

HCS D

**Human capital and social
development.**

2025 – volume 15, issue 3

Inson kapitali va ijtimoiy rivojlanish jurnali.

2025 – 15-jild, 3-son



O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM FAN VA**INNOVATSIYALAR VAZIRLIGI****SHAROF RASHIDOV NOMIDAGI SAMARQAND DAVLAT****UNIVERSITETI****Inson kapitali va ijtimoiy rivojlanish jurnali****Journal Human capital and social development****Журнал Человеческий капитал и социальное развитие****Jurnali****15-jild, 3-son (iyun) 2025.****Jurnal 2021-yilda tashkil topgan.****Davriyligi: har ikki oyda**

Davriy nashirning rasmiy nomi: “Inson kapitali va ijtimoiy rivojlanish”-“Human capital and social development”-“Человеческий капитал и социальное развитие” O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 19.05.2021 sanada berilgan №1179 guvohnomasi bilan ro‘yhatdan o‘tgan.

Junal: O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasi Rayosatining 2023-yil 30-noyabrdagi 342/3-son qarori bilan tasdiqlangan Iqtisodiyot fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) Ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan ilmiy nashrlar ro‘yhatiga kiritilgan.

Jurnal asoschilari: Sharof Rashidov nomidagi Samarqand davlat universiteti Inson resurslari va mahalla tarqqiyotini boshqarish instituti.

Nashr etuvchi: SamDU tahririy-nashriyot bo‘limi.

Xalqaro indeksi: ISSN 3030-3672

Tahririyat telefoni: +998 (94) 283 56 78, +998 (90) 502 13 03

Pochta manzili: 140104, Samarqand shahar., Universitet xiyoboni, 4

Web-sayt: www.hcsd.samdu.uz.

E-mail: muhridinrabbimov@gmail.com

«INSON KAPITALI VA IJTIMOYIY RIVOJLANISH»
«HUMAN CAPITAL AND SOCIAL DEVELOPMENT»
«ЧЕЛОВЕЧЕСКИЙ КАПИТАЛ И СОЦИАЛЬНОЕ РАЗВИТИЕ»
JURNALI

Bosh muharrir: t.f.d., prof. Xalmuradov Rustam Ibragimovich

Bosh muharrir o‘rinbosari: i.f.d., prof. Arabov Nurali Uralovich

Kotib: PhD, dots. Nasimov Ikrom Xusanovich

Texnik muharrir: assistent., Rabbimov Muxriddin Musoqul o‘g‘li

TAHRIRIYAT KENGASHI

O‘zFA akademigi, i.f.d., prof. Abdurahmonov Qalandar Xodjayivech

O‘zFA akademigi, i.f.d., prof. G‘ulomov Saidaxror Saidaxmedovich

DSc, professor Daler Mirpochoyev (Iqtisodiyot va savdo instituti, Tojikiston)

PhD, professor Arindam Banik (Xalqaro menejment instituti, Hindiston)

PhD, professor Jiye Li (Sian Jiatong universiteti, Xitoy Xalq Respublikasi)

PhD, professor Bayong Van Li (Yongnam universiteti, Janubiy Koreya)

PhD, professor Vonyong Li (Yongnam universiteti, Janubiy Koreya)

PhD, professor Yan Patterson (Kvinslend universiteti, Avstraliya)

PhD, dots. Djurakulov Shoxrux Davronovich (SamDU)

i.f.n., dots. Yuldashev Shamsiddin Qiyomiddinovich (SamDU)

i.f.n., dots. Nizamov Axtam Numonovich (SamDU)

i.f.n., dots. Bozorov Berdimurod Ulug‘murodovich (SamDU)

i.f.n., dots. Boboqulov Bahromqul Mamatkulovich (SamDU)

i.f.n., dots. Usmonova Dilafruz Karshiyevna (SamDU)

i.f.n., dots. Alibekova Saodat Lapasovna (SamDU)

PhD, dots. Ulug‘murodova Nodira Berdimuradovna (SamDU)

PhD, dots. Sharifov Shuhrat Saidahmadovich (SamDU)

PhD, dots. Bakayev Ziyovuddin Toshbolta o‘g‘li (SamDU)

PhD, dots. Karjavova Xurshida Abdumalikovna (SamDU)

PhD, dots. Mansurova Nargiza Shamsiddinovna (“Ipak yo‘li” turizm va madaniy meros xalqaro universiteti)

PhD, dots. Djalilov Faxriddin Azimovich (SamDU)

PhD, dots. Boltayev Burxon Sadinovich (SamDU)

PhD, dots. Maxmudova Mohinur Ravshanbekovna (SamDU)

IoT (INTERNET OF THINGS) XAVFSIZLIK MUAMMOLARINI BARTARAF ETISH USULLARI

U.B.Bekmurodov , Z.Q.Ruziyeva 

Oriental universiteti, Samarqand, O'zbekistan.

