MIRZO ULUG'BEK NOMIDAGI
O'ZBEKISTON MILLIY UNIVERSITETINING
JIZZAX FILIALI

# ZAMONAVIY INNOVATSION TADQIQOTLARNING DOLZARB MUAMMOLARI VA RIVOJLANISH TENDENSIYALARI: YECHIMLAR VA ISTIQBOLLAR

## RESPUBLIKA ILMIY-TEXNIK ANJUMAN MATERIALLARI TO‘PLAMI

15-16-MAY
2026-YIL

doi

Google Scholar

**O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI**

**MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI**

# ZAMONAVIY INNOVATSION TADQIQOTLARNING DOLZARB MUAMMOLARI VA RIVOJLANISH TENDENSIYALARI: YECHIMLAR VA ISTIQBOLLAR

***mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami***

**(2026-yil 15-16-may)**

**JIZZAX-2026**

ma’lumotlar, noaniq ma’lumotlar, buzilgan ma’lumotlar qabul qilinganda to‘g‘ri javob qaytarish imkonini beradi.

## Adabiyotlar.


1. Ramazon, M., & Abdusattor, B. (2023). MIKROSKOP YORDAMIDA HUJAYRALARDAGI QON VA OQ QON HUJAYRALARI SONI BO‘YICHA BEMORLARNING SOG‘LIG‘INI ANIQLASH. International Journal of Contemporary Scientific and Technical Research, 133-137.
2. Эшонкулов, Т., & Михлиев, Р. (2023). Тестовые алгоритмы для решение задачи таксномии. Информатика и инженерные технологии, 1(2), 150-153.
3. Haykin, S. "Neural Networks and Learning Machines." 3rd Edition, Pearson, 2008.
4. Mixliyev, R., & Mustafoyev, E. (2024). MIKROSKOPDAGI TASVIRLARDA HUJAYRALARNI SANASH VA ANIQLASH ALGORITMI. International Journal of scientific and Applied Research, 1(1), 30-32.
5. Alday M., Mustafoyev E., Mixliyev R. ONLAYN MIT APP INVERTOR PLATFORMASIDAN FOYDALANILGAN HOLDA TIMER VA BUDILNIK MOBIL ILOVASINI YARATISHNI O ‘RGATISH JARAYONI: https://doi. org/10.5281/zenodo. 14245095 //Journal of International science networks. – 2024. – Т. 1. – №. 3. – С. 88-94.
6. Goodfellow, I., Bengio, Y., Courville, A. "Deep Learning." MIT Press, 2016.
7. Mixliyev R., Eshonqulov T. TABIIY TASVIRLAR SIFATINI OSHIRISH USULLARI //International Journal of scientific and Applied Research. – 2024. – Т. 1. – №. 3. – С. 76-79.
8. Rumelhart, D. E., Hinton, G. E., Williams, R. J. "Learning representations by back-propagating errors." Nature, 1986.
9. Pardayev, S., & Mixliyev, R. (2024). HOZIRGI ZAMON MAKTAB O ‘QUVCHILARNING TA'LIM NATIJALARINI BAHOLASHNING ZAMONAVIY DIDAKTIK IMKONIYATLARI: https://doi. org/10.5281/zenodo. 14245187. Journal of International science networks, 1(3), 95-101.


# IOT TIZIMLARIDA KIBERXAVFSIZLIKNI TA’MINLASHNING MODELLARI


**Abdumalikov Akmaljon Abduxoliq o‘g‘li**, t.f.f.d., (PhD), O‘zMU Jizzax filiali, Kompyuter ilmlari va dasturlashtirish kafedrasi professori

**Hayitova.CH.H.**

Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetining Jizzax filiali 2-bosqich talabasi.

