Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

RAQAMLI ASRDA KIBERTERRORIZM: TAHLIL, XAVF-XATARLAR VA UNGA QARSHI KURASHISH STRATEGIYALARI

Bektemirova Saida Xusan qizi
O`zbekiston Respublikasi Ichki Ishlar Vazirligi
Tezkor Qidiruv departamenti Terrorizmga
qarshi kurashish xizmati yetakchi
muataxassisi katta leytenent
Tel: 99890 067 83 83
https://doi.org/10.5281/zenodo.23214694

Annotatsiya: Ushbu maqolada axborot-kommunikatsiya texnologiyalari shiddat bilan rivojlanayotgan hozirgi davrda paydo bo‘lgan eng xavfli tahdidlardan biri — kiberterrorizmning mohiyati, oqibatlari va rivojlanish tendensiyalari tahlil qilinadi. Muallif an’anaviy terrorizmning kiberfazoga ko‘chishi sabablari, muhim infratuzilmalarga yetkaziladigan zararlar va ushbu illatga qarshi milliy hamda xalqaro darajada kompleks kurashish mexanizmlarini yoritib beradi.
Kalit so`zlar: Kiberterrorizm, axborot xavfsizligi, kiberfazo, muhim infratuzilma, kritik obyektlar, kiberhujum, raqamli xavfsizlik.

Аннотация: В статье анализируются природа, последствия и тенденции развития кибертерроризма — одной из наиболее опасных угроз, возникших в эпоху стремительного развития информационно-коммуникационных технологий. Автор рассматривает причины переноса традиционного терроризма в киберпространство, ущерб, наносимый объектам критической инфраструктуры, а также механизмы комплексного противодействия этой угрозе как на национальном, так и на международном уровне.
Ключевые слова: Кибертерроризм, информационная безопасность, киберпространство, критическая инфраструктура, критически важные объекты, кибератака, цифровая безопасность.

Abstract: This article analyzes the nature, consequences, and development trends of cyberterrorism—one of the most dangerous threats to emerge in the current era of rapidly advancing information and communication technologies. The author examines the reasons behind the shift of traditional terrorism into cyberspace, the damage inflicted on critical infrastructure, and the mechanisms for a comprehensive response to this menace at both national and international levels.
Key words: Cyberterrorism, information security, cyberspace, critical infrastructure, critical facilities, cyberattack, digital security.

Mavzuning dilzarbligi: XXI asr — axborot va yuqori texnologiyalar asri. Texnologik taraqqiyot insoniyat uchun ulkan qulayliklar yaratish bilan birga, ilgari kuzatilmagan yangi turdagi tahdidlarni ham keltirib chiqardi. Shunday xavf-xatarlardan biri — an’anaviy terrorizmning raqamli makonga ko‘chishi natijasida shakllangan kiberterrorizmdir.

Hozirgi kunda energiya tizimlari, bank-moliya sektori, transport, harbiy obyektlar va davlat boshqaruvi to‘liq raqamlashtirilgan. Bu esa kiberterrorchilar uchun jismoniy zo‘ravonlik ishlatmasdan turib, butun boshli davlat yoki mintaqa barqarorligiga putur yetkazish imkoniyatini yaratadi. Shu bois kiberterrorizmga qarshi kurashish masalasi bugungi kunda har bir davlatning milliy xavfsizlik strategiyasida markaziy o‘rinni egallamoqda.

Kiberterrorizmning mohiyati va o‘ziga xos xususiyatlari:

Kiberterrorizm — bu siyosiy, mafkuraviy yoki ijtimoiy maqsadlarga erishish uchun kompyuter tizimlari, tarmoqlari va axborot infratuzilmasiga qasddan qilingan, insonlar hayotiga xavf tug‘diruvchi yoki jiddiy moddiy va ma’naviy zarar yetkazuvchi hujumdir.

An’anaviy terrorizm bilan solishtirganda, kiberterrorizm bir qancha o‘ziga xos xususiyatlarga ega:

Anonimlik va chegaralarning yo‘qligi: Hujum qiluvchi shaxs dunyoning istalgan nuqtasidan turib, masofadan turib harakat qila oladi va o‘z shaxsini yashirish ehtimoli yuqori.

Kam xarajat va yuqori samara: Jismoniy qurol-yarog‘ yoki portlovchi moddalar xarid qilish o‘rniga zararli dasturiy ta’minot (malware) yaratish yoki sotib olish moliyaviy jihatdan ancha arzon, ammo yetkaziladigan zarar ko‘lami ko‘p marta ortiq bo‘lishi mumkin.

