# IOT TARMOQLARI XAVFSIZLIK PROTOKOLLARINI TADQIQ QILISH

**Sodiqov Abduxakim**
*“University of management and future technologies”*
*Raqamli texnologiyalar fakulteti,*
*Telekommunikatsiya injiniringi mutaxasisligi yo‘nalishi magistranti*
*Ilmiy rahbar*: **Abdumalikov A.A**
*PhD. O‘ZMU Jizzax filiali Ilmiy tadqiqotlar,*
*Innovatsiyalar va ilmiy pedagog kadrlar tayyorlash bo‘limi boshlig‘i.*

**Annotatsiya**: *Ushbu maqolada Internet of Things (IoT) tarmoqlarida xavfsizlik protokollarini tadqiq qilish masalalari keng qamrovda o‘rganildi. Tadqiqot doirasida IoT arxitekturasi, qurilmalararo autentifikatsiya va ishonch tizimlari, ma’lumotlarni shifrlash mexanizmlari, kalitlarni boshqarish, yengil kriptografik protokollar, edge computing va blokcheyn texnologiyalarining xavfsizlikka ta’siri tahlil qilindi. Shuningdek, IoT xavfsizligini baholash mezonlari, anomaliyalarni aniqlash va multi-faktorli autentifikatsiya yondashuvlari ko‘rib chiqildi. Tadqiqot natijalari IoT tarmoqlarida samarali xavfsizlikni ta’minlash uchun standartlashtirilgan, moslashuvchan va innovatsion protokollarni joriy etish muhimligini ko‘rsatadi. So‘nggi yillarda IoT texnologiyalari global iqtisodiyotning turli sohalarida inqilob yasadi. IoT tarmoqlarining o‘sishi va ularning samaradorligini oshirishga bo‘lgan ehtiyoj ilg‘or texnologik echimlar va boshqaruv strategiyalarini tadqiq qilishni talab qilmoqda.*

**Kalit so‘zlar:** *IoT (Internet of Things), IoT tarmoqlari, xavfsizlik protokollari, autentifikatsiya, shifrlash, yengil kriptografiya, kalitlarni boshqarish, edge computing, blokcheyn, real vaqtli ma’lumotlarni boshqarish, anomaliyalarni aniqlash.*

**Abstract:** *This article comprehensively examines the issues of researching security protocols in Internet of Things (IoT) networks. The research analyzes the impact of IoT architecture, inter-device authentication and trust systems, data encryption mechanisms, key management, lightweight cryptographic protocols, edge computing, and blockchain technologies on security. IoT security assessment criteria, anomaly detection, and multi-factor authentication approaches are also considered. The research results demonstrate the importance of implementing standardized, flexible, and innovative protocols to ensure effective security in IoT networks. In recent years, IoT technologies have revolutionized various sectors of the global economy. The growth of IoT networks and the need to improve their efficiency require the study of advanced technological solutions and management strategies.*

**Keywords:** *IoT (Internet of Things), IoT networks, security protocols, authentication, encryption, lightweight cryptography, key management, edge computing, blockchain, real-time data management, anomaly detection.*

**KIRISH**

So‘nggi yillarda Internet of Things (IoT) texnologiyalarining jadal rivojlanishi natijasida kundalik hayot, sanoat, sog‘liqni saqlash, transport va energetika kabi sohalarda millionlab aqlli qurilmalar tarmoqqa ulanmoqda. IoT tizimlari orqali sensorlar, aktuatorlar va aqlli qurilmalar o‘zaro axborot almashib, avtomatlashtirilgan boshqaruvni ta’minlaydi. Biroq ushbu texnologiyalarning keng miqyosda joriy etilishi bilan bir qatorda xavfsizlik masalalari ham dolzarb muammoga aylanmoqda.

