

BOJXONA TIZIMIDA KIBERXAVFSIZLIKNI TA'MINLASH - DAVR TALABI

Rafikova Muattar Ravshanovna

Bojxona instituti "Ijtimoiy-gumanitar

fanlar" kafedrası boshlig'i,

pedagogika fanlari bo'yicha

falsafa fanlari doktori(PhD), dotsent, podpolkovnik

Nosirjonov Abdulaziz Sultonali o'g'li

O'zbekiston Respublikasi

Bojxona qo'mitasining Bojxona instituti,

Bojxona ishi yo'nalishi

1-kurs, 525-guruh kursanti

***Annotatsiya.** Ushbu maqolada bojxona tizimida kiberxavfsizlikni ta'minlash masalalari, kiberxavf-xatarlarning asosiy turlari, ularning bojxona faoliyatiga ta'siri hamda axborot xavfsizligini ta'minlashning zamonaviy usullari tahlil qilingan. Shuningdek, xalqaro tajriba asosida milliy bojxona tizimida kiberxavfsizlikni mustahkamlash yo'llari, xodimlarning axborot madaniyatini oshirish va texnik himoya vositalarini joriy etishning ahamiyati yoritib berilgan.*

***Kalit so'zlar:** Bojxona tizimi, raqamli texnologiyalar, kiberxavfsizlik, axborot xavfsizligi, elektron deklaratsiya, risklarni boshqarish, ma'lumotlarni himoya qilish, kiberhujumlar, DDoS, fishing va ijtimoiy muhandislik, xodimlarni o'qitish, kiberxavfsizlik siyosati, yagona interaktiv bojxona tizimi, E-Avtoyo'lovchi, Kiberxavfsizlik markazi.*

***Annotation.** This article analyzes the issues of ensuring cybersecurity in the customs system, the main types of cyber threats, their*

impact on customs activities, and modern methods of ensuring information security. It also highlights ways to strengthen cybersecurity in the national customs system based on international experience, the importance of improving the information culture of employees, and the introduction of technical protection tools.

Key words: *Customs system, digital technologies, cybersecurity, information security, electronic declaration, risk management, data protection, cyber attacks, DDoS, phishing and social engineering, employee training, cybersecurity policy, unified interactive customs system, E-Auto Passenger, Cybersecurity Center.*

O'zbekiston Respublikasi Bojxona tizimida ham so'nggi yillarda raqamli texnologiyalarni keng joriy etish yo'lida faol ish olib bormoqda. Ammo bu jarayonni tizimli ravishda boshqarish va uni xavflardan saqlash maqsadida yangi loyihalar va dasturlarni yaratishimiz kerak. Sirli axborotlar va ma'lumotlarning tarqalmasligi uchun dasturlarda xavfsizlik tizimini yaxshi rivojlantirgan bo'lishimiz kerak.

O'zbekiston Respublikasida 2022-yil 15-aprelda **“Kiberxavfsizlik to'g'risida”**gi 764-sonli qonun qabul qilingan bo'lib, ushbu qonunning maqsadi O'zbekistonning axborot makonida xavfsizlikni ta'minlashga qaratilgan. Unda axborot tizimlari va tarmoqlarini kiberhujumlardan himoya qilish, muhim axborot infratuzilmasini belgilash va uni himoyalash choralari ko'rsatilgan. Qonun davlat organlari, tashkilotlar va axborot tizimi vakillarining kiberxavfsizlik borasidagi majburiyatlarini belgilaydi, kiberxavfsizlik insidentlarini aniqlash, oldini olish va bartaraf etish tartibini yoritadi. Shuningdek, fuqarolar va tashkilotlarning huquqlari, vakolatli organlarning vazifalari hamda kiberxavfsizlikni ta'minlashga doir texnik va tashkiliy talablardan iborat. Shu jumladan **Bojxona qo'mitasi** axborot tizimlarining

xavfsizligini ta'minlashga alohida e'tibor qaratildi, **tizimda** so'nggi yillarda "Yagona interaktiv bojxona axborot tizimi", "E-Avtoyo'lovchi", "Risklarni tahlil qilish moduli" kabi elektron tizimlarni ishlab chiqildi. Elektron tizimlarni himoyalashda bojxona organlari **Milliy sertifikatlashtirilgan kiberxavfsizlik markazlari** bilan hamkorlik qilib kelmoqda [1].

Bojxona tizimi – davlat chegaralari orqali tovarlar va transport vositalarining harakatini nazorat qiluvchi muhim axborot infratuzilmasidir. Zamonaviy sharoitda bojxona jarayonlari to'liq raqamlashtirilmoqda. Elektron deklaratsiya, onlayn nazorat tizimlari, risklarni boshqarish modullari va xalqaro ma'lumot almashinuvi (masalan, WCO yoki ICS2 tizimlari) keng qo'llanilmoqda. Shu bois kiberxavfsizlik bojxona faoliyatining eng ustuvor yo'nalishlaridan biriga aylandi.

Kiberxavfsizlik — bu kompyuter tizimlari, tarmoqlar, dasturlar va ma'lumotlarni ruxsatsiz kirish, o'g'irlanish, buzilish yoki zarar yetkazilishidan himoya qilishga qaratilgan chora-tadbirlar tizimidir. Uning asosiy maqsadi – axborotning **maxfiyligi**, **butunligi** va **mavjudligini** ta'minlashdan iborat. Bugungi kunda kiberxavfsizlik davlat boshqaruvi, iqtisodiyot, bank tizimi, bojxona, transport, ta'lim va boshqa barcha raqamli infratuzilmalarning ishonchli faoliyat yuritishida muhim o'rin tutadi. Kiberxavfsizlik nafaqat texnik himoya vositalarini, balki inson omilini — ya'ni xodimlarning shu soha bo'yicha bilim va xabardorligini oshirishni ham o'z ichiga oladi[2].

