DAVLAT XIZMATLARINI RAQAMLASHTIRISHDA KIBERXAVFSIZLIK MUAMMOLARI VA ULARNI BARTARAF ETISH YO'LLARI

Sultonboyev Otabek Dilshodbek o‘g‘li
Ichki Ishlar Vazirligi Akademiyasi 3-bosqich kursanti
Kurbanov Tuygun Tuychiyevich
IIV Akademiyasi Saf qismi otryad komandiri, leytenant

Annotatsiya: Mazkur maqolada davlat xizmatlarini raqamlashtirish jarayonida yuzaga keladigan kiberxavfsizlik muammolari tizimli tahlil qilingan. Elektron hukumat platformalari, yagona interaktiv davlat xizmatlari portallari va milliy ma'lumotlar bazalarining zaif tomonlari, ular duch keladigan asosiy kiber tahdid turlari, huquqiy-tashkiliy kamchiliklar va inson omili bilan bog'liq xavflar ko'rib chiqilgan. Tadqiqot davomida xorijiy davlatlarning ilg'or tajribasi, xalqaro standartlar (ISO/IEC 27001, NIST Cybersecurity Framework) va O'zbekiston Respublikasining amaldagi qonunchiligi qiyosiy tahlil qilindi. Natijada, texnik, tashkiliy-huquqiy va kadrlar salohiyatini oshirishga yo'naltirilgan kompleks yechimlar taklif etilgan, jumladan, "Zero Trust" arxitekturasini joriy etish, ma'lumotlarni kriptografik himoyalash, kiber insidentlarga javob berish markazlarini (SOC/CERT) rivojlantirish va aholi hamda davlat xizmatchilarining kiber-savodxonligini oshirish bo'yicha tavsiyalar ishlab chiqilgan.

Kalit so'zlar: raqamli hukumat; kiberxavfsizlik; elektron davlat xizmatlari.

Kirish

So'nggi o'n yillikda dunyo mamlakatlarida davlat boshqaruvini raqamlashtirish jarayoni jadal sur'atlar bilan rivojlanmoqda. Elektron hukumat (e-government) tizimlari fuqarolarga soliq, ijtimoiy ta'minot, ta'lim, sog'liqni saqlash, mulkiy va boshqa xizmatlarni onlayn tartibda, tezkor va shaffof shaklda taqdim etish imkonini beradi. O'zbekistonda ham "Raqamli O'zbekiston – 2030" strategiyasi va "Yagona interaktiv davlat xizmatlari portali" (my.gov.uz) kabi loyihalar orqali davlat xizmatlarining raqamli transformatsiyasi izchil amalga oshirilmoqda.

Biroq, davlat xizmatlarining raqamlashtirilishi bilan bir qatorda, ularning kiberxavfsizligini ta'minlash muammosi ham dolzarblashib bormoqda. Davlat axborot tizimlari millionlab fuqarolarning shaxsiy, moliyaviy va biometrik ma'lumotlarini o'zida jamlaganligi sababli, ular kiberjinoyatchilar, davlat qo'llab-quvvatlaydigan hakerlik guruhlari va boshqa zararli aktorlar uchun

jozibali nishonga aylanmoqda. Kiberhujumlar natijasida yuzaga keladigan har qanday buzilish nafaqat moliyaviy zarar, balki fuqarolarning davlat institutlariga bo'lgan ishonchining pasayishiga, milliy xavfsizlikka tahdidga va kritik infratuzilmaning ishdan chiqishiga olib kelishi mumkin.

Mazkur maqolaning maqsadi — davlat xizmatlarini raqamlashtirish sharoitida yuzaga keladigan kiberxavfsizlik muammolarini kompleks tarzda tahlil qilish, ularning asosiy sabablarini aniqlash va amaliyotda qo'llash mumkin bo'lgan samarali yechimlar tizimini taklif etishdan iborat.

