

IOT XAVFSIZLIK CHORALARINING TAKOMILLASHTIRISH USULLARI

D.A.Raxmatullayev

TATV Qarshi filiali OAT va TX kafedrası assistent

***Annotatsiya.** "Internet of Things" (IoT) texnologiyalari tez sur'atlar bilan rivojlanib bormoqda va tobora ko'proq turmushimizning barcha jabhalarida qo'llanilmoqda. Biroq, IoT qurilmalarining ko'payishi bilan bir qatorda, ularning xavfsizligi bo'yicha masalalar ham kuchaymoqda. Ushbu ilmiy ish IoT qurilmalarining xavfsizlik choralari yaxshilashga bag'ishlangan bo'lib, hujumlardan himoyalash, ma'lumotlarni himoya qilish va xavfsizlik protokollarini modernizatsiya qilishga qaratilgan strategiyalar va texnologiyalarni o'z ichiga oladi.*

***Kalit so'zlar.** IoT (Internet of Things), Xavfsizlik Protokollari, Ma'lumotlarni himoyalash, Shifrlash algoritmlari, Autentifikatsiya usullari, Kiber tahdidla IoT qurilmalari, Tarmoq xavfsizligi, Hujum aniqlash tizimlari (IDS), IoT standartlar.*

METHODS OF IMPROVING IOT SECURITY MEASURES

D.A. Raxmatullayev

TATU Karshi branch OAT and TX department assistant

***Abstract.** Internet of Things (IoT) technologies are developing rapidly and are increasingly being used in all aspects of our lives. However, along with the proliferation of IoT devices, their security concerns are also increasing. This scientific work is devoted to improving the security measures of IoT devices and includes strategies and technologies aimed at protecting against attacks, protecting data and modernizing security protocols.*

Keywords. *IoT (Internet of Things), Security Protocols, Data Protection, Encryption Algorithms, Authentication Methods, Cyber Threats IoT Devices, Network Security, Intrusion Detection Systems (IDS), IoT Standards.*

Kirish. IoT texnologiyalari (Internet of Things) bizning kundalik hayotimizga tobora kirib bormoqda. Aqlli uyalar, salomatlikni monitor qiladigan gadjetlar va shahar infrastrukturasi boshqarish tizimlari kabi sohalar IoT orqali sezilarli darajada rivoj topmoqda. Biroq, IoT qurilmalarining ko'payishi bilan ularning xavfsizligiga bo'lgan tahdidlar ham ortib bormoqda. Bu maqola IoT qurilmalari xavfsizligiga qarshi kurashish usullarini va bu borada sun'iy idrokdan (AI) foydalanishning yangi imkoniyatlarini o'rganadi. IoTni kiber hujumlardan himoya qilish uchun turli xavfsizlik protokollari, jumladan zarur shifrlash algoritmlarini va fiziki xavfsizlik texnologiyalarini ishlab chiqish muhim ahamiyat kasb etadi. IoT qurilmalar uchun xavfsizlik choralarini amalga oshirishda shu jumladan end-to-end shifrlash, autentifikatsiya mexanizmlari va zararli trafikni aniqlash tizimlarini qo'llash zarurligidan tashqari, bu jarayonda qurilmaning samaradorligini pasaytirmaslik ham inobatga olinadi. Xavfsizlik tahlillari va sinovlarini o'tkazish jarayonida aniqlangan kamchiliklar IoT qurilmalarining dasturiy ta'minoti yangilanishlari va qattiq diski (firmware) takomillashuviga olib keladi. Shu bilan birga, IoT tarmoqlarini boshqarishda blokcheyn texnologiyalaridan foydalanish, bu tarmoqlarni ta'qib qilishni qiyinlashtiradi va ularda yuz beradigan ma'lumot almashtirish jarayonini xavfsiz va shaffof qiladi. Shundan tashqari, IoTni yanada xavfsiz qilish uchun sun'iy idrok algoritmlari va mashinaviy o'rganish yondashuvlaridan foydalanish tavsiya etiladi. AI tahlil qilish algoritmlari yordamida IoT qurilmalaridan yig'ilgan katta hajmdagi ma'lumotlarni real vaqt rejimida tahlil qilish imkoniyati mavjud bo'ladi. Bu yondashuvlar xavfsizlik tizimlariga anomal oqimlar yoki noo'rin faoliyat belgilari paydo bo'lishi bilan darhol munosabat qaytarish imkonini beradi, bu esa tavakkalchilikni sezilarli darajada kamaytiradi.

