



Ziyoda ABDULLAYEVA,
Toshkent axborot texnologiyalari universiteti dotsenti v.b
E-mail: z.abdullayeva.tatu@gmail.com

PhD M.Mamajonova taqrizi asosida

RAQAMLASHGAN JAMIYAT TIZIMIDA FUQAROLARNING ISHONCHINI OSHIRISH STRATEGIYALARI

Annotatsiya

Ushbu maqolada raqamlashtirilgan jamiyat sharoitida fuqarolarning davlat va raqamli institutlarga bo'lgan ishonchini oshirish strategiyalari yoritiladi. Elektron xizmatlarda shaffoflikni kuchaytirish, ma'lumotlar xavfsizligini ta'minlash, fuqarolar bilan ikki tomonlama muloqotni rivojlantirish, raqamli savodxonlikni oshirish va ochiq ma'lumotlar siyosatini kengaytirish bo'yicha yechimlar tahlil qilingan.

Kalit so'zlar: raqamli ishonch, ochiq ma'lumotlar, shaffoflik, kiberxavfsizlik, davlat xizmatlari, raqamli savodxonlik, ishonch modeli, elektron hukumat, ma'lumotlar himoyasi, kommunikatsiya, innovatsiya, fuqarolik ishtiroki, raqamli identifikatsiya, sun'iy intellekt, mas'uliyatli boshqaruv.

СТРАТЕГИИ ПОВЫШЕНИЯ ДОВЕРИЯ ГРАЖДАН В ЦИФРОВОМ ОБЩЕСТВЕ

Аннотация

В статье рассматриваются стратегии повышения доверия граждан в условиях цифрового общества. Анализируются меры по усилению прозрачности электронных услуг, обеспечению защиты данных, развитию двусторонней коммуникации государства с населением, повышению цифровой грамотности и расширению политики открытых данных.

Ключевые слова: цифровое доверие, открытые данные, прозрачность, кибербезопасность, госуслуги, цифровая грамотность, модель доверия, электронное правительство, защита данных, коммуникация, инновации, гражданское участие, цифровая идентификация, искусственный интеллект, ответственное управление.

STRATEGIES FOR INCREASING CITIZEN TRUST IN A DIGITAL SOCIETY

Annotation

This article explores strategies for increasing citizens' trust in a digital society. It examines approaches such as enhancing transparency in e-services, ensuring data protection, strengthening two-way communication between government and citizens, improving digital literacy, and expanding open data policies.

Keywords: digital trust, open data, transparency, cybersecurity, public services, digital literacy, trust model, e-government, data protection, communication, innovation, citizen participation, digital identity, artificial intelligence, responsible governance.

Kirish. Raqamlashtirish jarayoni davlat boshqaruvi, iqtisodiy faoliyat va ijtimoiy hayotning barcha jabhalarini tubdan o'zgartirmoqda. Ammo raqamli texnologiyalar qanchalik rivojlanmasin, ularning samaradorligi fuqarolarning ishonch darajasiga bog'liq. Shuning uchun ishonchni mustahkamlash – raqamli jamiyatning asosiy ustunidir.

Asosiy qism. Raqamlashgan jamiyat tizimi – bu jamiyat hayotining barcha sohalarini (ta'lim, sog'liqni saqlash, iqtisodiyot, davlat boshqaruvi, biznes, muloqot) raqamli texnologiyalar asosida ishlaydigan yaxlit tizimdir.

Raqamlashgan jamiyat – bu jamiyatda barcha jarayonlar qog'ozda emas, balki raqamli platformalarda, onlayn xizmatlar orqali amalga oshiriladigan model [1].

Raqamlashgan jamiyat tizimida fuqarolarning ishonchini oshirish strategiyalari mavzusida qilingan ilmiy ishlar tahlili:

R. Sodiqov (2021) – Raqamli davlat xizmatlarida shaffoflik va fuqarolar ishonchi tadqiqoti.

Sh. Jo'rayev (2020) – Kiberxavfsizlik va raqamli ishonch o'rtasidagi bog'liqlikni tahlil qilgan.

