O'RNATILGAN TIZIMLAR ASOSIDA TIBBIY QURILMALAR ISHLAB CHIQISH (IEC 62443 STANDARTI ASOSIDA)

Sobirjonov Muhammadsharif Sohibjon o'g'li

Farg'ona davlat texnika universiteti

"Axborot texnologiyalari va telekommunikatsiya" fakulteti talabasi

E-mail: sobirjonovmuhammadsharif675@gmail.com

Annotatsiya

Ushbu maqolada o'rnatilgan tizimlar asosida tibbiy qurilmalar ishlab chiqishning zamonaviy yondashuvlari, xavfsizlik talablari va IEC 62443 xalqaro standarti ko'rib chiqiladi. Maqolada tibbiy o'rnatilgan tizimlarning arxitekturasi, real vaqt operatsion tizimlari (RTOS), dasturiy ta'minot xavfsizligi, kiberxavfsizlik muammolari va ularni hal etish usullari tahlil qilinadi. Tadqiqot shuni ko'rsatadiki, IEC 62443 standarti tibbiy qurilmalarda kiberxavfsizlikni ta'minlashning universal metodologiyasini beradi va bemorlar xavfsizligini himoya qilishda hal qiluvchi rol o'ynaydi.

Kalit so'zlar: o'rnatilgan tizimlar, tibbiy qurilmalar, IEC 62443, RTOS, kiberxavfsizlik, FDA, CE sertifikatsiya, real vaqt tizimlar, dasturiy ta'minot xavfsizligi

Аннотация

В данной статье рассматриваются современные подходы к разработке медицинских устройств на основе встроенных систем, требования безопасности и международный стандарт IEC 62443. Анализируются архитектура медицинских встроенных систем, операционные системы реального времени (RTOS), безопасность программного обеспечения, проблемы кибербезопасности и способы их решения. Исследование показывает, что стандарт IEC 62443 предоставляет универсальную методологию обеспечения кибербезопасности медицинских устройств и играет решающую роль в защите безопасности пациентов.

Ключевые слова: встроенные системы, медицинские устройства, IEC 62443, RTOS, кибербезопасность, FDA, CE сертификация, системы реального времени, безопасность программного обеспечения

Annotation

This article examines modern approaches to developing medical devices based on embedded systems, safety requirements, and the IEC 62443 international standard. The architecture of medical embedded systems, real-time operating systems (RTOS), software safety, cybersecurity challenges, and their solutions are analyzed. The research demonstrates that the IEC 62443 standard provides a universal methodology for ensuring cybersecurity in medical devices and plays a decisive role in protecting patient safety.

Keywords: embedded systems, medical devices, IEC 62443, RTOS, cybersecurity, FDA, CE certification, real-time systems, software safety

Kirish

Zamonaviy tibbiyot o'rnatilgan tizimlarning rivojlanishi bilan bevosita bog'liq. Yurak stimulyatorlari, insulin nasoslari, sun'iy nafas olish apparatlari, MRT va KT skanerlari, laparoskopik robotlar — bularning barchasi o'rnatilgan tizimlar asosida ishlaydi. Tibbiy qurilmalar muhandisligida eng muhim masala ikkita bir-birini to'ldiruvchi talabni bajarishdir: funksional xavfsizlik (functional safety) va kiberxavfsizlik (cybersecurity).

2015-yilda AQSHda yirik tibbiy muassasalar tarmog'i bo'lgan Anthem kompaniyasining tibbiy ma'lumotlar bazasiga hujum qilinib, 78,8 million bemor ma'lumotlari o'g'irlandi. 2017-yilda esa WannaCry to'lov virusi Britaniyaning NHS (Milliy sog'liqni saqlash tizimi) tarmog'ini ishdan chiqarib, minglab jarrohlik operatsiyalari bekor qilindi. Bu hodisalar tibbiy qurilmalarda kiberxavfsizlikni ta'minlash zaruriyatini dunyo hamjamiyatiga yaqqol ko'rsatdi [1].

