



**RAQAMLI TIBBIYOTDA XAVFSIZLIK MUAMMOLARI VA ULARNI
BARTARAF ETISH USULLARI**

S.Sh.Muminova

Muhammad al-Xorazmiy nomidagi TATU Nurafshon filiali

Annotatsiya: *Raqamli tibbiyotda texnologik taraqqiyot natijasida sog'liqni saqlash tizimlarida keng ko'lamli raqamli infratuzilmalar joriy etilgan. Biroq, bu infratuzilmalar ma'lumotlarning maxfiyligi, yaxlitligi va foydalanuvchanligi nuqtai nazaridan jiddiy xavfsizlik muammolarini yuzaga keltirmoqda. Ushbu tezisda raqamli tibbiyot tizimlarida kuzatilayotgan asosiy xavfsizlik tahdidlari, jumladan, kiberhujumlar, ma'lumotlar sizib chiqishi, ichki hujumlar va tibbiy IoT qurilmalariga oid zaifliklar tahlil qilingan. Shuningdek, xavfsizlikni ta'minlash bo'yicha texnik, tashkiliy va me'yoriy yondashuvlar, hamda ularni bartaraf etish usullari ko'rib chiqilgan.*

Kalit so'zlar: *raqamli tibbiyot, axborot xavfsizligi, tibbiy informatika, kiberxavfsizlik, IoT tibbiyot qurilmalari, ma'lumotlar maxfiyligi, ransomware, elektron tibbiy yozuvlar, telemeditsina xavfsizligi, sog'liqni saqlash texnologiyalari*

KIRISH

Raqamli sog'liqni saqlash texnologiyalarining (masalan, elektron tibbiy yozuvlar, telemeditsina va IoT qurilmalari) keng qo'llanilishi tibbiyot xizmatlarining samaradorligini oshirgan bo'lsa-da, axborot xavfsizligi nuqtai nazaridan yangi muammolarni yuzaga keltirgan.

Jahon sog'liqni saqlash tashkiloti (WHO) ta'kidlaganidek, telemeditsina va elektron ma'lumot bazalaridan foydalanishning o'sishi sohada kiberxavflarning ham oshishiga olib kelmoqda. Kiberxavfsizlik sog'liqni saqlash tizimlarida elektron ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlashga qaratilgan muhim sohadir.

Biroq amaliyotda katta hajmdagi ma'lumotlar muntazam ravishda buzib kirishga uchraydi – so'nggi ma'lumotlarga ko'ra, har yili 50 milliondan ortiq bemor ma'lumotlari sog'liqni saqlash tashkilotlari tizimlarida noxush hollar oqibatida ochiqlanmoqda.

Shunday qilib, axborot xavfsizligi, sog'liqni saqlash texnologiyalari va tibbiy informatika mutaxassislari uchun raqamli sog'liq muhitidagi xavflarni o'rganish dolzarb ahamiyat kasb etadi. Ushbu tezisda raqamli tibbiyotda yuzaga kelayotgan xavfsizlik muammolari, ularning turlari va bartaraf etish usullari amaliy misollar bilan tahlil qilinadi.

ASOSIY QISM: MAVJUD XAVFSIZLIK MUAMMOLARI VA TURLARI

Raqamli tibbiyot tizimlari tobora murakkablashib borayotgani sababli, sohada quyidagi asosiy xavf-xatarlar va zaifliklar aniqlangan:

Ma'lumotlarning maxfiyligi va shaxsiylik buzilishi: Tibbiy yozuvlarga noqonuniy kirish va bemor ma'lumotlarini tarqatish eng keng tarqalgan tahdidlardandir. Global statistikaga ko'ra, har yili 50 milliondan ortiq bemor ma'lumotlari turli kiberhujum yoki xavfsizlik



buzilishlari sababli oshkor qilinmoqda. Bu holat bemorlarning maxfiy axborotlari himoyasining yetarli emasligini ko'rsatib, sog'liqni saqlash tizimlari uchun jiddiy muammo tug'diradi. Bundan tashqari, kiberhujumlar moliyaviy zararlar keltirish, xizmatlarni uzilishiga olib kelish va hatto bemorlarning hayotiga tahdid solishi mumkin

Ransomware hujumlari: Tibbiyot tashkilotlarida ransomware zararli dasturlari keng tarqalgan muammo hisoblanadi. Bunday hujumlar kasalxonalar va klinikalarning ma'lumotlar bazalarini shifrlab, tibbiyot xodimlarini tizimga kirish huquqidan mahrum qiladi, so'ngra ma'lumotlarni qayta tiklash uchun katta miqdorda to'lov talab etadi. Ransomware hujumlari natijasida diagnostika-aniqlash tizimlari to'xtab qolishi, bemorlarga xizmat ko'rsatishda uzilishlar yuzaga kelishi kuzatilgan.

