ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

KIBERXAVFSIZLIK VA KIBERTERRORIZMNING KESISHISHI: MUAMMOLAR VA YECHIMLAR

Abdusattorov Shahzod Abdumumin o‘g‘li

Annotatsiya: Ushbu maqolada kiberjinoyatchilikning boshqa turlari va kiberterrorizmning bir-biriga ta’siri va kiberxavfsizlikni ta’minlash borasidagi qiyinchiliklar haqida tahlil qilinadi.

Kalit so’zlar: Terrorizm, kibermakon, kiberxavfsizlik, kiberhujum, virus, BMT, Axborot texnologiyalari.

THE INTERSECTION OF CYBER SECURITY AND CYBER TERRORISM: CHALLENGES AND SOLUTIONS

Abstract: This article analyzes the interaction of other types of cybercrime and cyberterrorism and the challenges of cyber security.

Key words: Terrorism, cyber space, cyber security, cyber attack, virus, UN, Information technologies.

ПЕРЕСЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ И КИБЕРТЕРРОРИЗМА: ПРОБЛЕМЫ И РЕШЕНИЯ

Аннотация: В данной статье анализируется взаимодействие других видов киберпреступности и кибертерроризма, а также проблемы кибербезопасности.

Ключевые слова: Терроризм, киберпространство, кибербезопасность, кибератака, вирус, ООН, Информационные технологии.

Internet davrida korxonalar va muhi infratuzilmalar uchun samarali kompyuter tizimlariga bo‘lgan ishonch keskin o‘sdi. Axborot texnologiyalari va ularning xilma-xil qo‘llanilishidagi jadal taraqqiyot kompyuter foydalanuvchilari uchun bozor imkoniyatlaridan foydalanishdan daromad va foydani ko‘paytirishgacha bo‘lgan ko‘plab afzalliklarni keltirib chiqardi. Shunga qaramay, kompyuterlarni buzish, viruslar va boshqa kiberbuzilishlarning ko‘payishi biznes uchun butun dunyo bo‘ylab tahdid sifatida paydo bo‘lib, tijorat va sanoat operatsiyalarida mumkin bo‘lgan uzilishlarni keltirib chiqardi. So‘ngi paytlarda kiberxavfsizlik tahdidlari

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

kiberterrorizmning kuchayishi bilan tobora murakkablashib bormoqda. Natijada, axborot texnologiyalaridagi asosiy yo‘nalishi algoritm va protokollarni ishlab chiqishdan axborot tarmoqlarining mustahkamligi va ishonchliligiga o‘tdi.

Kompyuterning favqulodda vaziyatlarga javob berish guruhi (CERT) dasturiy ta’minot dasturi bilan bog‘liq muammolar hal qilindi, bu uning vorisi – AQShning kompyuter favqulodda vaziyatlarga tayyorgarligi jamoasi (US-CERT) tashkil etilishiga olib keldi. 2003-yilda Kibermakonni himoya qilish bo‘yicha Milliy strategiya joriy etilgan va Kongress kiberxavfsizlikni kuchaytirishga qaratilgan bir nechta favqulodda federal qonunlarni, jumladan Axborot xavfsizligini boshqarish to‘g‘risidagi Federal qonunni (FISMA; 2002), Axborot texnologiyalari (IT) boshqaruvini isloh qilish to‘g‘risidagi qonunni (2002) va Kiberxavfsizlikni tadqiq qilish va rivojlantirish to‘g‘risidagi qonun (2002). Bundan tashqari, Milliy xavfsizlik departamenti terroristik hujumlarning oldini olish uchun kibermakonni himoya qilishning o‘ziga xos missiyasi bilan tashkil etilgan. 2003-yilda Oq uy Federal hisoblash tizimlarining maxfiyligi, yaxlitligi va mavjudligini ta’minlash uchun AQSh Ichki xavfsizlik departamenti tarkibida Milliy kiberxavfsizlik bo‘limini (NCSD) tuzdi. Ushbu bo‘linma, shuningdek, federal axborot tizimlariga ta’sir qiladigan har qanday hodisaga darhol javob berish qobiliyatini ta’minlaydi, federal agentlik tarmoqlarini ma’lum zaifliklardan to‘g‘ri himoya qilishni ta’minlaydi va federal hukumatni 18 ta muhim infratuzilma tarmoqlarini himoya qilish bo‘yicha sa’y-harakatlarida qo‘llab-quvvatlaydi. Bundan tashqari, 2004 yilda Santa Klarada (Kaliforniya shtati) Kiberxavfsizlik bo‘yicha birinchi milliy sammit bo‘lib o‘tdi. Kiberxavfsizlikning ahamiyatini tushunish u taqdim etadigan va o‘zida mujassam etgan xavf-xatarlarga qarshi kurashning dastlabki bosqichidir. Jamiyatning xabardorligi bo‘lmasa, hukumatlar, harbiy tuzilmalar, muhim milliy infratuzilma tashkilotlari, korxonalar va jismoniy shaxslar o‘z-o‘zini himoya qilish uchun mazmunli choralar ko‘rmaydi. 2002-yilda “Raqamli Pearl Harbor” nomi bilan tanilgan AQShning muhim infratuzilma kiberxavfsizlik mashqlari Prezident Jorj Bush o‘z natijalaridan kiberxavfsizlikni hal qilish muhimligini ta’kidlash uchun foydalangani sababli alohida shuhrat qozondi[1]. Ushbu ogohlantirishlardan so‘ng, keng tarqalgan oqibatlarga olib keladigan asosiy muammo hal qilindi. Turli panellar,