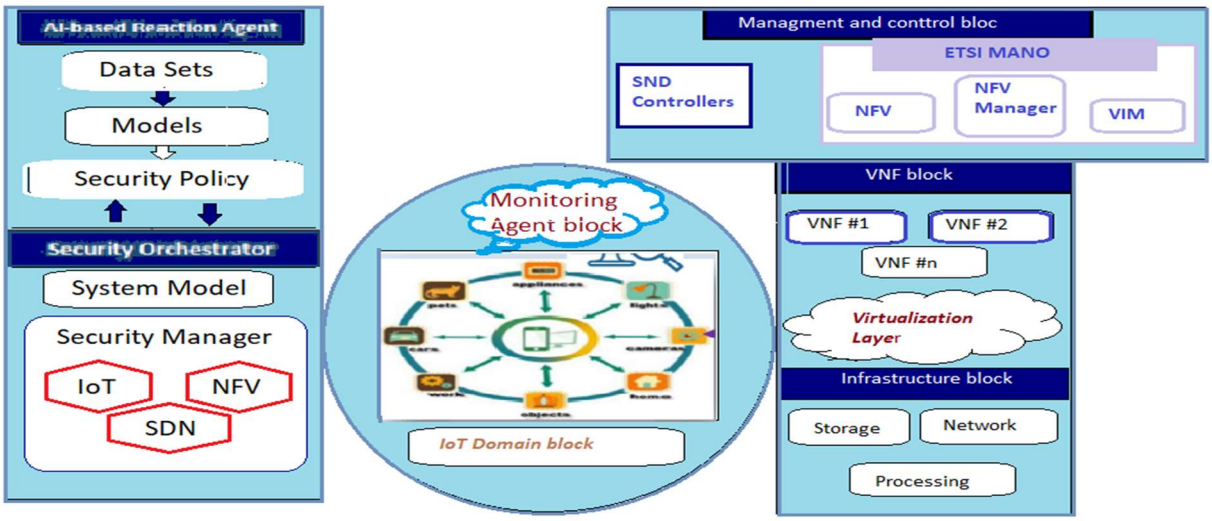
charoshayitova24@gmail.com

**Annotatsiya:**Ushbu maqolada Internet of Things (IoT) tizimlarida kiberxavfsizlik masalalarining dolzarb jihatlari tahlil qilinadi. So‘nggi yillarda IoT qurilmalari sonining jadal o‘sishi bilan birga, ularni nishonga oluvchi kiberxavf va tahdidlar murakkablashib bormoqda. Tadqiqotda IoT va OT tizimlaridagi asosiy zaiflik turlari, jumladan zaif autentifikatsiya, shifrlanmagan aloqa kanallari, firmware bilan bog‘liq muammolar hamda ta’minot zanjiri (supply chain) zaifliklari ko‘rib chiqilgan. Shuningdek, botnetlar, DDoS hujumlari, ransomware va sun’iy intellekt bilan kuchaygan tahdidlarning zamonaviy tendensiyalari tahlil qilingan.Maqolada xalqaro tajriba va standartlar asosida IoT xavfsizligini ta’minlashning samarali mexanizmlari, xususan secure-by-design tamoyili, Zero Trust arxitekturasi, ko‘p qatlamli himoya yondashuvi hamda sun’iy intellekt asosidagi monitoring tizimlari muhokama etiladi. O‘zbekiston sharoitida IoT loyihalarining milliy raqamli infratuzilma xavfsizligiga ta’siri baholanib, mavjud normativ-huquqiy baza va amaliy choralar tahlil qilinadi. Tadqiqot natijalari IoT tizimlarida kompleks va tizimli kiberxavfsizlik choralarini joriy etish zarurligini ko‘rsatadi.

**Kalit so‘zlar:** Internet of Things (IoT), IoT kiberxavfsizligi, Operational Technology (OT), IIoT, botnet, DDoS hujumlari, ransomware, sun’iy intellekt, supply chain zaifliklari, secure-by-design, Zero Trust arxitekturasi, kiberxavfsizlik standartlari, milliy raqamli infratuzilma, O‘zbekiston.

Bugungi kunda Internet of Things (IoT) — qurilmalar internet orqali bir-biriga ulanib, ma'lumot almashadigan tizim bo'lib, aqlli shaharlar, tibbiyot, uy xo'jaligi va transport sohasida keng qo'llanilmoqda.2025-yilda dunyo miqyosida IoT qurilmalari soni sezilarli darajada oshgan bo‘lib, yaqin yillarda ularning global miqdori yanada jadal o‘sishi kutilmoqda.Biroq, qurilmalar sonining o'sishi bilan birga kiberxavfsizlik xatarlari ham keskin ko'paymoqda: zaif autentifikatsiya, shifrlanmagan aloqa, eskirgan dasturiy ta'minot va "insecurity-by-design" muammolari tufayli botnet hujumlari, ma'lumot o'g'irlash va infratuzilmani buzish holatlari ko'paygan. Ushbu maqola IoT tizimlaridagi asosiy xatarlarni, ularning sabablarini va samarali himoya choralarini tahlil qiladi.