Ichki omillar (inson xatosi va ichki hujumlar): Tibbiyot muassasalari xodimlarining ehtiyotsizligi yoki noto'g'ri amaliyotlari ham xavfsizlik muammolariga olib keladi. Tadqiqotlar ko'rsatadiki, sog'liqni saqlash tizimidagi zaifliklarning ma'lum qismi xodimlarning bilim va tajribasi yetishmasligi bilan bog'liq. Masalan, kuchsiz parollardan foydalanganlik, kirish ma'lumotlarini boshqalar bilan bo'lishish yoki tanish bo'lmagan manzildan kelgan elektron xabardagi havolani bosish kabi holatlar ma'lumotlar o'g'irlanishiga olib kelishi mumkin.

Meditsina qurilmalari va IoT: Hozirgi vaqtda kasalxonalarda bemorga bog'langan o'nlab tibbiy qurilmalar (infuzion nasoslar, yurak stimulyatorlari, pulsoksimetrlar va boshqalar) internet yoki tarmoq orqali boshqariladi. Agar ushbu qurilmalarda xavfsizlik choralari yetarli darajada olinmasa, ularni buzish to'g'ridan-to'g'ri bemorning salomatligiga ta'sir qilishi mumkin. Tadqiqotlar shuni ko'rsatadiki, masofadan turib yurak stimulyatorlari va pulsoksimetrlarni buzish mumkinligi aniqlangan. Bu turdagi zaifliklar xakerlarga bemor ustidan nazorat o'rnatish imkoniyatini yaratadi.

Tarmoqlar va aloqa kanallarining himoyasizligi: Elektron tibbiy yozuvlar va tibbiy ilovalar ko'pincha simsiz (Wi-Fi) yoki keng polosali tarmoqlar orqali ulanishi sababli, ularning xavfsizligi muhim ahamiyatga ega. Bemor ma'lumotlarini uzatish paytida tarmoqqa yetarli darajada himoya qilinmagan bo'lsa, tarmoq trafiki ushlanishi va ma'lumotlar o'g'irlanishi mumkin. Masalan, man-in-the-middle hujumi orqali ochiq kanal orqali uzatilgan tibbiy yozuvlarga noqonuniy kirishlar amalga oshirilishi ma'lum. Shuningdek, tarmoqqa ulangan har bir oxirgi qurilma (kompyuter, smartfon, tibbiy qurilma) yana yangi tahdid manbai hisoblanadi.

Eskirgan tizimlar va dasturiy ta'minot: Ko'pchilik sog'liqni saqlash muassasalari eskirgan operatsion tizimlar va ilovalarni ishlatishda davom etmoqda. Bunday legacy-tizimlarda xavfsizlik yangilanishlari to'xtatilgach, ularni himoya qilish mumkinligi deyarli yo'qoladi. Ushbu zaiflikdan xakerlar foydalanib, tizim va ma'lumot bazasiga kirish huquqini qo'lga kiritishi mumkin. Masalan, bir necha yillardan buyon yangilanmay kelgan elektron sog'liq tizimida xavfsizlik fragmentlari paydo bo'lishi sodir bo'lgan.



XAVFSIZLIK MUAMMOLARINI BARTARAF ETISH USULLARI

Raqamli sog'liq tizimlarida xavfsizlik tahdidlarini kamaytirish uchun kompleks choralar qo'llanishi kerak. Bular orasida quyidagilar muhim ahamiyat kasb etadi:

Texnik chora-tadbirlar: Ma'lumotlarni uzatishda va saqlashda mustahkam shifrlash algoritmlaridan (masalan, AES yoki TLS/SSL) foydalanish zarur. Tizimlarga kirishda ikki va undan ortiq faktorli autentifikatsiyani joriy etish, parol siyosatini kuchaytirish ham o'ta muhim. Shuningdek, barcha server va qurilmalarda operatsion tizim va ilovalarni muntazam yangilab borish, xavfsizlik yamoqlarini (patch) o'rnatish lozim. Tarmoq infratuzilmasida segmentatsiya qo'llash, asosiy ma'lumot bazalari va tibbiy IoT qurilmalarni ajratib himoyalash orqali kiberhujum yuz berganda zarar darajasini kamaytirish mumkin. Bundan tashqari, favqulodda vaziyatlarda zaxira nusxa olish va xodimlarni favqulodda tiklash bo'yicha reja yaratish kutilmagan buzilishlardan kelib chiqadigan xavfni yengillashtiradi.

