KIBERXAVFSIZLIK TAHDIDLARI VA ULARNING TURLARI

Xusenova Latofat Amridinovna
Xalmuratov Omonboy Utamuratovich
ilmiy rahbar

Annotatsiya. *Mazkur tezisda kiberxavfsizlik tushunchasi, zamonaviy axborot makonida yuzaga kelayotgan asosiy tahdidlar va ularning klassifikatsiyasi tahlil qilinadi. Shuningdek, turli xil kiberhujumlarning xususiyatlari hamda ularning oldini olish mexanizmlari ko'rib chiqiladi.*

Kalit so'zlar: *kiberxavfsizlik, kiberhujum, phishing, malware, DDoS, axborot xavfsizligi.*

So'nggi yillarda O'zbekiston Respublikasida raqamli iqtisodiyotni rivojlantirish, davlat xizmatlarini elektron shaklga o'tkazish va axborot-kommunikatsiya texnologiyalarini keng joriy etish jarayonlari sezilarli darajada jadallashdi. Xususan, "Elektron hukumat to'g'risida"gi qonun, "Axborotlashtirish to'g'risida"gi qonun hamda axborot xavfsizligini ta'minlashga qaratilgan normativ-huquqiy hujjatlar asosida davlat va jamiyat hayotining ko'plab sohalari raqamlashtirilmoqda. Mazkur jarayonlar aholiga qulaylik yaratish bilan birga, axborot tizimlari va resurslarini himoya qilish masalasini dolzarb muammoga aylantirmoqda. Shu nuqtai nazardan, kiberxavfsizlikni ta'minlash davlat siyosatining ustuvor yo'nalishlaridan biri sifatida shakllanmoqda.

Shuningdek, raqamli infratuzilmaning kengayishi bilan bir qatorda turli xil kiber tahdidlar ham ortib bormoqda. Xususan, moliyaviy firibgarlik, phishing hujumlari, zararli dasturlar orqali ma'lumotlarni qo'lga kiritish kabi holatlar tez-tez uchramoqda. Bu esa nafaqat alohida foydalanuvchilar, balki bank-moliya tizimi, davlat organlari va biznes subyektlari uchun ham jiddiy xavf tug'diradi. Shu sababli, amaldagi qonunchilik va xalqaro tajriba asosida kiberxavfsizlik tahdidlarini tizimli tahlil qilish hamda ularning oldini olish mexanizmlarini takomillashtirish muhim ilmiy va amaliy ahamiyat kasb etadi.

O'zbekiston Respublikasining raqamli suverenitetini ta'minlash sharoitida kiberxavfsizlik tahdidlarining transformatsiyasi nafaqat texnologik, balki ijtimoiy-iqtisodiy xavfsizlikning fundamental asosi sifatida namoyon bo'lmoqda. Global kiber-makonda kuzatilayotgan "kiber-urushlar" va "kiber-josuslik" elementlari milliy segment uchun ham begona emas. Tadqiqotlar shuni ko'rsatadiki, O'zbekiston moliya-bank tizimi va davlat boshqaruvi apparatiga qaratilgan hujumlar o'zining murakkabligi bo'yicha yangi bosqichga ko'tarildi. Xususan, an'anaviy virusli dasturlardan ko'ra, sun'iy intellektga asoslangan adaptiv tahdidlar va inson psixologiyasini manipulyatsiya qiluvchi ijtimoiy muhandislik usullari ustunlik qilmoqda. O'zbekiston sharoitida kiber-tahdidlarning asosiy

xavf darajasi “Raqamli O‘zbekiston – 2030” strategiyasi doirasida joriy etilayotgan yagona elektron hukumat ekotizimi va banklararo tranzaksiyalarning markazlashganiga bog‘liqdir. Ushbu markazlashuv, bir tomondan qulaylik yaratsa, ikkinchi tomondan bitta nuqtadan tizimli xavfni keltirib chiqarish ehtimolini oshiradi.