[1] Öğün MN, Yurtsever S, Aslan M, Elburası M. Terrorist Use of Cyber Technology. Eskişehir Teknik Üniversitesi Bilim ve Teknoloji Dergisi B-Teorik Bilimler. 2021 Dec 12;9(Iconat Special Issue 2021):113-28. dergipark.org.tr

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

komissiyalar, qonunlar va qoidalar Oq uy, Kongress, Milliy xavfsizlik departamenti, Mudofaa departamenti, Milliy standartlar va texnologiyalar instituti va boshqa koʻplab tashkilotlardan kelib chiqqan holda milliy va xalqaro kiberxavfsizlikni yaxshilash zaruriyatini koʻrib chiqdi[2].

Bir qancha mualliflar kiberterrorizmga ta'rif berishga harakat qilishgan. Bunday ta'riflardan biri: "Kiberterrorizm axborotni qayta ishlash tizimlarini buzish, axborotni oʻzgartirish, yoʻq qilish yoki oʻgʻirlash uchun kompyuter tarmoqlaridan foydalanishni oʻz ichiga oladi, bunda garovga olish, milliy xavfsizlikka tahdid solishi mumkin boʻlgan qoʻporuvchilik, tajovuzkor, jinoiy yoki terroristik faoliyatni amalga oshirish yoki majburlashning boshqa shakllari". Sogʻlom kuchayib, keng tarqalib borayotgan kiberterrorizmning zararli oqibatlariga qarshi kurashish masalasi zamonaviy davlatlar va zamonaviy hayotning barcha jabhalari xavfsizligini ta'minlashning ustuvor yoʻnalishiga aylandi. Prezident G. Mindeli ta'kidlaganidek, "kiberterrorizmning halokatli oqibatlari koʻplab mamlakatlarda sezilmoqda va virtual makondan terroristik maqsadlarda foydalanish, dasturiy ta'minot va ma'lumotlardan virtual terrorizm uchun vosita sifatida foydalanishga qarshi kurashishning dolzarb zarurati mavjud"[3]. 1990-yillarning oxirlarida Avstraliya va Yangi Zelandiya oʻzlarining energiya tizimlariga kompyuter aralashuvi tufayli elektr ta'minotida bir qator uzilishlarni boshdan kechirdilar. Ushbu hodisa koʻpincha Internetdan urush vositasi sifatida foydalanishning eng dastlabki hujjatlashtirilgan namunasi sifatida tilga olinadi. 1992 yilda muhim Internet qurti 6000 ga yaqin kompyuterning ishdan chiqishiga sabab boʻldi, bu Mudofaa vazirligi xodimlarining kiberxavfsizlik sohasiga qiziqishini oshirdi. Kompyuterning favqulodda vaziyatlarga javob berish guruhi (CERT) dasturiy ta'minot dasturi bilan bogʻliq muammolar hal qilindi, bu uning vorisi - AQShning kompyuter favqulodda vaziyatlarga tayyorgarligi jamoasi (US-CERT) tashkil etilishiga olib keldi. 2003 yilda Kibermakonni himoya qilish boʻyicha Milliy strategiya joriy etilgan va Kongress kiberxavfsizlikni kuchaytirishga qaratilgan bir nechta favqulodda federal

