

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

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



KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI
mavzusidagi Xalqaro ilmiy-texnik anjuman materiallari to‘plami
2026-yil 25-26-sentabr

(1-qism)

JIZZAX-2026

Kompyuter ilmlari va muhandislik texnologiyalari. Xalqaro ilmiy-texnik anjuman materiallari to'plami – Jizzax: O'zMU Jizzax filiali, 2026-yil 25-26-sentabr. 507-bet.

Xalqaro miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy kompyuter ilmlari va muhandislik texnologiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globalashuv sharoitida davlatimizni yanada barqaror va jadal sur'atlar bilan rivojlantirish bo'yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e'tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma'ruza tezislari to'plamida mamlakatimiz va xorijlik turli yo'nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o'qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarining ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mas'ul muharrirlar: DSc.prof. Turakulov O.X., t.f.n., dots. Baboyev A.M.

Tahrir hay'ati a'zolari: p.f.d.(DSc), prof. Turakulov O.X., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), prof. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Aliqulov S.T., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dots. Alibayev S.X., t.f.f.d.(PhD), dots. Abdumalikov A.A., p.f.f.d.(PhD) Hafizov E.A., f.f.f.d.(PhD) dots., Norbekova B.Sh. p.f.f.d.(PhD) dots. Sindorov L.K., t.f.f.d.(PhD), dots. Nasirov B.U., b.f.f.d. (PhD) O'ralov A.I., p.f.n., dots. Aliqulov S.T., t.f.f.d.(PhD) Kuvandikov J.T., i.f.n., dots. Tsoy M.P., Sharipova S.F., Jo'rayev M.M.

Mazkur to'plamga kiritilgan ma'ruza tezislarining mazmuni, undagi statistik ma'lumotlar va me'yoriy hujjatlarning to'g'riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o'zlari mas'uldirlar.

12. Pen-Mouratov, S., Shukurov, N., and Steinberger, Y. Soil free-living nematodes as indicators of both industrial pollution and grazing activity in Central Asia", J. Ecological Indicators, 10 (2010) 955-967. <https://doi.org/10.1016/j.ecolind.2010.02.005>
13. Shukurov, N., Kodirov, O., Peitzsch, M., Kersten, M., Pen-Mouratov, S., Steinberger, Y. Coupling geochemical, mineralogical and microbiological approaches to assess the health of contaminated soil around the Almalyk mining and smelter complex, Uzbekistan. J. Science of the Total Environment. 2014, 476-477:447-459. <https://doi.org/10.1016/j.scitotenv.2014.01.031>
14. Pen-Mouratov, S., Shukurov, N., Rhakhmonkulova, Sh., Kodirov, O., Yua, J., Barness G., Kersten, M., Steinberger, Y. Successive development of soil ecosystems at abandoned coal-ash landfills. Ecotoxicology. 2014. <https://doi.org/10.1007/s10646-014-1227-5>
15. Bandowe, B.A.M., Shukurov, N., Leimer, S. Kersten M., Steinberger Y., Wilcke W. Polycyclic aromatic hydrocarbons (PAHs) in soils of an industrial area in semi-arid Uzbekistan: spatial distribution, relationship with trace metals and risk assessment. Environ Geochem Health. 2021, 43, 4847-4861. <https://doi.org/10.1007/s10653-021-00974-3>

BUYUMLAR INTERNETI TIZIMLARIGA BO‘LADIGAN TAHDIDLAR VA KIBERHUJUMLARNI ANIQLASH MUAMMOLARI

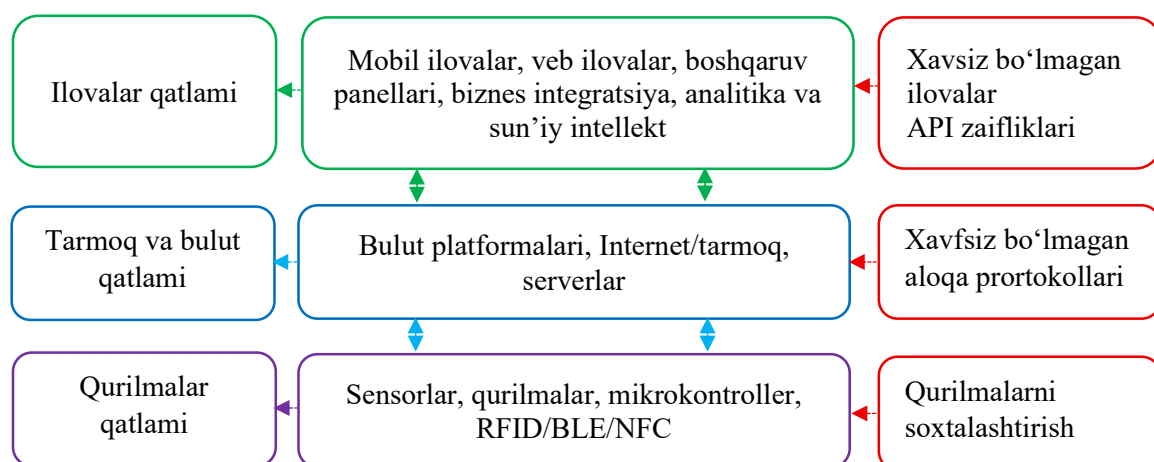
*Phd, dots. Kadirov Mir-Xusan Mirpulatovich,
Zokirova Feruza Ravshanovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti
mirhusank@gmail.com*