Kiberxavfsizlik tahdidlarining tasnifida **APT (Advanced Persistent Threats)** hujumlari eng jiddiy xavf hisoblanadi. Bu turdagi hujumlar uzoq vaqt davomida tizimda sezilmasdan qolishi va strategik ma’lumotlarni sizdirishi bilan xarakterlanadi. O‘zbekistondagi yirik korxonalarda qo‘llanilayotgan eskirgan dasturiy ta’minotlar va “legacy systems” (meros bo‘lib qolgan tizimlar) bunday hujumlar uchun ochiq eshik bo‘lib xizmat qilmoqda. Shuningdek, so‘nggi yillarda “Ransomware-as-a-Service” (RaaS) modeli orqali amalga oshirilayotgan tovlamachilik hujumlari mahalliy biznes sub’ektlari uchun katta moliyaviy yo‘qotishlarga sabab bo‘lmoqda. Ushbu jarayonda kiber-jinoyatchilar nafaqat ma’lumotlarni shifrlaydi, balki ularni ochiq tarmoqqa chiqarish bilan tahdid qilib, ikki tomonlama shantaj usulini qo‘llamoqda. O‘zbekiston qonunchiligida kiber-gigiyena va kiber-savodxonlik masalalari bo‘yicha normativlar mavjud bo‘lsa-da, amaliyotda “inson omili” eng zaif nuqta bo‘lib qolmoqda. Ijtimoiy muhandislikning lokal ko‘rinishlari, masalan, Telegram messenjeridagi milliy brendlar yoki davlat tashkilotlari nomidan ochilgan soxta botlar orqali amalga oshirilayotgan fishing hujumlari aholining raqamli savodxonligi texnologik taraqqiyotdan orqada qolayotganini ko‘rsatadi.

Matematik nuqtai nazardan kiberxavfsizlikni ta’minlashda ma’lumotlar yaxlitligi va maxfiyligini baholash uchun entropiya ko‘rsatkichlari va kriptografik barqarorlik ko‘rsatkichlari qo‘llaniladi. Milliy kriptografik standartlar asosida ishlab chiqilgan algoritmlar (masalan, O‘z DSt 1106:2009) kvant kompyuterlari davrida yangicha himoya qatlamlarini talab qiladi. Post-kvant kriptografiyasi metodlarini milliy infratuzilmaga integratsiya qilish masalasi bugun ilmiy jamoatchilik oldida turgan o‘ta dolzarb vazifadir. Bunda axborot tizimining xavfsizlik holatini quyidagi formula yordamida baholash mumkin:

$$S = \sum_{i=1}^{n} (P_i * V_i) - R_{tech}$$

Bunda P_i– tahdidning yuzaga kelish ehtimoli, V_i – tizimning zaiflik darajasi, R_{tech} – joriy etilgan texnik himoya vositalarining samaradorlik koeffitsienti.

Formula mantig’i quyidagicha:

1. Har bir tahdid uchun individual xavf darajasi hisoblanadi: P_i*U_i.
2. Barcha tahdidlar bo’yicha havflar yig’indisi olinadi: ∑(P_i*U_i).
3. Texnik himoya vositalarining samaradorligi umumiy xavfdan ayriladi: $R_{tech.}$

Hisoblashga misol:

Tahdid turi	**P_i**	**U_i**	**P_i*U_i.**
Phishing	0.7	0.8	0.56
DDoS	0.4	0.6	0.24
Ransomware	0.5	0.9	0.45
Yig'indi			**1.25**

O‘zbekistonda kiber-muhitni sog‘lomlashtirish uchun “Nolga teng ishonch” (Zero Trust Architecture) tamoyilini davlat darajasida tatbiq etish zarur. Bu tamoyilga ko‘ra, tizim ichidagi yoki tashqarisidagi har qanday so‘rov shubhali deb hisoblanadi va har safar qayta autentifikatsiyadan o‘tkaziladi. Shu bilan birga, bulutli texnologiyalar (Cloud Computing) va narsalar interneti (IoT) qurilmalarining milliy segmentda kengayishi yangi turdagi kiber-fizik tahdidlarni keltirib chiqarmoqda. Masalan, “aqlli shahar” tizimlarining kiber-hujumga uchrashi real fizik zararga (transport tizimi yoki energetika tarmog‘ining ishdan chiqishiga) olib kelishi mumkin.

O’zbekistonda kibertahdidlar statistikasi 2022-2024 yillar oralig’ida quyidagicha bo’lganligi aniqlangan:

Ko’rsatkich	Qiymat
Ro’yxatga olingan kiberxujumlar soni (2023)	1200+ (CERT.UZ ma’lumoti)
Phishing hujumlarning o’sishi (2022-2023)	+45%
RaaS hujumlardan zarar ko’rgan biznes subyektlari	230 ta kompaniya
Bank-moliya tizimiga qaratilgan hujumlar ulushi	38%
Davlat tizimlariga qaratilgan hujumlar	27%
Oddiy fuqarolarga qaratigan hujumlar	35%