[2] Mukekhe WG. Information System Infrastructure Management Influence On Cyber-Terrorism in Directorate of Criminal Investigation, Nairobi City County, Kenya.. 2021. ku.ac.ke

[3] Miller T, Staves A, Maesschalck S, Sturdee M, Green B. Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. International Journal of Critical Infrastructure Protection. 2021 Dec 1;35:100464. [HTML]

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

qonunlarni, jumladan Axborot xavfsizligini boshqarish to‘g‘risidagi Federal qonunni (FISMA; 2002), Axborot texnologiyalari (IT) boshqaruvini isloh qilish to‘g‘risidagi qonunni (2002) va kiberxavfsizlikni tadqiq qilish va rivojlantirish to‘g‘risidagi qonun (2002). Bundan tashqari, Milliy xavfsizlik departamenti terroristik hujumlarning oldini olish uchun kibermakonni himoya qilishning o‘ziga xos missiyasi bilan tashkil etilgan. 2003 yilda Oq uy Federal hisoblash tizimlarining maxfiyligi, yaxlitligi va mavjudligini ta'minlash uchun AQSh Ichki xavfsizlik departamenti tarkibida Milliy kiberxavfsizlik bo‘limini (NCSD) tuzdi. Ushbu bo‘linma, shuningdek, federal axborot tizimlariga ta'sir qiladigan har qanday hodisaga darhol javob berish qobiliyatini ta'minlaydi, federal agentlik tarmoqlarini ma'lum zaifliklardan to‘g‘ri himoya qilishni ta'minlaydi va federal hukumatni 18 ta muhim infratuzilma tarmoqlarini himoya qilish bo‘yicha sa'y-harakatlarida qo‘llab-quvvatlaydi. Bundan tashqari, 2004 yilda Santa Klarada (Kaliforniya shtati) Kiberxavfsizlik bo‘yicha birinchi milliy sammit bo‘lib o‘tdi. Kiberxavfsizlikning ahamiyatini tushunish u taqdim etadigan va o‘zida mujassam etgan xavf-xatarlarga qarshi kurashning dastlabki bosqichidir. Jamiyatning xabardorligi bo‘lmasa, hukumatlar, harbiy tuzilmalar, muhim milliy infratuzilma tashkilotlari, korxonalar va jismoniy shaxslar o‘z-o‘zini himoya qilish uchun mazmunli choralar ko‘rmaydi. 2002-yilda "Raqamli Pearl Harbor" nomi bilan tanilgan AQShning muhim infratuzilma kiberxavfsizlik mashqlari Prezident Jorj Bush o‘z natijalaridan kiberxavfsizlikni hal qilish muhimligini ta'kidlash uchun foydalangani sababli alohida shuhrat qozondi. Ushbu ogohlantirishlardan so‘ng, keng tarqalgan oqibatlarga olib keladigan asosiy muammo hal qilindi[4]. Turli panellar, komissiyalar, qonunlar va qoidalar Oq uy, Kongress, Milliy xavfsizlik departamenti, Mudofaa departamenti, Milliy standartlar va texnologiyalar instituti va boshqa ko‘plab tashkilotlardan kelib chiqqan holda milliy va xalqaro kiberxavfsizlikni yaxshilash zaruriyatini ko‘rib chiqdi. Atrof-muhitni muhokama qilishda foydalaniladigan lingvistik asoslar resurslarni taqsimlash, qarorlarni muvofiqlashtirish, rejalarni ishlab chiqish va o‘zaro maqsadlarga erishish uchun qo‘llaniladigan yondashuvlar ustidan sezilarli ta’sirga ega. Kiberxavfsizlik sohasi turli jabhalar va sohalarni o‘z ichiga oladi, uning geografik

[4] Bak-Coleman JB, Alfano M, Barfuss W, Bergstrom CT, Centeno MA, Couzin ID, Donges JF, Galesic M, Gersick AS, Jacquet J, Kao AB. Stewardship of global collective behavior. Proceedings of the National Academy of Sciences. 2021 Jul 6;118(27):e2025764118. pnas.org