Me'yoriy va tashkiliy chora-tadbirlar: Sog'liqni saqlash tashkilotlari ko'plab xalqaro va mahalliy standart va qonunchilikka mos ravishda ishlashi lozim. Misol uchun, AQShda HIPAA, Yevropada GDPR kabi standartlarda bemor ma'lumotlarini himoya qilish talablari aniq belgilangan. Tizimlarga doimiy audit o'tkazish, xavfsizlik siyosatlarini ishlab chiqish va amaliyotni nazorat qilish zarur. Shuningdek, xodimlar uchun muntazam ravishda kiberxavfsizlik bo'yicha treninglar, briefinglar va maxsus mashg'ulotlar o'tkazish lozim. Tadqiqotlar kiberxavfsizlik bo'yicha maxsus o'quv dasturlarini joriy etish, xodimlarning tayyorgarligini oshirish va kiberhujumlarga qarshi ko'nikmalarni rivojlantirishni tavsiya qiladi. Ichki protseduralar, foydalanishni nazorat tizimi va ma'lumotlar boshqaruvi siyosatini qat'iy amalga oshirish kerak.

Uskuna va dasturiy ta'minotni xavfsizlikdan boshlab loyihalash: Tibbiy IoT qurilmalarni ishlab chiquvchilar xavfsizlikni loyiha bosqichida inobatga olishi, qurilmalarga o'rnatilgan dasturiy ta'minotni muntazam yangilab borishi lozim. Qurilmalarda noyob autentifikatsiya kalitlari, o'zgarmas identifikatorlar va mustahkam kodlash mexanizmlari joriy etilishi zarur. Eskirgan qurilmalarni yangilar bilan bosqichma-bosqich almashtirish, legacy platformalarni xatar keltirib chiqarmaydigan zamonaviy yechimlarga o'tkazish tavsiya etiladi. Masalan, ishlab chiqaruvchilar tibbiy qurilmalarni maxfiy ma'lumotni shifrlash, kirishni bloklash mexanizmlari bilan ta'minlashi lozim.

Hamkorlik va ma'lumot almashish: Sog'liqni saqlash tashkilotlari, kiberxavfsizlik mutaxassislari va hukumat organlari o'rtasida hamkorlikni kuchaytirish lozim. Hujumlar haqida tezkor ma'lumot almashish, xavf-xatarlarni oldindan xabardor qilish va tegishli bo'limlar bilan tajriba ulashish samarali bo'ladi. Shuningdek, kiberxavfsizlik bo'yicha jamoaviy amaliy treninglar, konferensiyalar va seminarlar tashkil etish orqali xodimlarning xabardorligini oshirish mumkin. Mazkur chora-tadbirlar butunlay omillarni kompleks ko'rib chiqish va tajriba almashinuvi orqali amalga oshirilishi tibbiyot tizimlarining xavfsizligini mustahkamlaydi.



XULOSA

Raqamli sog'liqni saqlash sohasidagi xavfsizlik muammolari ko'p qirrali bo'lib, bemor ma'lumotlarining maxfiyligi, tizimning ishonchliligi va xizmatlarning uzluksizligi nuqtai nazaridan katta tahdidlar yaratadi. Tahlillar shuni ko'rsatadiki, bu muammolarni bartaraf etishda inson omilini yaxshilash, zamonaviy texnik chora-tadbirlarni amalga oshirish va tartibga soluvchi me'yorlarni qattiq joriy etish asosiy o'rin tutadi. Xulosa o'rnida aytish mumkinki, sog'liqni saqlash tashkilotlari va axborot xavfsizligi mutaxassislari hamkorligida raqamli tibbiyot tizimlarining himoya darajasini oshirish bo'yicha doimiy va kompleks chora-tadbirlar ishlab chiqish zarur. Faol xalqaro hamkorlik, standartlarga muvofiq ishlash va muntazam monitoring raqamli sog'liq muassasalarida ishonchli kiberxavfsizlikni ta'minlashda muhim omil bo'lib hizmat qiladi.

Foydalanilgan adabiyotlar

1. Ewoh P., Vartiainen T. Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. Journal of Medical Internet Research. 2024;26:e46904. DOI: 10.2196/46904.
2. World Health Organization. WHO/Europe launches guide to strengthen cybersecurity in digital health (News release). 26 March 2025.
3. Gebeyew A.S., Zemene W., Tilahun B.C. va boshq. Digital health data security practices among health professionals in low-resource settings: cross-sectional study in Amhara Region, Ethiopia. BMC Medical Informatics and Decision Making. 2025;25:60. DOI: 10.1186/s12911-025-02902-2.