IoT tarmoqlari an’anaviy kompyuter tarmoqlaridan farqli o‘laroq, resurslari cheklangan, energiya tejamkor va ko‘pincha himoyasi zaif qurilmalardan tashkil topadi. Bu esa ularni kiberhujumlar uchun oson nishonga aylantiradi. Ruxsatsiz kirish, ma’lumotlarni o‘g‘irlash, xizmatdan voz kechish (DoS) hujumlari va qurilmalarni masofadan boshqarib olish kabi tahdidlar IoT tizimlari barqarorligiga jiddiy xavf tug‘diradi. Shu sababli IoT tarmoqlarida axborot xavfsizligini ta’minlash uchun maxsus xavfsizlik protokollarini ishlab chiqish va tadqiq etish muhim ilmiy-amaliy masala hisoblanadi. IoT tizimlarni tarmoq hujumlaridan ma’lumotlarning og‘irlanishidan va tarmoqning noto‘g‘ri ishlashidan himoya qilish uchun tegishli xavfsizlik choralarini ko‘rish zarur.

Ushbu maqolada IoT tizimlarida IoT xavfsizligini ta’minlash bo‘yicha ilg‘or yondashuvlar va metodologiyalar ko‘rib chiqiladi.

**ASOSIY QISM**

IoT Xavfsizligi: IoT tizimlarining xavfsizligi juda muhim. Agar IoT tizimlari to‘g‘ri xavfsizlantirilmasa, ular tarmoq hujumlariga va ma’lumotlarning yo‘qolishiga olib kelishi mumkin. IoT xavfsizligi bilan bog‘liq asosiy muammolarni ko‘rib chiqamiz:

Ma’lumotlarni himoya qilish: IoT tizimlarida o‘tkazilayotgan ma’lumotlar o‘rta tarmoqlarda o‘g‘irlash yoki buzilish xavfiga duch keladi. Ma’lumotlarni uzatishda shifrlash, autentifikatsiya va maxfiylikni ta’minlash uchun ilg‘or texnologiyalar, masalan, AES (Advanced Encryption Standard) va TLS (Transport Layer Security) protokollari ishlatiladi. Shifrlash texnologiyalari IoT tizimlarida ma’lumotlarning xavfsizligini ta‘minlashning eng samarali usuli hisoblanadi.

Tarmoq xavfsizligi: IoT tizimlari juda ko’p qurilmalardan iborat bolib, ular o‘zaro bog‘langan holda ishlaydi. Shuning uchun tarmoqni himoya qilish juda muhimdir. Tarmoq xavfsizligi uchun olov devorlari, intrusion detection systems (IDS), intrusion prevention systems (IPS) va VPN (Virtual Private Network) kabi himoya vositalarini qo‘llash talab etiladi. Bu vositalar yordamida tarmoqdagi barcha kirish nuqtalari nazorat qilinadi va hujumlarni aniqlash tizimi orqali tarmoqning himoyasi mustahkamlanadi.

IoT tarmoqlarining arxitekturasi va xavfsizlik talablari. IoT tarmoqlari odatda uch qatlamli arxitekturaga ega: sezgirlik (sensor) qatlami, tarmoq qatlami va ilova qatlami. Har bir qatlam o‘ziga xos xavfsizlik talablariga ega bo‘lib, umumiy tizim himoyasi ushbu qatlamlarning uzviy ishlashiga bog‘liq.

Sensor qatlamida qurilmalar jismoniy muhitdan ma’lumot yig‘adi va uzatadi. Ushbu qatlamda autentifikatsiya va ma’lumot yaxlitligini ta’minlash muhim hisoblanadi. Tarmoq qatlamida ma’lumotlarni uzatish xavfsizligi, marshrutlash himoyasi va shifrlash asosiy

vazifa bo‘lsa, ilova qatlamida foydalanuvchi ma’lumotlarini himoyalash va ruxsatlarni boshqarish dolzarb ahamiyat kasb etadi.

IoT tarmoqlariga xos xavfsizlik tahdidlari. IoT tarmoqlari ochiq va taqsimlangan muhitda ishlagani sababli turli xil tahdidlarga duch keladi. Qurilmalar sonining ko‘pligi va ularning cheklangan hisoblash quvvatiga egaligi xavfsizlik mexanizmlarini murakkablashtiradi.

Asosiy tahdidlar qatoriga ruxsatsiz qurilma ulanishi, soxta identifikatsiya, ma’lumotlarni tarmoq orqali tutib olish, zararli dasturlar tarqalishi va xizmat ko‘rsatishni izdan chiqaruvchi hujumlar kiradi. Ushbu tahdidlarni bartaraf etishda samarali xavfsizlik protokollarini qo‘llash muhim ahamiyatga ega.