Jadvalda IoT tizimlarining xavfsizligini takomillashtirish uchun qo'llanilishi mumkin bo'lgan turli xil xavfsizlik choralarini, ularning maqsadlarini, qo'llaniladigan texnologiyalarni va kutilayotgan natijalarni ta'riflaydi.

Xavfsizlik Chorolari	Tavsif	Takomillashtirish Usullari
Autentifikatsiya va Avtorizatsiya	IoT qurilmalarini himoyalash va foydalanishni nazorat qilish	- Kuchli parollar va ko'p faktorli autentifikatsiya (2FA) qo'llash - Avtorizatsiya darajalarini belgilash va foydalanuvchilarni nazorat qilish
Shifrlash	Ma'lumotlarni himoya qilish uchun shifrlash vositalari	- Qurilmalarda va uzatish vaqtida ma'lumotlarni shifrlash (TLS/SSL) - Qat'iy shifrlash standartlarini joriy qilish
Tarmoq Xavfsizligi	Tarmoqqa hujumlarning oldini olish va tarmoq xavfsizligini ta'minlash	- Xavfsizlik devorlari (firewall) va tarmoqni aniqlash tizimlari (IDS/IPS) o'rnatish - Virtual xususiy tarmoqlar (VPN) foydalanish
Firmware va Dasturiy Ta'minot Yangilanishlari	Qurilmalarni yangilab, himoyasini kuchaytirish	- Avtomatik yangilanish tizimlarini joriy qilish - Xavfsizlik yamog'larini muntazam ravishda o'rnatish
Qurilma boshqaruvi va monitoring	Qurilmalarning xavfsizlik holatini doimiy kuzatish	- IoT qurilmalarini boshqarish platformalarini ishlatish - Real vaqtda monitoring va ogohlantirish tizimlarini o'rnatish
Ma'lumotlar xavfsizligi va Maxfiylik	Ma'lumotlarning xavfsizligini ta'minlash va maxfiyligini saqlash	- Ma'lumotlarni anonimlashtirish va pseudonimizatsiya qilish - Ma'lumotlar oqimining xavfsizligini ta'minlash
Fizik xavfsizlik	IoT qurilmalarining fizik xavfsizligini ta'minlash	- Qurilmalarni fizik ravishda himoya qilish, masalan, qulflangan kabinetlar va qulf qo'llash - Muhit xavfsizligini ta'minlash (masalan, video nazorat tizimlari)

Xavfsizlik Choralari	Tavsif	Takomillashtirish Usullari
Qo'shimcha xavfsizlik mexanizmlari	Qo'shimcha xavfsizlik choralari	- Xavfsizlik monitoringi xizmatlarini jalb qilish - Penetratsion testlar va xavfsizlik auditi o'tkazish

Quyidagi jadvalda IoT xavfsizlik choralarini takomillashtirish usullari keltirilgan.

Ushbu usullar IoT qurilmalar va tarmoqlarni himoya qilishda samarali natijalar berishi mumkin. Har bir xavfsizlik chorasi o'ziga xos jihatlari bilan ajralib turadi va kompleks xavfsizlik yondashuvi uchun birgalikda qo'llanilishi kerak.

Iot texnologiyasini takomillashtirish usullari. IoT (Internet of Things) texnologiyalari orqali turli qurilmalar va sensorlar Internetga ulanib, yaxlit ma'lumotlar oqimini yaratish imkoniyatiga ega bo'lib, bu texnologiya turli sohalar, jumladan aqlli uyalar, sanoat, sog'liqni saqlash va chakana savdo kabi sohalarda keng qo'llaniladi. IoT texnologiyasini takomillashtirish usullari quyidagilarni o'z ichiga oladi.

Energiya Samadorligi. IoT qurilmalar ko'pincha cheklangan energiya resurslariga ega. Energiya tejash sxemalari va texnikalarini, masalan, "Energy Harvesting" yoki bateriya hayoti uzaytirish texnologiyalarini takomillashtirish muhimdir.

Aloqa Protokollari. Bluetooth Low Energy (BLE), ZigBee, LoRa va 5G kabi aloqa protokollarini rivojlantirish orqali IoT qurilmalarining uzatilish masofasini oshirish va energiya samaradorligi yaxshilanadi.

Kiberxavfsizlik. IoT qurilmalar sonining ko'payishi kiber tahdidlarni ham oshiradi. Shifrlash, yangi autentifikatsiya mexanizmlari, va qurilmalar o'rtasida xavfsizlik dasturlarini yaxshilash zarur.