Adabiyotlar Tahlili Va Muammoning Qo'yilishi

Elektron hukumat kiberxavfsizligi mavzusi xalqaro ilmiy adabiyotda faol o'rganilmoqda. Birlashgan Millatlar Tashkilotining E-Government Development Index (EGDI) hisobotlari, Xalqaro Telekommunikatsiya Ittifoqi (ITU) tomonidan chop etiladigan Global Cybersecurity Index, shuningdek, NIST (AQSh Milliy standartlar va texnologiyalar instituti) va ENISA (Yevropa Ittifoqining kiberxavfsizlik agentligi) tomonidan ishlab chiqilgan uslubiy hujjatlar davlat sektorida axborot xavfsizligini ta'minlashning nazariy va amaliy asoslarini belgilaydi.

Tadqiqotchilar ta'kidlashicha, davlat axborot tizimlaridagi zaifliklarning aksariyati uch asosiy omilga bog'liq: birinchidan, tizimlarning arxitekturaviy va texnologik eskirganligi; ikkinchidan, kiberxavfsizlik sohasidagi huquqiy-tashkiliy bazaning yetarli darajada rivojlanmaganligi; uchinchidan, davlat xizmatchilari va fuqarolarning kiber-savodxonlik darajasining pastligi. Shu bilan birga, mavjud adabiyotlarda ushbu uch omilni bir-biri bilan uzviy bog'liq holda, kompleks yondashuv asosida bartaraf etish zarurligi alohida ta'kidlanadi, bu esa mazkur tadqiqotning dolzarbligini belgilaydi.

Tadqiqot Metodologiyasi

Tadqiqot jarayonida ilmiy bilishning quyidagi umumnazariy va maxsus metodlaridan foydalanildi:

- tizimli va qiyosiy tahlil metodi — turli mamlakatlarning elektron hukumat kiberxavfsizligi tajribasini solishtirish uchun;
- kontent-tahlil metodi — xalqaro standartlar, me'yoriy-huquqiy hujjatlar va ilmiy adabiyotlarni o'rganish uchun;
- tasniflash metodi — kiber tahdidlarni turkumlarga ajratish va ularning davlat xizmatlariga ta'sirini baholash uchun;
- induktiv-deduktiv metod — aniqlangan muammolar asosida umumlashtirilgan yechimlar va tavsiyalar shakllantirish uchun.

Tadqiqot uchun manba sifatida xalqaro tashkilotlarning ochiq hisobotlari, milliy qonunchilik hujjatlari (jumladan, "Axborotlashtirish to'g'risida"gi, "Shaxsga doir ma'lumotlar to'g'risida"gi qonunlar) va sohaga oid ilmiy-amaliy nashrlar tahlil qilindi.

Natijalar Va Tahlil

4.1. Davlat axborot tizimlariga xos asosiy zaifliklar

Davlat xizmatlarini raqamlashtirish jarayonida quyidagi tizimli zaifliklar aniqlandi:

1. Infratuzilma zaifligi — ko'plab davlat muassasalarida eskirgan server va tarmoq uskunalari, yangilanmagan operatsion tizimlar va litsenziyalanmagan dasturiy ta'minotdan foydalanish davom etmoqda, bu esa ma'lum zaifliklardan (known vulnerabilities) foydalangan hujumlar ehtimolini oshiradi.

2. Markazlashgan bo'lmagan boshqaruv — turli vazirlik va idoralarning axborot tizimlari bir-biridan mustaqil, turli standartlar asosida yaratilgani sababli, yagona kiberxavfsizlik siyosatini amalga oshirish qiyinlashadi.

3. Identifikatsiya va avtorizatsiya tizimidagi kamchiliklar — ko'p tizimlarda ikki bosqichli autentifikatsiya (2FA/MFA) joriy etilmagan, bu esa parol o'g'irlash orqali ruxsatsiz kirish xavfini kuchaytiradi.

4. Ma'lumotlarni shifrlashning yetarli emasligi — uzatiladigan va saqlanadigan ma'lumotlarning barcha turlari uchun zamonaviy kriptografik algoritmlar to'liq qo'llanilmaydi.

5. Kadrlar salohiyatining yetishmasligi — malakali kiberxavfsizlik mutaxassislarining davlat sektoridagi yetishmovchiligi va ularning xususiy sektorga nisbatan past ish haqi tufayli ushlab qolinmasligi.