IoT tarmoqlarida autentifikatsiya va identifikatsiya protokollari. IoT tarmoqlarida qurilmalarni aniqlash va ularning haqiqiyligini tekshirish xavfsizlikning asosiy komponentlaridan biridir. An’anaviy autentifikatsiya mexanizmlari resurs talabchan bo‘lgani sababli IoT uchun moslashtirilgan yengil protokollar ishlab chiqilgan. Eng ko‘p qo‘llaniladigan yondashuvlar orasida simmetrik va assimmetrik kriptografiyaga asoslangan autentifikatsiya protokollari mavjud. Qurilmalar o‘rtasida ishonchli aloqa o‘rnatish uchun kalitlarni xavfsiz almashish mexanizmlari qo‘llaniladi. Yengil kriptografik algoritmlar IoT qurilmalarining energiya sarfini kamaytirgan holda yetarli darajada xavfsizlikni ta’minlaydi.

Ma’lumotlarni uzatishda xavfsizlik protokollari. IoT tarmoqlarida ma’lumotlarni uzatish jarayonida maxfiylik va yaxlitlikni ta’minlash muhim vazifa hisoblanadi. Shu maqsadda transport va ilova qatlamlarida maxsus xavfsizlik protokollari qo‘llaniladi. Datagram Transport Layer Security (DTLS) protokoli IoT muhitida keng qo‘llanilib, UDP asosidagi aloqalarda shifrlash va autentifikatsiyani ta’minlaydi. Shuningdek, yengil HTTPS va CoAP protokoli bilan birgalikda ishlovchi xavfsizlik mexanizmlari resurslari cheklangan qurilmalar uchun mos yechim sifatida qaraladi.

Ma’lumotlar almashish protokollari: IoT tizimlarida ma’lumotlarni uzatish uchun samarali protokollar kerak. MQTT (Message Queuing Telemetry Transport) va CoAP (Constrained Application Protocol) kabi protokollar, ayniqsa kichik qurilmalar va tarmoq resurslari cheklangan bo‘lsa, samarali ishlaydi. Ular tarmoqlarda ma’lumotlarni qisqa

va tezkor ravishda uzatishga imkon beradi.

Masalan, MQTT protokoli tezkor ma’lumot uzatish uchun ideal, bu tarmoqning yuqori yuklanishini oldini oladi.

Kalitlarni boshqarish va kriptografik himoya. IoT tarmoqlarida kalitlarni yaratish, saqlash va yangilash jarayonlari murakkab muammo hisoblanadi. Qurilmalar sonining ko‘pligi va ularning uzoq muddatli ishlashi kalitlarni samarali boshqarishni talab etadi. Kalitlarni boshqarish protokollari markazlashtirilgan va taqsimlangan yondashuvlarga asoslanadi.

Markazlashtirilgan usullarda boshqaruv serveri orqali kalitlar nazorat qilinadi, taqsimlangan usullarda esa qurilmalar o‘zaro ishonch asosida aloqa o‘rnatadi. Har ikki yondashuvning afzallik va cheklovlari mavjud bo‘lib, tizim talablari asosida tanlanadi.

IoT xavfsizligida yengil protokollarning ahamiyati. IoT qurilmalarining hisoblash

quvvati va energiya resurslari cheklanganligi sababli an’anaviy xavfsizlik protokollarini to‘liq qo‘llasv h har doim ham imkoniyat bermaydi. Shu bois yengil (lightweight) xavfsizlik protokollari ishlab chiqilmoqda. Bunday protokollar kam xotira talab qiladi, tez ishlaydi va energiya tejamkorligi bilan ajralib turadi. Yengil shifrlash algoritmlari va soddalashtirilgan autentifikatsiya mexanizmlari IoT tizimlarining umumiy xavfsizlik darajasini oshiradi.

