

KIBERTERRORIZMNING ZAMONAVIY TAHDIDLARI EKSTREMIZMNING YANGI
SHAKLI SIFATIDA

Abdulfaizova Durдона Ikromjon qizi
“University of economics and pedagogy”
NOTM o‘qituvchisi

Annotatsiya: Maqolada kiberterrorizmning zamonaviy tahdidlari, ularning shakllari va kiberhujumlarning jismoniy terrorizmga nisbati tahlil qilingan. Maqolada, kiberhujumlarning tarixi, mashhur kiberhujumlar, ularning moliyaviy zararlar va jamiyatga keltirgan salbiy oqibatlari yoritilgan. Kiberterrorizmning keng miqyosda va masofadan amalga oshirilishi, hamda qurol talab qilmasligi haqida batafsil ma'lumot berilgan.

Kalit so'zlar: kiberterrorizm, kiberhujum, axborot texnologiyalari, internet xavfsizligi, terrorizm, kompyuter xavfsizligi, kiberjinoiyat.

Аннотация: В статье анализируются современные угрозы кибертерроризма, их формы и соотношение кибератак и физического терроризма. В статье рассказывается об истории кибератак, известных кибератаках, их финансовых потерях и негативных последствиях для общества. Подробно описано, как кибертерроризм может осуществляться в больших масштабах и удаленно, а также не требует оружия.

Ключевые слова: кибертерроризм, кибератака, информационные технологии, Интернет-безопасность, терроризм, компьютерная безопасность, киберпреступность.

Annotation: the article analyzes the modern threats of cyberterrorism, their forms and the ratio of cyber attacks to physical terrorism. The article covers the history of cyberattacks, popular cyberattacks, their financial losses and the negative consequences they have caused to society. Cyberterrorism has been described in detail as being performed on a large scale and remotely, as well as not requiring weapons.

Keywords: cyberterrorism, cyberbullying, information technology, internet security, terrorism, computer security, cybercrime.

Bugungi kunda kiberterrorizm ijtimoiy tarmoqlarda ommalashib bormoqda. Uning virusli dasturlarni tarqatish, parollarni buzib kirish, kredit karta va boshqa bank rekvizitlaridagi mablag'larni o'zlashtirish talon-toroj qilish, shuningdek, internet orqali qonunga zid axborotlar, xususan, bo'hton, ma'naviy buzuq ma'lumotlarni tarqatish kabi turlari mavjud. Internet foydalanish kengayib, kompyuter tizmlari murakkablashib borgan sari kiberterrorizm xavfi ham kengaymoqda. Terroristlar uchun kiberterrorizmga asoslangan hujumlar jismoniy hujumlarga qaraganda bir qancha afzalliklarga ega. Kiberhujumlar masofadan, keng ko'lamda amalga oshirilishi mumkin. Shuningdek kiberterrorizmni amalga oshirish uchun qurol yarog' talab qilinmasligi ham terroristlarga ortiqcha katta mablag' sarflashni talab qilmaydi.

Kiberterrorizmning turli xil ta'riflari mavjud.

Kiberterroristik harakat (kiberhujum) - kompyuterlar va axborot kommunikatsiya vositalari yordamida amalga oshirilgan, odamlarning hayoti va sog'lig'iga bevosita xavf tug'diradigan yoki potentsial xavf tug'dirishi mumkin bo'lgan, moddiy obyektlarga katta zarar yetkazishi yoki shunga olib kelishi mumkin bo'lgan, ijtimoiy xavfli oqibatlarining boshlanishi yoki maqsadi bo'lgan siyosiy sababdir¹.

