RAQAMLI TRANSFORMATSIYA VA KIBERXAVFSIZLIK: DAVLAT BOSHQARUVI VA MOLIYAVIY BARQARORLIK XAVFI

Kurbonov Erkin Shavkatovich

Annotatsiya: Mazkur tezisda davlat boshqaruvida raqamli transformatsiya jarayonlari va ular bilan bog‘liq kiberxavfsizlik muammolari tahlil qilinadi. Xalqaro tajriba va statistik ma’lumotlar asosida raqamli infratuzilmaning moliyaviy barqarorlikka ta’siri o‘rganiladi.

Kalit so‘zlar: raqamli transformatsiya, kiberxavfsizlik, davlat boshqaruvi, moliyaviy barqarorlik, raqamli infratuzilma

Annotation: This thesis analyzes the process of digital transformation in public administration and associated cybersecurity challenges. Based on international experience and recent statistics, the study explores the impact of digital infrastructure on fiscal sustainability.

Key words: digital transformation, cybersecurity, public administration, fiscal sustainability, digital infrastructure

Аннотация: В диссертации анализируются процессы цифровой трансформации в государственном управлении и связанные с этим вопросы кибербезопасности. На основе международного опыта и статистических данных изучается влияние цифровой инфраструктуры на финансовую стабильность.

Ключевые слова: цифровая трансформация, кибербезопасность, государственное управление, финансовая устойчивость, цифровая инфраструктура

XXI asrda davlat boshqaruvida raqamli texnologiyalar jadal sur’atlarda joriy etilmoqda. Raqamli transformatsiya orqali davlat xizmatlarining ochiqligi, tezkorligi va fuqarolar bilan o‘zaro aloqasi yuqori darajaga ko‘tarilmoqda. Biroq bu imkoniyatlar bilan birga, davlat moliyasi va boshqaruv tizimlari kiberxavfsizlik tahdidlari ostida qolmoqda.

Ushbu mavzuning dolzarbligi shundaki, 2020-yillardan boshlab global siyosiy va iqtisodiy kun tartibiga chiqdi. Davlatlarning raqamli xizmat ko‘rsatish darajasi ortgani sari, ular duch kelayotgan tahdidlar ham murakkablashib bormoqda. O‘zbekiston ham raqamli transformatsiya strategiyasini ishlab chiqib, 2022–2026 yillarda amalga oshirishni belgiladi. Biroq, raqamli infratuzilma himoyasini ta'minlash bo‘yicha tizimli strategiyalar yetarli emas. Shu bois, mavzu ilmiy, siyosiy va iqtisodiy jihatdan dolzarb va zamonaviy tahdidlarni bartaraf etishga qaratilgan.

Mavzuning muammosi

Raqamli texnologiyalarni tezkor joriy etish va ularning hayotimizdagi roli tobora kengayib borayotgan bir paytda, davlat boshqaruvi tizimlari kiberhujumlar va ma’lumotlar xavfsizligiga oid muammolarga duch kelmoqda. Ayniqsa, davlat moliyasi, raqamli xizmatlar va fuqarolarga ko‘rsatiladigan onlayn xizmatlar tizimi zaifliklarga ega bo‘lib, bu O‘zbekiston uchun ham global xavf manbaiga aylanmoqda.

2023-yilga kelib, dunyo bo‘yicha kiberhujumlar soni 400 mingdan oshib, davlat sektorining ulushi 35% ga yetdi (OECD, 2024). Bu raqamlar davlat infratuzilmasining zaif himoyalanganligini anglatadi.

Muammoga ilmiy yechimlar

Zero Trust Architecture: foydalanuvchini doimiy identifikatsiya asosida tekshirish va kirishni qat’iy boshqarish modeli;

Cyber Governance modeli: raqamli xavfsizlikni davlat siyosatining ajralmas qismi sifatida boshqarish tizimi;

Malakali inson kapitali: davlat xizmatchilari uchun maxsus raqamli xavfsizlik kurslari va majburiy malaka oshirish;

Monitoring va tezkor javob berish tizimlari: xakerlik urinishlarini real vaqt rejimida aniqlash va zararsizlantirish tizimlari;

Xalqaro tajriba asosida qonunchilikni takomillashtirish (Estoniya, AQSh, Isroil tajribasi).

McKinsey (2024) hisob-kitoblariga ko‘ra, 2023-yilda dunyo bo‘yicha davlat sektorlariga qilingan kiberhujumlar soni 38 foizga oshgan. Ayniqsa, moliyaviy va soliq boshqaruvi, raqamli tender platformalari va davlat xaridlari tizimlariga qilingan hujumlar global miqyosda xavotir uyg‘otmoqda.

1-jadval.