Amaliy qo‘llanilish va muammolar. IoT xavfsizlik protokollari aqlli shaharlar, sanoat IoT, tibbiy monitoring tizimlari va aqlli uy texnologiyalarida keng qo‘llanilmoqda. Ushbu sohalarda ma’lumotlar xavfsizligini ta’minlash inson hayoti va muhim infratuzilmalar barqarorligi bilan bevosita bog‘liq. Shu bilan birga, protokollarni joriy etishda moslashuvchanlik, yangilanish mexanizmlarining murakkabligi va standartlashtirish muammolari mavjud. Bu esa IoT xavfsizligi bo‘yicha doimiy ilmiy tadqiqotlar olib borishni talab etadi.

Standartlashtirish tashkilotlarining IoT xavfsizligidagi o‘rni. IoT xavfsizlik protokollarining samarali ishlashi ko‘p jihatdan xalqaro standartlarga bog‘liq. Turli ishlab chiqaruvchilar tomonidan yaratilgan qurilmalar o‘zaro mos ishlashi uchun yagona xavfsizlik talablariga ehtiyoj mavjud. Shu sababli bir qator xalqaro tashkilotlar IoT xavfsizligini standartlashtirish bo‘yicha faoliyat olib bormoqda. Masalan, Xalqaro standartlashtirish tashkiloti (ISO) va Xalqaro elektrotexnika komissiyasi (IEC) IoT tizimlari uchun xavfsizlik talablarini belgilovchi standartlarni ishlab chiqmoqda. Ushbu standartlar qurilmalarni ro‘yxatdan o‘tkazish, autentifikatsiya darajalari, kriptografik algoritmlardan foydalanish va xavfsizlik siyosatlarini joriy etishni qamrab oladi. Standartlarga rioya qilish IoT tarmoqlarida xavfsizlikni bir maromda ta’minlashga yordam beradi.

IoT tarmoqlarida ishonch modeli va xavfsizlik siyosatlari. IoT tizimlarida ishonch modeli qurilmalar va foydalanuvchilar o‘rtasidagi munosabatlarni belgilovchi muhim komponent hisoblanadi. An’anaviy tarmoqlarda ishonch ko‘pincha markaziy boshqaruvga asoslangan bo‘lsa, IoT muhitida dinamik va moslashuvchan ishonch modellari talab etiladi. Ishonch modeli asosida xavfsizlik siyosatlari ishlab chiqilib, qurilmalarga beriladigan ruxsatlar va cheklovlar aniqlanadi. Bunday siyosatlar kontekstga bog‘liq holda, masalan, qurilmaning joylashuvi, holati yoki tarmoq yuklamasiga qarab o‘zgarishi mumkin. Natijada IoT tizimlarida moslashuvchan va aqlli xavfsizlik mexanizmlari shakllanadi.

IoT xavfsizlik protokollarida blokcheyn texnologiyasidan foydalanish. So‘nggi yillarda blokcheyn texnologiyasi IoT xavfsizligini oshirishda istiqbolli yondashuv sifatida qaralmoqda. Blokcheynning markazlashtirilmagan tuzilishi IoT tarmoqlarida yagona nosozlik nuqtasini bartaraf etishga imkon beradi. Blokcheynga asoslangan xavfsizlik protokollari qurilmalar identifikatsiyasini saqlash, tranzaksiyalarni tasdiqlash va jurnal yuritish vazifalarini bajaradi. Har bir qurilmaning harakati blokcheynga yozilishi natijasida ma’lumotlar soxtalashtirilishining oldi olinadi. Shu bilan birga, ushbu yondashuv hisoblash resurslariga bo‘lgan talabni oshirishi mumkin, bu esa yengil blokcheyn yechimlarini ishlab chiqishni talab etadi.

IoT tizimlarida xavfsiz yangilash (Secure Update) mexanizmlari. IoT qurilmalarining

uzoq muddat ishlashi ularni muntazam yangilab borishni taqozo etadi. Agar yangilash jarayoni himoyalanmagan bo‘lsa, hujumchilar zararli dasturlarni qurilmaga o‘rnatishi mumkin. Xavfsiz yangilash mexanizmlarida raqamli imzolar va yaxlitlikni tekshirish usullari qo‘llaniladi. Qurilma faqat ishonchli manbadan kelgan va tekshiruvdan o‘tgan dasturiy ta’minotni qabul qiladi. Ushbu yondashuv IoT tarmoqlarida ekspluatatsiya jarayonida xavfsizlikni doimiy saqlab turishga xizmat qiladi.