Kiberterrorizm aslida axborot texnologiyalari ichki faoliyatiga noqonuniy aralashish, kompyuterda mavjud dasturlar yoki malumotlarni maqsadli ravishda yo'q qilish, zarar keltirish, davlat organlarining muhim qismlari faoliyatini izdan chiqarish bilan birga insonlar hayotiga

¹Kiberjinoiyatchilikka qarshi kiberoxavfsizlik: Abdurasul IMINOV, IIV Akademiyasi Axborot texnologiyalari kafedrasi boshlig'i, podpolkovnik

xavf solish, moddiy zarar keltirish yoki ommaviy qo'rqitish, harbiy nizolara kabi turli zararli oqibatlarini keltirib chiqarishga qaratilgan harakatdir.²

NATO tashkiloti tomonidan kiberterrorizmga "kompyuter yoki aloqa tarmoqlaridan foydalanish yoki ulardan foydalanishda qo'rqivni vujudga keltirish yoki jamiyatni g'oyaviy maqsadda qo'rqitish uchun yetarli darajada vayronagarchilik yoki buzilishlarni keltirib chiqaradigan kiberhujum" deb ta'rif beriladi.³

Amerika Qo'shma Shtatlarining Federal qidiruv byurosi "kiberterrorizm" ni "axborot, kompyuter tizimlari, kompyuter dasturlari va ma'lumotlarga qarshi oldindan rejalashtirilgan, siyosiy sabablarga ko'ra hujum qilish, bu submilliy guruhlar yoki yashirin agentlar tomonidan noharbiy maqsadlarga qarshi zo'ravonlikka olib keladi" deb ta'riflaydi.⁴

Kiberterrorizm atamasi 1980-yil AQSHlik ilmiy xodim Berli kalin tomonidan muomilaga kiritilgan. Dunyoning birinchi kiber hujumi 1988-yilda sodir bo'lgan. Ushbu hujum Morris qurtlari nom bilan mashxur bo'lgan.. AQSH Boston ilmiy muzeyi sobiq egasi Robert Tappan Morris (Robert Tappan Morris), birinchi internet qurtlaridan birini yaratdi va uni 1988 yil 2 noyabr kuni Massachusetts Texnologiya Institutida ishladi. Natijada, Qo'shma Shtatlarda 6000 internet saytlari falaj bo'lib, buning natijasida jami zarar 96,5 million dollarni tashkil etdi.

Shundan so'ng bir qancha kiberhujumlar uyushtirildi. Quyida ularning eng yiriklari berilgan.

Melissa 1999. Melissa elektron pochta orqali yuborilgan birinchi zararli kod bo'ldi. 1999 yil mart oyida u dunyodagi yirik kompaniyalarning serverlarini ishdan bo'shatdi. Bu virus virusga qarshi yangi e-pochta orqali yuboriladigan elektron pochta xabarlarini serverlariga juda kuchli yukni keltirib chiqarishi sababli yuz berdi. Shu bilan birga, ularning faoliyati juda sekin yoki to'liq to'xtatildi. Foydalanuvchilar va kompaniyalar uchun Melissa virusidan zarar 80 million dollarga baholandi. Bundan tashqari, u yangi turdagi virusning "ajdodlari" bo'ldi.

Mafiaboy 2000. Bu 16 yoshli Kanadalik maktab o'quvchisi tomonidan boshlangan dunyoning birinchi DDoS hujumlaridan biri edi. 2000-yil fevral oyida bir nechta jahonga mashhur saytlar (Amazon dan Yahoo ga), bu erda hacker Mafiaboy zaiflikni aniqlashga muvaffaq bo'ldi. Natijada, resurslar faoliyati deyarli bir hafta davomida to'xtatildi. To'liq miqyosdagi hujumdan zarar ko'rilganligi juda jiddiy bo'lib, 1,2 milliard dollarga baholandi.