Z. Abduvaliyeva (2022) – Raqamli savodxonlikning ishonch shakllanishiga ta'siri.

O. Qodirov (2021) – Elektron hukumat platformalarida foydalanuvchi tajribasini o'rgangan.

M. Nurmatova (2020) – Biometrik identifikatsiya va ishonch mexanizmlari.

A. Tursunov (2021) – Korrupsiyani kamaytirish va ishonchni oshirish.

B. Xasanov (2020) – “Raqamli O'zbekiston – 2030” strategiyasida ishonchni oshirish yo'llari.

S. Karimova (2022) – Elektron sog'liqni saqlash tizimi va fuqarolar ishonchi.

U. Ergashev (2021) – Aqli shahar loyihalarida ishonch mexanizmlari.

D. Yusupov (2020) – Shaxsiy ma'lumotlar boshqaruvi va fuqarolar ishonchi.

L. Abdullayeva (2021) – Raqamli kommunikatsiya orqali fuqarolar ishonchini oshirish.

X. To'xtaboyev (2022) – Raqamli iqtisodiy ekotizimda ishonch modellarini tadqiq qilgan.

S. Raxmonov (2020) – Onlayn to'lov tizimlarida xavfsizlik va ishonch.

M. G'afforova (2021) – Raqamli ta'lim tizimida ishonch indikatorlari.

T. Sayfullayev (2022) – Davlat xizmatlarida qulaylik va ishonch o'zaro ta'siri.

Shoshana Zuboff (2020) – Maxfiylik va raqamli kapitalizm ishonchiga ta'siri.

Don Tapscott (2021) – Blockchain orqali fuqarolar ishonchini oshirish.

Tim Berners-Lee (2021) – Web 3.0 va Solid platformasi orqali raqamli ishonch.

Ethan Zuckerman (2020) – Foydalanuvchi markaziy internet modeli va ishonch.

Helen Nissenbaum (2020) – Ma'lumot maxfiyligi va ishonch normalari.

Richard Thaler (2020) – Nudge tamoyillari va raqamli tizimlarda ishonch.

Cass Sunstein (2021) – Raqamli qaror qabul qilish tizimida fuqarolar ishonchi.

Anthony Giddens (2020) – Institutsional ishonch nazariyasi raqamli jamiyatga qo'llanilishi.

Mavzuning dolzarbligi: Bugungi kunda fuqarolar davlat va biznes xizmatlarining katta qismini onlayn borishi, raqamli xizmatlar ommalashgani sayin, ma'lumotlar xavfsizligi va shaffoflik talabi oshganligi, kiberhujumlar, shaxsiy ma'lumotlarning o'g'irlanishi va xizmatlarning murakkabligi fuqarolarning ishonchini kamayishi, raqamli identifikatsiya tizimlari, elektron imzo va biometrik autentifikatsiya fuqarolarning xizmatlarga ishonchini oshirish uchun zarurligi, raqamli savodxonlik darajasi oshgani sayin, foydalanuvchilar tizimlardan ishonch bilan foydalanishi, korrupsiyani

kamaytirish va jarayonlarni avtomatlashtirish fuqarolarning raqamli jamiyatga ishonchini mustahkamlash hisoblanadi [2,3].

Ilmiy yangilik: Raqamlashgan jamiyatda fuqarolar ishonchini oshirish bo'yicha taklif etilayotgan strategiyada blokcheyn asosida shaffof transaksiyalar monitoringi, AI-ga tayangan real vaqtli xatarlarni baholash modeli, hamda foydalanuvchi maxfiyligini dinamik boshqaruvchi adaptiv identifikatsiya tizimi birlashtiriladi. Ushbu yondashuv mavjud tizimlardan farqli ravishda ishonchni avtomatlashtirilgan, o'lchab bo'ladigan va shaxsiylashtirilgan ko'rsatkichlar orqali baholash imkonini yaratadi.

