



RAQAMLI MAKONDA KIBERXAVFSIZLIK TAHDIDLARINI BOSHQARISH VA ULARGA QARSHI KURASHISHNING DOLZARB MASALALARI

Fargʻona viloyati Dangʻara tuman 3-son texnikumi oʻqituvchilari

Maxkamova Shalolaxon Yusupjonovna

Oʻrinov Sherzodjon Dilmurodjon oʻgʻli

Annotatsiya: Mazkur maqolada raqamli makon sharoitida kiberxavfsizlik tahdidlarining mohiyati, kelib chiqish sabablari va turlari, shuningdek, ularni boshqarish hamda ularga qarshi samarali kurashish masalalari keng yoritilgan. Axborotlashgan jamiyatda shaxs, jamiyat va davlat manfaatlarini himoyalashda kiberxavfsizlikning tutgan oʻrni tahlil qilingan. Kiberjinoyatchilikka qarshi kurashishning tashkiliy, texnik va huquqiy mexanizmlari, kiberxavfsizlik madaniyatini shakllantirish yoʻllari va amaliy tavsiyalar keltirilgan.

Kalit soʻzlar: axborot, axborot xavfsizligi, kiberxavfsizlik, kiberjinoyatchilik, kiber tahdidlar, raqamli makon, maxfiylik, yaxlitlik, mavjudlik, kibernudofaa.

XXI asrda axborot va raqamli texnologiyalar jamiyat taraqqiyotining asosiy harakatlantiruvchi kuchiga aylandi. Bugungi kunda iqtisodiyot, taʼlim, sogʻliqni saqlash, bank-moliya, sanoat va davlat boshqaruvi tizimlari axborot texnologiyalariga tayanib faoliyat yuritmoqda. Raqamli makonning kengayishi bilan bir qatorda axborot resurslari strategik ahamiyat kasb etib, ularni himoyalash masalasi dolzarb vazifaga aylandi.

Raqamli transformatsiya jarayonlari inson hayotini yengillashtirishi bilan birga, yangi xavf-xatarlarni ham yuzaga keltirmoqda. Kiber makonda sodir boʻlayotgan hujumlar shaxsiy maʼlumotlarning oshkor boʻlishi, moliyaviy zararlar,



ijtimoiy ishonchning pasayishi va milliy xavfsizlikka tahdid tug'dirishi mumkin. Shu bois kiberxavfsizlik masalasi global muammo sifatida qaralmoqda.

Axborot xavfsizligi va kiberxavfsizlik tushunchalari

Axborot xavfsizligi — axborotni ruxsatsiz kirish, oshkor etish, o'zgartirish yoki yo'q qilishdan himoyalashga qaratilgan chora-tadbirlar majmuasidir. Axborot xavfsizligi uch asosiy tamoyilga tayanadi: maxfiylik, yaxlitlik va mavjudlik.

Kiberxavfsizlik esa kiber makonda joylashgan tizimlar, tarmoqlar, qurilmalar va ma'lumotlarni kiberhujumlardan himoyalashga qaratilgan kompleks faoliyatdir. U axborot xavfsizligining muhim tarkibiy qismi bo'lib, zamonaviy raqamli infratuzilmani himoyalashni ko'zda tutadi.

Raqamli makon va uning xususiyatlari

Raqamli makon — bu axborot-kommunikatsiya texnologiyalari asosida shakllangan, internet tarmog'i, mobil aloqa, sun'iy intellekt, bulutli hisoblash va raqamli platformalarni o'z ichiga olgan virtual muhitdir. Ushbu makonning asosiy xususiyatlari ochiqlik, tezkorlik, globallik va interaktivlik hisoblanadi. Raqamli makonda ma'lumotlar juda katta hajmda yaratiladi va uzatiladi, bu esa ularni samarali boshqarish va himoyalashni talab qiladi.

Raqamli makonning rivojlanishi davlatlar o'rtasidagi axborot almashinuvini jadallashtirdi, iqtisodiy integratsiyani kuchaytirdi va masofaviy xizmatlar ko'lamini kengaytirdi. Shu bilan birga, ushbu jarayon kiber tahdidlarning transmilliy xarakter kasb etishiga olib keldi. Endilikda bir davlat hududida amalga oshirilgan kiberhujum boshqa davlat infratuzilmasiga ham salbiy ta'sir ko'rsatishi mumkin.

Raqamli makon — internet, kompyuter tarmoqlari, mobil qurilmalar va bulutli texnologiyalar orqali bog'langan virtual muhitdir. Ushbu muhitda axborot tezkor almashinadi, xizmatlar avtomatlashtiriladi va masofaviy muloqot imkoniyatlari



kengayadi. Biroq ochiqlik va tezkorlik kiber tahdidlar uchun ham qulay sharoit yaratadi.

Kiber tahdidlarning turlari va manbalari

Kiber tahdidlar texnik, tashkiliy va inson omiliga bog‘liq omillar natijasida yuzaga keladi. Texnik tahdidlarga zararli dasturlar, tarmoq hujumlari va dasturiy ta‘minotdagi zaifliklar kiradi. Tashkiliy tahdidlar esa axborot xavfsizligi siyosatining yetarli darajada ishlab chiqilmaganligi va nazorat mexanizmlarining sustligi bilan bog‘liq.

Inson omiliga bog‘liq tahdidlar eng xavfli hisoblanadi. Chunki foydalanuvchilarning bexosdan qilgan xatolari, parollarning zaifligi yoki ijtimoiy muhandislik hujumlariga uchrashi kiberhujumlarning muvaffaqiyatli amalga oshishiga sabab bo‘ladi. Shu bois kiber tahdidlarning oldini olishda texnik choralar bilan bir qatorda inson omiliga ham alohida e‘tibor qaratish zarur.