OPEN ACCESS

HCSD

Correspondence

Bekmurodov Ulug'bek Bahrom o'g'li

Oriental universiteti dotsenti PhD

Email: ulugbek_bekmurodov@mail.ru

Tel: +998 97 912 00 53

Ruziyeva Zulfiya Qurvonovna

Oriental universiteti magistri

Email: ruziyevazulfiya299@gmail.com

Tel: +998 90 281 83 18

Received: 16 May 2025

Revised: 26 May 2025

Accepted: 26 June 2025

Published: 30 June 2025

Funding source for publication:

Samarkand State University.

Publisher's Note: HCSD stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: Journal Human capital and social development © 2 by Samarkand State University is licensed <https://creativecommons.org/licenses/by-nc/4.0/>

Annotatsiya: Mazkur dissertatsiya ishida Internet of Things (IoT) tizimlarida uchraydigan axborot xavfsizligi muammolari chuqur tahlil qilinib, ularni bartaraf etishning zamonaviy usullari ishlab chiqilgan. IoT tizimlarining arxitekturasini, ularning xavfsizlik jihatidan zaif tomonlari, mavjud tahdidlar va himoya mexanizmlari ilmiy asosda yoritilgan. Tadqiqotda ayniqsa kam resursli IoT qurilmalarining shifrlash va autentifikatsiya bilan bog'liq cheklovlarini hisobga olgan holda, samarali xavfsizlik yondashuvlari (shifrlash algoritmlari, anomaliya aniqlash, Zero Trust modeli, edge computing asosidagi yondashuvlar) taklif etilgan. Dissertatsiyada ishlab chiqilgan model va usullar maxsus test muhitida tajriba asosida sinovdan o'tkazilib, ularning samaradorligi amaliy jihatdan baholangan. Ish natijalari IoT infratuzilmalarini yanada ishonchli qilishda qo'llanishi mumkin.

Kalit so'zlar: IoT, narsalar interneti, axborot xavfsizligi, autentifikatsiya, shifrlash, kiberxavfsizlik, anomaliyani aniqlash, edge computing, Zero Trust.

МЕТОДЫ ПРЕОДОЛЕНИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ В IoT (ИНТЕРНЕТЕ ВЕЩЕЙ)

Аннотация: В диссертации представлен глубокий анализ проблем информационной безопасности, возникающих в системах Интернета вещей (IoT), и разработаны современные методы их устранения. Архитектура систем Интернета вещей, уязвимости их безопасности, существующие угрозы и механизмы защиты рассматриваются на научной основе. В исследовании предлагаются эффективные подходы к обеспечению безопасности (алгоритмы шифрования, обнаружение аномалий, модель Zero Trust, подходы на основе периферийных вычислений), особенно с учетом ограничений шифрования и аутентификации устройств Интернета вещей с низкими ресурсами. Разработанные в диссертации модели и методы были экспериментально проверены в специальной тестовой среде, а их эффективность оценена на практике. Результаты работы могут быть использованы для повышения надежности инфраструктур Интернета вещей.

Ключевые слова: IoT, Интернет вещей, информационная безопасность, аутентификация, шифрование, кибербезопасность, обнаружение аномалий, периферийные вычисления, Zero Trust.

METHODS FOR ELIMINATING SECURITY PROBLEMS IN THE IoT (INTERNET OF THINGS)

Abstract: This dissertation work provides a thorough analysis of information security problems encountered in Internet of Things (IoT) systems and develops modern methods for their elimination. The architecture of IoT systems, their security vulnerabilities, existing threats and protection mechanisms are scientifically covered. The study proposes effective security approaches (encryption algorithms, anomaly detection, Zero Trust model, edge computing-based approaches), especially taking into account the limitations of low-resource IoT devices related to encryption and authentication. The models and methods developed in the dissertation were tested experimentally in a special test environment and their effectiveness was evaluated in practice. The results of the work can be used to make IoT infrastructures more reliable.

Keywords: IoT, Internet of Things, information security, authentication, encryption, cybersecurity, anomaly detection, edge computing, Zero Trust.

Kirish.

So‘nggi yillarda raqamli texnologiyalar rivojlanishining yangi bosqichi — narsalar interneti (IoT, Internet of Things) tushunchasi global axborot makonida keng e‘tibor qozonmoqda. Turli qurilmalar, sensorlar, mashinalar va dasturiy tizimlarning internet orqali o‘zaro bog‘lanib ishlashi natijasida ishlab chiqarishdan tortib kundalik hayotgacha bo‘lgan barcha sohalarida IoT texnologiyalari faol joriy qilinmoqda. Jahon miqyosida milliardlab qurilmalarning birlashtirilgan tarmoqlar orqali ishlashi raqamli transformatsiyani tezlashtirishga, samaradorlikni oshirishga hamda real vaqt rejimida monitoring va boshqaruv imkoniyatlariga zamin yaratmoqda. Biroq IoT texnologiyalarining jadal rivojlanishi bilan birga, ularning axborot xavfsizligi masalalari tobora dolzarb bo‘lib bormoqda. IoT qurilmalari o‘zining apparat va dasturiy chegaralanishlari tufayli ko‘plab xavfsizlik zaifliklariga ega. Ularning ko‘pchiligi shifrlash, autentifikatsiya yoki yangilanish tizimlari bilan yetarlicha ta‘minlanmagan bo‘lib, turli xakerlik hujumlariga ochiq bo‘lib qolmoqda. Ayniqsa, markazlashmagan tizimlar, past resursli mikrokontrollerlar va yirik tarmoqli muhitlar mavjud bo‘lgan sharoitda an‘anaviy xavfsizlik yondashuvlari samarasiz hisoblanadi.