Ma'lumotlarni Qayta Ishlash. IoT yaratgan katta ma'lumot oqimini qayta ishlash qobiliyatini oshirish uchun edge computing va fog computing kabi yangi texnologiyalarni joriy qilish.

Sensor Texnologiyalari. Aniqlikni va mustahkamlikni yaxshilash uchun yangi yoki yaxshi sensorlar ishlab chiqishga e'tibor berish talab etiladi.

O'z-o'zini Tuzatuvchi Tarmoqlar. IoT tarmoqlari o'zini avtomatik tarzda tuzatishi va optimallashtirishi mumkin bo'lgan texnologiyalarni ishlab chiqish.

Foydalanuvchi Interfeyslari. Foydalanuvchi tajribasini yaxshilash va aqlli qurilmalar orqali oson navigatsiya qilish uchun intuitiv interfeyslar yaratish.

XULOSA. IoT qurilmalar xavfsizligini ta'minlashda yangi texnologiyalar va yondashuvlar aniqlanmoqda. Ushbu ilmiy ishda tadqiq etilgan texnologiyalar va strategiyalar IoT qurilmalari va tarmoqlar uchun yangi avlod xavfsizlik echimlarini yaratishga yordam beradi. Bu usullar IoT ekotizimini yanada ishonchli va yaxlit qilishga xizmat qiladi va keng qo'llaniladigan IoT texnologiyalari va qurilmalaridan foydalanish xavfsizligini oshirishda muhim ahamiyatga ega bo'ladi.

FOYDALANILGAN ADABIYOTLAR

1. Normurodov, A. D., & Rustamov, A. B. (2023). INTERNET-BUYUMLAR IOT AFZALLIKLARI VA XAVFSIZLIK MUAMMOLARI. *INNOVATSION IQTISODIYOTNI SHAKLLANTIRISHDA AXBOROT KOMMUNIKATSIYA TEXNOLOGIYALARINING TUTGAN O'RNINI*, 1(1).
2. Uzakov, O. S., Raxmatullayev, D. A., Bekmatov, A. K., & Dilmurodov, Z. D. (2023). IOT TEXNOLOGIYALARI XAVFSIZLIGIDA SMART HOUSELARNI MOBIL QURILMALAR YORDAMIDA BOSHQARISH. *ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ*, 23(7), 105-107.
3. Raxmatullayev, D. A. (2024). AXBOROT XAVFSIZLIGI SOHASIDA TAQSIL OLADIGAN TALABALARNING KEBIR XAVFSIZLIKNI O'ZGARTIRISH METODIKASINI TAKOMILLASHTIRISH. *TADQIQOTLAR*, 30(3), 103-107.
4. Dildora, I. (2023). AXBOROT XAVFSIZLIGINI TA'MINLASHDA RISKLARNI BOSHQARISH FAOLIYATI SAMARADORLIGINING ASOSIY TAVSIFLARI. In *Uz-Conferences* (Vol. 1, No. 1, pp. 83-86).
5. Бекматов, А. К., Кутдусова, Э. Р., Мукимов, Ш. И., & Давлатова, Н. Н. (2023). ПРОГРЕССИВНЫЕ ТЕНДЕНЦИИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. *Экономика и социум*, (6-1 (109)), 1264-1270.

6. Абдувалиев, А. А., Дилмуродов, З. Д., & Рахматуллаев, Д. А. (2023). РАҚАМЛИ ИҚТИСОДИЁТ ШАРОИТИДА ТУРИЗМ СОҲАСИ ГЕОАХБОРОТ МОДЕЛИНИНГ ЙЎНАЛИШЛАРИ. *Экономика и социум*, (5-1 (108)), 959-963.
7. Asad o'g'li, R. D., Kurbonmaxmatovich, B. A., & Zuhridin Dostmurod o'g, D. (2023). АХБОРОТ ХАВФСIZLIGIDA SUN'IY INTELLEKT TIZIMLARINI QO'LLANILISHI. *TALIM DUNYODAGI FAN VA INNOVATSION G'OYALAR*, 23(4), 19-22.
8. Эгамбердиев, Ҳ., Рахматуллаев, Д., & Дилмуродов, З. (2023). ГРУНТ ВА ЕР УСТИ СУВ ОҚИМЛАРИНИНГ ЎЗARO ТАЪСИРИНИНГ МАТЕМАТИК МОДЕЛИ. *Евразийский журнал академических исследований*, 3(1 Part 3), 107-113.