IoT texnologiyalari sanoat avtomatizatsiyasi, aqlli shaharlar, tibbiyot, transport va uy xo'jaligi sohalarida fundamental o'zgarishlarni keltirib chiqarmoqda.IoT Analytics ma’lumotlariga ko‘ra, so‘nggi yillarda global miqyosda ulangan IoT qurilmalari soni barqaror o‘sish sur’atini namoyon etmoqda. Tahlillar ushbu o‘sish tendensiyasi yaqin yillarda ham davom etishini ko‘rsatmoqda.Ushbu o'sish IoT qurilmalarining cheklangan hisoblash resurslari (xotira, protsessor quvvati, energiya sarfi) va ko'pincha “insecurity-by-design” tamoyiliga asoslangan loyihalash jarayonlari bilan birga kiberxavfsizlik sohasida jiddiy muammolarni keltirib chiqarmoqda.




1-rasm. IoT tizimi xavfsizligini oshirish uchun mashinani o‘qitish algoritmlaridan foydalanish

Olib borilgan tadqiqotlardan olingan tahlillarga ko'ra, IoT qurilmalariga qaratilgan hujumlar soni 13,6 milliarddan oshgan, kunlik o'rtacha hujumlar esa 820 mingdan yuqori bo'lgan. Ushbu ko'rsatkich o'tgan yilga nisbatan sezilarli o'sishni ko'rsatadi. Cloudflare hisobotida qayd etilishicha, 2025-yilda Mirai botnetining yangi variantlari orqali 22,2 Tbps quvvatdagi rekord DDoS hujumi sodir bo'lgan. Nozomi Networks ma'lumotlariga ko'ra, OT (Operational Technology) protokollariga (Modbus, Ethernet/IP, BACnet) qaratilgan hujumlar 84% ga oshgan, ransomware hujumlari esa OT tizimlarida 46% ga ko'paygan. Ushbu tendentsiyalar IoT va OT tizimlarining bir-biriga integratsiyalashuvi (IIoT) natijasida yuzaga kelmoqda.

O'zbekiston Respublikasida “Raqamli O'zbekiston-2030” strategiyasi doirasida IoT texnologiyalari jadal joriy etilmoqda: aqlli shahar loyihalari, transport monitoringi, aqlli energiya tarmoqlari va 5G infratuzilmasi faol rivojlanmoqda. Biroq, UZCERT ma'lumotlariga ko'ra, 2025-yilda mamlakatda kibertahdidlar soni oshgan, xususan IoT va 5G qurilmalariga qaratilgan hujumlar asosiy yo'nalishlardan biri hisoblanadi. Ko'pgina IoT qurilmalari hali ham zaif autentifikatsiya, eskirgan firmware va shifrlanmagan aloqa kabi muammolarga ega.

Mavjud ilmiy adabiyotlarda IoT kiberxavfsizligi masalalari keng yoritilgan bo‘lsa-da, so‘nggi yillarda shakllanayotgan yangi tahdid tendensiyalari yetarli darajada tizimli tahlil qilinmagan. Xususan, sun’iy intellekt bilan kuchaygan hujumlar, ta’minot zanjiri bilan bog‘liq zaifliklar hamda IoT va OT tizimlari kesishmasida yuzaga kelayotgan murakkab tahdidlar alohida chuqur tadqiqotni talab qiladi. Shu bilan birga, O‘zbekiston sharoitida IoT loyihalarining milliy xavfsizlikka ta’siri va himoya choralarining amaliy samaradorligini tizimli o‘rganish dolzarb ilmiy masalalardan biri bo‘lib qolmoqda.