Tahli va natijalar

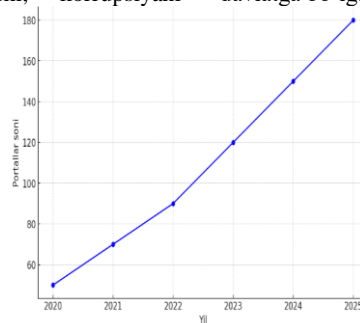
Raqamlashgan jamiyat tizimida fuqarolarning ishonchini oshirish strategiyasi birinchi omili shaffoflikni kuchaytirishdir:

Ochiq ma'lumotlar bazalarini kengaytirish.

Elektron xizmatlar natijalarini kuzatish imkoniyati.

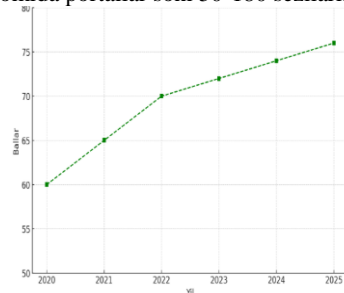
Qaror qabul qilish jarayonlarini onlayn kuzatish.

Shaffof ekotizim korrupsiyani kamaytiradi va fuqarolarning davlatga bo'lgan munosabatini musbat shakllantiradi [4].



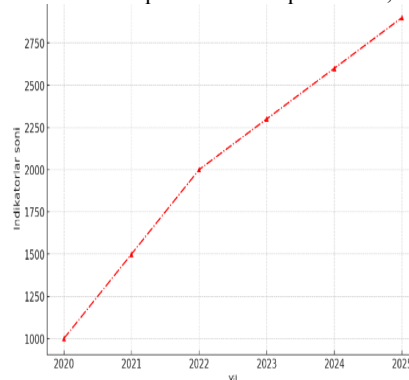
1-rasm. Ochiq ma'lumotlar bazasini o'sishishi

Ochiq ma'lumotlar portallari soni – yillar davomida portallar soni 50-180 sezilarli oshgani keltirilgan [6].



2-rasm. ODIN ortishi (2020-2025)

ODIN (Open Data Inventory) ballari – O'zbekiston ochiqlik bahosi barqaror o'sib, 60 ballidan 76 ballgacha yetgan.



3-rasm. Real vaqtda statistik indikatorlar soni ortishi (2020-2025)

Real vaqtda statistik indikatorlar soni – indikatorlar soni 1000 dan 2900 gacha oshgan, bu jamoatchilik uchun ma'lumot ochiqligini ko'rsatadi [7,8].

Raqamlashgan jamiyat tizimida fuqarolarning ishonchini oshirish strategiyasi ma'lumotlar xavfsizligini ta'minlash:

Kuchli kriptografiya foydalanish.

Zero-trust modeli foydalanish.

Kiberxavfsizlik bo'yicha doimiy monitoring qilish.

Ma'lumotlar buzilishiga qarshi javob mexanizmlari berish [5].

Kuchli kriptografiya asosida fuqarolar ishonchini oshirish strategiyasi bir nechta asosiy yo'nalishlarni o'z ichiga oladi.

Davlat xizmatlarida end-to-end shifrlashni joriy etish. Elektron hukumat portallari, soliq tizimi, onlayn reyestrlar va tibbiy ma'lumotlar bazalarida barcha ma'lumot almashinuvi shifrlangan kanallar orqali amalga oshirilishi kerak.

Zamonaviy kriptografik algoritmlarga o'tish. AES-256, ECC (Elliptic Curve Cryptography) kabi algoritmlar milliy standart sifatida joriy qilinishi kerak. Bu tez ishlash, yuqori darajadagi himoya va kvant kompyuterlarga qarshi barqarorlikni ta'minlaydi.