Shu sababli, IoT tizimlarida xavfsizlikni ta‘minlash uchun innovatsion, moslashuvchan va samarali yondashuvlarni ishlab chiqish zarurati tug‘ilmoqda. Ushbu dissertatsiyada IoT tizimlarida mavjud bo‘lgan asosiy xavfsizlik tahdidlari aniqlanadi, tahlil qilinadi va ularni bartaraf etishning zamonaviy texnik-uslubiy yechimlari taklif etiladi. Xususan, ma‘lumotlarni himoyalash, tarmoqli tahdidlarni

aniqlash, qurilma darajasidagi xavfsizlikni ta‘minlash kabi yo‘nalishlarda ilg‘or algoritmlar, arxitektura modellar va tajriba asosidagi sinovlar orqali muammoga kompleks yondashuv amalga oshiriladi.

Mavzu bo‘yicha adabiyotlarni tahlili.

So‘nggi yillarda Internet of Things (IoT) texnologiyalarining jadal rivojlanishi axborot almashinuvi, monitoring va avtomatlashtirish jarayonlarini tubdan o‘zgartirdi. IoT yechimlari sanoat, sog‘liqni saqlash, energetika, transport va kundalik hayotda (aqlli uylar, aqlli shaharlar) keng qo‘llanila boshladi. Biroq, mazkur texnologiyaning ommaviylashuvi bilan birga, uning xavfsizlik muammolari ham tobora dolzarb tus olmoqda. Shu bois, ilmiy adabiyotlarda IoT xavfsizlik muammolari va ularni bartaraf etish mexanizmlari bo‘yicha ko‘plab tadqiqotlar olib borilgan.

IoT xavfsizligi sohasidagi klassik nazariy manbalar, xususan Kevin Ashton (2009) tomonidan IoT atamasining birinchi bor ilmiy muomalaga kiritilishi, shuningdek, Gubbi va boshqalar (2013) tomonidan IoT arxitekturasining qatlamli modeli (perception, network, application layers) asosida tahlili, bu boradagi asosiy konseptual asoslarni belgilab berdi. Ushbu ishlarda IoT tizimlarida millionlab qurilmalar o‘zaro ulanib, real vaqt rejimida ma‘lumot uzatishi natijasida yuzaga keladigan xavfsizlik ehtiyojlari ilgari surilgan.

Xavfsizlik muammolari haqida olib borilgan adabiyotlar tahlilida Roman, Zhou va Lopez, Sicari va boshqalar kabi olimlar asarlari alohida o‘rin tutadi. Ular IoT qurilmalarida keng tarqalgan zaifliklar — identifikatsiya va autentifikatsiya mexanizmlarining

zaifligi, firmware yangilanishlarining yetishmasligi, ma'lumotlar shifrlanishining kamligi va botnet hujumlar (Mirai kabi)ning keng ko'lamli tahdidlari haqida so'z yuritgan. Ayniqsa, IoT qurilmalarning past energiya sarfi va kam hisoblash quvvatiga ega bo'li ularni an'anaviy xavfsizlik protokollarini qo'llashdan mahrum qilmoqda.

Ushbu muammolarni bartaraf etishga doir ilmiy adabiyotlar orasida Granjal, Monteiro va Silvaning "Secure communication for IoT" asari, Novoning "Blockchain-based distributed access control" tadqiqoti e'tiborga loyiqdir. Ular IoT xavfsizligini ta'minlashda blokcheyn texnologiyasidan foydalanish, lightweight (yengil) kriptografik algoritmlarni joriy etish, edge computing asosida markazlashtirilmagan xavfsizlikni tashkil etish kabi zamonaviy yondashuvlarni asoslab bergan.

Shuningdek, NIST SP 800-183 va ISO/IEC 30141 kabi xalqaro standartlar IoT xavfsizligini ta'minlash uchun qatlamli yondashuv, xavfsiz identifikatsiya, moslashuvchan ruxsatnomalar va uzluksiz monitoring kabi amaliy tavsiyalarni ilgari suradi. OWASP IoT Top 10 loyihasida esa eng keng tarqalgan o'nta xavfsizlik muammosi (standart parollar, zaif autentifikatsiya, shifrlanmagan ma'lumotlar uzatish, noto'g'ri API integratsiyalari va boshqalar) ko'rsatilgan va ular uchun bartaraf etish strategiyalari ishlab chiqilgan.