Tadqiqot ishida asosan IoT tizimlaridagi kiberxavfsizlik zaifliklarini tizimli tahlil qilish, kuzatilgan eng dolzarb tahdidlarni aniqlash va samarali himoya strategiyalarini taklif etilgan. Bunga ko‘ra tadqiqotning asosiy vazifalari quyidagilar:

- IoT va OT tizimlaridagi asosiy zaiflik turlarini tasniflash va ularning statistik ko'rsatkichlarini keltirish;
- Real hujum misollari (BADBOX 2.0, Mirai variantlari, OT ransomware) va ularning oqibatlarini tahlil qilish;
- Xalqaro standartlar (ETSI EN 303 645, IEC 62443, ISO/IEC 27400) va O'zbekiston qonunchiligiga asoslangan himoya choralarini baholash;

O'zbekistonning raqamli infratuzilmasini himoya qilish bo'yicha amaliy tavsiyalar ishlab chiqish. Maqola quyidagi tuzilishga ega: birinchi bo'limda IoT kiberxavfsizligining nazariy asoslari va dolzarb zaifliklar tasnifi beriladi; ikkinchi bo'limda 2025–2026 yillarda kuzatilgan real hujumlar va statistika tahlil qilinadi; uchinchi bo'limda himoya mexanizmlari va standartlar ko'rib chiqiladi; xulosada umumiy natijalar va istiqbollar bayon etiladi. IoT qurilmalari o‘ziga xos texnik cheklovlarga ega: kichik xotira hajmi, zaif protsessor va batareya quvvati. Bu xususiyatlar ularni an’anaviy kompyuter va serverlardan tubdan farq qiladi. Shu bilan birga, ko‘plab qurilmalar loyihalash bosqichida xavfsizlikni ikkinchi darajali masalaga aylantiradi – “insecurity-by-design” deb ataluvchi yondashuv. Natijada, 2025–2026 yillarda IoT qurilmalariga qaratilgan hujumlar soni va murakkabligi rekord darajaga chiqdi. Eng keng tarqalgan va eng xavfli zaifliklardan biri – zaif autentifikatsiya va standart (default) parollar. Ko‘pgina qurilmalar zavoddan “admin/admin”, “12345” yoki shunga o‘xshash oddiy parollar bilan chiqadi. Palo Alto Networks 2025-yil hisobotiga ko‘ra, korporativ tarmoqlarda IoT qurilmalaridan keladigan ulanishlarning deyarli yarmi (48,2%) yuqori xavf darajasiga ega. Brute-force va dictionary hujumlari soni esa 3,48 milliardga yetgan. Bu holat ochiq internetga ulangan qurilmalarda ayniqsa xavfli, chunki Telnet yoki SSH protokollari faol bo‘lib, botnet tashkil etish uchun asosiy kirish nuqtasi bo‘lib qolmoqda.

Yana bir muhim muammo – aloqa kanallarining shifrlanmagan yoki zaif shifrlanganligi. Ko‘p qurilmalar hali ham HTTP protokolidan foydalanadi yoki TLS 1.2 dan eski versiyalarni ishlatadi. Natijada man-in-the-middle (MitM) hujumlari osonlashadi. Bitdefender 2025 IoT hisobotida qayd etilishicha, hujumlarning 1,35% to‘g‘ridan-to‘g‘ri ochiq aloqa orqali sodir bo‘lgan. Bu esa aqlli kameralar tasvirlari, tibbiy sensorlar ma’lumotlari yoki uy qurilmalari telemetriyasini o‘g‘irlashga olib keladi. Firmware bilan bog‘liq muammolar ham juda katta. Nozomi Networks ma’lumotlariga ko‘ra, IoT buzilishlarining 60% dan ortig‘i aynan eskirgan yoki yangilanmagan firmware zaifliklaridan kelib chiqadi. Ko‘pgina qurilmalar OTA (Over-The-Air) yangilanishni qo‘llab-quvvatlamaydi yoki foydalanuvchilar bu jarayonni e’tiborsiz qoldiradi. 2025–2026 yillarda eng ko‘p ekspluatatsiya qilingan zaifliklar orasida Use After Free (CWE-416) turidagi xatolar va Siemens, Hanwha Vision, Cisco qurilmalariga ta’sir qiluvchi bir qancha CVE’lar bor edi. Cheklangan resurslar tufayli kuchli kriptografik algoritmlarni ishlatish qiyinlashadi. Kichik qurilmalarda AES-256 yoki murakkab autentifikatsiya mexanizmlarini qo‘llash o‘rniga zaif yoki umuman shifrlashsiz aloqa ishlatiladi. Forescout 2025 hisobotida IoT qurilmalariga qaratilgan ekspluatatsiya holatlari 19% ga oshgani qayd etilgan.

