KIBERXAVFSIZLIKNING AHAMIYATI VA UNING TURLARI

Rizayeva Farangiz Xoldorovna
Jahon Iqtisodiyoti va Diplomatiya Universiteti magistri
rizayeva06@mail.ru

Annotatsiya. *Ushbu maqolada kiberxavfsizlikni ta’minlashga bo‘lgan zaruriyatning ahamiyati va kiberxavfsizlikning o‘ziga xos turlari hamda O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlashga qaratilgan chora-tadbirlar yoritilgan.*

Kalit so‘zlar: *kibertahdid, kiberxavfsizlik, kiberxavfsizlik turlari, tarmoq xavfsizligi, ilovalar xavfsizligi, dasturiy ta’minot xavfsizligi.*

Smartfonlar, planshetlar, noutbuklar va kommpyuterlar, axborot texnologiyalari infratuzilmalaridan, xususan, mobil va Wi-Fi internetidan foydalanuvchilar soni kun sayin emas, balki, soat sayin ortib bormoqda. Bularning barchasi katta hajmdagi foydalanuvchilar ma’lumotlarining shakllanishiga va bu ma’lumotlarning xavfsizligi va saqlanishi bilan bog‘liq ulkan muammolarni shakllantirmoqda. Zero, bugungi kunda ushbu ma’lumotlarga ega chiqish orqali nafaqat foydalanuvchilarga moddiy yoki ma’naviy ziyon yetqazish balki, butun boshli mamlakatlar tanazzuliga sabab bo‘lish hech gap emas. Chunki to‘g‘ri tahlil qilingan va qayta ishlangan ma’lumotlar hatto atom bombasidan ham xavfliroq qurol hisoblanadi. Shu sabab ham kiberxavfsizlikni ta’minlash va kiberhujumlarning oldini olish dunyo miqyosida keyingi 10 yillikda hal qilinishi lozim bo‘lgan asosiy muammolardan biriligicha saqlanib kelmoqda. Mashhur iqtisodiy nashlardan birida chop etilgan maqolada keltirilishicha, 2023-yilda kiberhujumlar sezilarli darajada oshishi natijasida kibertahdidlar qurbonlari soni 343 milliondan ortgan. 2021 va 2023 yillar oralig‘ida ma’lumotlarning buzilishi bilan bo‘gliq holatlar 72 foizga o‘sib, avvalgi rekordni yangilagan[15].

Tobora ortib borayotgan kibertahdidlar onlayn bank parollarini saqlashga beparvolik tufayli pul yo‘qotish tahdididan tortib, asosan kiberxavfsizlikning zaif tomonlari tufayli yuzaga keladigan kompyuter viruslari, zararli dasturlar yoki josuslarga qarshi dasturlar hujumlarigacha yuzaga kelmoqda. Bu esa kiberxavfsizlik soha va yo‘nalishlarga qarab maxsus turlarga bo‘lish va tor mutaxassisliklar doirasida o‘rganishga bo‘lgan zaruratni yuzaga chiqarmoqda. Xususan, quyida IT xizmatlari va konsalting xizmatlari ko‘rsatuvchi IBM kompaniyasi ta’riflariga ko‘ra quyidagicha kiberxavfsizlik turlari mavjud[16].

Muhim infratuzilmalar xavfsizligi (Critical infrastructure security). Bu jamiyat milliy xavfsizlik, iqtisodiy salomatlik va jamoat xavfsizligiga bog‘liq bo‘lgan kompyuter tizimlari, ilovalari, tarmoqlari, ma'lumotlari va raqamli aktivlarini himoya qiladi. Bunda bir sektorga qilingan hujum tezda boshqalarga tarqalishi mumkin, bu esa butun

[15] https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/
[16] https://www.ibm.com/topics/cybersecurity

tizimlarni buzadigan domino ta'sirini yaratadi. Shuningdek ushbu tizim xavfsizligini ta’minlash milliy xavfsizlik masalasi ham sanaladi.

Tarmoq xavfsizligi(Network security). Tarmoq xavfsizligi deganda kompyuter tarmog‘i infratuzilmasini ruxsatsiz kirish, noto‘g‘ri foydalanish, o‘zgartirish yoki xizmat ko‘rsatishni rad etishdan himoya qilish amaliyoti tushuniladi. U tarmoqlarni kibertahdidlardan himoya qilish va ularning maxfiyligi, yaxlitligi va mavjudligini ta'minlash uchun turli texnologiyalar, jarayonlar va siyosatlarni amalga oshirishni o‘z ichiga oladi. Bu yangi va rivojlanayotgan kibertahdidlarni bartaraf etish uchun muntazam yangilanishlar va tuzatishlarni talab qiladigan doimiy jarayon.