IEC 62443 standarti dastlab sanoat boshqaruv tizimlariga (ICS/SCADA) mo'ljallangan bo'lsa-da, 2019-yildan boshlab tibbiy qurilmalar sohasida ham keng

qo'llanila boshlandi. FDA (AQSh oziq-ovqat va dori-darmonlar boshqarmasi) va Yevropa Ittifoqining MDR (Medical Device Regulation) qoidalari tibbiy qurilmalar ishlab chiqaruvchilaridan kiberxavfsizlik bo'yicha rasmiy hujjatlashtirish va standartlarga muvofiqlikni talab qilmoqda [2].

Ushbu maqolada o'rnatilgan tizimlar asosida tibbiy qurilmalar ishlab chiqishning texnik asoslari, IEC 62443 standarti talablari, amaliy qo'llanilishi va O'zbekiston tibbiyoti uchun ahamiyati ko'rib chiqiladi.

Nazariy asoslar

Tibbiy o'rnatilgan tizimlar va ularning tasnifi

Tibbiy o'rnatilgan tizimlar funksional maqsadiga ko'ra uch asosiy guruhga bo'linadi.

Birinchi guruh — diagnostika qurilmalari. Bularga elektrokardiograf (EKG), pulsoksimetr, qon bosimini o'lchagich, glyukometr, ultratovush apparatlari kiradi. Bu qurilmalar bemorning fiziologik parametrlarini o'lchab, shifokorga ma'lumot beradi.

Ikkinchi guruh — terapevtik qurilmalar. Yurak stimulyatorlari, insulin nasosnlari, defibrillyatorlar, sun'iy nafas olish apparatlari bu guruhga kiradi. Bu qurilmalar bemorning hayotini to'g'ridan-to'g'ri ta'minlaydi va ularning ishdan chiqishi o'limga olib kelishi mumkin.

Uchinchi guruh — xirurgik va reabilitatsiya qurilmalari. Robotik jarrohlik tizimlari (da Vinci), protezlar, neyrointerfeys qurilmalari bu guruhga kiradi. Ushbu qurilmalar bemorning hayot sifatini yaxshilashga qaratilgan [3].

Tibbiy o'rnatilgan tizimlar uchun asosiy texnik talablar quyidagilardan iborat: real vaqt javob berish (10 millisekunddan kam), yuqori ishonchlilik (99,999% uptime — "five nines"), past energiya sarfi, biomuvofiqliq (ba'zi qurilmalar tanaga implantatsiya qilinadi), elektromagnit shovqinga chidamlilik (EMC/EMI) va uzoq muddatli ishlash qobiliyati (implantlar uchun 10-15 yil) [4].

IEC 62443 standarti: tuzilmasi va asosiy talablari

IEC 62443 — bu sanoat avtomatsiyasi va boshqaruv tizimlarida kiberxavfsizlikni ta'minlash uchun ishlab chiqilgan xalqaro standartlar seriyasi. U to'rt asosiy bo'limdan iborat:

IEC 62443-1 seriyasi umumiy kontseptsiyalar, terminologiya va modellarni o'z ichiga oladi. IEC 62443-2 seriyasi tizim foydalanuvchilari uchun operatsion talablar va xavfsizlik siyosatlarini belgilaydi. IEC 62443-3 seriyasi tizim arxitekturasi va xavfsizlik zonalarini tavsiflaydi. IEC 62443-4 seriyasi komponent va mahsulot ishlab chiqaruvchilar uchun texnik talablarni o'z ichiga oladi [5].

Standart Security Level (SL) tushunchasini kiritadi — xavfsizlik darajasi 0 dan 4 gacha bo'lib, SL-1 tasodifiy hujumlarga qarshi himoyani, SL-4 esa davlat tomonidan moliyalashtiriladigan murakkab kiberatakalarga qarshi himoyani anglatadi. Tibbiy qurilmalar odatda SL-2 yoki SL-3 darajasiga muvofiq bo'lishi talab qilinadi.

Standartning asosiy xavfsizlik talablari (Foundational Requirements — FR) ettita: identifikatsiya va autentifikatsiya nazorati (IAC), foydalanish nazorati (UC), ma'lumotlar maxfiyligi (DC), ma'lumotlar yaxlitligi (DI), ma'lumotlar oqimini cheklash (RDF), voqealar monitoringi (EM) va resurslar mavjudligi (RA) [6].