Keng ko‘lamli ta’sir: Bitta kritik obyektga (masalan, atom elektr stansiyasi yoki suv ta’minoti tizimi) qilingan kiberhujum millionlab insonlar hayotini xavf ostiga qo‘yishi mumkin.

Muhim Infratuzilmalarga Tahdid va Kiberguruhlar Taktikasi:

Terrorchi tashkilotlar raqamli texnologiyalardan asosan uchta yo‘nalishda foydalanmoqda:

Tashviqot va yollash (rekrutatsiyalash): Ijtimoiy tarmoqlar va messenjerlar orqali ekstremistik g‘oyalarni targ‘ib qilish va yangi a’zolarni yollash.

Moliyalashtirish: Kriptovalyutalar va anonim to‘lov tizimlari orqali noqonuniy moliyaviy operatsiyalarni amalga oshirish.

To‘g‘ridan-to‘g‘ri kiberhujumlar: Davlat organlari saytlarini ishdan chiqarish (DDoS-hujumlar), ma’lumotlar bazasini o‘g‘irlash yoki bloklash (ransomware), energiya va transport tizimlarini izdan chiqarish.

Xalqaro amaliyotda 2015-yilda Ukrainadagi elektr tarmoqlariga qilingan kiberhujum (BlackEnergy) natijasida yuz minglab aholi chiroqsiz qolgani yoki Eron yadro dasturiga qarshi qo‘llanilgan Stuxnet kompyuter qurtining sanoat obyektlarini ishdan chiqargani kibertahdidlarning jiddiyligini amalda isbotladi.

Kiberterrorizmga Qarshi Kurashish Mexanizmlari:

Kiberterrorizmga qarshi samarali kurashish birgina davlatning kuch-g‘ayrati bilan cheklana olmaydi. Bu kompleks va ko‘p bosqichli yondashuvni talab etadi:

1. Huquqiy Bazani Takomillashtirish.

Kibermakonda sodir etiladigan jinoyatlar va kiberterrorchilik harakatlari uchun aniq huquqiy javobgarlikni belgilovchi qonunchilik tizimini mustahkamlash lozim. Xususan, O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni ushbu sohadagi munosabatlarni tartibga solishda muhim poydevor bo‘lib xizmat qilmoqda.

2. Xalqaro Hamkorlikni Kuchaytirish.

Kiberfazo hududiy chegaralarga ega bo‘lmagani sababli, BMT, SHHT, YEXHT kabi xalqaro va mintaqaviy tashkilotlar doirasida kiberxavfsizlik bo‘yicha ma’lumot va tajriba almashish, tezkor choralar ko‘rish mexanizmlarini yo‘lga qo‘yish zarur.

3. Muhim Axborot Infratuzilmasi Obyektlarini Himoyalash.

Davlat va xususiy sektorga tegishli strategik obyektlarning (banklar, energetika, tibbiyot, harbiy tizimlar) kiberhimoyasini doimiy ravishda monitoring qilish va eng zamonaviy axborot xavfsizligi texnologiyalarini joriy etish talab etiladi.

4. Kadrlar Tayyorlash va Raqamli Savodxonlik.

Kiberxavfsizlik sohasida yuqori malakali mutaxassislarni (oq xakerlar, tahlilchilar) tayyorlash bilan birga, oddiy aholining kibergiyena va raqamli savodxonligini oshirish zarur. Chunki ko‘pincha insondagi e’tiborsizlik (firoqlik/phishing va ijtimoiy muhandislik) kiberhujumlar uchun birinchi "eshik" vazifasini o‘taydi.

Kiberterrorizm — bu kelajakning emas, bugungi kunning real va o‘ta xavfli tahdididir. U nafaqat alohida tizimlar, balki tutash davlatlarning milliy xavfsizligi va barqarorligiga bevosita xavf tug‘diradi.

Ushbu tahdidga qarshi turish uchun davlatlar o‘rtasidagi xalqaro hamkorlikni chuqurlashtirish, milliy kiberxavfsizlik infratuzilmasini muntazam modernizatsiya qilish hamda jamiyatda raqamli madaniyat va xavfsizlik ko‘nikmalarini shakllantirish davr talabidir. Faqatgina texnik, huquqiy va ijtimoiy choralar majmuasi orqali raqamli kelajagimiz xavfsizligini ta’minlash mumkin.

FOYDALANILGAN ADABIYOTLAR RO`YXATI:

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. 2022-yil.
2. Gordon, S., & Ford, R. (2006). Cyberterrorism? Computers & Security, 25(7), 467-473.
3. Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies.
4. Xalqaro kiberxavfsizlik va axborot huquqiga oid ilmiy maqolalar to‘plamlari.