Tadqiqot metodologiyasi.

Mazkur tadqiqotning asosiy maqsadi – zamonaviy raqamli muhitda Internet of Things (IoT) tizimlarining axborot xavfsizligiga tahdid soluvchi muammolarni tahlil qilish hamda ularni bartaraf etishning innovatsion texnologik va texnik-uslubiy yechimlarini ishlab

chiqishdan iborat. Tadqiqotning metodologik asosi sifatida ilmiy tahlil, sistemali yondashuv, modellash, eksperimental sinov, solishtirma tahlil va ekspert baholash kabi metodlardan foydalanilgan.

Tahlil va natijalar.

Zamonaviy raqamli iqtisodiyot sharoitida Internet of Things (IoT) texnologiyalari hayotimizning turli sohalariga chuqur kirib bormoqda. Tibbiyot, transport, sanoat avtomatikasi, energetika, agrar soha va "aqlli uy" tizimlari bu boradagi eng dolzarb yo'nalishlardir. Shu bilan birga, ushbu texnologiyalar xavfsizlik bo'yicha jiddiy tahdidlarni keltirib chiqarmoqda. Bu tahdidlarning manbai IoT qurilmalarning texnik va funksional xususiyatlari, ulardagi xavfsizlik protokollarining yetarlicha shakllanmaganligi va murakkab hujum vektorlariga nisbatan himoyasizlik bilan bog'liq.

IoT qurilmalar, odatda, kichik quvvatli protsessorlar, cheklangan tezkor va doimiy xotiraga ega. Shu sababli, ularni zamonaviy kriptografik algoritmlar (masalan, RSA, AES-256) bilan himoyalash texnik jihatdan murakkab hisoblanadi. Resurs tanqisligi muhitida yengil kriptografik yechimlar talab etiladi, biroq ular ko'p hollarda tahdidlar oldida zaif bo'ladi.

IoT tizimlarida qurilmalar ko'pincha tarmoqqa avtomatik ulanadi va doimiy identifikatsiyadan o'tmaydi. Bu esa "man-in-the-middle" (oraliq uzilish), "spoofing" (qurilmani soxtalashtirish) va "replay" (takrorlab uzatish) kabi hujumlar uchun ochiq eshik bo'lib xizmat qiladi. Xususan, O'zbekiston hududida amalda foydalanilayotgan uy-ro'zg'or uchun mo'ljallangan IoT qurilmalarining 60% dan ortig'i zavod sozlamalaridagi oddiy foydalanuvchi parollarini

o'zgartirmasdan ishlatilayotgani kuzatilgan.

IoT sohasida xalqaro miqyosda yagona xavfsizlik standartlari mavjud emas. Har bir ishlab chiqaruvchi o'z tizimi asosida xavfsizlik siyosatini tuzadi, natijada IoT ekotizimida fragmentatsiyalashgan (bo'lingan) xavfsizlik muhiti yuzaga keladi. Bu esa global xavfsizlikni muvofiqlashtirishni qiyinlashtiradi. Masalan, MQTT yoki CoAP kabi yengil protokollar tezkor ma'lumot almashinuvi uchun qulay bo'lsa-da, ularning aksariyati end-to-end shifrlashni o'z ichiga olmaydi.

Ko'plab foydalanuvchilar IoT qurilmalarning xavfsizlik jihatlarini ikkinchi darajali deb hisoblab, asosan ularning funktsionalligiga urg'u berishadi.

Bu esa xavfsizlik sozlamalarini faollashtirmaslik, doimiy yangilanishlarni o'rnatmaslik, ishonchsiz Wi-Fi tarmoqlardan foydalanish singari xavfli holatlarga olib keladi. O'zbekiston hududidagi dastlabki kuzatuvlarda, IoT foydalanuvchilarining atigi 25–30% qismi xavfsizlik siyosatlarini bilishi aniqlangan.

IoT qurilmalar orasida himoyasiz tarmoq tugunlarining mavjudligi ularni yirik botnet tarmoqlari uchun qulay nishonga aylantiradi. Masalan, Mirai botneti tarixdagi eng yirik DDoS hujumlarini aynan IoT qurilmalari orqali amalga oshirgan. Bu kabi holatlar ko'rsatadiki, bitta qurilmaning zaifligi butun tarmoqning ishdan chiqishiga olib kelishi mumkin.