IoT xavfsizlik protokollarini baholash va testlash usullari. Xavfsizlik protokollarining samaradorligini aniqlash uchun ularni turli sharoitlarda sinovdan o‘tkazish zarur. IoT muhitida testlash jarayonlari laboratoriya va real tarmoq sharoitida amalga oshiriladi. Baholash mezonlariga hujumlarga chidamlilik, energiya sarfi, kechikish va hisoblash yuklamasi kiradi.

Maxsus simulyatsiya muhitlari yordamida protokollarning turli tahdidlarga qarshi reaksiyasi o‘rganiladi. Ushbu tahlillar asosida protokollar takomillashtiriladi va amaliy joriy etish uchun mos variantlar tanlanadi.

Kelajak istiqbollari va tadqiqot yo‘nalishlari. IoT xavfsizlik protokollarini rivojlantirishda sun’iy intellekt, o‘z-o‘zini moslashtiruvchi tizimlar va kontekstga asoslangan xavfsizlik yondashuvlari istiqbolli yo‘nalishlar sifatida qaralmoqda. Kelajakda IoT qurilmalari xavfsizlik tahdidlarini mustaqil aniqlab, mos choralarni ko‘ra oladigan darajaga yetishi kutilmoqda. Bundan tashqari, kvant hisoblash texnologiyalarining rivojlanishi mavjud kriptografik protokollarni qayta ko‘rib chiqishni talab qiladi. Shu bois kvantga chidamli xavfsizlik protokollarini ishlab chiqish IoT xavfsizligida muhim ilmiy yo‘nalishga aylanmoqda.

Multi-faktorli autentifikatsiya va qurilmalararo ishonch tizimlari. IoT tarmoqlarida

qurilmalararo aloqa ko‘pincha avtomatlashtirilgan va masofadan boshqariladi. Shu sababli faqat parol yoki kalitga asoslangan autentifikatsiya yetarli emas. Multi-faktorli autentifikatsiya yondashuvi — qurilmaning identifikatsiyasi uchun bir nechta tekshiruv bosqichlarini qo‘llash — xavfsizlikni sezilarli oshiradi. Bu yondashuvda quyidagilar qo‘llaniladi:

Kriptografik kalitlar;

Biometrik yoki fizikal parametrlar (masalan, qurilma joylashuvi, signal xususiyatlari);

Davriy kriptografik tokenlar yoki vaqtga bog‘liq tekshiruvlar.

Shunday qilib, IoT tarmoqlarida qurilmalararo ishonch tizimi shakllanadi, bu esa hujumchilarning tizimga kirish imkoniyatini kamaytiradi.

Edge computing va xavfsizlik protokollarini optimallashtirish. Edge computing yondashuvi IoT qurilmalarini markaziy serverlarga bog‘lamay, ularning yaqinida hisoblash imkoniyatlarini yaratadi. Bu yondashuv:

Ma’lumotlar uzatishda kechikishni kamaytiradi;

Xavfsizlik protokollarini lokal ravishda ishlatish imkonini beradi;

Shifrlash va autentifikatsiya jarayonlarini tezlashtiradi.

Edge computing bilan birga ishlatiladigan yengil protokollar va lokal kalit boshqaruvi IoT tarmoqlarining barqarorligi va tezkor xavfsizligini oshiradi.

Anomaliyalarni aniqlash va xavfsizlik monitoring. IoT tarmoqlari uchun xavfsizlik

monitoringi real vaqt rejimida muhim ahamiyatga ega. Anomaliyalarni aniqlash algoritmlari yordamida:

Trafikdagi g‘ayritabiiy naqshlar;

Qurilmalar noto‘g‘ri ishlashi;

Hujumga urinishlar aniqlanadi.

Sun’iy intellektga asoslangan yondashuvlar va oddiy statistika metodlari birgalikda qo‘llanilib, IoT xavfsizligi monitoringini yanada samarali qiladi. Shu bilan birga, monitoring ma’lumotlari protokollarni optimallashtirish va yangilash uchun asos bo‘lib xizmat qiladi.

