KIBERTERRORIZM VA UNDAN HIMOYALANISHGA QARATILGAN SAMARALI STRATEGIYALARNI YARATISH

Milliy g‘oya va Huquq kafedrasi katta o‘qituvchisi (PhD)
Abdupattayev Hasanboy
Qo‘qon Davlat Universiteti Matematika kafedrasi 2-bosqich talabasi
Ahmadjonova Oygul

Annotatsiya

Raqamli transformatsiya jarayonlari jadal rivojlanayotgan davrda davlat va jamiyat xavfsizligiga eng katta tahdidlaridan biri – kiberterrorizmdir. Kiberterrorizmning mohiyati, asosiy ko‘rinishlari va infratuzilmalarga ko‘rsatadigan ta’siri tobora kuchayib bormoqda. Ushbu maqolada kiberterrorizmning nazariy talqinlari, uning zamonaviy shakllari va unga qarshi samarali himoya mexanizmlarini shakllantirish masalalari tahlil qilinadi. Shuningdek, milliy xavfsizlikning yangi bosqichida axborot makonini himoyalashning ustuvor yo‘nalishlari ko‘rsatib beriladi.

Kalit so‘zlar: kiberterrorizm, axborot xavfsizligi, kiberhujum, raqamli infratuzilma, himoya strategiyalari, zamonaviy xavf.

Kirish

Hozirgi globallashuv jarayonida axborot-kommunikatsiya texnologiyalarining keng qo‘llanilishi bilan bir qatorda, kiberxavfsizlik masalalariga bo‘lgan ehtiyoj ham sezilarli darajada ortib bormoqda. Xalqaro ekspertlar fikriga ko‘ra, raqamli makonga qaratilgan har qanday hujumlar ichida kiberterrorizm eng xavflisi sifatida

e’tirof etiladi. Chunki kiberterrorizm nafaqat moddiy-texnik infratuzilmaga zarar yetkazadi, balki jamiyatda qo‘rquv va beqarorlik muhitini shakllantirish orqali siyosiy va ijtimoiy tizimlarga ta’sir ko‘rsatadi.

Mazkur tushuncha XX asr oxiridan boshlab ilmiy adabiyotlarda keng qo‘llanila boshlagan bo‘lsada, uning mazmun-mohiyati axborot texnologiyalari rivojlanishiga qarab yanada murakkablashib bormoqda. Kiberterrorizmga oid nazariy qarashlar bir-biridan farqlanib, ayrim holatlarda subyektiv yondashuvlar ustuvorlik qilmoqda.

Kiberterrorizm tushunchasining nazariy asoslari

Kiberterrorizmni talqin qilishda turli yondashuvlar mavjud. Ayrim tadqiqotchilar uni oddiy kiberjinoyatdan farqlab, aniq siyosiy maqsadga qaratilgan, vahima va qo‘rquv uyg‘otuvchi harakatlar sifatida baholaydilar.

Olimlar fikricha, kiberterroristik harakatning asosiy belgilari:

Maqsadli rejalashtirilgan bo‘lishi;

Zarar yetkazish orqali jamiyatda qo‘rquv uyg‘otish;

Muhim infratuzilmani izdan chiqarishga qaratilganligi;

Axborot tizimlarini qurol sifatida ishlatilishi.

Klassik talqinda kiberjinoyatdan farqli ravishda, kiberterrorizm doimo mafkuraviy, siyosiy yoki strategik maqsadni ko‘zlaydi.Kiberterrorizmning asosiy shakllari

Bugungi kunda kiberterrorizmning quyidagi shakllari keng tarqalgan:

1. DDoS hujumlari

Haddan tashqari ko‘p so‘rov bilan tizimlarni ishdan chiqarish orqali davlat portallari, bank tizimi yoki shifoxonalar faoliyati falaj qilinadi.

2. Zararli dasturlar orqali hujumlar

Ransomware, viruslar va troyanlar orqali tizimlar bloklanadi yoki ma’lumotlar shifrlanib, to‘lov talab qilinadi.

3. Hayotiy muhim infratuzilmaga hujumlar

Energetika, transport, suv ta’minoti, tibbiyot tizimlariga qaratilgan hujumlar eng xavfli natijalarga olib kelishi mumkin.

4. Axborot manipulyatsiyasi

Ijtimoiy tarmoqlarda yolg‘on xabarlar, feyklar tarqatish, aholida vahima uyg‘otish – zamonaviy kiberterrorizmning eng ko‘p qo‘llanayotgan ko‘rinishidir.

Kiberterrorizmning jamiyatga ta’siri

Kiberterrorizmning oqibatlari ko‘p qirrali bo‘lib, u nafaqat texnik tizmlarga, balki jamiyatning ijtimoiy-psixologik barqarorligiga ham zarar yetkazadi.

Iqtisodiy zarar – milliardlab yo‘qotishlar, tizimlarning to‘xtashi.

Siyosiy xavfsizlikka tahdid – davlat boshqaruv jarayonining falaj bo‘lishi.

Jamiyatda vahima – terrorizmning asosiy maqsadi aholi orasida qo‘rquv paydo qilishdir.

Axborot xavfsizligining buzilishi – maxfiy ma’lumotlarning oshkor bo‘lishi.

Kiberterrorizmdan himoyalanish strategiyalari

Zamonaviy davrda kiberterrorizmga qarshi kurashish kompleks yondashuvni talab etadi.

1. Axborot xavfsizligi boshqaruv tizimini kuchaytirish

ISO/IEC 27001 standartlarini joriy etish, zaifliklarni aniqlash va ularni tezkor bartaraf etish.

2. Kuchli autentifikatsiya

Ko‘p bosqichli parollar, biometrik himoya, 2FA tizimlari.

3. Tarmoq monitoringi

IDS/IPS, SIEM tizimlari orqali real vaqt rejimida hujumlarni aniqlash.

4. Xodimlar va foydalanuvchilarni o‘qitish

Kiberhujumlarning katta qismi insonning e’tiborsizligi oqibatidir, shuning uchun raqamli savodxonlikni oshirish muhimdir.

5. Milliy va xalqaro hamkorlik

Davlatlararo kiberxavfsizlik markazlari o‘rtasida ma’lumot almashish va birgalikda tahdidlarga qarshi kurashish.

Xulosa

Yuqoridagi tahlillardan kelib chiqib, quyidagi xulosalarga kelish mumkin:

Kiberterrorizm raqamli texnologiyalar rivojlanishi bilan birga yanada murakkablashib, jamiyat xavfsizligi uchun global tahdiddir.

Kiberhujumlar nafaqat texnik tizimlarga, balki jamiyatning ijtimoiy va psixologik barqarorligiga ham katta ta’sir ko‘rsatadi.

Himoya tizimlari moddiy texnik choralar bilan cheklanib qolmasdan, inson omili, ma’lumotlar madaniyati, davlat siyosati va xalqaro hamkorlikni o‘z ichiga olishi kerak.

Faqat kompleks, tizimli va strategik yondashuvgina jamiyatni kiberterrorizm xavfidan samarali himoya qilishi mumkin.

Adabiyotlar

1.Mirziyoyev Sh.M. “Raqamli O‘zbekiston – 2030” strategiyasi.

2.Aliyev R. Axborot xavfsizligi asoslari. Toshkent, 2021.

3.Smith J. Cyberterrorism: Global Threats and Responses. London, 2020.

4.Karimov A. Kiberxavfsizlikning huquqiy asoslari. Toshkent, 2022.

5.Yusupov M. Raqamli tahdidlar va ularning oldini olish. 2023.