O‘zbekistonning raqamli transformatsiya jarayoni kiberxavfsizlik tahdidlarining ham miqyos, ham sifat jihatidan evolyutsiyasiga sabab bo‘ldi. Tadqiqot natijalari shuni ko‘rsatadiki, milliy kiber-makonda ijtimoiy muhandislik usullari texnik zaifliklardan ko‘ra ko‘proq xavf tug‘dirmoqda va bu holat aholining raqamli savodxonligi hamda kiber-gigiyena madaniyati texnologik taraqqiyot sur’atlaridan ortda qolayotganini tasdiqlaydi. Bank-moliya va davlat xizmatlari segmentida “Zero Trust” (Nolga teng ishonch) modelining to‘liq joriy etilmaganligi, shuningdek, lokal serverlarda ma’lumotlar bazasini himoyalashda post-kvant kriptografiyasi kabi innovatsion yechimlarning yetishmasligi tizimli kiber-xatarlarni kuchaytirmoqda. Ayniqsa, sun’iy intellekt yordamida yaratilayotgan deepfake va adaptiv fishing hujumlari an’anaviy himoya tizimlarini chetlab o‘tishga qodirligi sababli, milliy kiber-qalqon tizimini intellektual monitoring algoritmlari bilan boyitish strategik zaruriyat hisoblanadi.

Kelgusida O‘zbekiston kiber-suverenitetini ta’minlash uchun nafaqat texnik infratuzilmani yangilash, balki institutsional va huquqiy bazani ham kiber-muhitning dinamik o‘zgarishlariga moslashtirish lozim. Bunga erishish uchun davlat va xususiy sektor hamkorligida (PPP) milliy kiber-operatsiyalar markazlarini (SOC)

takomillashtirish, kiber-jinoyatlarga qarshi kurashishda xalqaro standartlarni lokalizatsiya qilish va kadrlar tayyorlash tizimida “kiber-psixologiya” yo‘nalishini rivojlantirish taklif etiladi. Ma’lumotlarning kriptografik barqarorligini ta’minlashda milliy standartlarni kvant hisoblashlari tahdidiga tayyorlash va hududiy darajadagi kiber-insidentlarga tezkor javob berish guruhlarini (CERT) kengaytirish milliy iqtisodiyotning raqamli barqarorligini kafolatlaydi. Shunday qilib, kompleks kiber-strategiya nafaqat himoya vositasi, balki mamlakatning xalqaro reytinglardagi nufuzini oshiruvchi va xorijiy investitsiyalar uchun xavfsiz raqamli muhit yaratuvchi asosiy omil bo‘lib xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. O‘zbekiston Respublikasining Qonuni. Kiberxavfsizlik to‘g‘risida. O‘RQ-764-son. 2022-yil 15-aprel.
2. O‘zbekiston Respublikasi Prezidentining Farmoni. “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida. PF-6079-son. 2020-yil 5-oktyabr.
3. O‘zbekiston Respublikasi Prezidentining Qarori. Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi faoliyatini yanada takomillashtirish chora-tadbirlari to‘g‘risida. PQ-3549-son. 2018-yil 19-fevral.
4. O‘z DSt 1106:2009. Axborot texnologiyasi. Ma'lumotlarni kriptografik muhofaza qilish. Shifrlash algoritmi. (O‘zbekiston davlat standarti).
5. Ganiyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Darslik. – Toshkent: Aloqachi, 2019. – 420 b.
6. Mitnick, K. D., & Simon, W. L. The Art of Deception: Controlling the Human Element of Security. – Wiley Publishing, Inc., 2002. (Ijtimoiy muhandislik bo‘yicha dunyodagi asosiy qo‘llanma).
7. Hadnagy, C. Social Engineering: The Science of Human Hacking. – 2nd Edition. Wiley, 2018. – 320 p.
8. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. – 3rd Edition. Wiley, 2020. – 1232 p.
9. Sattarov A.R. “O‘zbekistonda kiberjinoyatchilikning o‘ziga xos xususiyatlari va ularga qarshi kurashish strategiyalari.” // Axborot texnologiyalari va telekommunikatsiya muammolari. – Toshkent, 2023.
10. Xamidov J.K. “Bank tizimida ijtimoiy muhandislik hujumlarini matematik modellashtirish.” // O‘zbekiston Milliy universiteti xabarlari. – 2024, №2.
11. Humayun, M., et al. “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study.” // IEEE Access, vol. 8, 2020.

12. Radziwill, N. M., & Benton, M. C. "Cybersecurity Management with the Zero Trust Framework." // Software Quality Professional, 2021.
13. www.cert.uz
14. https://www.itu.int
15. www.kaspersky.com.