1-jadval

O'zbekiston va xorijiy ilmiy manbalarda xavfsizlik yechimlari eng samarali yo'llari

Yondashuv turi	Tavsif	Afzalliklari
Yengil kriptografiya	AES-128, ECC, SHA-3 asosida qisqartirilgan modullar	Kam resurs, tez ishlash
Blockchain asosida autentifikatsiya	Tarqatilgan, o'zgarimas identifikatsiya tizimi	Markazsiz, xavfsiz, shaffof
AI asosidagi tahdid aniqlash	Neyron tarmoqlar orqali tahdidlarni oldindan bashoratlash	O'z-o'zini o'rgatuvchi, real vaqtli
Edge computing xavfsizligi	Ma'lumotni bulut emas, qurilmaga yaqin tugunlarda qayta ishlash	Tizimga hujum qilinadigan vaqtni kamaytiradi
Zero Trust yondashuvi	Har bir qurilma har bir ulanishda qayta autentifikatsiyadan o'tadi	Ruxsatsiz kirishning oldi olinadi

Resurslari cheklangan IoT qurilmalar uchun moslashtirilgan AES-128, ECC va SHA-3 kabi algoritmlar xavfsizlikni ta'minlashda optimal hisoblanadi. Ular past energiya sarfi va tezkor ishlashi bilan ajralib turadi. Bu yondashuv sensorli qurilmalar, aqlli uyingohlar va tibbiy moslamalar uchun ayniqsa muhimdir.

IoT qurilmalar orasida markazsiz va ishonchli identifikatsiya tizimi yaratadi. Bu usul orqali ma'lumotlar

o'zgartirilmaydigan bloklarga yoziladi va har bir qurilma ishonchli tarzda ro'yxatga olinadi. Bu esa qurilmalararo hujumlar va soxta qurilma ulanishi tahdidining oldini oladi.

Sun'iy intellekt (AI) yordamida qurilmadagi noan'anaviy xatti-harakatlar aniqlanadi va real vaqt rejimida tahdid bashorat qilinadi. Neyron tarmoqlar asosida qurilgan tizimlar avvalgi tajribalardan o'rganib, yangi hujum turlariga nisbatan moslasha oladi.

IoT qurilmalardan kelgan ma'lumotlar bulutga yuborilmasdan, yaqin "chekka" serverlarda qayta ishlanadi. Bu yondashuv axborot oqimining kechikishini kamaytiradi, shuningdek hujumchilarning tarmoqqa kirish vaqtini qisqartiradi.

Har bir qurilmaning har bir ulanishi alohida autentifikatsiyadan o'tkaziladi. Bu yondashuv "ishonch, lekin tekshir" o'rniga "hech kimga ishonma" tamoyiliga asoslanadi. Bu orqali ichki tarmoqda ham ruxsatsiz kirishlar qat'iy nazorat qilinadi.

O'zbekistonda Internet of Things (IoT) texnologiyalari jadal sur'atlar bilan rivojlanayotgan bo'lsa-da, ularning xavfsizligini ta'minlash borasida muayyan yondashuvlar va texnologiyalar qo'llanilmoqda. Quyidagi tahlilda mamlakat miqyosida IoT xavfsizligini

ta'minlashda qo'llanilayotgan asosiy yondashuvlar, ularning amaliy samaradorligi, joriy etilish darajasi va yuzaga kelayotgan muammolar chuqur tahlil qilinadi.

Avvalo, yengil kriptografiya (lightweight cryptography) yo'nalishi eng ko'p qo'llanilayotgan texnologiya bo'lib, hozirda 12 ta loyiha doirasida joriy etilgan. Ushbu yondashuv resurslar cheklangan kichik qurilmalar uchun juda mos bo'lib, uning samaradorligi 4,6 ball bilan baholangan. Shu bilan birga, amaliyotda qo'llanish darajasi 65 foizni tashkil etadi. Asosiy muammo esa – past energiyali va cheklangan xotiraga ega qurilmalarda bu texnologiyani optimallashtirishda davom etayotgan texnik qiyinchiliklardir.

2-jadval

O'zbekistonda IoT xavfsizlik yondashuvlari bahosi

Yondashuv turi	Qo'llanilgan loyihalar soni	Samaradorlik bahosi	Amaldagi qo'llanish darajasi, %	Asosiy to'siqlar
Yengil kriptografiya	12	4,6	65	Resurslar cheklanganligi
Blockchain asosida autentifikatsiya	7	4,2	48	Yuridik-huquqiy noaniqlik
AL asosidagi tahdid aniqlash	5	4,0	34	AL modelga oid malaka yetishmovchiligi
Edge computing xavfsizligi	3	3,8	27	Infratuzilma yetarli emas
Zero Trust yondashuvi	4	4,1	40	Avtorizatsiya jarayoni murakkabligi

Ikkinchi yirik yondashuv – Blockchain asosida autentifikatsiya tizimi. U 7 ta loyihada sinovdan o'tkazilgan bo'lib, 4,2 ball samaradorlikka ega va 48 foizlik joriy etilish darajasiga yetgan. Biroq bu yondashuvning keng qo'llanilishiga yuridik va normativ-huquqiy noaniqliklar to'sqinlik qilmoqda. Bunday tizimlar markazlashmagan va shaffof bo'lishi

bilan afzallik bersa-da, huquqiy moslashuvchanlik talab etiladi.

