AXOLINI TEXNOGEN TUSDAGI FAVQULODDA VAZIYAT XISOBLANGAN "KIBER TERRORIZM" XURUJIDAN XIMOYA QILISH HAMDA TERRORCHILIK OQIBATLARINI MINIMALLASHTIRISH.

Bozorov Umidjon Negboevich
Navoiy viloyati FVB XFXUM o'qituvchisi.

Annotatsiya. *Texnologiyalar hukmron bo'lgan davrda kiber terrorizm xavfi katta bo'lib, milliy xavfsizlik va aholi farovonligi uchun katta xavf tug'diradi. Ushbu maqola jamiyatni kiber terrorizmdan himoya qilish zarurligini o'rganib chiqadi va bunday hujumlarning oqibatlarini minimallashtirish uchun kompleks strategiyalar zarurligini ta'kidlaydi. Tadqiqot hozirgi adabiyotlarni o'rganadi, mavjud usullarni tahlil qiladi, natijalarni taqdim etadi va xulosalar chiqarish va aholini himoya qilish bo'yicha samarali choralarni taklif qilish uchun mustahkam muhokamaga kirishadi.*

Kalit so'zlar: *kiber terrorizm, Favqulodda vaziyatlarga tayyorgarlik, xavflarni kamaytirish, hodisalarga javob berish, Milliy xavfsizlik, axborot xavfsizligi, muhim infratuzilmani muhofaza qilish.*

Kiber terrorizm zamonaviy muammolarni ifodalaydi, bu erda yomon niyatli aktyorlar raqamli zaifliklardan muhim infratuzilmani buzish, xizmatlarni buzish va nozik ma'lumotlarni buzish uchun foydalanadilar. Dunyo tobora o'zaro bog'liq bo'lib borar ekan, kiber terrorizmning potentsial oqibatlari kuchayib, jamiyatni ushbu texnogen favqulodda vaziyatlardan himoya qilish uchun proaktiv va ko'p qirrali yondashuvni talab qiladi.

Mavjud adabiyotlarni sinchkovlik bilan o'rganish kiber tahdidlarning rivojlanayotgan tabiatini va kiber terrorchilarning o'sib borayotgan murakkabligini ochib beradi. Olimlar kiber landshaftni, shu jumladan tahdidlarni o'rganish, zaifliklarni baholash va davlat va nodavlat aktyorlarning rolini yaxlit tushunish zarurligini ta'kidlaydilar. Adabiyot, shuningdek, muhim infratuzilmalarning o'zaro bog'liqligini ta'kidlab, bir sektorga kiber hujumning boshqalarga ta'sir qilishi mumkin bo'lgan domino ta'sirini ta'kidlaydi.

Kiber terrorizm muammosini hal qilish uchun ko'p qirrali metodologiya talab qilinadi. Bunga kiberxavfsizlik bo'yicha mustahkam chora-tadbirlarni ishlab chiqish va amalga oshirish, tahdidlarni faol ravishda yig'ish va hodisalarga javob berish tizimini yaratish kiradi. Davlat idoralari, xususiy korxonalar va xalqaro sheriklar o'rtasidagi hamkorlikdagi harakatlar kiber tahdidlarga muvofiqlashtirilgan javob berish uchun juda muhimdir. Metodlar bo'limi, shuningdek, kiber mudofaani kuchaytirish uchun shaxslar va tashkilotlarga vakolat berishda ta'lim va xabardorlik dasturlarining rolini o'rganadi.

Aholini kiber terrorizmdan himoya qilish texnologik, tashkiliy va siyosiy tadbirlarni birlashtirgan keng qamrovli va ko'p qirrali yondashuvni o'z ichiga oladi. Kiber terrorizm oqibatlarini minimallashtirishning ba'zi asosiy strategiyalari:

Milliy Kiberxavfsizlik Strategiyasi:

- Aniq maqsadlar, siyosat va harakatlar rejalarini belgilaydigan kuchli milliy kiberxavfsizlik strategiyasini ishlab chiqish va amalga oshirish.