Alohida e’tibor berish kerak bo‘lgan soha – supply chain zaifliklari. Qurilmalar ishlab chiqarish yoki yetkazib berish jarayonida buzilishi mumkin. 2025-yilda

BADBOX 2.0 botneti orqali 10 milliondan ortiq Android asosidagi IoT qurilmalari (TV boxlar, projektorlar, infotainment tizimlari) zavodda virus bilan jihozlangan holda sotilgan. Bunday hujumlar hujumchiga darhol kirish imkonini beradi va millionlab qurilmani residential proxy yoki ad-fraud tarmoqlariga aylantiradi.

Masshtabli botnetlar va DDoS hujumlari ham IoT ekotizimining eng og‘riqli nuqtalaridan biri. Mirai va uning yangi variantlari (Aisuru/TurboMirai, Kimwolf, Murdoc) 2025–2026 yillarda faol bo‘lib qoldi. Aisuru botneti 29,7 Tbps rekord DDoS hujumini amalga oshirgan. Botnetlar asosan routerlar, IP-kameralar va IoT sensorlaridan tashkil topgan. Oxirgi yillarda AI bilan kuchaygan hujumlar va OT/IoT chegarasidagi tahdidlar alohida e’tiborga loyiq. Jahon iqtisodiy forumi hisobotlarida sun’iy intellekt bilan bog‘liq zaifliklar eng tez rivojlanayotgan tahdid yo‘nalishlaridan biri sifatida qayd etilgan. Shu bilan birga, sanoat (OT) tizimlariga qaratilgan ransomware hujumlari ham sezilarli darajada oshgan bo‘lib, asosiy sanoat protokollariga nisbatan hujumlar ko‘lami kengayib bormoqda.O‘zbekiston kontekstida bu zaifliklar “Raqamli O‘zbekiston-2030” strategiyasi doirasida joriy etilayotgan aqlli shaharlar, transport monitoringi, energiya tarmoqlari va 5G loyihalari uchun jiddiy xavf tug‘diradi. UZCERT ma’lumotlariga ko‘ra, 2025-yilda mamlakatda kibertahdidlar soni oshgan, xususan IoT va 5G qurilmalariga qaratilgan hujumlar asosiy yo‘nalishlardan biri bo‘lgan.

IoT tizimlaridagi zaifliklarni bartaraf etish uchun ko‘p qatlamli yondashuv (defense-in-depth) zarur. Bu yondashuv qurilma loyihalash bosqichidan tortib, foydalanuvchi darajasidagi oddiy choralar va davlat siyosatigacha bo‘lgan barcha darajalarni qamrab oladi. 2025–2026 yillarda xalqaro tajriba va hisobotlar (ETSI, IEC, Nozomi Networks, NIST) asosida eng samarali choralar quyidagilardan iborat. Avvalo, qurilma loyihalash bosqichidan xavfsizlikni birinchi o‘ringa qo‘yish kerak – bu secure-by-design tamoyili. ETSI EN 303 645 standarti IoT qurilmalari uchun minimal xavfsizlik talablarini belgilab bergan bo‘lib, u default parollarni taqiqlash, kuchli autentifikatsiyani majburiy qilish va OTA yangilanishlarini qo‘llab-quvvatlashni talab etadi. Ushbu standartni qo‘llash zaifliklar sonini 50% gacha kamaytirishi mumkin. O‘zbekistonda “Raqamli O‘zbekiston-2030” dasturi va “Kiberxavfsizlik to‘g‘risida”gi qonun doirasida bunday talablarni majburiy joriy etish mumkin – masalan, davlat buyurtmasi bilan sotib olinadigan IoT qurilmalariga ETSI yoki IEC 62443 standartlariga moslik sertifikatini talab qilish orqali. Ikkinchi muhim qadam autentifikatsiya va avtorizatsiyani mustahkamlash. Default parollarni majburiy o‘zgartirish va ko‘p faktorli autentifikatsiya (MFA yoki 2FA) joriy etish brute-force hujumlarini 90% gacha kamaytiradi. X.509 sertifikatlari yoki token asosidagi autentifikatsiya mexanizmlari kichik qurilmalar uchun ham samarali bo‘lib, ularni joriy etish orqali qurilma botnetga qo‘shilish ehtimoli keskin pasayadi. Aloqa kanallarini himoya qilish ham markaziy o‘rin tutadi. TLS 1.3 yoki DTLS protokollari, AES-256 yoki ChaCha20 algoritmlari va end-to-end shifrlashni qo‘llash man-in-the-middle hujumlarini 80% gacha kamaytiradi. Bu chorani joriy etish aqlli kameralar, tibbiy sensorlar va transport monitoring tizimlarida shaxsiy ma’lumotlar o‘g‘irlanishining oldini oladi. Tarmoq darajasida segmentatsiya va monitoring zarur. IoT qurilmalarini alohida VLAN yoki subnetga joylashtirish, firewall va IDS/IPS tizimlarini o‘rnatish, Zero Trust arxitekturasini qo‘llash ichki tarqalishni 70% gacha bloklaydi. Nozomi