Kiber tahdidlar texnik, tashkiliy va inson omiliga bog‘liq omillar natijasida yuzaga keladi. Ularning asosiy turlari quyidagilar: zararli dasturlar (viruslar, troyanlar, ransomware), fishing va ijtimoiy muhandislik hujumlari, DDoS hujumlari, ma‘lumotlarni o‘g‘irlash, shaxsiy hayot daxlsizligini buzish, moliyaviy firibgarlik.

Kiberjinoyatchilik va uning oqibatlari

Kiberjinoyatchilik — axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlar majmuasidir. Unga noqonuniy kirish, axborotni o‘g‘irlash, firibgarlik, shaxsiy ma‘lumotlardan ruxsatsiz foydalanish va kiber shantaj kiradi.

Kiberjinoyatchilikning oqibatlari juda keng ko‘lamli bo‘lib, iqtisodiy zararlar bilan bir qatorda ijtimoiy va psixologik muammolarni ham keltirib chiqaradi. Tashkilotlar uchun moliyaviy yo‘qotishlar, obro‘-e‘tibor pasayishi va faoliyatning



vaqtincha to‘xtab qolishi kabi salbiy holatlar yuzaga keladi. Davlat miqyosida esa milliy xavfsizlikka tahdid kuchayadi.

Kiberjinoyatchilik — axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlar majmuasidir. U iqtisodiy zararlar, obro‘-e‘tibor yo‘qolishi, ijtimoiy beqarorlik va huquqiy muammolarga olib keladi. Kiberjinoyatchilar ko‘pincha moliyaviy manfaat ko‘zlab harakat qiladilar.

Kiberxavfsizlikni ta‘minlashda tashkiliy va texnik choralar

Kiberxavfsizlikni ta‘minlash kompleks yondashuvni talab etadi. Bunga axborot xavfsizligi siyosatini ishlab chiqish, texnik himoya vositalarini joriy etish, risklarni boshqarish, xodimlarni o‘qitish va doimiy monitoring kiradi.

Huquqiy-me‘yoriy asoslar

Kiberxavfsizlikni ta‘minlashda milliy va xalqaro huquqiy me‘yorlar muhim ahamiyatga ega. O‘zbekiston Respublikasida axborot xavfsizligiga oid qonunlar, qarorlar va standartlar mavjud bo‘lib, ular kiber makonda huquqiy tartibotni ta‘minlashga xizmat qiladi.

Kiberxavfsizlik madaniyati va ta‘lim

Kiberxavfsizlik madaniyatini shakllantirish jamiyat barqarorligi uchun muhimdir. Aholining raqamli savodxonligini oshirish, foydalanuvchilarga xavfsiz internetdan foydalanish qoidalarini o‘rgatish kiber tahdidlarning oldini olishga yordam beradi.

Ta‘lim va davlat muassasalarida kiberxavfsizlik

Ta‘lim muassasalari va davlat tashkilotlarida axborot tizimlarining ishonchli ishlashi kiberxavfsizlikka bevosita bog‘liq. Ularni himoyalash milliy manfaatlar nuqtayi nazaridan ham muhim hisoblanadi.



Xulosa qilib aytganda, raqamli makonda kiberxavfsizlik tahdidlarini boshqarish va ularga qarshi kurashish bugungi globallashuv sharoitida eng dolzarb masalalardan biri hisoblanadi. Raqamli texnologiyalarning jadal rivojlanishi axborot almashuvini yengillashtirgan bo'lsa-da, kiberjinoyatchilik va kiber tahdidlar ko'lamining kengayishiga ham sabab bo'lmoqda.

Kiberxavfsizlikni ta'minlashda faqatgina texnik himoya vositalaridan foydalanish yetarli emas. Tashkiliy, huquqiy va ma'rifiy choralarni uyg'unlashtirish orqali kompleks himoya tizimini shakllantirish zarur. Ayniqsa, aholining raqamli savodxonligini oshirish va kiberxavfsizlik madaniyatini rivojlantirish muhim ahamiyatga ega.

Kelajakda sun'iy intellekt, katta ma'lumotlar va avtomatlashtirilgan monitoring tizimlari asosida kiberxavfsizlikni ta'minlash yanada samarali bo'ladi. Shu bois davlat, ta'lim muassasalari va xususiy sektor o'rtasidagi hamkorlikni kuchaytirish orqali barqaror va xavfsiz raqamli muhitni yaratish mumkin.

Xulosa qilib aytganda, raqamli makonda kiberxavfsizlik tahdidlarini boshqarish va ularga qarshi kurashish bugungi kunning eng dolzarb masalalaridan biridir. Texnik, tashkiliy, huquqiy va ma'rifiy choralarni uyg'unlashtirish orqali barqaror va xavfsiz raqamli muhitni shakllantirish mumkin.

Foydalanilgan adabiyotlar ro'yxati

1. A. U. Anorboyev. Kiberjinoyatchilik va unga qarshi kurashish muammolari. – T.: 2020.
2. S. K. Ganiyev, S. T. Xudoyqulov. Kiberxavfsizlik asoslari. – T.: 2020.
3. N. S. Salayev, R. N. Ro'ziyev. Kiberjinoyatchilikka qarshi kurashishning milliy va xalqaro standartlari. – T.: 2018.
4. ISO/IEC 27001. Information Security Management Systems.



5. OECD. Cybersecurity Risk Management. – Paris, 2020.
6. ENISA. Cybersecurity Threat Landscape. – 2021.
7. O‘zbekiston Respublikasi axborot xavfsizligiga oid normativ-huquqiy hujjatlari.
8. www.lex.uz
9. www.iiv.uz
10. www.cert.uz
11. www.unesco.org