Energiya tejamkorligi va xavfsizlik protokollarining uyg‘unligi. IoT qurilmalarining ko‘pi batareya bilan ishlaydi. Shifrlash va autentifikatsiya jarayonlari qurilmalar resurslariga yuqori yuk tushiradi. Shu sababli xavfsizlik protokollarini ishlab chiqishda:

Kriptografik algoritmlarning energiya sarfi;

Shifrlash va autentifikatsiya tezligi;

Ma’lumotlarni qayta ishlash samaradorligi e’tiborga olinadi. Optimal yondashuvlar qurilmaning uzoq muddat ishlashini ta’minlab, tizim xavfsizligini pasaytirmaydi.

IoT xavfsizligida mashhur protokollarni tadqiq qilish. IoT xavfsizligini ta’minlashda

keng qo‘llaniladigan protokollar va ularning xususiyatlari:

MQTT (Message Queuing Telemetry Transport): yengil va tezkor, lekin shifrlash va autentifikatsiya alohida qo‘shimcha talab qiladi.

CoAP (Constrained Application Protocol): cheklangan resursli qurilmalar uchun mo‘ljallangan, DTLS bilan ishlaydi.

LwM2M (Lightweight Machine to Machine): IoT qurilmalarni boshqarish va yangilashda xavfsizlikni ta’minlash imkonini beradi.

Zigbee va LoRaWAN protokollari: sensor tarmoqlarida xavfsizlik va kalitlarni boshqarish imkoniyatlarini beradi.

Har bir protokolning afzalliklari va cheklovlari mavjud bo‘lib, IoT tarmoq talablari va qurilma xususiyatlariga qarab tanlanadi.

Kiberxavfsizlik tahdidlarining yangi tendensiyalari. IoT tizimlaridagi tahdidlar tez o‘zgarib bormoqda. Jumladan:

- Qurilmalarni botnetga aylantirish (Masalan, Mirai hujumi);
- Masofadan boshqarish va shifrlangan trafik orqali hujumlar;
- Qurilmalarni tarmoqqa ruxsatsiz ulash.

Ushbu tendensiyalar IoT xavfsizlik protokollarini doimiy takomillashtirish va standartlashtirishni talab qiladi. Shu bilan birga, xavfsizlikni sun’iy intellekt yordamida real vaqt rejimida monitoring qilish istiqbolli yo‘nalishdir.

Yangilanishlar va ularni boshqarish: IoT qurilmalarining xavfsizligini ta’minlash uchun ularni doimiy yangilab turish kerak. Bu yangilanishlar xavfsizlik teshiklarini tuzatish va tizimning uzluksiz ishlashini ta’minlash uchun zarur. Shu bilan birga, tizimni yangi xavfsizlik zaifliklariga qarshi himoya qilish uchun yangilanishlar real vaqt rejimida amalga oshirilishi kerak. Xavfsizlik yangilanishlarini avtomatik tarzda amalga oshirish imkoniyati IoT tizimlarining xavfsizligini kuchaytiradi.

**XULOSA**

Mazkur maqolada Internet of Things (IoT) tarmoqlarida xavfsizlik protokollarini tadqiq qilish, ularning ishlash mexanizmlari, afzallik va cheklovlari keng qamrovda o‘rganildi. Tadqiqot natijalari shuni ko‘rsatadiki, IoT tarmoqlari an’anaviy kompyuter tarmoqlaridan farqli o‘laroq, cheklangan resursli qurilmalar, ko‘p sonli ulanish nuqtalari va ochiq muhit bilan xarakterlanadi. Shu sababli ularni himoya qilish uchun maxsus, yengil va samarali xavfsizlik protokollariga ehtiyoj mavjud.

Maqolada IoT xavfsizligidagi asosiy komponentlar: autentifikatsiya, qurilmalararo ishonch tizimi, ma’lumotlarni shifrlash, kalitlarni boshqarish, yengil kriptografik algoritmlar, edge computing va blokcheyn texnologiyalari kabi yondashuvlar batafsil tahlil qilindi.

Shuningdek, multi-faktorli autentifikatsiya, real vaqt monitoringi va anomaliyalarni aniqlash algoritmlari IoT tarmoqlarida kiberhujumlarni oldini olish va tizim barqarorligini ta’minlashda muhim ahamiyatga ega ekanligi ko‘rsatildi.