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

ko‘lami raqamli ob’ektlar geosiyosiy chegaralardan mustaqil ravishda faoliyat yuritadigan barcha hududlarni qamrab oladi. Ular birga yashaydigan va ishtirok etadigan ushbu domen kibermakon deb nomlanadi. Ko‘pgina kontekstlarda kiberxavfsizlik muhiti ushbu domendan foydalanish, kengaytirish va tartibga solish bilan bog‘liq barcha global o‘zaro ta’sirlarni ham o‘z ichiga oladi. Qasddan qilingan harakatlardan ta’sirlangan shaxslar kiberxavfsizlik intsidentlariga duchor bo‘ladilar va agar bu harakatlar to‘sqinlik qilish, foydalanish imkoniyatini buzish yoki ma’lumotlarning ta’sirlanishi, o‘zgartirilishi yoki yo‘q qilinishiga olib keladigan bo‘lsa – zamonaviy axborot va telekommunikatsiya texnologiyalarining asosiy xususiyatlari – ular kiberhujumlar deb tasniflanadi. So‘nggi tadqiqot ma’lumotlari shuni ko‘rsatadiki, xakerlik noqonuniy kiberfaoliyatning eng keng tarqalgan shakli bo‘lib qolmoqda; ammo, bunday harakatlar ortidagi motivlar vaqt o‘tishi bilan sezilarli o‘zgarishlarga uchradi. Kibermakonda paydo bo‘ladigan asosiy muammo bu xakerlik harakatining o‘zi emas, balki asosiy motivatsiyadir. Dastlabki kiber hodisalarga IT xodimlari o‘rtasidagi hayajonli, shaxslararo mojarolar, moliyaviy daromadlar va dushman xorijiy kuchlarning harakatlari sabab bo‘lgan. Kiberhujumlar rivojlanishda davom etishi va chastotasi va murakkabligi oshishi kutilmoqda. Ushbu yutuqlar nafaqat tajovuzkorlarga yashirincha harakat qilish va texnik hujumlarni yanada samarali amalga oshirish imkonini beradi, balki o‘zgaruvchan vaziyatlar, shartlar va hodisalarga javoban o‘z taktikasini moslashtirishga imkon beradi. Slammer va Blaster kabi yuqori darajadagi virus tarqalishining keng tarqalgan e’tibori virus hujumlarini kiberjinoyatchi tashkilotlarga tobora ko‘proq jalb qildi. Ushbu korxonalar an’anaviy dasturiy ta’minot ishlab chiqish korxonalariga o‘xshash moliyaviy va tashkiliy tuzilmalar bilan ishlaydi. Bu ortib borayotgan e’tibor kompaniyalarni kiberhujumlar ularning obro‘siga yetkazishi mumkin bo‘lgan potentsial zarardan xabardor bo‘lishiga olib keldi. Natijada, kompaniyalar o‘zlarining raqobatdosh ustunliklarini buzishi mumkin bo‘lgan har qanday virus hujumlari yoki hujumlarini oshkor qilishga undaydilar. Bundan tashqari, kiberhujumlar yanada qulayroq bo‘lib, cheklangan tajribaga ega bo‘lgan va taniqli bo‘lishni xohlaydigan shaxslarga samarali hujumlarni amalga oshirish va huquqni muhofaza qilish organlarining tekshiruvidan qochish imkonini beradi. Kamroq tajribaga ega bo‘lgan nishonlarga nisbatan murakkab hujumlarni amalga oshirish imkoniyatiga qaramay, zaif shaxslardan foydalanadigan oddiy, past texnologiyali hujumlar va tuzoqlarning oldini olish muammosi bo‘lib