6. Huquqiy-me'yoriy bazadagi bo'shliqlar — kiber insidentlar to'g'risida xabar berish tartib-taomillari, javobgarlik chegaralari va idoralararo hamkorlik mexanizmlarining aniq belgilanmaganligi.

7. Uchinchi tomon (yetkazib beruvchilar) xavfi — dasturiy ta'minot va uskunalarni xorijiy yetkazib beruvchilardan olish natijasida yuzaga keladigan "ta'minot zanjiri" (supply chain) xavfsizligi masalalari.

4.2. Asosiy kiber tahdid turlari va ularning ta'siri

Davlat axborot tizimlariga xos bo'lgan asosiy kiber tahdid turlari va ularning ehtimoliy oqibatlari quyidagi jadvalda umumlashtirilgan:

Tahdid turi Qisqacha tavsifi Davlat xizmatlariga ta'siri

Fishing va ijtimoiy muhandislik Foydalanuvchi va xodimlarni aldab, login-parol yoki shaxsiy ma'lumotlarni egallash Elektron hukumat portallariga ruxsatsiz kirish, identifikatsiya tizimining buzilishi

DDoS hujumlari Serverlarni ortiqcha so'rovlar bilan to'ldirib ishdan chiqarish Onlayn xizmatlarning vaqtincha ishlamay qolishi, aholi ishonchining pasayishi

Zararli dasturlar va ransomware Tizimga kirib, ma'lumotlarni shifrlash yoki yo'q qilish Ma'lumotlar bazasining shifrlanishi, davlat xizmatlarining to'xtab qolishi

Ma'lumotlar sızıb chiqishi (data leakage) Shaxsiy va maxfiy ma'lumotlarning ruxsatsiz oshkor bo'lishi Fuqarolar shaxsiy ma'lumotlarining uchinchi shaxslar qo'liga tushishi

Insayder tahdidlar Tizimga qonuniy kirish huquqiga ega xodimlarning suiste'mol qilishi Ichki nazoratning zaiflashishi, ma'lumotlarning maqsadli buzilishi

Eskirgan dasturiy ta'minot (legacy systems) Yangilanmagan tizimlardagi ma'lum zaifliklardan foydalanish Kritik infratuzilmaning barqarorligiga tahdid

1-jadval. Davlat axborot tizimlariga xos asosiy kiber tahdidlar tasnifi

4.3. Institutsional va huquqiy muammolar

Texnik zaifliklardan tashqari, davlat xizmatlarini raqamlashtirishda institutsional va huquqiy xarakterdagi muammolar ham muhim o'rin tutadi. Xususan, kiberxavfsizlik bo'yicha yagona idoralararo muvofiqlashtirish mexanizmining yetarli darajada shakllanmaganligi, davlat va xususiy sektor o'rtasida ma'lumot almashish (public-private partnership) tizimining zaifligi, shuningdek, kiber insidentlar yuzasidan jinoiy-huquqiy javobgarlikni belgilash va xalqaro huquqiy hamkorlikni amalga oshirishdagi qiyinchiliklar mavjud. Bundan tashqari, shaxsiy ma'lumotlarni himoya qilish bo'yicha qonunchilikning amaliyotga to'liq tatbiq etilmaganligi fuqarolarning ma'lumotlariga nisbatan qo'shimcha xavf yaratadi.

Yechimlar Va Tavsiyalar

Yuqorida aniqlangan muammolarni bartaraf etish uchun quyidagi kompleks, ko'p bosqichli yondashuv asosidagi yechimlar taklif etiladi. Yechimlar texnik, tashkiliy-boshqaruv, huquqiy va kadrlar salohiyati bo'yicha to'rt yo'nalishga ajratilgan.

