratilib, ularning tibbiy axborot tizimlaridagi namoyon bo‘lish shakllari tahlil qilindi. DREAD modeli yordamida esa tahdidlarning ta’sir darajasi, ekspluatatsiya qilish osonligi, aniqlanish ehtimoli, ta’sir ko‘lami va takrorlanish imkoniyatlari bo‘yicha ballik baholash amalga oshirildi. Bu yondashuv axborot xavfsizligiga oid xatarlarni ustuvorlik bo‘yicha tartiblash va amaliy choralarni belgilash imkonini berdi.

1-jadval.
Tibbiy axborot tizimlari xavfsizligini tadqiq etish metodlari jadvali

Metod	**Tavsif**	**Amaliy ahamiyati**
Nazariy tahlil	Xalqaro standartlar (ISO/IEC 27001, ISO 27799, HIPAA, GDPR, NIS2) chuqur o‘rganilib, TAT xavfsizligi uchun nazariy asos yaratildi.	Nazariy asoslarni mustahkamladi.
Statistik tahlil	Ransomware hujumlari, ma’lumotlar sizib chiqishi va qurilmalar zaifliklari haqidagi xalqaro hisobotlar tahlil qilindi.	Xavfsizlik buzilishlarining real ko’rinishini statistik dalillar bilan asoslab berdi.
Tizimli yondashuv	Zero Trust arxitekturasi, HL7 FHIR va SMART on FHIR protokollari, OAuth 2.0 va IoMT xavfsizligi bo’yicha modellar ishlab chiqildi.	Arxitektura va integratsiya jarayonlarini modellashtirish imkonini berdi.
Risk baholash	STRIDE orqali tahdidlar tasniflandi, DREAD modeli asosida xavf darajalari ballik usulda baholandi.	Tahdidlarni ustuvorlashtirish va samarali himoya choralarini belgilash imkonini berdi.

ActaCAMU
№ 11 2025
ISSN: 2181-4155



1-rasm. Tibbiy axborot tizimlari xavfsizligini tadqiq etishda qo‘llanilgan metodlarning ahamiyati ulushi

Diagrammadan ko‘rinib turibdiki, tizimli yondashuv va nazariy tahlil metodlari asosiy ilmiy asos bo‘lib xizmat qilgan bo‘lsa, statistik tahlil va risk baholash metodlari amaliy natijalarni tasdiqlash va tahdidlarni ustuvorlashtirishda muhim o‘rin tutdi. Shu tarzda, metodlarning uyg‘un qo‘llanilishi tibbiy axborot tizimlarida axborot xavfsizligini boshqarish bo‘yicha kompleks va ishonchli tahlilni ta’minladi.

Umuman olganda, nazariy tahlil, statistik ma’lumotlarni solishtirish, tizimli modellashtirish va risk baholash metodlarining uyg‘un qo‘llanilishi tibbiy axborot tizimlarining axborot xavfsizligini boshqarish bo‘yicha kompleks va ilmiy asoslangan tahlilni ta’minladi.

Xulosa. So‘nggi yillarda tibbiy axborot tizimlari axborot xavfsizligini boshqarish bo‘yicha yangi yondashuvlar shakllandi. Xususan, Zero Trust arxitekturasi, API xavfsizligi protokollari, IoMT xavfsizlik standartlari va riskga asoslangan boshqaruv tizimlari sog‘liqni saqlash muassasalari uchun ustuvor yo‘nalish bo‘lib qoldi. Ransomware hujumlari va ma’lumot buzilishlari kuchaygan sharoitda TAT xavfsizligini ta’minlash faqat texnik choralar emas, balki normativ-huquqiy, tashkiliy va ilmiy izlanishlarni ham talab etmoqda.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidentining Farmoni “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida.
2. Jahon sog‘liqni saqlash tashkiloti (WHO). *Global Strategy on Digital Health 2020–2025.*
3. O‘zbekiston Respublikasi Vazirlar Mahkamasining qarori, 08.09.2025 yildagi 570-son “Sog‘liqni saqlash tizimini raqamlashtirish jarayonlarini yanada jadallashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida” qarori
4. Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review Computers 2024, 13(2), 41; https://doi.org/10.3390/computers13020041
5. ISO/IEC 27799:2016 — *Health informatics — Information security management in health.*
6. O‘zbekiston Respublikasi “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonuni (2019).
7. European Union General Data Protection Regulation (GDPR, 2016).
8. World Health Organization. *Global Strategy on Digital Health 2020–2025*. Geneva: WHO, 2021.

9. Abouelmehdi, K., et al. “Big healthcare data: preserving security and privacy.” *Journal of Big Data*, 2018.
10. Shojaei, P., et al. “Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review.” *Computers*, 2024.
11. U.S. Department of Health and Human Services. *Health Industry Cybersecurity Practices (HICP) 2023*.
12. FDA. *Cybersecurity in Medical Devices: Quality System Considerations*. Final Guidance, 2023–2025.
13. European Union Agency for Cybersecurity (ENISA). *NIS2 Directive Implementation Guidelines*, 2023–2025.