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

qolmoqda. Ushbu hodisalar korxonalarga xavfsizlikni buzish maxsus bilimga muhtoj bo‘lmasdan sodir bo‘lishi mumkinligi haqida aniq eslatma bo‘lib xizmat qiladi. Kiberhujumlarning turli shakllari mavjud bo‘lib, ularning barchasi oxir-oqibat maqsad – jabrlanuvchi va maqsad atrofida aylanadi, ular aktivlarni to‘g‘ridan-to‘g‘ri yo‘q qilishdan tortib, maxfiylik, yaxlitlik va ruxsat berilgan kirishdan foydalanishgacha bo‘lishi mumkin. Birinchisi to‘g‘ridan-to‘g‘ri kiberterrorizm sohasiga to‘g‘ri keladi, ikkinchisi esa odatda “boshqa narsa” deb ataladi, ko‘proq tasodifiy xakerlik deb nomlanadi. Shuni ta’kidlash kerakki, ushbu harakatlar uchun motivatsiyalar juda xilma-xil bo‘lishi mumkin. Xakerlar, odatda, yosh shaxslar qiziquvchanlik tufayli tizimlar va tarmoqlarni buzishga intilishlari mumkin bo‘lsada, kiber jinoyatchilar va terrorchilar, birinchi navbatda, mos ravishda pul daromadlari va zarar etkazish istagi bilan boshqariladi. Bundan tashqari, sanoat xakerlari ham xodimlar ichida, ham o‘rtasida raqobat va ochko‘zlik bilan turtki bo‘ladi. Raqamli soha jamiyat qo‘rquvi uchun asosiy maydondir. O‘ttiz yildan kamroq vaqt ichida biz bu dunyoni son-sanoqsiz yo‘llar bilan bog‘ladik. Bizning kundalik hayotimizning barcha jabhalarida – energiya, transport va aloqadan moliya, suv va oziq-ovqatgacha bo‘lgan ushbu murakkab tarmoqqa tayanishimiz shubhasizdir. Turli sohalardagi shaxslar, jumladan, ilg‘or akademik tadqiqotlar, turli razvedka xizmatlari, yuqori biznes va texnologiya sektorlari milliy va global darajada kiberdomen xavfsizligiga shubha bildirmoqda. Ushbu jamoalar bunday tizimlarning xavfsizlik chegaralarini sinab ko‘rish, zaifliklarni tekshirish va raqamli infratuzilmalarning yaxlitligiga xavf tug‘dirishi mumkin bo‘lgan usullarni hal qilish usullarini faol ravishda izlamoqda. Yaqinda global miqyosda e’lon qilingan xavfsizlik hisoboti buni qo‘llab-quvvatlab, keng tarqalgan xavotirni ochib beradi. Hatto yaxshi moliyalashtiriladigan texnologik kuchlarga qarshi minimal resurslar bilan boshlangan kichik miqyosli kiberoperatsiyalar ham ajoyib natijalar berdi, bu ko‘plab yuqori darajadagi va muvaffaqiyatli faoliyatlardan dalolat beradi. Kiberterrorchilar o‘z maqsadlari ta’sirini maksimal darajada oshirish uchun zamonaviy raqamli mavjudligimiz haqiqatini jismoniy vositalari bilan uyg‘unlashtirib, o‘zlari qo‘llayotgan vositalarning og‘irligi va salohiyatini tushunadilar. Kiberterrorizm ko‘p qirrali, biroz murakkab bo‘lmagan tushuncha bo‘lib, jinoiy terrorchilik harakatlarini amalga oshirishga qaratilgan kiber sohadagi faoliyatga taalluqlidir. Madaniy, diniy va falsafiy yo‘nalishlarda ekstremizmning kuchayib borayotganiga guvoh bo‘lganimizdek, ushbu mafkuralarni tarqatish uchun internetdan foydalanishning ham

