ROBOTOTEXNIKA TIZIMLARIDA KIBERXAVFSIZLIK MUOMMOLARI

Abdiraxmonova Zebo Xurramovna
Shahrisabz Davlat pedogogika instituti
"Boshlang'ich ta'lim" sirtqi ta'lim yo'nalishi
4-kurs talabasi

Annotatsiya: Ushbu maqolada zamonaviy robototexnika tizimlarining kiber-tahdidlarga nisbatan zaifliklari tahlil qilinadi. Sanoat va xizmat ko'rsatish robotlarining tarmog'ga ulanishi ortishi bilan ularga nisbatan masofaviy hujumlar xavfi ham ortib bormoqda. Tadqiqotda asosiy xavfsizlik protokollari va tizimning barqarorligini ta'minlash usullari ko'rib chiqiladi.

Kalit so'zlar: robototexnika, kiberxavfsizlik, IoT, axborot xavfsizligi, tarmoq xavfsizligi.

Abstract: This article analyzes the vulnerabilities of modern robotic systems to cyber threats. As the connectivity of industrial and service robots to networks increases, the risk of remote attacks on them is also growing. The study examines the main security protocols and methods for ensuring system stability.

Keywords: Robotics, cybersecurity, IoT (Internet of Things), information security, network security.

Аннотация: В данной статье анализируются уязвимости современных робототехнических систем к киберугрозам. По мере увеличения подключения промышленных и сервисных роботов к сетям возрастает и риск удалённых атак на них. В исследовании рассматриваются основные протоколы безопасности и методы обеспечения устойчивости системы.

Ключевые слова: Робототехника, кибербезопасность, IoT (Интернет вещей), информационная безопасность, сетевая безопасность.

Kirish. Robototexnika zamonaviy texnologiyalarning eng tez rivojlanayotgan sohalaridan biri hisoblanadi. Bugungi kunda robotlar ishlab chiqarish, tibbiyot, transport, logistika va xizmat ko'rsatish sohalarida keng qo'llanilmoqda. Sanoat robotlari ishlab chiqarish jarayonlarini avtomatlashtiradi, tibbiy robotlar murakkab operatsiyalarni bajarishda yordam beradi, xizmat ko'rsatish robotlari esa inson mehnatini yengillashtiradi.

Robototexnika tizimlari ko'pincha kompyuter tarmoqlari, sensorlar, sun'iy intellekt algoritmlari hamda bulutli texnologiyalar bilan integratsiyalashgan holda ishlaydi. Bu esa robotlarni masofadan boshqarish, ularning ish faoliyatini monitoring qilish va samaradorligini oshirish imkonini beradi.

Biroq robototexnika tizimlarining tarmoqlarga ulanishi ularni turli kiberxavflarga ham duchor qiladi. Kiberhujumlar robotlarning boshqaruv tizimlarini buzishi, ma’lumotlarni o‘zgartirishi yoki ishlab chiqarish jarayonlariga zarar yetkazishi mumkin. Ayrim holatlarda bunday hujumlar inson hayotiga ham xavf tug‘dirishi mumkin.

Shu sababli robototexnika tizimlarida kiberxavfsizlikni ta’minlash masalasi bugungi kunda dolzarb ilmiy va amaliy muammolardan biri hisoblanadi. Ushbu maqolaning maqsadi robototexnika tizimlarida uchraydigan asosiy kiberxavfsizlik muammolarini aniqlash hamda ularni bartaraf etish yo‘llarini tahlil qilishdan iborat.

Mazkur tadqiqot robototexnika tizimlarida kiberxavfsizlik muammolarini o‘rganishga qaratilgan bo‘lib, quyidagi ilmiy usullardan foydalanildi.

Birinchidan, robototexnika va kiberxavfsizlik sohasidagi ilmiy adabiyotlar tahlil qilindi. Xalqaro ilmiy maqolalar, texnologik kompaniyalar hisobotlari hamda axborot xavfsizligi standartlari o‘rganildi.

Ikkinchidan, robototexnika tizimining asosiy komponentlari – sensorlar, boshqaruv modullari, aloqa kanallari va dasturiy ta’minot tizimli tahlil usuli yordamida o‘rganildi. Bu robototexnika tizimlarida qaysi qismlar kiberhujumlarga ko‘proq moyil ekanligini aniqlash imkonini berdi.

Uchinchidan, robototexnika tizimlarida yuzaga kelishi mumkin bo‘lgan kiberxavflar risk tahlili orqali baholandi. Ushbu tahlil kiberhujumlarning robototexnika tizimlariga ta’sir darajasini aniqlashga yordam berdi.

Tadqiqot natijalari robototexnika tizimlarida bir nechta asosiy kiberxavfsizlik muammolari mavjudligini ko‘rsatdi.

1.Tarmoq xavfsizligi bilan bog‘liq muammolar.