Kiberxavfsizlik markazi tomonidan 2020-yil II choragi bo'yicha monitoring natijalari chop etildi, unda davlat organlari va tashkilotlarida axborot va kiberxavfsizlikni ta'minlash reytingi aniqlandi. Reyting Kiberxavfsizlik markaziga davlat organlari

tomonidan axborot va kiberxavfsizlikni monitoring qilish tizimi doirasida taqdim etilayotgan ma'lumotlar asosida baholandi. Reyting natijalariga ko'ra, eng yuqori o'rin egallagan tashkilotlar top-10 taligiga Adliya vazirligi, **Bojxona** qo'mitasi, Iqtisodiy taraqqiyot va kambag'allikni qisqartirish vazirligi, qator bank va boshqa tashkilotlar, jumladan, joylardagi ijro hokimiyati organlari kirdi. **Bojxona** qo'mitasi top 10 talikning 3-o'rnini 88 bal bilan egalladi[3].

Bojxona axborot tizimlari ko'plab nozik ma'lumotlarni o'z ichiga oladi: tijorat sirlarini, shaxsiy ma'lumotlarni, bojxona deklaratsiyalari, tranzaktsion ma'lumotlar va boshqalar. Shu sababli, ushbu tizimlar kiberhujumlarga, ma'lumotlarning o'g'irlanishi, buzilishi, xizmat ko'rsatishning to'xtatilishi kabi tahdidlarga qarshi ishonchli himoyaga muhtoj hisoblanadi[4].

Zamonaviy bojxona tizimlari xalqaro savdo, transport va logistika zanjirining asosiy bo'g'ini bo'lib, ularda katta hajmdagi iqtisodiy, moliyaviy va shaxsiy ma'lumotlar qayta ishlanadi. Ushbu tizimlarning samarali ishlashi xalqaro bojxona idoralari, transport kompaniyalari, logistika operatorlari, soliq organlari va boshqa davlat tuzilmalari o'rtasidagi uzluksiz axborot almashuviga tayanadi. Axborot almashuvi deganda esa, bojxona infratuzilmasining barqaror faoliyati uchun kiberxavfsizlikni ta'minlash eng muhim omillardan biri sanaladi. Bojxona tizimiga qaratilgan kiber tahdidlar qatoriga xakerlik hujumlari, zararli dasturlar, DDoS (tarqatilgan xizmatdan mahrum etish) hujumlar, fishing (soxta elektron xat va havolalar orqali ma'lumot o'g'irlash) usullari kiradi. Ko'plab kiberhujumlar aynan inson omili orqali — xodimning ehtiyotsizligi yoki xabardorligi yetarli emasligi sababli amalga oshirilishi mumkin. Shuning uchun, texnik himoya vositalarini kuchaytirish bilan bir qatorda, xodimlarning kiberxavfsizlik

bo'yicha bilim va malakasini oshirish ham ustuvor vazifa va xodimlarni doimo ma'lumot bilan ta'minlash kerak hisoblanadi.

Xulosa qilib aytganda, bojxona tizimida kiberxavfsizlikni ta'minlash bugungi raqamli davrda davlat xavfsizligi va iqtisodiy barqarorlikning muhim omilidir. O'zbekiston bojxona organlarida "Yagona interaktiv bojxona tizimi", "E-Avtoyo'lovchi" va "Risklarni tahlil qilish moduli" kabi elektron loyihalarning yaratilishi bilan bir qatorda, ularni kiberxavflardan himoya qilish zarurati oshib bormoqda. 2022-yilda qabul qilingan "Kiberxavfsizlik to'g'risida"gi qonun ushbu yo'nalishda huquqiy asos bo'lib xizmat qiladi. Shuningdek, kiberxavfsizlikni ta'minlashda inson omili ham muhim rol o'ynaydi — bojxona xodimlarida axborot madaniyatini oshirish, fishingga (soxtalashtirilgan elektron xatlar orqali ma'lumot o'g'irlash) qarshi o'qitish, xavfsizlik siyosatini to'g'ri tushuntirish zarur. Umuman olganda, bojxona tizimida kiberxavfsizlikni mustahkamlash davlat xavfsizligi va raqamli iqtisodiyotning barqaror rivojlanishiga xizmat qiladi.

Foydalanilgan adabiyotlar

1. **O'zbekiston Respublikasining** 15-aprel 2022-yil "Kiberxavfsizlik to'g'risida"gi 764-sonli Qonuni.
2. O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi rasmiy sayti — mitc.uz.
3. <https://kun.uz/>
4. **World Customs Organization (WCO).** *ICT Guidelines and SAFE Framework of Standards.* <https://www.wcoomd.org>
5. **World Customs Organization (WCO).** *SAFE Framework and Capacity Building.*

6. National Institute of Standards and Technology (NIST).
Cybersecurity Awareness Training.

URL: <https://www.nist.gov/cyberframework>

7. European Union Agency for Cybersecurity (ENISA).
Cybersecurity Training and Awareness.