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

ko‘payishiga guvoh bo‘ldik. Biroq, Internetdan foydalanish shunchaki muloqot va nutq bilan chegaralanmaydi. Bundan tashqari, ushbu radikal fraktsiyalar tomonidan terror hujumlarini amalga oshirishni muvofiqlashtirish va strategiya qilish uchun foydalaniladi. Shunday qilib, ushbu haqiqatni to‘liq tekshirish zarur. Terrorchilar tomonidan kiber vositalardan bunday foydalanishga qarshi kurashish uchun kiberterrorizm nimaga olib kelishi va terror guruhlari kibersoha haqida nimani tushunishi haqida aniq belgilangan doiraga ega bo‘lish zarur. Qisqaroq qilib tushuntirganda, samarali kiberxavfsizlik strategiyasi proaktiv boshqaruvni, ochiq muloqotni, moddiy resurslarni, amaliy tadqiqotlarga e’tiborni qaratishni, hamkorlar bilan hamkorlikni va doimiy rivojlanib borayotgan zamonaviy sharoitda xavfsizlik choralarini amalga oshirish uchun javobgarlikni taqsimlashni ta’minlaydigan ilg‘or tajribalarga asoslangan boshqaruv tizimini talab qiladi. Ko‘p tarmoqli usul jamoaning barcha ishtirokchilari korporativ missiyani tan olishlari, qaysi ma’lumotlar, aktivlar va tizimlar ustuvor e’tiborga olinishini aniqlashlari va keyin ularni arxitektura va tijoratga yo‘naltirilgan strategik rivojlanish bilan kelishilgan holda ta’minlashga harakat qilishlarini nazarda tutadi. Kiberxavfsizlik – bu jamoaviy sport, hamkorlikdagi yondashuv, bu erda kuchli kiberxavfsizlik tamoyillari, xavflarni boshqarish va resurslarni taqsimlash missiya natijalariga ta’sir qiladi. Shu sababli, tashkilotlar yuqori sifatli kibermutaxassislarni jalb qila olmasa va ushlab turolmasa yoki zarur bo‘lgan malakali ishchi kuchi resurslarini ushlab turolmasa, davlatlar muammoga duch kelishadi. Kiberxavfsizlik strategiyalarini amalga oshirish bo‘yicha ilg‘or tajribalar va alohida tavsiyalar berildi. Kiberxavfsizlik bo‘yicha ilg‘or amaliyotlar kiberxavfsizlik xavfini yumshata oladigan chora-tadbirlarning keng qamrovli va o‘lchanadigan ro‘yxatini taklif etadi, garchi alohida mamlakatlar va tashkilotlarning kibermakonda xavfsizligini ta’minlash ko‘p qirrali vazifadir. Ko‘pgina kiberxavfsizlik hisobotlarining asosiy mavzusi resurslar tashkilotning eng muhim aktivlariga to‘planishi kerak, chunki ular tarmoq hujumi xavfini ifodalaydi, ularni hal qilish va kamaytirish kerak. Shu bilan birga, malakali ishchilarning yetishmasligi tufayli o‘sib borayotgan xavfsizlik bo‘shlig‘i xavfsizlik strategiyasining bajarilishini kamaytiradi, bu esa o‘z navbatida xavfsizlik hodisalarining oldini olish, aniqlash va ularga javob berish qobiliyatini pasaytiradi. Kiberxavfsizlik strategiyalari fuqarolarni, infratuzilmani va maxfiy ma’lumotlarni himoya qilish hamda tashkilotlar, davlatlar va jahon iqtisodiyotining normal ishlashini ta’minlash uchun muhim asosiy masaladir. Kiberxavfsizlik tizimi