Annotatsiya. Ushbu maqolada Buyumlar interneti (Internet of Things) tizimlari, ularning zamonaviy raqamli infratuzilmalardagi o‘rni hamda IoT ekotizimlariga nisbatan yuzaga kelayotgan kiberxavfsizlik tahdidlari tahlil qilingan. IoT qurilmalarining arxitekturasini, ulardagi aloqa kanallari va apparat-dasturiy komponentlarda uchraydigan asosiy zaifliklar, jumladan, xizmat ko‘rsatishni rad etish, ortiqcha yuklanish, xotira bilan bog‘liq zaifliklar, imtiyozlarni oshirish hamda kodni masofadan bajarish bilan bog‘liq tahdidlar tahlil qilingan.

Kalit so‘zlar: Buyumlar interneti (IoT), IoT kiberxavfsizligi, IoV, IoMT, IIoT, kiberhujumlar, xavfsizlik zaifliklari, IoT botnet.

Hozirgi jamiyatimizning optimallashtirilgan xizmatlarga bo‘lgan talabi aqlli shaharlarda sensorlar va buyruqlarni amalga oshirish mexanizmlarini joylashtirishni talab qiladi. Bunday qurilmalar turli sohalarda ma’lumotlarni chuqur tahlil qilish orqali yechimlarni taqdim etish uchun hisoblash resurslaridan foydalanish imkonini beradi [1]. Buyumlar interneti tarmoq kontsepsiyasi bo‘lib, unda jismoniy qurilmalar (buyumlar) sensorlar, dasturiy ta’minot va aloqa vositalari bilan

jihozlangan. Buyumlar interneti xayotimizning ajralmas qismiga aylangani uchun ularga nisbatan tahdidlar soni ham paralell ortib bormoqda. Yovuz niyatli foydalanuvchilar IoT tarmoqdagi aloqada va qurilmalarning xususiyatlarida zaifliklarni ko'rsatish mumkin. Hozirgi kunda buyumlar interneti bir nechta sohalarda, jumladan, transport vositalari interneti (IoV), tibbiy buyumlar interneti (IoMT) va sanoat buyumlari interneti (IIoT) da keng qo'llanilmoqda [2, 3]. Hozirgi kunda IoT IoV, IoMT, IIoT tizimlariga kiberhujumlar soni ortib bormoqda. 1-rasmda IoT arhitekturasini va tizimlariga bo'ladigan tahdidlar ko'rsatilgan.