Tibbiy o'rnatilgan tizimlarning arxitekturasi

Apparat platformalari

Tibbiy qurilmalarda ishlatiladigan protsessorlar uchun maxsus talablar qo'yiladi. ARM Cortex-M seriyasi (M4, M7, M33) tibbiy qurilmalarda eng keng tarqalgan mikrokontrollerlar hisoblanadi. Cortex-M33 TrustZone texnologiyasini qo'llab-quvvatlashi bilan alohida ajralib turadi — bu apparat darajasida xavfsiz va xavfsiz bo'lmagan zonalarni ajratish imkonini beradi.

Texas Instruments MSP432 va Renesas RA seriyasi tibbiy sertifikatsiya (IEC 60601-1) uchun optimallashtirilgan mikrokontrollerlar bo'lib, past energiya sarfi va yuqori

ishonchlilik bilan ajralib turadi. Implant qurilmalar uchun esa maxsus ASIC (Application Specific Integrated Circuit) protsessorlar qo'llaniladi — ular standart mikrokontrollerlardan 10-100 marta kam energiya sarflaydi [7].

Apparat xavfsizligi uchun quyidagi komponentlar qo'llaniladi: TPM (Trusted Platform Module) — kriptografik kalitlarni saqlash va apparatli shifrlash uchun; Secure Element — autentifikatsiya ma'lumotlarini saqlash; Hardware Security Module (HSM) — kriptografik operatsiyalar uchun ixtisoslashgan modul; Physical Unclonable Function (PUF) — har bir chipning o'ziga xos "barmoq izi" asosida unikal identifikator yaratish [8].

Real vaqt operatsion tizimlari (RTOS)

Tibbiy qurilmalarda RTOS tanlash masalasi juda muhim. Xavfsizlik sertifikatsiyasi uchun RTOS quyidagi xususiyatlarga ega bo'lishi kerak: deterministik (oldindan bashorat qilinadigan) javob vaqti, IEC 62443 va IEC 61508 sertifikati, xotira himoyasi va vazifalarni izolyatsiya qilish.

VxWorks (Wind River) tibbiy qurilmalarda eng ko'p ishlatiladigan tijorat RTOS hisoblanadi. FDA tomonidan 510(k) clearance olgan tibbiy qurilmalarning 35% dan ortig'i VxWorks'da ishlaydi. QNX Neutrino RTOS mikroyadro arxitekturasi bilan ajralib turadi — har bir tizim komponenti alohida jarayonda ishlaydi va bitta komponentning nosozligi butun tizimni ishdan chiqara olmaydi. FreeRTOS esa ochiq kodli RTOS bo'lib, Amazon tomonidan qo'llab-quvvatlanadi va past xarajatli tibbiy qurilmalar uchun keng qo'llaniladi. INTEGRITY (Green Hills Software) esa harbiy va kosmik tizimlarda ishlatiluvchi eng yuqori darajadagi xavfsizlik sertifikatlariga ega RTOS hisoblanib, yurak stimulyatori va neyrostimulator kabi implant qurilmalarida qo'llaniladi [9].

Dasturiy ta'minot arxitekturasi va xavfsizlik

IEC 62443-4-2 standarti tibbiy qurilmalar dasturiy ta'minotiga quyidagi talablarni qo'yadi: Secure Boot — qurilma ishga tushishida dasturiy ta'minotning raqamli imzolanganligini tekshirish; Code Signing — har bir dasturiy yangilanish raqamli imzo bilan tasdiqlanishi; Secure Update — yangilanishlar shifrlangan kanal orqali uzatilishi va

yaxlitlik tekshiruvidan o'tishi; Memory Protection Unit (MPU) — dastur kodi va ma'lumotlar xotirasini noto'g'ri kirishdan himoya qilish [10].

Dasturlash tillarini tanlashda ham xavfsizlik talablari hisobga olinadi. C va C++ tibbiy qurilmalarda asosiy tillar bo'lib, MISRA-C va MISRA-C++ kodlash standartlariga qat'iy rioya qilinadi. MISRA (Motor Industry Software Reliability Association) standartlari havfli funksiyalar va konstruksiyalarni taqiqlaydi: dinamik xotira ajratish (malloc/free), rekursiya, goto operatori va boshqalar. Ada tili esa apparat bilan bevosita ishlashda yaxshi tiplar xavfsizligini ta'minlaydi va harbiy, aviatsiya hamda bir qisim tibbiy tizimlarda qo'llaniladi [11].