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

vaqt o‘tishi bilan tahdidlarning davriy yangilanishini, iqtisodiy faollik darajasiga moslashtirilgan va yangi texnologiyalardagi o‘zgarishlar, ijtimoiy media platformalaridan ko‘proq foydalanish, bulutli hisoblash va onlayn xizmatlarga o‘tish bilan shakllantirilishini talab qiladi. Kiberxavfsizlik strategiyalarining asosiy maqsadi kiberhujum xavfini kamaytirish va shu orqali fuqarolar, korxonalar va hukumatlarga o‘zlarining kundalik faoliyatini internetdan foydalanish bilan bog‘liq bo‘lgan tahdidlardan xavfsiz davom ettirishga imkon berishdir. Ko‘pgina mamlakatlar kiberxavfsizlik bo‘yicha o‘zlarining milliy strategiyalarini ishlab chiqdilar va bu davlatlar ushbu strategiyalar bo‘yicha agressiv harakat qilmoqdalar. Biroq, bu strategiyalarning kamchiliklari shundaki, ular ko‘pincha kelajakni rejalashtirishdan ko‘ra strategiyalar ishlab chiqilgan vaqtda ma’lum tahdidlarga javob beradi. Kiberxavfsizlik tarmoq va axborotning yaxlitligini himoya qilish uchun zarur bo‘lgan chora-tadbirlardan iborat. Xavfsizlikni rejalashtirish ushbu mudofaa choralarini buzish yoki zararsizlantirish uchun maxsus ishlab chiqilgan chora-tadbirlarni tavsiflaydi. Xavfsizlikni boshqarish, aksincha, aniq maqsadlarga erishish uchun resurslarni rejalashtirish, tashkil etish, rag‘batlantirish va nazorat qilish jarayonidir. Xavfsizlikni boshqarishda maqsad tarmoqlarni himoya qilish va qabul qilinadigan xavfsizlik darajasini saqlab qolishdir. Kiberxavfsizlik va xavfsizlikni rejalashtirishning xavfsizlikni boshqarish elementlari, keyin esa, texnik va ma’muriy tajriba va xavfsizlik sohalarini integratsiya qilish qobiliyatini o‘z ichiga oladi. Kibermakonning taxminiy zaifligini yoki muhim infratuzilmaga hujumlar kuchayib borayotganini tasdiqlovchi dalillar kamligining dastlabki empirik kashfiyoti Milliy tadqiqot kengashini hukumat organlariga batafsilroq ma’lumot taqdim etishni tavsiya qilishga undadi. Eng tez-tez foydalaniladigan zaifliklar to‘g‘risidagi ma’lumotlar, shuningdek, ko‘plab tashkilotlar uchun eng katta xavf tug‘diradigan yoki eng katta zarar etkazuvchi hujumlar to‘g‘risidagi ma’lumotlar strategik rejalashtirish va hodisalarga javob berishga yordam beradi. Texnik hamjamiyat tomonidan aytilgan da’volar, agar biror narsa bo‘lsa, yanada aniqroq bo‘ldi. Bryus Scheinerning ta’kidlashicha, kiberxavfsizlikning hozirgi holatiga nisbatan pessimistik qarashlar qo‘shimcha tekshirishni talab qiladi. Siyosatchilar kiberxavfsizlikda barqaror inqiroz va xavfsizlikning yo‘qligiga shunchalik aminlarki, ular yuzaga kelishi mumkin bo‘lgan salbiy ta’sirlardan qat’i nazar, xavfsizlik sohasidagi har qanday yutuqlarni qo‘llab-quvvatlashga moyildirlar. Kiberterrorizmning tabiati, ko‘lami va maqsadlarini o‘rganish natijasida olingan bir

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

kuzatish qiziq haqiqatni ochib berdi. 11-sentabrdan keyingi davrdan so‘ng, kiberterrorizm kuzatilishi mumkin bo‘lgan hodisalarni aniq tasvirlashdan ko‘ra, asosan ritorik vosita sifatida qo‘llanilgani aniq. Kiberterrorizmning amalga oshirilishi mumkinligi haqidagi keng tarqalgan qabul qilingan taxmin empirik ma’lumotlar bilan tasdiqlanganmi yoki yo‘qmi, degan so‘rov o‘tkazilmagan. Xulosa qilib aytganda, bizning sohamizdagi aksariyat adabiyotlarda mavjud bo‘lgan markaziy ta’kid, kiberterrorizmning yaqinlashib kelayotgan xavfi, to‘g‘risidagi yonodshuvi noto‘g‘ri. Kiberxavfsizlik texnologiyalarining rivojlanishi tobora murakkablashib borayotgan tahdidlarga mos keladi. Biroq, raqamli identifikatsiyani kuchaytirish, tarmoq barqarorligini kuchaytirish, dasturlarimiz uchun dasturiy ta’minotni yetkazib berish zanjirini tekshirish, mashinani o‘rganish uchun ma’lumotlarga ko‘proq tayanish va texnologik jihatdan mumkin bo‘lgan va xavfsiz saqlanadigan va oson kirish mumkin bo‘lgan shifrlashni amalga oshirish uchun qo‘shimcha vositalarga ehtiyoj ortib bormoqda. Bundan tashqari, sud-tibbiyot ekspertizasi va hodisalarga javob berish, shuningdek, yashirin tahdidlar uchun kodni tahlil qilish va zararli dasturlarni bartaraf etish uchun sun’iy intellektni qo‘llash, boshqa talablar qatorida qo‘llab-quvvatlashga ehtiyoj bor. Bundan tashqari, kiber-fizik tizimlar va narsalar internetining rivojlanishi yangi vositalarni yaratishni talab qiladi. Nihoyat, hozirgidan ko‘ra kengroq manfaatdor tomonlarni jalb qilgan holda internet boshqaruvini takomillashtirish jiddiy o‘ylantiriladigan mavzu bo‘lib, Milliy kiberxavfsizlikni kuchaytirish bo‘yicha komissiyaning diqqat markazida bo‘ladi. Texnologik yutuqlar ishonchli internetga olib kelishini ta’minlash uchun samarali va shaffof boshqaruv muhim ahamiyatga ega. Kiberxavfsizlik sohasi ko‘pincha mulk huquqlari aniq belgilanmagan dunyoda ishlaydi, ayniqsa murakkab kompyuter tili va butun dunyo bo‘ylab qimmatli aktivlar va shaxsiy identifikatorlarning harakati uchun mas’ul bo‘lgan tizimlarni tartibga soluvchi qoidalar bilan bog‘liq. Buzilgan yoki o‘g‘irlangan kompyuter kodi muammosini hal qilish bo‘yicha hozirgi harakatlar odatda bunday kodni aniqlashni, kompyuter kodini tez-tez yangilashni yoki mas’uliyatni o‘z ichiga oladi.