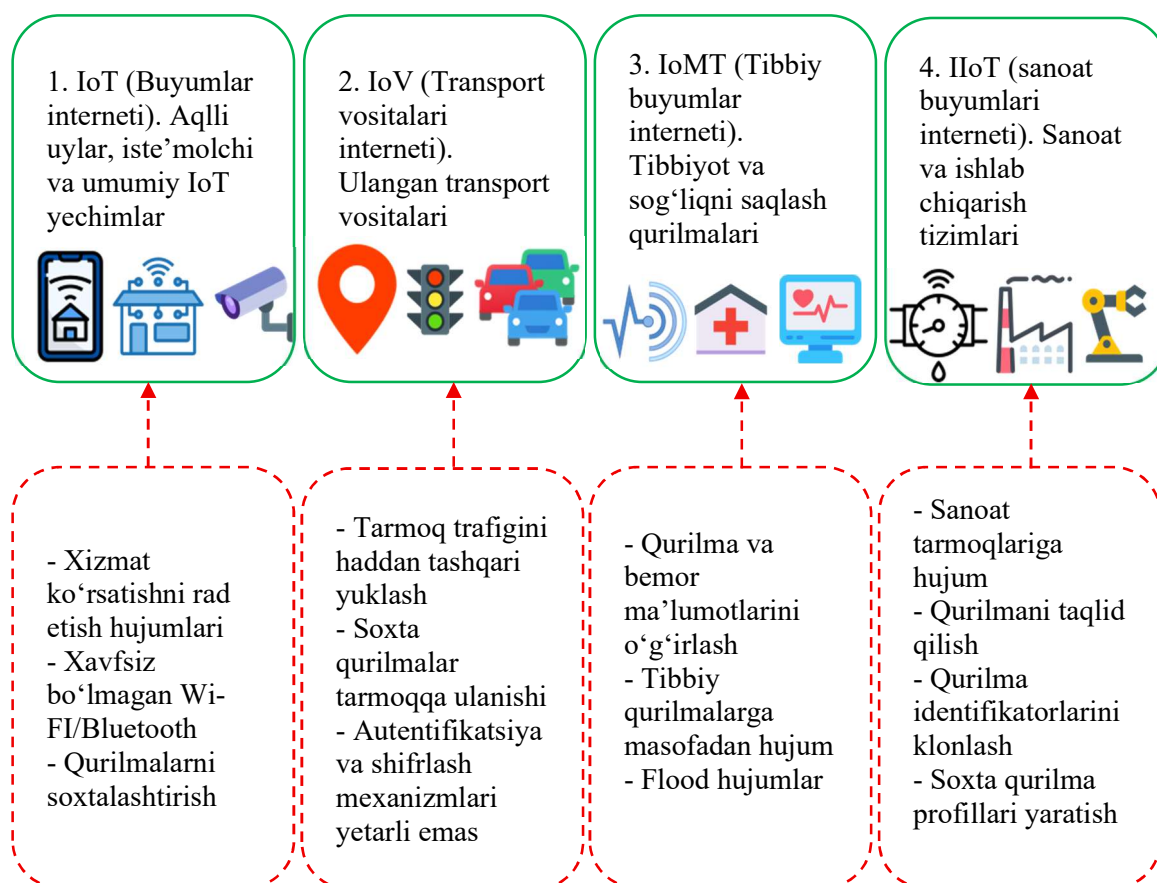


1-rasm. IoT arhitekturasini va tizimlariga bo'ladigan tahdidlar

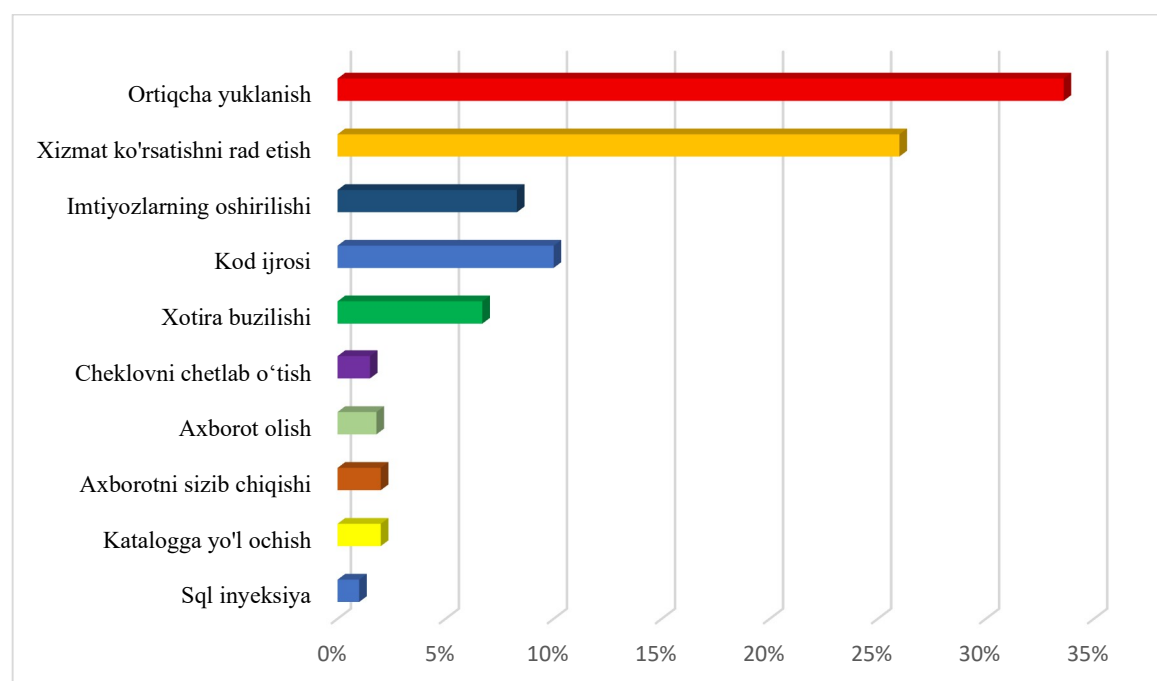
Hujumchilar foydalanishi mumkin bo'lgan sohalarga kelsak, IoT tarmoqdagi aloqada va qurilmalarning xususiyatlarida zaifliklarni taqdim etadi. 2-rasmda IoT, IoV, IoMT, IIoT tizimlarida qo'llaniladigan qurilmalar va ularga bo'ladigan zaifliklar keltirilgan.