Estoniyadagi kiber hujum 2007. 2007 yil aprel oyida bo'lib o'tgan voqealarni birinchi kiber urush deb atash mumkin. Keyinchalik, Estoniyada tibbiy resurslar va onlayn xizmatlar bilan shug'ullanadigan kompaniya uchun hukumat va moliyaviy saytlar bir vaqtning o'zida uzilib qoldi. Bu zarba juda sezilarli edi, chunki o'sha paytlarda E-hukumat Estoniyada faoliyat yuritgan va bank to'lovlari deyarli butunlay onlayn edi. Kiber hujum butun davlatni falaj qildi. Bundan tashqari, bu Ikkinchi jahon urushidagi Sovet askarlari haykali o'tkazilishiga qarshi mamlakatda ro'y bergan ommaviy noroziliklarning fonida sodir bo'ldi.

Gauss, 2012. Ushbu virus - zararli kompyuterlardan moliyaviy ma'lumotni o'g'irlab ketgan bank tujjorini tandemda ishlagan amerikalik va isroil hackerlari yaratgan. 2012 yilda Gauss Liviya, Isroil va Falastin bandargohlariga hujum qilganida u kiber qurol sifatida ko'rilgan. Keyinchalik ma'lum bo'lgach, kiber hujumning asosiy vazifasi Livan banklarining terroristlar uchun mumkin bo'lgan maxfiy ko'magi haqida ma'lumotni tekshirish edi.

WannaCry, 2017. 300 mingta kompyuter va dunyoning 150 mamlakati - bu virus qurbonlari bo'ldi. 2017-yilda dunyoning turli burchaklarida shaxsiy kompyuterlarga Windows operatsion tizimi kirib keldi ,qattiq diskda saqlanadigan ma'lumotlarga kirishni to'sib qo'yishdi, ammo uni 300 dollarga qaytarishga va'da berishdi. Mazkur to'lovni rad etganlar, barcha ma'lumotlarini yo'qotishdi. WannaCry'dan olingan zarar 1 milliard dollarga baholanmoqda. Uning muallifi hali ham noma'lum.

²“ Kiberterrorizm: milliy va xalqaro xavfsizlikka tahdid” Dilafruz Turdiyeva

³ Centre of Excellence Defence Against Terrorism, ed. (2008). Responses to Cyber Terrorism. NATO science for peace and security series. Sub-series E: Human and societal dynamics, ISSN 1874-6276.

⁴ Centre of Excellence Defence Against Terrorism, ed. (2008). Responses to Cyber Terrorism. NATO science for peace and security series. Sub-series E: Human and societal dynamics, ISSN 1874-6276.

Xulosa sifatida aytishimiz mumkinki, kiberterrorizmning zamonaviy tahdidlari shiddat bilan o'sib bormoqda va katta zararlarni keltirib chiqarmoqda. kiberterrorizm zamonaviy tahdidlardan biri bo'lib, internet va axborot texnologiyalarining rivojlanishi bilan tobora kuchaymoqda. Uning salbiy oqibatlari faqat davlatlar yoki iqtisodiyotlarga zarar yetkazish bilan cheklanmaydi, balki jamiyatda xavotir, qo'rquv va ishonchsizlikni ham keltirib chiqaradi. Kiberhujumlar, masofadan amalga oshirilishi, osonlik bilan kengayishi va jismoniy qurol talab qilmasligi sababli, terroristlar uchun samarali va kam xarajatli vosita bo'lib qolmoqda.

Foydalanilgan adabiyotlar:

1. Kiberjinoyatchilikka qarshi kibexavfsizlik: Abdurasul IMINOV, IIV Akademiyasi Axborot texnologiyalari kafedrasini boshlig'i, podpolkovnik
2. Kiberterrorizm: milliy va xalqaro xavfsizlikka tahdid" Dilafruz Turdiyeva
3. Centre of Excellence Defence Against Terrorism, ed. (2008). Responses to Cyber Terrorism. NATO science for peace and security series. Sub-series E: Human and societal dynamics, ISSN 1874-6276.
4. Kiberterrorizm: Entsiklopediya site: uz.wikiqube.net
5. Zamonaviy internet tarixidagi eng katta kiberhujum: Uz.termotools.com sayti