FOYDALANILGAN ADABIYOTLAR:

1. Mukekhe WG. Information System Infrastructure Management Influence On Cyber-Terrorism in Directorate of Criminal Investigation, Nairobi City County, Kenya.. 2021. ku.ac.ke

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

2. Öğün MN, Yurtsever S, Aslan M, Elburası M. Terrorist Use of Cyber Technology. Eskişehir Teknik Üniversitesi Bilim ve Teknoloji Dergisi B-Teorik Bilimler. 2021 Dec 12;9(Iconat Special Issue 2021):113-28. dergipark.org.tr

3. Saul B, Heath K. Cyber terrorism and use of the internet for terrorist purposes. Research Handbook on International Law and …. 2021. [HTML]

4. Weiss M, Biermann F. Cyberspace and the protection of critical national infrastructure. Journal of Economic Policy Reform. 2023. [HTML]

5. Gilad A, Pecht E, Tishler A. Intelligence, cyberspace, and national security. Defence and Peace Economics. 2021. researchgate.net

6. AlDaajeh S, Saleous H, Alrabaee S, Barka E, Breitinger F, Choo KK. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security. 2022 Aug 1;119:102754. unil.ch

7. Schultz Jr EE. Wednesday, May 9, 1990 10: 30 am to 10: 45 am. In13th Department of Energy Computer Security Group Conference. osti.gov

8. Miller T, Staves A, Maesschalck S, Sturdee M, Green B. Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. International Journal of Critical Infrastructure Protection. 2021 Dec 1;35:100464. [HTML]

9. Lallie HS, Shepherd LA, Nurse JR, Erola A, Epiphaniou G, Maple C, Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security. 2021 Jun 1;105:102248. nih.gov

10. Breyer SG, Stewart RB, Sunstein CR, Vermeule A, Herz M. Administrative Law and Regulatory Policy: Problems, Text, and Cases [Connected eBook with Study Center]. Aspen Publishing; 2022 Feb 25. [HTML]

11. Health Organization W. Towards a global guidance framework for the responsible use of life sciences: summary report of consultations on the principles, gaps and challenges of biorisk …. 2022. who.int

12. Kim DKD, Kreps GL. An analysis of government communication in the United States during the COVID-19 pandemic: recommendations for effective government health risk communication. World Medical & Health Policy. 2020. nih.gov

13. Bak-Coleman JB, Alfano M, Barfuss W, Bergstrom CT, Centeno MA, Couzin ID, Donges JF, Galesic M, Gersick AS, Jacquet J, Kao AB. Stewardship of

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

global collective behavior. Proceedings of the National Academy of Sciences. 2021 Jul 6;118(27):e2025764118. pnas.org

14. Howard J, Huang A, Li Z, Tufekci Z, Zdimal V, Van Der Westhuizen HM, Von Delft A, Price A, Fridman L, Tang LH, Tang V. An evidence review of face masks against COVID-19. Proceedings of the National Academy of Sciences. 2021 Jan 26;118(4):e2014564118. pnas.org

15. Sebhatu A, Wennberg K, Arora-Jonsson S, Lindberg SI. Explaining the homogeneous diffusion of COVID-19 nonpharmaceutical interventions across heterogeneous countries. Proceedings of the National Academy of Sciences. 2020 Sep 1;117(35):21201-8. pnas.org