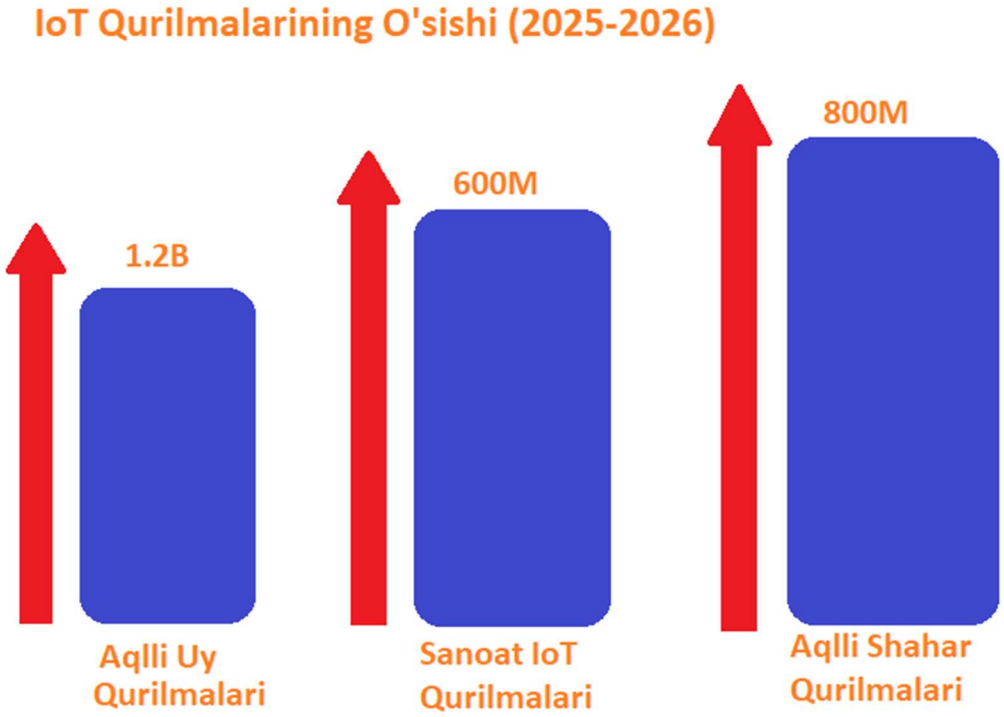
Networks yoki shunga o‘xshash AI asosidagi monitoring tizimlari anomaliyalarni real vaqtda aniqlab, yangi hujumlarni oldindan sezishga yordam beradi.Firmware va dasturiy ta’minotni doimiy yangilab turish – eng oddiy, lekin eng samarali choralaridan biri. Imzo qo‘yilgan OTA yangilanishlarini majburiy qilish va rollback imkoniyatini ta’minlash firmware zaifliklarini 60% gacha kamaytiradi. Foydalanuvchilar uchun bu jarayonni avtomatiklashtirish va eslatmalar yuborish zarur.

AI va mashinaviy o‘rganishdan foydalanish yangi avlod tahdidlarga qarshi samarali qurol bo‘lib chiqmoqda. Xatti-harakat tahlili orqali anomaliyalarni aniqlash AI bilan kuchaygan reconnaissance va moslashuvchan exploitlarni 50% gacha oldindan sezishga imkon beradi.