Maqolada ko‘rib chiqilgan protokollar — MQTT, CoAP, LwM2M, Zigbee va LoRaWAN — IoT qurilmalari va tarmoqlarining xususiyatlariga mos ravishda tanlanishi zarurligi aniqlanib, har bir protokolning afzalliklari va cheklovlari tahlil qilindi. Shu bilan birga, IoT xavfsizlik protokollarini baholashda hisoblash quvvati, energiya tejamkorligi, kechikish va samaradorlik kabi omillar muhim ahamiyat kasb etadi. Tahlillar shuni ko‘rsatadiki, IoT xavfsizligini ta’minlash doimiy monitoring, standartlashtirilgan protokollar, moslashuvchan xavfsizlik siyosatlari va innovatsion yondashuvlarni (masalan, sun’iy intellekt va blokcheyn) qo‘llashni talab qiladi. Kelajakda IoT tarmoqlari xavfsizlik protokollarini yanada optimallashtirish, kvantga chidamli kriptografik yechimlarni joriy etish va qurilmalararo avtomatik moslashuvchan xavfsizlik tizimlarini ishlab chiqish istiqbollari mavjud. IoT tarmoqlaridagi xavfsizlik protokollarini tadqiq qilish nafaqat texnologik, balki iqtisodiy va ijtimoiy jihatdan ham muhim ahamiyatga ega bo‘lib, tizimlarning ishonchliligi, barqarorligi va foydalanuvchilar ma’lumotlarining xavfsizligini ta’minlashda strategik rol o‘ynaydi. Shuningdek, IoT tizimlarida real vaqtli ma’lumotlarni boshqarish va xavfsizligini ta’minlash zamonaviy texnologiyalarning rivojlanishida muhim ahamiyat kasb etadi. Samarali boshqarish algoritmlari yordamida ma’lumotlarni tezda yig‘ish va tahlil qilish, xavfsizlik choralari orqali tizimni himoya qilish mumkin. IoT tizimlarining xavfsizligini ta’minlashda ilg‘or texnologiyalar va metodologiyalarni qo‘llash muhimdir. Bu tizimlarning ishlash samaradorligini oshirish va ulardan maksimal darajada foydalanish uchun doimiy yangilanishlar va takomillashtirishlar zarur.

**FOYDALANILGAN ADABIYOTLAR:**

1. Axmedov J.J., IoT texnologiyalari va xavfsizlik protokollari, Ilm Ziyo, Toshkent, 2022, 276 bet.

2. Qodirov D.X., Kompyuter tarmoqlari va ularning xavfsizligi, O‘zbekiston milliy ensiklopediyasi, Toshkent, 2020, 312 bet.

3. Journal of scientific research and their solutions “Ilmiy tadqiqotlar va ularning yechimlari jurnali” Volume 9, issue 01, 2026, pp. 711–715 bet.

4. ISO/IEC 30141:2018, Internet of Things (IoT) Reference Architecture, ISO/IEC, Geneva, 2018.

5. Haydarov S.S., Sun’iy intellekt va IoT tizimlari, Akademnashr, Toshkent, 2021, 288 bet.

6. Alimuhamedov A.A., Axborot xavfsizligi asoslari, Fan va texnologiya, Toshkent, 2021, 248 bet.

7. Rasulov B.M., Aqlli qurilmalar tarmoqlari va xavfsizlik masalalari, Innovatsion rivojlanish nashriyoti, Toshkent, 2023, 220 bet.

8. Lee I., Lee K., The Internet of Things (IoT): Applications, investments, and challenges for enterprises, Business Horizons, 2015, Vol. 58, No. 4, pp. 431–440.

9. Stojmenovic I., IoT security and privacy: Design principles and approaches, IEEE Internet of Things Journal, 2014, Vol. 1, No. 1, pp. 1–12.

10. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A., Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, 2015, Vol. 76, pp. 146–164.

11. Akyildiz, I. F., & Vuran, M. C. (2010). "IoT uchun xavfsizlik protokollari." IEEE Communications Magazine, 48(5), 64-70.