Sun'iy intellekt (AI) asosidagi tahdid aniqlash tizimlari hozircha 5 ta loyiha doirasida sinovdan o'tkazilgan. Ularning samaradorlik ko'rsatkichi 4,0 ball deb baholangan, qo'llanish darajasi esa 34 foiz atrofida. Bu yondashuvning asosiy muammosi – AI model va algoritmlar bilan ishlay oladigan mutaxassislar

yetishmasligi hisoblanadi. Bu esa rivojlanmaganligi ushbu texnologiyani tizimlarning keng ko'lamda joriy kengaytirishga to'sqinlik qilmoqda. etilishini sekinlashtirmoqda.

Edge computing xavfsizligi esa IoT muhitida ma'lumotlarni qurilmaga yaqin tugunlarda qayta ishlash orqali tizimga hujum qilish vaqtini qisqartirishga yordam beradi. Hozirda 3 ta loyihada bu yondashuv qo'llanilgan bo'lib, samaradorligi 3,8 ball, qo'llanish darajasi esa 27 foizni tashkil etmoqda. Infratuzilmaning yetarli darajada

rivojlanmaganligi ushbu texnologiyani kengaytirishga to'sqinlik qilmoqda.

So'nggi tahlil qilinadigan yondashuv – Zero Trust modelidir. Bu yondashuv har bir qurilma va foydalanuvchini har bir aloqada autentifikatsiyadan o'tkazishni talab qiladi. U 4 ta loyihada joriy etilgan, samaradorlik bahosi 4,1 ball bo'lib, amaldagi qo'llanish darajasi 40 foizga teng. Zero Trust tizimining asosiy to'siqlari autentifikatsiya jarayonining murakkabligi va uni soddalashtirish mexanizmlarining yetishmasligidir.

3-jadval

Tajriba asosidagi IoT xavfsizlik modeli natijalari (O'zbekiston misolida)

Yondashuv turi	Xavfsizlik samaradorligi (0–5)	Ishlash tezligi (ms)	Hujumga barqarorlik (0–5)	Resurs talabchanligi (RAM, MB)
Yengil kriptografiya (AES-lite, ECC)	4.6	12	4.2	1.8
Blockchain autentifikatsiya	4.2	37	4.5	5.1
AI asosidagi tahdid aniqlash	4.0	45	4.7	6.4
Edge computing xavfsizligi	3.8	19	3.9	2.3
Zero Trust modeli	4.1	27	4.6	3.8

Yengil kriptografiya tajriba davomida eng balansli natija ko'rsatdi: xavfsizlik samaradorligi yuqori, ishlash tezligi eng tez (12 ms), va resurs talabchanligi eng kam (1.8 MB). Bu uni IoT qurilmalar uchun eng mos deb topadi.

Blockchain asosida autentifikatsiya yondashuvi xavfsizlik darajasi bo'yicha yuqori (4.5), biroq resurs va vaqt talabchanligi ko'p (5.1 MB, 37 ms). Shu sababli bu yondashuv real vaqtli qurilmalarda qo'llanishi cheklangan.

AI asosidagi tahdid aniqlash tahdidlarni aniqlashda yuqori aniqlik ko'rsatgan (4.7), lekin ishlash tezligi past va resurslar ko'p talab etadi. Bu esa undan faqat quvvatli serverlarda foydalanishni maqsadga muvofiq qiladi.

Edge computing yechimlari markazlashtirilmagan tahlilni ta'minlagani uchun xavfsizlik jihatdan qoniqarli (3.9), ishlash tezligi ham yaxshi (19 ms). Ammo infratuzilma talablari sababli joriy qilishda qiyinchiliklar mavjud.

Zero Trust yondashuvi foydalanuvchi va qurilma xavfsizligini kuchli nazorat qiladi. Hujumga barqarorlik darajasi yuqori (4.6), lekin bu modelda autentifikatsiya jarayoni murakkab va vaqt talab qiladi.

Xulosa.

Ushbu tadqiqot natijalari shuni ko'rsatdiki, O'zbekiston sharoitida Internet of Things (IoT) texnologiyalarining jadal rivojlanishi

bilan bir qatorda, ularning axborot xavfsizligini ta'minlash masalasi ham dolzarb muammo bo'lib qolmoqda. IoT qurilmalarining ko'pchiligi past hisoblash quvvatiga, cheklangan xotiraga va yengil arxitekturaga ega bo'lib, bu ularni an'anaviy xavfsizlik yondashuvlariga nisbatan zaif qiladi.

Tadqiqotda qo'llanilgan tahliliy yondashuvlar orqali eng samarali xavfsizlik strategiyalari – yengil kriptografiya, blockchain asosidagi autentifikatsiya, sun'iy intellekt yordamida tahdid aniqlash, edge computing va Zero Trust modeli sifatida aniqlangan. Har bir yondashuvning samaradorligi, joriy etilish darajasi, muammolari va texnik ko'rsatkichlari (ishlash tezligi, resurs talabchanligi) amaliy loyihalar asosida baholandi.