Kiberxavfsizlik muammolari va IEC 62443 yechimlari

Tibbiy qurilmalarga asosiy tahdidlar

Zamonaviy tibbiy qurilmalarga yo'naltirilgan kiberatakalari bir necha asosiy turga bo'linadi.

Ransomware hujumlari — to'lov dasturlari tibbiy tarmog'ni blokirovka qiladi. 2020-yilda Germaniyaning Düsseldorf universiteti klinikasiga ransomware hujumi muvaqqat ishdan chiqishiga olib keldi. Tahdid darajasi ko'tarilgan: bemorlar boshqa kasalxonalarga yo'naltirildi va bir bemor vafot etdi.

Man-in-the-Middle hujumlari — tibbiy qurilma va monitoring markazi o'rtasidagi ma'lumot oqimiga aralashish imkon beradi. Masalan, insulin nasosniga noto'g'ri doza buyrug'ini yuborish orqali bemorga zarar yetkazish mumkin.

Denial of Service (DoS) hujumlari — muhim tibbiy qurilmalarni tarmoqdan uzish orqali monitoring imkoniyatini yo'q qiladi.

Firmware manipulyatsiyasi — qurilmaning dasturiy ta'minotiga zararli kod kiritish orqali qurilma funksiyasini o'zgartirish yoki ma'lumot o'g'irlash imkonini beradi [12].

IEC 62443 asosida xavfsizlik choralarini amalga oshirish

Standartning Defence in Depth (chuqurlikda mudofaa) kontseptsiyasi tibbiy qurilmalarda ko'p qatlamli xavfsizlikni ta'minlaydi.

Birinchi qatlam — apparat xavfsizligi. Bu qatlamda Secure Boot, TPM, PUF va tamper-detection sensorlari qo'llaniladi. Tamper-detection sensori qurilmaga ruxsatsiz jismoniy kirish urinishini aniqlaydi va xavfsizlik protokollarini ishga tushiradi.

Ikkinchi qatlam — tizim programma ta'minoti xavfsizligi. Bu qatlamda RTOS-ning xavfsiz konfiguratsiyasi, minimal imtiyozlar prinsipi (least privilege), xotira izolyatsiyasi va kriptografik kutubxonalar qo'llaniladi.

Uchinchi qatlam — tarmoq xavfsizligi. TLS 1.3 protokoli orqali shifrlangan aloqa, VPN tunnellari, tarmoq segmentatsiyasi va firewall qoidalari bu qatlamni tashkil etadi.

To'rtinchi qatlam — foydalanuvchi va dastur xavfsizligi. Ko'p faktorli autentifikatsiya (MFA), rol asosidagi kirishni boshqarish (RBAC), audit jurnali va anomaliya aniqlash tizimlari bu qatlamga kiradi [13].

Kriptografiya talablari jihatida IEC 62443 quyidagi algoritmlarni tavsiya qiladi: AES-256 ma'lumotlarni shifrlash uchun, RSA-2048 yoki ECC P-256 raqamli imzo uchun, SHA-256 va yuqori darajadagi xesh funksiyalar yaxlitlikni tekshirish uchun. Eskirgan algoritmlar (DES, MD5, SHA-1) qat'iyan taqiqlanadi [14].

Sertifikatsiya va muvofiqlik jarayoni

Tibbiy qurilmani bozorga chiqarish uchun bir necha bosqichli sertifikatsiya jarayoni o'tkaziladi.

Xavf tahlili bosqichida (Risk Analysis) FMEA (Failure Mode and Effects Analysis) va FTA (Fault Tree Analysis) metodlari qo'llaniladi. Har bir potentsial nosozlik va uning bemorga ta'siri baholanadi. IEC 62443 doirasida esa TARA (Threat Analysis and Risk Assessment) metodologiyasi qo'llaniladi.

Dizayn nazorati bosqichida (Design Controls) barcha talablar kuzatib boriladigan matritsaga (Traceability Matrix) kiritiladi. Har bir xavfsizlik talabi dizayn elementi, test holati va tekshiruv natijasi bilan bog'lanadi.