Yakuniy nuqta xavfsizligi(Endpoint security). Bu tarmoqqa ulanadigan yakuniy nuqtalar aniqrog‘i individual qurilmalarning himoyasini anglatadi. Ushbu yakuniy nuqtalarga shaxsiy kompyuterlari, noutbuklar, smartfonlar, planshetlar, serverlar va boshqa qurilmalar kiradi. Yakuniy nuqta xavfsizligi ushbu qurilmalarni zararli dasturlar, to‘lov dasturlari, fishing hujumlari va ruxsatsiz kirish kabi tahdidlardan himoya qilishga qaratilgan. Yakuniy nuqta xavfsizligi tashkilotlarni kiberxavfsizlik tahdidlaridan himoya qilish uchun juda muhimdir, chunki yakuniy nuqtalar ko‘pincha qimmatli ma'lumotlar va tarmoqlarga to‘g‘ridan-to‘g‘ri kirishlari tufayli hujumlarning nishoni hisoblanadi.

Ilova xavfsizligi(Application security). Bu lokal server va bulutda ishlaydigan ilovalarni himoya qiladi, ilovalar va tegishli ma'lumotlarga ruxsatsiz kirish va ulardan foydalanishni oldini oladi. Shuningdek, u xakerlar tarmoqqa kirish uchun foydalanishi mumkin bo‘lgan dastur dizaynidagi kamchiliklar yoki zaifliklarning oldini oladi. DevOps va DevSecOps kabi zamonaviy ilovalarni ishlab chiqish usullari xavfsizlik va xavfsizlik testlarini ilovalarni ishlab chiqish jarayoniga birlashtiradi.

Bulutli xavfsizlik(Cloud security). Bu tashkilotning bulutga asoslangan xizmatlari va aktivlarini — ilovalar, ma’lumotlar, saqlash, ishlab chiqish vositalari, virtual serverlar va bulutli infratuzilmani himoya qiladi. Umuman olganda, bulutli xavfsizlik umumiy javobgarlik modelida ishlaydi, bunda bulut provayderi ular yetkazib beradigan xizmatlar va ularni yetkazib berish uchun foydalaniladigan infratuzilmani ta'minlash uchun javobgardir. Mijoz o‘z ma'lumotlarini, kodlarini va bulutda saqlaydigan yoki boshqaradigan boshqa aktivlarini himoya qilish uchun javobgardir. Tafsilotlar foydalaniladigan bulut xizmatlariga qarab farq qiladi.

Axborot xavfsizligi(Information security). Bu tashkilotning barcha muhim ma'lumotlarini – raqamli fayllar va ma'lumotlar, qog‘oz hujjatlari, fizik ommaviy axborot vositalari, hatto inson nutqini ruxsatsiz kirish, oshkor qilish, foydalanish yoki o‘zgartirishdan himoya qilish bilan bog‘lik. Ma'lumotlar xavfsizligi, raqamli ma'lumotlarni himoya qilish axborot xavfsizligining quyi to‘plami va kiberxavfsizlik bilan bog‘liq infoSec choralarining aksariyatining asosiy mavzusidir.

Mobil xavfsizlik. Mobil xavfsizlik smartfonlar va mobil qurilmalarga xos bo‘lgan turli fanlar va texnologiyalarni, jumladan, mobil ilovalarni boshqarish (MAM) va korporativ mobillikni boshqarish (EMM) ni o‘z ichiga oladi. Yaqinda mobil xavfsizlik

yagona konsoldan bir nechta so‘nggi nuqtalar - mobil qurilmalar, ish stollari, noutbuklar va boshqalar uchun konfiguratsiya va xavfsizlikni boshqarish imkonini beruvchi yagona so‘nggi nuqtani boshqarish (UEM) yechimlarining bir qismi sifatida mavjud.

O‘zbekiston Respublikasida ham keyingi yillarda kiberxavfsizlikni ta’minlashga hukumat doirasidagi muhim strategik yo‘nalish sifatida qaralib bir qator qonun va qonun osti hujjatlari qabul qilinib kelinmoqda. Xususan, O‘zbekiston Respublikasi Davlat xavfsizlik xizmati raisining 2023-yil 4-sentabrdagi 91-son buyrug‘iga asosan qabul qilingan “O‘zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash darajasini baholash tartibi to‘g‘risida”gi nizom[17], O‘RQ-764-sonli “Kiberxavfsizlik to‘g‘risida”gi qonuni[18], “Kiberxavfsizlik markazi” Davlat Unitar Korxonasining tashkil etishi hamda 2024-yil uchun Davlat budjeti tomonidan ushbu korxona faoliyatini yanada rivojlantishi uchun 56250,9 million so‘m mablag‘larning jalb etilishi shular jumlasidandir.

FOYDALANILGAN ADABIYOTLAR VA SAYTLAR

1. “O‘zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash darajasini baholash tartibi to‘g‘risida”gi nizom
2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni
3. “2024-yil uchun O‘zbekiston Respublikasining Davlat Budjeti to‘g‘risida”gi O‘zbekiston Respublikasi Qonuni
4. https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/
5. https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#statistic2
6. https://csec.uz/uz/news/maqolalar/o-zbekiston-respublikasi-kiberxavfsizligi-2023-yil-hisoboti/

[17] https://www.lex.uz/uz/docs/-6615573?query=kiberxavfsizlik&exact=1#sr-1
[18] https://www.lex.uz/uz/docs/-5960604?query=kiberxavfsizlik&exact=1#sr-1