Dunyo davlatlarida davlat sektoriga nisbatan kiberhujumlar statistikasi (2021–2023)

№	Yillar	Kiberhujumlar soni (ming)	Davlat sektoridagi ulushi (%)
1	2021	245	22%
2	2022	292	29%
3	2023	403	35%

Manba: *OECD Global Cybersecurity Outlook, 2024*

Raqamli infratuzilma o‘sib borar ekan, “Cyber Governance” tamoyillariga asoslangan boshqaruv mexanizmlari muhim ahamiyat kasb etmoqda. Harvard Kennedy School (2022) raqamli xavfsizlikni davlat moliyaviy barqarorligining asosi deb hisoblaydi:

"Digital infrastructure is the nervous system of government. If it fails, the state itself is paralyzed." (Harvard Kennedy School, 2022)

Xalqaro tajribalar

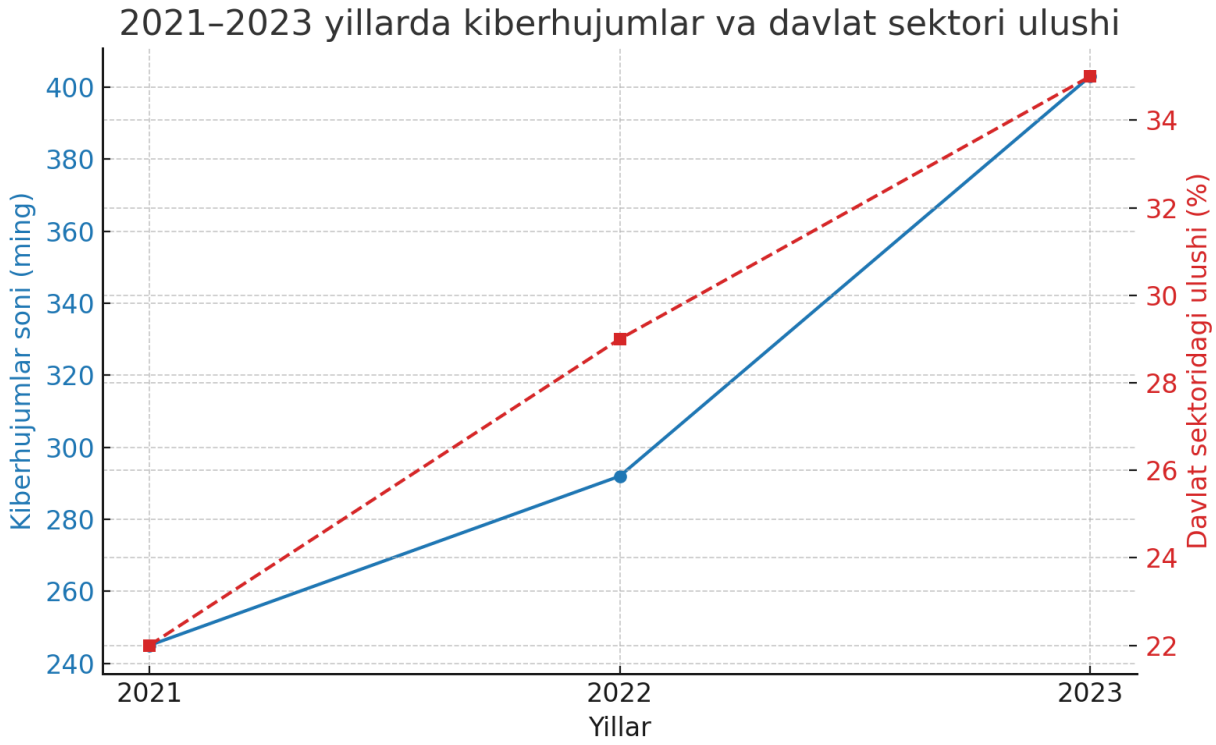
Estoniya 2007-yilgi keng qamrovli kiberhujumdan so‘ng, butun boshqaruv tizimini qayta ko‘rib chiqdi. 2023-yilga kelib Estoniya 99% davlat xizmatlarini onlayn ko‘rsatadi va Global Cybersecurity Index’da 2-o‘rinni egalladi (ITU, 2023).

Isroil har yili kiberxavfsizlik sohasiga 1 milliard dollardan ortiq investitsiya ajratib, innovatsion texnologiyalar yordamida davlat moliya platformalarini avtomatik monitoring qiladi.

AQSh esa 2021-yildan boshlab barcha federal agentliklarda “Zero Trust Architecture” modelini bosqichma-bosqich joriy etmoqda. Bu model foydalanuvchini doimiy tekshiruv asosida tanib olish orqali moliyaviy va boshqaruv ma’lumotlarini muhofaza qiladi.