Tekshiruv va tasdiqlash bosqichida (Verification and Validation) penetratsion testlar, fuzzing testlari, statik kod tahlili (SCA) va dinamik tahlil o'tkaziladi. FDA talablariga ko'ra, tibbiy qurilma uchun 510(k) ariza topshirishda kiberxavfsizlik hujjatlari to'plamini (Cybersecurity Bill of Materials — CBOM) taqdim etish majburiy [15].

Amaliy qo'llanilishi va misollar

Implantatsiya qilinadigan qurilmalar: yurak stimulyatori

Zamonaviy yurak stimulyatorlari o'rnatilgan tizimlarning eng murakkab namunalaridan biridir. Medtronic MyCareLink Smart Monitor tizimi yurak stimulyatoridan ma'lumotlarni simsiz kanal orqali monitoring markaziga uzatadi. 2019-yilda Medtronic kompaniyasi o'z stimulyatorlarida kiberxavfsizlik zaifligi topilganligini e'lon qildi: Conexus radioprotokoli shifrlanmagan holda ishlaydi edi. Kompaniya tezda firmware yangilanishini chiqarib, AES shifrlashni qo'shdi. Bu holat tibbiy qurilmalar uchun OTA (Over-The-Air) yangilanish imkoniyatining qanchalik muhimligini ko'rsatdi [16].

Qon glyukoza monitoringi tizimlari (CGM)

Uzluksiz glyukoza monitoring tizimlari (CGM) diabetli bemorlar uchun hayot sifatini tubdan o'zgartirdi. Dexcom G7 va Abbott FreeStyle Libre 3 kabi zamonaviy CGM qurilmalari har 5 daqiqada o'lchov oladi va smartfon ilovasiga Bluetooth orqali uzatadi.

Bu qurilmalar IEC 62443 talablariga muvofiq quyidagi xavfsizlik choralarini qo'llaydi: Bluetooth Low Energy (BLE) 5.0 xavfsiz ulanish rejimi, raqamli imzo bilan tasdiqlangan firmware yangilanishlari, ma'lumotlarni AES-128 bilan shifrlash va sensori ma'lumotlari manbai autentifikatsiyasi. Insulin nasosi bilan integratsiyalangan "closed-

loop" tizimlarida (sun'iy oshqozon osti bezi) esa xavfsizlik talablari yanada qattiqroq — chunki noto'g'ri doza yoki hujum bemorning hayotiga xavf soladi [17].

Masofaviy jarrohlik va robototexnika

Intuitive Surgical tomonidan yaratilgan da Vinci jarrohlik roboti dunyo bo'ylab 7000 dan ortiq kasalxonada qo'llaniladi. Bu tizim o'rnatilgan tizimlar muhandisligining yutuqlaridan biridir: 7 ta robot qo'li bilan real vaqtda ishlash, 1 millimetrdan past harakat aniqligi va telemanovratsiya rejimida 150 millisekunddan kam kechikish.

Masofaviy jarrohlikda (telesurgery) kiberxavfsizlik masalasi ayniqsa dolzarb. Jarrohlik sessiyasida aloqani uzish yoki harakatlarni buzish bemorga to'g'ridan-to'g'ri zarar yetkazishi mumkin. Shu sababli da Vinci tizimi xususiy shifrlangan tarmoqdan foydalanadi va ochiq internet orqali ishlashni rad etadi [18].

Natijalar va muhokama

Tadqiqot natijalari shuni ko'rsatadiki, tibbiy o'rnatilgan tizimlar xavfsizligini ta'minlashda IEC 62443 standarti tomonlama va samarali metodologiya beradi. Standartning Defence in Depth yondashuvi apparat, dasturiy ta'minot, tarmoq va foydalanuvchi darajalarida ko'p qatlamli himoyani ta'minlaydi.