IoT Analytics GmbH tashkilotining statistikasiga ko'ra 2025-yilda ulangan IoT qurilmalarining soni butun dunyo bo'ylab 21.1 milliardga yetgan [4]. Bu o'z navbatida buyumlar internetiga bo'ladigan hujumlarni oshishiga olib kelgan. O'tkazilgan tahlillarga ko'ra [5, 6, 7], yovuzli niyatli foydalanuvchilar tomonidan qurilma barqarorligini buzishni yoki asosiy xotira kamchiliklaridan foydalanish orqali xizmat ko'rsatishni rad etish va ortiqcha yuklanishni hosil qiladigan zaifliklardan keng foydalanilgan. Imtiyozni oshirish va kod orqali amalga oshirish zaifliklari nisbatan kamroq bo'lsa-da, ular ta'siri kattaroq, chunki ular buzilgan qurilmalar ustudan to'liq nazoratni beradi.

O'tkazilgan tahlillar shuni ko'rsatadiki, IoT ekotizmlari bo'yicha amalga oshirilayotgan kiberhujumlar nomutanosibligini ko'rsatadi, bunda qurilmalarning murakkabligi ularning xavfsizlik zaifliklariga duchor bo'lish ehtimolini sezilarli darajada oshiradi. 3-rasmda 2025 yilda IoT ekotizimlariga nisbatan bo'lgan zaifliklar keltirilgan.



2-rasm. IoT, IoV, IoMT, IIoT tizimlarida qo'llaniladigan qurilmalar va ularga bo'ladigan zaifliklar



3-rasm. IoT ekotizimlariga nisbatan bo'lgan zaifliklar

IoT botnet hujumlari va avtomatlashtirilgan skanerlashlar keskin oshgan. Transport sektori 2025 yil davomida eng ko'p hujumga uchragan soha bo'ldi.

Tibbiyot va sog‘liqni saqlash sektori IoT qurilmalariga qaratilgan hujumlar eng tez o‘sayotgan yo‘nalishlardan biri sifatida qayd etilgan.

O‘tkazilgan tahlillar shuni ko‘rsatdiki, IoT texnologiyalarining jadal rivojlanishi va ularning transport, sog‘liqni saqlash, sanoat hamda boshqa muhim sohalarga keng joriy etilishi ushbu tizimlarning kiberxavfsizligini ta‘minlash masalasini dolzarb muammolardan biriga aylantirmoqda. IoT qurilmalarining soni va xilma-xilligi ortib borishi natijasida IoT, IoV, IoMT va IIoT ekotizimlarida mavjud zaifliklardan foydalanishga qaratilgan kiberhujumlar soni ham oshib bormoqda.

Foydalanilgan adabiyotlar ro‘yxati:

[1] Talari S. et al. A review of smart cities based on the internet of things concept //Energies. – 2017. – T. 10. – №. 4. – C. 421.

[2] Gupta B. B., Quamara M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols //Concurrency and computation: Practice and experience. – 2020. – T. 32. – №. 21. – C. e4946.

[3] Alfahaid, A.; Alalwany, E.; Almars, A.M.; Alharbi, F.; Atlam, E.; Mahgoub, I. Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey. Sensors 2025, 25, 3341. <https://doi.org/10.3390/s25113341>

[4] <https://iot-analytics.com/number-connected-iot-devices/>

[5] [https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat %20Landscape%202025_v1.2.pdf](https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf)

[6] https://cdn.prod.website-files.com/645a4534705010e2cb244f50/6995ff8b24e61fc6cce7cd6a_Nozomi-Networks-OT-IoT-Security-Report-2H25.pdf

[7] https://blogapp.bitdefender.com/hotforsecurity/content/files/2025/10/2025_iot_security_report.pdf

NASOS STANSIYALARINING ENERGIYA SAMARADORLIGINI NEYRON TARMOQLAR ASOSIDA OSHIRISH

t.f.d.professor Mamatov Narzillo Solidjonovich

*"TIQXMMI" MTU Raqamli texnologiyalar va Sun'iy intellekt kafedrası
mudiri*

m_narzullo@mail.ru

Axrorov Muhammadjon Shodi o‘g‘li

Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universitetining Jizzax fililali

axrorov0204@gmail.com

Annotatsiya. Mazkur maqolada zamonaviy elektr energetika tizimlarining muhim tarkibiy qismi hisoblangan nasos stansiyalarida energiya resurslaridan samarali foydalanish masalalari yoritilgan. Nasos agregatlarining yuqori miqdorda