5.1. Texnik yechimlar

- "Zero Trust" (nol ishonch) arxitekturasini joriy etish — tarmoq ichidagi har bir so'rovni, foydalanuvchi joylashuvidan qat'i nazar, doimiy tekshirishga asoslangan model orqali ruxsatsiz kirishlarning oldini olish.
- Ko'p bosqichli autentifikatsiya (MFA) va biometrik identifikatsiyani barcha davlat portallari uchun majburiy qilish.
- Ma'lumotlarni end-to-end shifrlash — uzatish va saqlash bosqichlarida zamonaviy kriptografik standartlarni (masalan, AES-256, TLS 1.3) qo'llash.
- Davlat bulut infratuzilmasini (GovCloud) yaratish — barcha davlat axborot tizimlarini yagona, markazlashgan xavfsizlik standartlariga ega bulut muhitiga ko'chirish.
- Doimiy monitoring va tahdidlarni aniqlash tizimlarini (SIEM, IDS/IPS) joriy etish, sun'iy intellekt asosidagi anomaliyalarni aniqlash algoritmlaridan foydalanish.

• Muntazam zaifliklarni baholash (penetration testing) va "bug bounty" dasturlarini yo'lga qo'yish orqali tizimdagi zaifliklarni oldindan aniqlash.

• Zaxira nusxalash (backup) va falokatlardan keyin tiklash (disaster recovery) rejalarini har bir davlat tizimi uchun ishlab chiqish va muntazam sinovdan o'tkazish.

5.2. Tashkiliy-boshqaruv yechimlari

• Milliy darajada yagona Kiberxavfsizlik markazi (SOC) va kompyuter insidentlariga tezkor javob berish markazi (CERT/CSIRT) tarmog'ini kuchaytirish va barcha davlat idoralarini unga ulash.

• Har bir davlat muassasasida axborot xavfsizligi bo'yicha mas'ul shaxs (CISO) lavozimini joriy etish va uning vakolatlarini normativ hujjatlar bilan mustahkamlash.

• Davlat va xususiy sektor o'rtasida kiberxavfsizlik bo'yicha strategik hamkorlik (Public-Private Partnership) mexanizmini yo'lga qo'yish, tahdidlar to'g'risidagi ma'lumotlarni real vaqt rejimida almashish tizimini yaratish.

• Kiber insidentlarni boshqarish bo'yicha yagona reglament va javobgarlik zanjirini (incident response plan) ishlab chiqish hamda uni davriy mashg'ulotlar orqali sinash.

5.3. Huquqiy-me'yoriy yechimlar

• Shaxsiy ma'lumotlarni himoya qilish to'g'risidagi qonunchilikni xalqaro standartlarga (masalan, Yevropa Ittifoqining GDPR tajribasiga) muvofiqlashtirish va uning amaliy ijrosini kuchaytirish.

• Davlat axborot resurslarining tasniflanishi (maxfiylik darajalari bo'yicha) va har bir toifa uchun aniq xavfsizlik talablarini belgilovchi me'yoriy hujjatlarni takomillashtirish.

• Kiber jinoyatlar bo'yicha jinoiy javobgarlikni kuchaytirish va xalqaro huquqiy hamkorlik (jumladan, Budapesht konventsiyasi tamoyillari asosida) mexanizmlarini rivojlantirish.

• Davlat xizmatlari uchun dasturiy ta'minot va uskunalarni xarid qilishda kiberxavfsizlik talablarini majburiy tender shartiga aylantirish ("security by design" tamoyili).

5.4. Kadrlar salohiyati va ijtimoiy ong yechimlari

Davlat xizmatchilari uchun kiberxavfsizlik bo'yicha majburiy va davriy malaka oshirish kurslarini joriy etish.

Oliy ta'lim tizimida axborot xavfsizligi yo'nalishi bo'yicha kadrlar tayyorlashni kengaytirish va davlat sektorida ishlash uchun moliyaviy rag'batlantirish choralarini ko'rish.

Aholi orasida kiber-savodxonlikni oshirish bo'yicha ommaviy axborot kampaniyalarini (fishing, ijtimoiy muhandislikdan himoyalanish bo'yicha) muntazam tashkil etish.