- Davlat idoralari, xususiy sektor tashkilotlari va xalqaro sheriklar o'rtasida tahdidlarni aniqlash va javob choralarini muvofiqlashtirish bo'yicha hamkorlikni rivojlantirish.

Xatarlarni baholash va yumshatish:

- Muhim infratuzilma, asosiy tarmoqlar va davlat tizimlaridagi zaifliklarni aniqlash uchun xavflarni muntazam baholashni o'tkazish.

-Kiberxavfsizlik himoyasini kuchaytirish uchun maqsadli yumshatish strategiyalari bilan yuqori xavfli hududlarni birinchi o'ringa qo'ying va hal qiling.

Davlat-Xususiy Sheriklik:

- Axborot almashish, hodisalarga javob berish va kiberxavfsizlik bo'yicha qo'shma tashabbuslarni kuchaytirish uchun davlat tashkilotlari va xususiy sektor tashkilotlari o'rtasida mustahkam hamkorlik o'rnatish.

- Xususiy sektorni ilg'or tajribalarni qabul qilishga va o'z tarmoqlari va tizimlarini himoya qilish uchun kiberxavfsizlik choralariga sarmoya kiritishga undash.

Hodisalarga Javob Berishni Rejalashtirish:

- Kiberhujumlarni aniqlash, ularga javob berish va ulardan xalos bo'lish uchun aniq tartib-qoidalarni o'z ichiga olgan voqealarga javob berishning keng qamrovli rejalarini ishlab chiqish va muntazam ravishda yangilab turish.

- Kiber favqulodda vaziyatda muvofiqlashtirilgan va samarali javob berish uchun tegishli manfaatdor tomonlarni jalb qilgan holda muntazam mashg'ulotlar va mashqlarni o'tkazish.

Imkoniyatlarni oshirish va o'qitish:

- Hukumat, huquqni muhofaza qilish va xususiy sektorda kiberxavfsizlik bo'yicha mutaxassislarning malakasini oshirish uchun o'quv dasturlariga mablag ' sarflang.

- Aholining kiber tahdidlar to'g'risida xabardorligini oshirish va keng aholi orasida kiber gigiena qoidalarini targ'ib qilish.

Xalqaro Hamkorlik:

- Kiber tahdidlarni bartaraf etish va ilg'or tajribalarni almashish uchun xalqaro hamkorlik bilan shug'ullanish.

- Kiber jinoyatchilarni ekstraditsiya qilish va jinoiy javobgarlikka tortish uchun boshqa davlatlar bilan ishlash, kiber terrorizmga qarshi global harakatlarni rivojlantirish.

Texnologik Eechimlar:

- Muhim infratuzilma va nozik ma'lumotlarni himoya qilish uchun kirishni aniqlash tizimlari, xavfsizlik devorlari va shifrlash kabi ilg'or kiberxavfsizlik texnologiyalarini ishlab chiqish va joylashtirish.

- Rivojlanayotgan kiber tahdidlardan oldinda qolish uchun tadqiqot va ishlanmalarga sarmoya kiriting.

Normativ Choralar:

- Tashkilotlarning tegishli xavfsizlik choralarini amalga oshirishini ta'minlash uchun kiberxavfsizlik qoidalarini bajarish va yangilash.

-Tashkilotlarni kiberxavfsizlikni birinchi o'ringa qo'yishni rag'batlantirish uchun kiberxavfsizlik standartlariga rioya qilmaslik oqibatlarini aniqlash.

Doimiy Monitoring va tahdidlarni aniqlash:

-Real vaqt rejimida kiber tahdidlarni aniqlash va ularga javob berish uchun tarmoqlar va tizimlarning doimiy monitoringini amalga oshirish.

- Leverage threat intelligence so'nggi kiber tahdidlar va zaifliklar haqida xabardor bo'lish uchun ozuqa beradi.