Fuqarolar uchun shaffoflik darajasini oshirish. Raqamli tizimlar qanday ma'lumot yig'ishi, uni qaysi shaklda saqlashi va kimlar bilan almashishi fuqaroga aniq ko'rsatilishi zarur.

Xavfsiz identifikatsiya ekotizimi. ID-kartalar, biometrik ma'lumotlar va davlat xizmatlariga kirish yagona PKI platformasi bilan himoyalaniishi kerak.

Kiberhujumlarga qarshi doimiy monitoring. AI asosidagi anomaliya aniqlash tizimlari orqali potentsial xatarlarni oldindan aniqlash mumkin.

Kuchli kriptografiyaning joriy etilishi natijasida kutiladigan ijobiy ta'sirlar:



4-rasm. Zero-Trust modelini ishlash prinsipi

Zero-Trust modeli "Hech kimga ishonma, hamma narsani tekshir" (Never trust – Always verify) tamoyiliga asoslanadi. Ushbu yondashuvda hatto tizim ichidagi foydalanuvchilar ham avtomatik ravishda ishonchli deb qabul qilinmaydi, balki ularning har bir harakati, qurilmasi va kirish huquqi real vaqt rejimida tekshiriladi. Bu model raqamli jamiyatda ma'lumotlar xavfsizligini oshirish orqali fuqarolarning tizimga bo'lgan ishonchini kuchaytiradi, chunki unda har bir foydalanuvchi identifikatsiyalanadi, har bir so'rov nazorat qilinadi va har bir jarayon audit qilinadi.

Shuningdek, Zero-Trust modeli ma'lumotlarning doimiy monitoringi va auditiga tayanadi. Har bir kirish, har bir so'rov, har bir o'zgarish jurnalga yoziladi va sun'iy intellekt yordamida tahlil qilinadi. Bu esa tizimni nafaqat himoya qiladi, balki potentsial xavflarni oldindan ko'rish imkonini beradi. Fuqarolar uchun bunday yondashuv shuni anglatadiki, ularning ma'lumotlari nazoratsiz yoki yashirin holda ishlatilmaydi, balki har bir jarayon shaffof va boshqariladigan bo'ladi.

Zero-Trust modeli raqamlashgan jamiyat uchun nafaqat texnik himoya strategiyasi, balki fuqarolar ishonchini oshiruvchi psixologik va ijtimoiy mexanizm sifatida ham xizmat qiladi. Har bir foydalanuvchi faoliyati izchil tekshirilib, ma'lumotlar qat'iy shifrlanib, kirish huquqlari minimal darajada cheklangan sharoitda fuqarolar raqamli xizmatlar xavfsizligiga ishonadi. Bu modelni davlat, bank, sog'liqni saqlash, ta'lim va transport tizimlariga keng joriy etish raqamli ekotizimning barqarorligini ta'minlaydi.

Fuqarolar ishonchining barqaror o'sishi. Ma'lumotlar shifrlangan holda uzatilishi va himoya mexanizmlarining shaffofligi fuqarolarda xavfsizlik hissini oshiradi.

Kiberxavflarning keskin kamayishi. Shifrlash orqali ma'lumotlar sizib chiqishi, MITM hujumlari, phishing va ijtimoiy muhandislik hujumlarining oldi olinadi.

Davlat tizimlariga bo'lgan ishonchning kuchayishi. Raqamli hukumatning sifatli himoyaga ega bo'lishi uning obro'sini oshiradi.

Iqtisodiy samaradorlik. Firibgarlik holatlarini kamaytirish orqali jamiyatda iqtisodiy barqarorlik ta'minlanadi.