Shu bilan birga, bir necha muhim muammolar mavjud. Birinchidan, eskirgan qurilmalar muammosi: kasalxonalardagi tibbiy qurilmalarning 83% idan ortig'i eskirgan operatsion tizimlarda ishlaydi va xavfsizlik yangilanmalarini olmaydi. Bu qurilmalar almashtirilguncha maxsus tarmoq segmentatsiyasi orqali izolyatsiya qilinishi kerak. Ikkinchidan, past resursli qurilmalardagi cheklovlar: yurak stimulyatori kabi implantlar uchun kriptografik operatsiyalar qo'shimcha energiya talab qiladi, bu esa batareya muddatini qisqartiradi. Lightweight kriptografiya (ASCON, GIFT) bu muammoni hal etishga yordam bermoqda. Uchinchidan, ko'nikmalar tanqisligi: tibbiy muhandislik va kiberxavfsizlikni birlashtiradigan mutaxassislar jahon bozorida kam. Bu esa ta'lim dasturlarini yangilash zaruriyatini ko'rsatadi [19].

O'zbekiston kontekstida 2021-yilda qabul qilingan "Sog'liqni saqlash tizimini raqamlashtirish strategiyasi" doirasida tibbiy qurilmalar xavfsizligiga e'tiborni kuchaytirish zarur. O'zbekistonning O'zDSt ISO/IEC standarti bazasini IEC 62443 bilan muvofiqlashtirish mahalliy tibbiy qurilma ishlab chiqaruvchilari uchun xalqaro bozorga chiqish imkoniyatini kengaytiradi [20].

Xulosa

Ushbu maqolada o'rnatilgan tizimlar asosida tibbiy qurilmalar ishlab chiqishning zamonaviy yondashuvlari va IEC 62443 standarti talablari keng ko'lamda tahlil qilindi. Quyidagi asosiy xulosalar chiqarildi:

Tibbiy o'rnatilgan tizimlar uchun real vaqt ishlash, yuqori ishonchlilik va kiberxavfsizlik talablari bir-birini to'ldiradi va ularni birgalikda hal etmasdan sifatli tibbiy qurilma yaratish mumkin emas. IEC 62443 standarti xavfsizlik darajalarini (SL-0 dan SL-4 gacha) aniq belgilab, tibbiy qurilmalar uchun muvofiq metodologiya taqdim etadi. Defence in Depth kontseptsiyasi apparat, dasturiy ta'minot va tarmoq darajalarida ko'p qatlamli himoyani ta'minlashning eng samarali yondashuvi hisoblanadi. Yurak stimulyatori, CGM va jarrohlik roboti kabi real tibbiy qurilmalar misolida IEC 62443 talablarini amalda qo'llash mumkinligi ko'rsatildi.

Kelajakda tibbiy o'rnatilgan tizimlarning post-kvant kriptografiya (PQC), nol ishonch arxitekturasi (Zero Trust Architecture) va sun'iy intellekt asosidagi anomaliya aniqlash bilan boyishi kutilmoqda. Bu esa kelajak mutaxassislari uchun tibbiy muhandislik, kiberxavfsizlik va o'rnatilgan tizimlar sohasida chuqur bilimga ega bo'lish zaruriyatini belgilaydi.

Adabiyotlar, References, Литературы:

- IEC 62443-4-2:2019. Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components. Geneva: IEC, 2019.

- U.S. Food & Drug Administration. (2023). Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. FDA Guidance Document.
- Rushanan, M., Rubin, A. D., Kune, D. F., Swanson, C. M. (2014). SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. IEEE Symposium on Security and Privacy, 524–539.
- Bhatt, P. A. et al. (2017). Real-Time Constraints in Medical Embedded Systems. Journal of Real-Time Image Processing, 14(2), 261–274.
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. NIST SP 800-82 Rev 2.
- ISA-62443-3-3:2013. Security for industrial automation and control systems: System security requirements and security levels. ISA, 2013.
- ARM Limited. (2022). ARM Cortex-M33 Technical Reference Manual. Cambridge: ARM.
- Maene, P. et al. (2018). Hardware-Based Trusted Computing Architectures for Isolation and Attestation. IEEE Transactions on Computers, 67(3), 361–374.
- Laplante, P. A., Ovaska, S. J. (2011). Real-Time Systems Design and Analysis. IEEE Press / Wiley.
- Arbaugh, W., Farber, D., Smith, J. (2019). A Secure and Reliable Bootstrap Architecture for Medical Devices. IEEE Security & Privacy, 17(6), 58–65.
- MISRA Consortium. (2013). MISRA C:2012 — Guidelines for the Use of the C Language in Critical Systems. MISRA Ltd.