O'zbekistonda ayniqsa yengil kriptografiya keng qo'llanilayotgan texnologiya bo'lib, u yuqori tezlik va past resurs talabchanligi tufayli IoT qurilmalari uchun optimal yechimdir.

Blockchain esa xavfsizlik darajasi yuqoriligi bilan ajralib tursa-da, yuridik-huquqiy cheklovlar tufayli keng joriy etilishi sekin bormoqda. AI asosidagi yondashuvlar tahdidlarni aniqlashda ustunlikka ega bo'lsa-da, mutaxassislar tanqisligi va resurslar yetishmovchiligi muammo bo'lmoqda. Edge computing va Zero Trust yondashuvlari esa infratuzilma va autentifikatsiya murakkabligi sababli keng joriy etilmagan.

Tajribaviy tahlillar shuni ko'rsatdiki, har bir yondashuv o'zining kontekstual afzallik va cheklovlariga ega bo'lib, IoT xavfsizligini ta'minlashda ko'p darajali va kombinatsiyalangan yondashuv zarurligini taqozo etadi. O'zbekiston uchun istiqbolli yo'nalish sifatida resurslarga moslashtirilgan yengil kriptografik tizimlar, zamonaviy huquqiy mexanizmlar bilan uyg'unlashtirilgan blockchain autentifikatsiyasi va lokal bazali edge tizimlar asosida xavfsizlikni kuchaytirish taklif etiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Ashton, K. (2009). That 'Internet of Things' Thing. RFID Journal.
2. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems.
3. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks.
4. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks.
5. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials.
6. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal.
7. National Institute of Standards and Technology (NIST). (2020). Special Publication 800-183: Networks of 'Things'.
8. International Organization for Standardization. (2018). ISO/IEC 30141: Internet of Things Reference Architecture.

CONTENTS

1	SAMARQAND VILOYATIDA INVESTITSION - INNOVATSION FAOLLIKNI OSHIRISH HOLATI VA INVESTITSİYALARNING TARKIBIY XUSUSIYATLARI	
	Bektemirov Abdumalik Bektemirovich, Axrorov Abbos Aslamjon o'g'li	4-13
2	“YASHIRIN IQTISODIYOT”GA METODOLOGIK YONDASHUVNI TAKOMILLASHTIRISH	
	Abduvohidov Najmiddin Rahmatullaevich	14-19
3	OILA TADBIRKORLIGINI RIVOJLANTIRISH DASTURI DOIRASIDA BANKLAR TOMONIDAN AMALGA OSHIRILGAN ISHLARNING AHAMIYATLI JIHLARI	
	Z.D.Niyozov , A.A.Axrorov	20-24
4	HUDUDIIY INVESTITSIYA JOZIBADORLIGINI OSHIRISHNING TASHKILIY-IQTISODIY MEXANIZMLARINI TAKOMILLASHTIRISH	
	Bektemirov Abdumalik Bektemirovich, Ergasheva Aziza Xasan qizi	25-34
5	DESTINATION MANAGEMENT AND BRANDING: CREATING COMPETITIVE ADVANTAGE IN GLOBAL TOURISM	
	Nasimov Dilmurod Abdullayeich, Sirojiddinova Shahrizoda	35-42
6	TA'LIM MUASSASALARIDA RESURLARDAN SAMARALI FOYDALANISH TAMOIYILLARI	
	Meliboyev Ibroxim Mavlon o'g'li	43-47
7	SUN'IY INTELLEKT ASOSIDA MA'LUMOTLARNI TAHLIL QILISH VA BASHORATLASH ALGORITMLARINI ISHLAB CHIQISHNING NAZARIY VA AMALIY ASOSLARI	
	Bekmurodov Ulug'bek Bahrom o'g'li, Shomirzayev Farruh Akram o'g'li	48-55
8	SAMARQAND VILOYATIDA INVESTITSION-QURILISH JARAYONLARI ISHTIROKCHILARI FAOLIYATINING ASOSIY KO'RSATKICHLARI TAHLILI	
	Abduvaliyev Bekzod Muxiddin o'g'li	56-61
9	TURISTIK XIZMATLAR VUJUDGA KELISHINING XUSUSIYATLARI VA RIVOJLANISH BOSQICHLARI	
	Umirzoqova Muxabbat Ismatjon qizi	62-67
10	TURAR-JOY KO'CHMAS MULK OBYEKLARINI BAHOLASH XIZMATLARI SAMARADORLIGINI OSHIRISH USULLARINI TAHLILI	
	A.S.Suyunov, B.M.Abduraimov, B.A.Suyunov	68-73
11	BANK XIZMATLARIDA AN'ANAVIY XIZMATDAN RAQAMLI XIZMATGA O'TISHNING AHAMIYATLI JIHLARI	
	Niyozov Zuxur Davronovich, Bektemirov Bunyodjon Mamasaliyevich	74-78
12	MINTAQAVIY TRANSPORT INFRATUZILMASINI RIVOJLANTIRISHDA DAVLAT XUSUSIY SHERIKLIK MEXANIZMLARINING QO'LLANILISHI VA ULARNING USTUVOR YO'NALISHLARI	
	Rahmonov Rasul Ne'matovich	79-86
13	POTENTIAL AND POSSIBILITIES OF UTILISATION OF CULTURAL HERITAGE FOR TOURISM DEVELOPMENT IN SAMARKAND	
	Mukhsin Khidirov, Umida Shodieva	87-91
14	O'ZBEKISTON IQTISODIYOTIDA XORIJIY INVESTITSİYALARNI RAG'BATLANTIRISHDA ERKIN IQTISODIY ZONALARNING O'RNI	
	Abdurahmonov Azizbek Akram o'g'li	92-99
15	IoT (INTERNET OF THINGS) XAVFSIZLIK MUAMMOLARINI BARTARAF ETISH USULLARI	
	Bekmurodov Ulug'bek Bahrom o'g'li , Ruziyeva Zulfiya Qurvonovna	100-106