O‘zbekiston sharoitida bu choralar quyidagi tarzda amalga oshirilishi mumkin:

- Davlat loyihalarida (aqlli shaharlar, transport monitoringi) xalqaro standartlarni majburiy qilish va sertifikatsiya tizimini joriy etish
- UZCERT va Kiberxavfsizlik markazi orqali IoT qurilmalarini muntazam audit qilish va zaifliklar bazasini yuritish
- Cyber University va boshqa ta’lim muassasalarida IoT xavfsizligi bo‘yicha maxsus dasturlarni kengaytirish (2025–2026 yillarda 1200+ mutaxassis tayyorlash rejalashtirilgan)
- Foydalanuvchilar uchun ommaviy ogohlantirish kampaniyalarini o‘tkazish: default parollarni o‘zgartirish, firmware yangilash va xavfsiz tarmoq sozlamalari haqida oddiy qo‘llanmalar tarqatish

Ushbu choralar majmui joriy etilsa, IoT qurilmalariga qaratilgan hujumlar soni sezilarli darajada kamayadi va milliy raqamli infratuzilma xavfsizligi mustahkamlanadi.



2-rasm. IoT Qurilmalarining O’sishi

2025–2026 yillar IoT tizimlari uchun hal qiluvchi bosqich bo‘ldi: qurilmalar soni 21 milliarddan 25 milliardga yetdi, ammo hujumlar soni va murakkabligi ham rekord darajaga chiqdi. Kunlik 820 mingdan ortiq hujum, 22,2 Tbps DDoS rekordi, AI bilan kuchaygan botnetlar va OT tizimlariga qaratilgan ransomware tahdidlari IoT nafaqat imkoniyat, balki jiddiy xavf manbaiga aylanganini ko‘rsatmoqda.Biroq, secure-by-design tamoyili, Zero Trust arxitekturasi, AI monitoring va qonunchilik choralarini birgalikda qo‘llash orqali ko‘p tahdidlarni oldini olish mumkin. O‘zbekiston uchun bu sohada xalqaro tajribani o‘rganish, mutaxassislar tayyorlash va majburiy standartlarni joriy etish strategik ahamiyatga ega. Aks holda, “Raqamli O‘zbekiston-2030” doirasidagi aqlli shaharlar, transport va energiya loyihalari katta xavf ostida qolishi mumkin.

Kelajakda IoT xavfsizligi nafaqat texnik masala, balki milliy xavfsizlikning ajralmas qismiga aylanadi. Bugundan boshlab choralar ko‘rish – bu nafaqat texnologiyani himoya qilish, balki raqamli kelajakni xavfsiz qurish demakdir.

## Foydalanilgan adabiyotlar


1. Alimuhamedov A.A. Axborot xavfsizligi asoslari. – Toshkent: Fan va texnologiya, 2021.
2.Qodirov D.X. Kompyuter tarmoqlari va ularning xavfsizligi. – Toshkent: O‘zbekiston Milliy Ensiklopediyasi, 2020.
3.Haydarov S.S. Sun’iy intellekt va IoT tizimlari. – Toshkent: Akademnashr, 2021.
4.O‘zbekiston Respublikasi Prezidenti. “Raqamli O‘zbekiston – 2030” strategiyasi to‘g‘risidagi Farmon. – Toshkent, 2020.
5.O‘zbekiston Respublikasi Kiberxavfsizlik markazi (UZCERT). O‘zbekiston Respublikasida kiberxavfsizlik holati bo‘yicha yillik hisobot. – Toshkent, 2025.
6.ISO/IEC 30141:2018. Internet of Things (IoT) – Reference Architecture. – Geneva: ISO/IEC, 2018.
7.ISO/IEC 27400:2022. Cybersecurity — IoT Security and Privacy — Guidelines. – Geneva: ISO, 2022.
8.ETSI EN 303 645 V2.1.1. Cyber Security for Consumer Internet of Things: Baseline Requirements. – ETSI, 2020.
9.Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead // Computer Networks. – 2015.
10.World Economic Forum. Global Cybersecurity Outlook 2026. – Geneva, 2026.


## BULUTLI PLATFORMALAR ASOSIDA TALABALARNING RAQAMLI KOMPETENTLIGINI RIVOJLANTIRISH METODIKASI


**Mamaraimov Abror Kamalidin o‘g’li**