Chidamlilik va tiklanishni rejalashtirish:

- Kiber hujumlarning ta'sirini minimallashtirish va tez tiklanishni ta'minlash uchun chidamlilik strategiyasini ishlab chiqish.

- Voqeadan keyin normal holatga tezda qaytishni osonlashtirish uchun muhim tizimlar va ma'lumotlar uchun zaxira va tiklash rejalarini amalga oshirish.

Ushbu strategiyalarni o'z ichiga olgan yaxlit va proaktiv yondashuvni qo'llash orqali hukumatlar aholini kiber terrorizmdan himoya qilish qobiliyatini oshirishi va bunday hujumlarning oqibatlarini minimallashtirishi mumkin. Bundan tashqari, kiberxavfsizlik to'g'risida xabardorlik va hamkorlik madaniyatini rivojlantirish rivojlanayotgan kiber tahdidlarga qarshi mustahkam himoyani yaratishda juda muhimdir.

Muhokama bo'limi topilmalarni tanqidiy tahlil qiladi, muammolarni va takomillashtirish yo'nalishlarini hal qiladi. U kiberxavfsizlik choralarining axloqiy oqibatlarini, maxfiylik va xavfsizlik o'rtasidagi muvozanatni va kiber terrorizmga qarshi kurashda xalqaro hamkorlikning rolini o'rganadi. Bo'lim, shuningdek, paydo bo'layotgan tahdidlarga doimiy moslashish zarurligini va kiberxavfsizlik infratuzilmasining ahamiyatini o'rganadi.

Xulosa va takliflar:

Xulosa qilib aytganda, jamiyatni kiber terrorizmdan himoya qilish hukumatlar, xususiy tashkilotlar va jismoniy shaxslar ishtirokida birgalikda harakat qilishni talab qiladi. Maqolada kiber hamkorlik uchun xalqaro asoslarni ishlab chiqish, tadqiqot va ishlanmalarga doimiy sarmoyalar kiritish va standartlashtirilgan kiberxavfsizlik amaliyotini o'rnatish taklif etiladi. Rivojlanayotgan tahdid landshaftiga qarshi kurashish uchun proaktiv va moslashuvchan yondashuv zarurligini ta'kidlaydi.

Jamiyat texnologiyalarga ko'proq ishonganligi sababli, kiber terrorizmdan himoya qilish doimiy ustuvor vazifa bo'lishi kerak. Keng qamrovli strategiyalarni

amalga oshirish, hamkorlikni rivojlantirish va paydo bo'layotgan tahdidlardan oldinda bo'lish orqali davlatlar kiber terrorizm oqibatlarini minimallashtirishi va o'z aholisining xavfsizligi va xavfsizligini ta'minlashi mumkin.

ADABIYOTLAR:

1. J. Carr, "Anti-Forensic Methods Used by Jihadist Web Sites," ESecurity Planet, 2010.

2. A.K. Cronin, "The diplomacy of counterterrorism lessons learned, ignored and disputed," International Research Group on Political Violence (IRGPV), pp. 1-8, 2002.

3. Cyberterrorism Defense Initiative , "CDI: Cyberterrorism First Responder (CFR)", Available online at http://cyberterrorismcenter.org/cfr.html. de Borchgrave, T. Sanderson and J. Harned, "Force multiplier for intelligence," Centre for Strategic and International Studies, 2007.

4. M. M. Elmusharaf , "Cyber Terrorism:The new kind of terrorism", Computer Crime Research Center, Accessed 20086 October, Available online at http://www.crimeresearch.org/articles/Cyber_Terrorism_new_kind_Terrorism.

5. J. Gearson, "The Nature of Modern Terrorism", The Political Quarterly, vol. 73, pp. 7-24, 2002.

6. S. Gordon and R. Ford, "Cyberterrorism?", Computers & Security, vol. 21, pp. 636-647, 2002.