Raqamlashgan jamiyat tizimida fuqarolarning ishonchini oshirish strategiyasida Zero-Trust modelidan foydalanish:

Raqamlashgan jamiyatning shakllanish jarayonida ma'lumotlar almashinuvi, davlat xizmatlarining elektron ko'rinishga o'tishi, onlayn to'lovlar, masofaviy identifikatsiya va raqamli hujjat aylanishining kengayishi axborot xavfsizligiga bo'lgan talabni keskin oshirdi. Fuqarolar o'z ma'lumotlarining qanday saqlanishi, kimlar tomonidan ko'rilishi va ulardan foydalanish jarayonining qanchalik xavfsiz ekaniga e'tibor qaratmoqda. Agar raqamli tizimlar ishonchli bo'lmasa, fuqarolarning ulardan foydalanish faolligi pasayadi, natijada raqamlashtirish siyosati samaradorligi ham tushadi. Shu sababli davlat va xususiy tashkilotlar oldida fuqarolarning ishonchini barqaror saqlash va oshirish asosiy strategik vazifaga aylandi.

Raqamlashgan jamiyat tizimida fuqarolarning ishonchini oshirish strategiyasi ma'lumotlar xavfsizligini ta'minlashda kiberxavfsizlik bo'yicha doimiy monitoring qilish.

Raqamlashgan jamiyatda fuqarolar ishonchini oshirish uchun barcha raqamli platformalar va ma'lumotlar oqimlari real vaqt rejimida uzluksiz kuzatuv va tahlil qilinishi zarur. Doimiy monitoring tizimi foydalanuvchi faolligi, tarmoq trafiklari, kirishlar, tranzaksiyalar va shubhali harakatlarni avtomatik aniqlab, ularni tezkor baholaydi hamda potentsial tahdidlarni dastlabki bosqichda to'xtatadi.

Ma'lumotlar buzilishiga qarshi qo'llaniladigan mexanizmlarning yana bir dolzarb jihati — bu zudlik bilan xabar berish va shaffoflikni ta'minlashdir. Fuqarolar o'z ma'lumotlari buzilgan yoki xavf ostida qolganda bunga darhol xabardor bo'lishi lozim. Xalqaro tajribada bunday holatlarda 24–72 soat ichida rasmiy bildirishnoma berish talabi mavjud, chunki kechikish fuqarolarning ishonchini yo'qotadi. Vaqtida berilgan rasmiy xabar esa fuqarolarga o'z hisoblarini himoya qilish, parollarni almashtirish, moliyaviy yo'qotishlarning oldini olishga imkon beradi. Bu esa davlatning raqamli tizimlariga nisbatan ishonchni oshiradi.

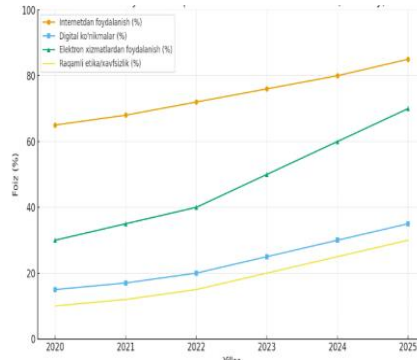
Raqamlashgan jamiyat tizimida fuqarolarning ishonchini oshirish strategiyasi omili raqamli savodxonlik bo'lib, u quyidagilarni o'z ichiga oladi:

Elektron xizmatlardan foydalanish.

Internetdagi xavflarni bilish.

Ma'lumotlar almashinuvi madaniyati.

Raqamli etikani anglash.



5-rasm. 2020–2025 yillar uchun raqamli savodxonlik ortishi

Rasmda internetdan foydalanish eng yuqori o'sigani ko'rish mumkin (65% -85%), raqamli ko'nikmalar asta-sekin yaxshilanganini (15% -35%), elektron xizmatlardan foydalanish 30% dan 70% ga o'siganligi, raqamli etika va xavfsizlik xabardorligi ham asta ortganligi (10% -30%) keltirilgan [9].