Davlat muassasalarida ichki kiber-gigiyena madaniyatini shakllantirish — parollarni boshqarish, shubhali xat va havolalarni aniqlash bo'yicha amaliy trening va simulyatsiyalarni o'tkazish.

Muhokama

Tahlil natijalari shuni ko'rsatadiki, davlat xizmatlarini raqamlashtirishda kiberxavfsizlikni ta'minlash faqat texnik masala emas, balki tashkiliy, huquqiy va ijtimoiy jihatlarni qamrab oluvchi kompleks tizimli muammodir. Faqat texnik vositalarga (masalan, yangi dasturiy ta'minot yoki uskunalarga) sarmoya kiritish, agar u tashkiliy boshqaruv va kadrlar salohiyatini oshirish bilan uyg'unlashtirilmasa, kutilgan natijani bermaydi. Xalqaro tajriba (Estoniya, Janubiy Koreya, Singapur kabi mamlakatlarning elektron hukumat modellari) shuni ko'rsatadiki, muvaffaqiyatli raqamli transformatsiya, birinchi navbatda, kiberxavfsizlikni loyihalashtirish bosqichidan boshlab tizimga singdirish ("security by design") tamoyiliga asoslanadi.

Shu bilan birga, taklif etilgan yechimlarni amalga oshirish bir qator cheklovlar bilan bog'liq — bu, avvalambor, moliyaviy resurslarning cheklanganligi, malakali kadrlar tanqisligi va davlat idoralari o'rtasidagi muvofiqlashtirishning murakkabligidir. Shu sababli, yechimlarni bosqichma-bosqich, ustuvorlik darajasiga ko'ra amalga oshirish, dastlab eng kritik axborot tizimlarini (soliq, bank-moliya, sog'liqni saqlash sohalarini) qamrab olishdan boshlash maqsadga muvofiqdir.

Xulosa

Xulosa qilib aytganda, davlat xizmatlarini raqamlashtirish jarayonida kiberxavfsizlikni ta'minlash zamonaviy davlat boshqaruvining ustuvor vazifalaridan biriga aylanmoqda. O'tkazilgan tahlil davomida aniqlangan asosiy muammolar — texnik infratuzilmaning eskirganligi, institutsional muvofiqlashtirishning yetishmasligi, huquqiy bazadagi bo'shliqlar va kadrlar salohiyatining pastligi — o'zaro bog'liq bo'lib, ularni faqat kompleks yondashuv asosida bartaraf etish mumkin.

Taklif etilgan texnik (Zero Trust, MFA, shifrlash, SOC/CERT), tashkiliy-huquqiy (CISO instituti, PPP mexanizmi, qonunchilikni takomillashtirish) va kadrlar salohiyatini oshirishga yo'naltirilgan chora-tadbirlar davlat axborot tizimlarining barqarorligini, fuqarolar ma'lumotlarining xavfsizligini va, natijada, raqamli davlat xizmatlariga bo'lgan jamoatchilik ishonchini sezilarli darajada oshirishga xizmat qiladi. Kelgusi tadqiqotlar sun'iy intellekt asosidagi kiberhimoya vositalarining davlat sektoridagi samaradorligini chuqurroq o'rganishga qaratilishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni

(yangi tahriri). — Toshkent, 2023.
2. O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni. — Toshkent, 2019.
3. O'zbekiston Respublikasi Prezidentining "Raqamli O'zbekiston – 2030" strategiyasini tasdiqlash to'g'risida"gi Farmoni.
5. International Telecommunication Union (ITU). Global Cybersecurity Index (GCI) Report. — Geneva: ITU Publications.
6. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework), Version 1.1. — Gaithersburg, MD: NIST.
7. International Organization for Standardization. ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva: ISO.
8. United Nations Department of Economic and Social Affairs (UN DESA). E-Government Survey: Digital Government in the Decade of Action for Sustainable Development. — New York: United Nations.
9. European Union Agency for Cybersecurity (ENISA). Threat Landscape Report. — Athens: ENISA.
10. European Parliament and Council. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.
11. Council of Europe. Convention on Cybercrime (Budapest Convention), ETS No. 185.
1. York: Little, Brown and Company.