Ko‘plab robototexnika tizimlari internet yoki lokal tarmoqlar orqali boshqariladi. Agar tarmoq xavfsizligi yetarli darajada ta’minlanmagan bo‘lsa, kiberhujumchilar robot tizimiga noqonuniy kirishi mumkin. Bunday holatda robot boshqaruvini egallab olish yoki tizim faoliyatini to‘xtatib qo‘yish ehtimoli mavjud.

2.Dasturiy ta’minot zaifliklari.

Robototexnika tizimlari murakkab dasturiy ta’minot asosida ishlaydi. Agar ushbu dasturlarda xatoliklar yoki xavfsizlik kamchiliklari mavjud bo‘lsa, kiberhujumchilar ulardan foydalanishi mumkin. Ayniqsa dasturiy ta’minotni muntazam yangilamaslik tizim xavfsizligiga jiddiy xavf tug‘diradi.

3.Sensor ma’lumotlariga ta’sir qilish.

Robotlar atrof-muhit haqida ma’lumotni sensorlar orqali qabul qiladi. Agar hujumchilar sensorlardan kelayotgan ma’lumotlarni o‘zgartira olsa, robot noto‘g‘ri

qarorlar qabul qilishi mumkin. Bu sanoat robotlarida ishlab chiqarish jarayoniga zarar yetkazishi mumkin.

4.IoT qurilmalari bilan bog‘liq xavflar.

Ko‘plab robototexnika tizimlari Internet of Things texnologiyalari bilan integratsiyalashgan. IoT qurilmalari ko‘pincha oddiy xavfsizlik tizimlariga ega bo‘lgani sababli ular orqali robot tizimiga kirish ehtimoli mavjud.

Robototexnika tizimlarida kiberxavfsizlikni ta’minlash uchun bir qator choralar zarur.

Birinchidan, robototexnika tizimlarida ko‘p darajali xavfsizlik mexanizmlarini joriy etish muhim hisoblanadi. Bunga autentifikatsiya tizimlari, ma’lumotlarni shifrlash hamda tarmoq monitoringi kiradi.

Ikkinchidan, robototexnika tizimlarida ishlatiladigan dasturiy ta’minotni muntazam ravishda yangilab borish zarur. Bu yangi aniqlangan xavfsizlik zaifliklarini bartaraf etishga yordam beradi.

Uchinchidan, sun’iy intellekt asosidagi xavfsizlik tizimlari kiberhujumlarni aniqlash va ularga tezkor javob berishda samarali bo‘lishi mumkin.

Bundan tashqari, robototexnika tizimlari uchun xalqaro xavfsizlik standartlarini ishlab chiqish va ularni amaliyotga joriy etish ham muhim ahamiyatga ega.

Xulosa.

Xulosa qilib aytganda, robototexnika tizimlari zamonaviy texnologik rivojlanishda muhim rol o‘ynaydi. Biroq ularning tarmoqlar bilan integratsiyalashuvi kiberxavfsizlik muammolarini yuzaga keltirmoqda. Tadqiqot natijalari robototexnika tizimlarida asosiy xavflar tarmoq xavfsizligi zaifliklari, dasturiy ta’minot xatoliklari, sensor ma’lumotlariga ta’sir qilish hamda IoT qurilmalari bilan bog‘liq ekanligini ko‘rsatdi.

Robototexnika tizimlarida kiberxavfsizlikni ta’minlash uchun zamonaviy himoya texnologiyalarini joriy etish, dasturiy ta’minotni muntazam yangilash hamda xavfsizlik standartlariga amal qilish zarur. Kelajakda robototexnika tizimlarining yanada rivojlanishi bilan kiberxavfsizlik masalalariga alohida e’tibor qaratish muhim bo‘lib qoladi.

Foydalanilgan adabiyotlar:

[1] O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida PF-6079-son Farmoni. 05.10.2020.

[2]Giyazov B. B. & Hazratqulov B. A. Raqamli iqtisodiyotda kiberxavfsizlikka bo‘lgan ehtiyoj va uning iqtisodiy ta’siri. Miasto Przyszłości, 2025; 60: 427–431. – Raqamli transformatsiya va kiberxavfsizlik tahlili

[3]ISO/IEC 27001:2022 – Information Security Management Systems – Requirements. International Organization for Standardization. – Xalqaro axborot xavfsizligi boshqaruv standartlari (maqolada ISMS asos sifatida qo‘llanadi).

[4]Cybersecurity Ventures. Official Cybercrime Report 2025. – Jahon kiber jinoyatchilik tendensiyalari va zararlar prognozi.

[5] Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson, 2020.

[6]Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley, 2015.

[7]UzCERT (O‘zbekiston Respublikasi Axborot xavfsizligi markazi) rasmiy statistik ma’lumotlari (2024–2025). – O‘zbekiston bo‘yicha kiberxavfsizlik holati va statistik ko‘rsatkichlar.