O‘zbekiston misolida

O‘zbekistonda 2022–2023 yillarda raqamli platformalar (my.gov.uz, E-soliq, Openbudget.uz) faol joriy etildi. Biroq, Raqamli texnologiyalar vazirligi ma’lumotlariga ko‘ra, hali ham aksariyat davlat tashkilotlari raqamli xavfsizlik siyosatini to‘liq ishlab chiqmagan. 2023-yilda O‘zbekistonning ayrim viloyatlarida 11 ta davlat tashkiloti ma’lumotlar bazasiga noqonuniy kirishga urinish holatlari qayd etilgan (Raqamli xavfsizlik markazi, 2024).



1-infografika. 2021–2023 yillarda global kiberhujumlar soni va davlat sektorining ulushi.

2021–2023 yillarda global kiberhujumlar soni va davlat sektorining ulushi tasvirlangan grafik quyidagicha:

Ko‘k chiziq: jami kiberhujumlar soni (mingta);

Qizil chiziq: davlat sektoriga to‘g‘ri kelgan foiz ulushi (%).

Kiberxavfsizlik bugungi kunda faqat texnik muammo emas, balki moliyaviy, siyosiy va boshqaruviy barqarorlik garovi hisoblanadi. Raqamli transformatsiyaning ijobiy natijalari faqatgina xavfsizlik choralari bilan uyg‘unlashgandagina to‘liq samara beradi.

"Cybersecurity is no longer just an IT issue — it's a public governance priority." (World Bank, 2023)

Shu bois, O‘zbekiston uchun ham quyidagi yo‘nalishlar dolzarb hisoblanadi:

Davlat sektorida kiberxavfsizlik siyosatini qonuniy va institutsional darajada mustahkamlash;

Moliyaviy axborot tizimlarida "Zero Trust" modelini bosqichma-bosqich joriy etish;

Davlat xizmatchilarini kiberxavfsizlik bo‘yicha tayyorlash va doimiy malaka oshirish tizimini yaratish;

Raqamli platformalarda xakerlikka qarshi monitoring va tezkor javob tizimlarini kuchaytirish;

Xalqaro tajriba va texnologiyalarni tatbiq etish orqali milliy xavfsizlikni mustahkamlash.

Bu yo‘nalishlardagi strategik harakatlar orqali nafaqat raqamli boshqaruv samaradorligi, balki davlat moliyasi xavfsizligi ham yuqori darajada ta'minlanadi.

YAKUNIY XULOSA VA TAKLIFLAR

Raqamli transformatsiya – bu nafaqat texnologik yangilanish, balki moliyaviy va siyosiy barqarorlikni ta’minlashga xizmat qiluvchi jarayondir. Kiberxavfsizlik choralari bu transformatsiyaning muvaffaqiyatli kechishini belgilaydi.

Shu bois, quyidagi takliflar dolzarb hisoblanadi:

Raqamli xavfsizlik strategiyasini davlat boshqaruvi reformalari bilan uyg‘unlashtirish;

Har bir yangi raqamli xizmatni joriy etishdan oldin xavfsizlik auditi o‘tkazish;

Mahalliy va xalqaro tajriba asosida raqamli qonunchilikni rivojlantirish;

Kiberxavfsizlik bo‘yicha davlat-xususiy sheriklik asosida investitsiyalarni jalb qilish;

Axborot texnologiyalari bo‘yicha mustaqil monitoring institutlarini shakllantirish va ularning faoliyatini qonuniylashtirish.

Kiberxavfsizlik – davlat suverenitetining yangi ifodasi, raqamli mustaqillikning muhim kafolati hisoblanadi. Bu boradagi har qanday sustkashlik davlat moliyasi, axborot suvereniteti va jamiyat ishonchiga salbiy ta’sir qilishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Deloitte. (2023). *Cyber Governance in Public Financial Systems*. Deloitte Insights. www2.deloitte.com

2. Harvard Kennedy School. (2022). *Digital Infrastructure and the Modern State*. Cambridge, MA: Harvard University.

3. ITU. (2023). *Global Cybersecurity Index Report*. International Telecommunication Union. www.itu.int

4. McKinsey & Company. (2024). *Global Cyber Threat Landscape Report*. McKinsey Digital. www.mckinsey.com

5. OECD. (2024). *Global Cybersecurity Outlook*. Paris: Organisation for Economic Co-operation and Development. www.oecd.org

6. Raqamli texnologiyalar vazirligi. (2023). *O‘zbekiston raqamli infratuzilmasining xavfsizlik holati* (analitik sharh). Toshkent.

7. Raqamli xavfsizlik markazi. (2024). *Kiberxavf-xatarlar va davlat sektorida holatlar bo‘yicha sharh*. O‘zbekiston Respublikasi Raqamli xavfsizlik agentligi.

8. World Bank. (2023). *Cybersecurity and Public Governance: A Global Outlook*. Washington, DC: The World Bank Group. www.worldbank.org