Raqamlashgan jamiyat tizimida fuqarolarning ishonchini oshirish strategiyasi omili davlat–fuqaro o'rtasidagi munosabat bir tomonlama bo'lmasligi kerak. Samarali mexanizmlar:

Onlayn murojaatlar platformasi tashkil etish.

Chatbotlar va tezkor javob tizimi joriy qilish.

Virtual majlislar va jamoatchilik fikrini o'rganish vositalari joriy qilish.

Fuqarolarning raqamli muhokamalarda ishtirokini jalb qilish.

Raqamlashgan jamiyat tizimida fuqarolarning ishonchini oshirish strategiyasi omili boshqaruvning adolatli, javobgar va izchil bo'lishidir.

Hisobotlilik, qarorlar va natijalar bo'yicha javob berish.

Qonuniylik.

Ochiq e'lon qilingan qarorlar.

Barcha fuqarolar uchun teng imkoniyatlar yaratish.

Mas'uliyatli boshqaruv bo'lmasa, eng zamonaviy texnologiya ham ishonch yaratmaydi [10].

Xulosa va takliflar. Raqamlashgan jamiyat sharoitida fuqarolarning ishonchini mustahkamlash davlat boshqaruvi va raqamli xizmatlarning barqaror ishlashini ta'minlovchi eng muhim omillardan biridir. Tahlillar shuni ko'rsatadiki, ishonchni oshirish faqat texnologik yechimlar bilan cheklanib qolmaydi, balki shaffoflik, ma'lumotlar xavfsizligi, raqamli savodxonlik, ochiq ma'lumotlar siyosati va samarali kommunikatsiya kabi ko'p qirrali strategiyalar uyg'unligini talab qiladi.

Raqamlashgan jamiyatda fuqarolar ishonchini oshirish kompleks yondashuvni talab qiladi: texnologik infratuzilma, inson omili, boshqaruv sifati va shaffoflik o'zaro uyg'un holda ishlagan taqdirdagina raqamli tizimlarga bo'lgan ishonch barqaror shakllanadi. Yanada mukammal raqamli jamiyat qurish uchun aynan shu omillarni birgalikda rivojlantirish muhim ahamiyatga ega.

ADABIYOTLAR

1. Avazov, S., & Lee, S. (2022). E-Government Services Adoption in Uzbekistan: An Empirical Validation of Extended Version of the Unified Model of Electronic Government Acceptance (UMEGA). *Journal of Policy Studies*, page 37(3).
2. Muydinov, E. A. (2024). Prospects for Digital Uzbekistan 2030: Development of a Digital Government System. *Web of Journals*, page 2(7).
3. Mo'ydinjonova, D. I. (2022–2023). Raqamli iqtisodiyotda axborot xavfsizligini ta'minlash usullari, 600-605 bet.
4. Saveljeva, J., Shipp, L., Mersinas, K., Panteli, N., & Mushtaq, H. (2025). A Survey on Digital Trust: Towards a Validated Definition. *Digital*, 5(2), page 14.
5. Shipp, L., Mersinas, K., Panteli, N., & Mushtaq, H. (2023). A Conceptual Exploration of Digital Trust. *UKAIS 2023* page 1-12.
6. Bodó, B. (2022). Maintaining trust in a technologized public sector. *Policy & Society*, 41(3), page 414–429.
7. Lim, H. L. J., Kang, X., Li, T., Wang, H., & Chu, C.-K. (2021). On the Trust and Trust Modelling for the Future Fully-Connected Digital World: A Comprehensive Study, page 43-45.
8. Buhnova, B. (2022). Trust Management in the Internet of Everything, 12-14 bet.
9. Kumar, A., Malik, A., Batra, I., Ahmad, N., & Johar, S. (2022). Digital society social interactions and trust analysis model. *PeerJ Computer Science*, page 1-12.
10. Dubrov, D. I. (2025). The Problem of Digital Trust and Readiness to Use Digital Technologies among Adolescents and Parents. *Population and Economics*, page 58-70.