16	СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УСЛУГ ПО ОЦЕНКЕ ОБЪЕКТОВ ЖИЛОЙ НЕДВИЖИМОСТИ (НА ПРИМЕРЕ РЫНКА ЖИЛЬЯ Г. САМАРКАНДА)	
	A.C.Суюнов, Б.А.Суюнов	107-114
17	TURIZM SOHASINI KLASSTERLASHTIRISHNING INNOVATSION OMILLARI VA XUSUSIYATLARI	
	Botirov Og'abek Jasurbek o'g'li	115-118
18	INNOVATSION USULLARDAN FOYDALANISH ORQALI TABIIY TURISTIK RESURLARNI SAMARALI RIVOJLANTIRISH YO'LLARI	
	Rabbimov Muxriddin Musoqul o'g'li, Samiyeva Muxlisa Olim qizi	119-123
19	XIZMAT KO'RSATISH KORXONALARIDA RESURS TA'MINOTI TUSHUNCHASI, MAZMUNI VA IQTISODIY MOHIYATI	
	Arziqulova Oybarchin Eshquvat qizi	124-130
20	RAQAMLI IQTISODIYOT SHAROITIDA DAVLAT BOSHQARUVINING RIVOJLANISH TENDENSIYALARI	
	Sanakulova Iroda Abrorovna	131-135
21	QISHLOQ XO'JALIGI MAHSULOTLARINI QAYTA ISHLASH INFRATUZILMASINI RIVOJLANTIRISH ISTIQBOLLARI	
	Nurimbetov Timur Uzakbergenovich	136-140
22	HUDUDIY IQTISODIYOTNI RIVOJLANTIRISHDA TURISTIK-INNOVATSION KLASSTERLARNING INSTITUTSIONAL ASOSLARI VA RIVOJLANISH MEXANIZMLARI	
	Erbo'tayev Azimjon Qahramon o'g'li	141-148
23	INNOVATSION RIVOJLANISH SHAROITIDA INSON KAPITALINING KICHIK BIZNES RIVOJLANISHIGA TA'SIRI	
	Eshbo'riyev Umarbek Rashidovich	149-155
24	SAMARQAND VILOYATIDA MUZEY TURIZMINI RIVOJLANTIRISHNING IQTISODIY SAMARADORLIGI	
	Yulduz Pirnazarovna Urunbayeva	156-163
25	ELEKTRON TIJORATNING RIVOJLANISHI VA UNING ZAMONAVIY TENDENSIYALARI	
	Tashmatov Sharaf Urokboyevich	164-170
26	TADBIRKORLIK RISKI VA TAVAKKALCHILIK: NAZARIY DIFFERENSIYA HAMDA ULARNING BOSHQARUVDAGI AHAMIYATI	
	Abduxamid Abdumalikovich Bektemirov	171-178
27	OLIY TA'LIM TIZIMIDA RAQAMLI PLATFORMALARDAN FOYDALANISH SAMARADORLIGINI OSHIRISH	
	Boynazarova Iroda Mahmud qizi	179-185
28	ДВУХЭТАПНЫЙ МЕТОД ГРУППИРОВКИ БУЛЕВЫХ ПРИЗНАКОВ И ПОСТРОЕНИЕ ИНФОРМАТИВНЫХ ПРИЗНАКОВ В ВЫДЕЛЕННЫХ ГРУППАХ	
	Порсаев Ганиджон Мухамедович	186-193
29	RESEARCH ON MARKETING INNOVATION OF CHINESE MUSEUM CULTURAL AND CREATIVE PRODUCTS FROM THE PERSPECTIVE OF EXPERIENTIAL MARKETING	
	Nasimov Ikrom Khusanovich, Guang Yang	194-200
30	TURIZM SOHASINING INNOVATSION FAOLLIGI VA RAQOBATBARDOSHLIGINI OSHIRISH HOLATI TAHLILI	
	Xaitov Oxunjon Nomoz o'g'li	201-206