GLOBAL AXBOROT MAKONIDA KIBERTERROR TAHDIDLARI

Muxammatqulov Shohruhbek Erkin o‘g‘li

Annotasiya. *Bugungi global axborot makonida kiberterror tahdidlari kun sayin ortib bormoqda. Makur tahdidlar nafaqat inson hayotiga balki davlat manfaatlariga ham jiddiy zarar yetkazishi yoki uni parchalanishiga sabab bo‘lishi mumkin. Ushbu maqolada global axborot makonida kiberterror tahdidlari va unga qarshi kurashishning zamonaviy mafkuraviy va texnologik mexanizmlari xususida so‘z boradi. Shuningdek, ushbu maqola mavzusiga doir rasmiy va ilmiy adabiyotlardagi nazariy qarashlar umumlashtirilib mavjud muammo yuzasidan taklif va tavsiyalar keltiriladi.*

Kalit so‘zlar: *Axborot xavfsizligi, kiberterror tahdidlari, zamonaviy tendensiyalar, mafkuraviy polegon, texnologik omillar.*

CYBERTERROR THREATS IN THE GLOBAL INFORMATION SPACE

Abstract. *In today's global information space, cyber-terrorist threats are increasing day by day. Insidious threats can cause serious damage not only to human life, but also to the interests of the state or cause its disintegration. This article talks about the threats of cyber-terror in the global information space and the modern ideological and technological mechanisms of combating it. Also, the theoretical views of the official and scientific literature on the topic of this article are summarized and suggestions and recommendations are given regarding the existing problem.*

Key words: *Information security, cyberterrorist threats, modern trends, ideological battlefield, technological factors.*

КИБЕРТЕРРОРИЧЕСКИЕ УГРОЗЫ В МИРОВОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Аннотация. *В современном глобальном информационном пространстве с каждым днем возрастают кибертеррористические угрозы. Коварные угрозы могут нанести серьезный ущерб не только жизни человека, но и интересам*

государства или вызвать его распад. В данной статье говорится об угрозах кибертерроризма в глобальном информационном пространстве и современных идеологических и технологических механизмах борьбы с ним. Также обобщаются теоретические взгляды официальной и научной литературы по данной теме, даются предложения и рекомендации относительно существующей проблемы.

Ключевые слова: *информационная безопасность, кибертеррористические угрозы, современные тенденции, идеологическое поле боя, технологические факторы.*

KIRISH

Hozirgi axborotlashgan davrda globallashuv jarayoni tobora kengayib, dunyo mafkuraviy manzarasining yangicha ko‘rinishi va rivojlanishiga o‘z ta’sirini o‘tkazib kelmoqda. Bugungi tahlikali va murakkab zamonda esa turli-tuman g‘oyalar kurashi axborot xurujlari orqali taqdim etilishi natijasida barcha jamiyat va davlatlarning fuqarolari, ayniqsa yoshlar xushyor va sergak bo‘lishlari o‘ta muhim ahamiyat kasb etadi[1]. Axborot xaffsizligidan farqli o‘laroq dunyoga tahdid solayotgan yana bir katta muammo bu kiberhujumlarning tahdidlaridir.

ADABIYOTLAR TAHLILI VA METODLAR

Kiberterrorchilik - maxsus xakkerlik dasturlari orqali kompyuter tarmoqlari boshqaruv tizmini egallab olish, viruslar yordamida kompyuter tizimlarini ishdan chiqarish kabi xunrezliklarni amalga oshiradi. Bugungi kunda aynan ushbu tushuncha axborot tehnologiyalari sohalaridagi ko‘p turdagi jinoyatlarni o‘zida birlashtiradi[2]. Virus va boshqa zararli dasturlar orqali axborot tizimlarini ishdan chiqaradi hamda katta daromadga ega bo‘ladi. Statistik ma’lumotlar tahliliga ko‘ra virtual jinoyatchilar o‘zlarining bunday xatti-harakati bilan 110 milliard dollardan ziyod moliyaviy zarar keltirar ekan. Bunday huquqbuzarliklarni oldini olish uchun yiliga 270 milliard dollardan ortiq mablag‘ sarflanmoqda. Tadqiqotchilarning fikriga ko‘ra: dunyodagi eng ko‘p qirg‘in daromad keltiradigan biznes– narkotik moddalar savdosining yillik hajmi 288 milliard dollarni tashkil qiladi va bu kiberjinoyatchilikdan kelayotgan daromaddan ancha kamdir. Dastlab, kiberterror atamasi 1980-yilda AQSHning xavfsizlik va qidiruv institutining katta ilmiy xodimi Barri Kollin tomonidan qo‘llanilgan. Ma’lumotlarga qaraganda Internetda sodir etilgan ilk jinoyat 1983-yil “Arpanet” internetga aylanmasidan oldin sodir etilgan. Bizning jamiyatimiz, iqtisodiyotimiz va muhim infratuzilmalarimiz asosan kompyuter tarmoqlari va axborot

texnologiyalari faoliyatiga bog‘liq bo‘lib qoldi. Axborot texnologiyalariga ehtiyojimiz oshgani sayin kiberhujumlar yanada jozibador va potentsial halokatni yuzaga keltiradi. Xalqaro statistik ma’lumotlarga qaraganda, kiber hujumlar tufayli keladigan zarar har yili 114 milliard dollarga tushadi. Agar kiberhujumlardan uni oldini olish uchun kompaniyalarning ajratgan vaqtlari hisoblansa, kiber hujumlarning umumiy qiymati 385 milliard AQSh dollarini tashkil etadi[3]. Shu jumladan, kiber hujumlar qurbonlari ham sezilarli darajada o‘smoqda. Nima uchun kiber hujumlar gullab-yashnamoqda? Buning sababi shundaki, kiberhujumlar jismoniy hujumlarga qaraganda arzon, qulay va kamroq xavfga egadir[4]. Kiber jinoyatchilar faqat kompyuter va Internet aloqasidan tashqari bir necha xarajatlarni talab qiladilar. Ular geografiya va masofa bilan chegaralanmagan. Internetning noma’lum xususiyati tufayli ularni aniqlash va javobgarlikka tortish qiyin. Axborot tehnologiyalari tizimlariga qarshi hujumlar juda jozibadorligini hisobga olib, kiberhujumlarning soni o‘sib borishi kutilmoqda.

NATIJALAR

Kiberxavfsizlik turli xil kiberhujumlar atrofidagi muammolarni tushunishga va har qanday raqamli va axborot texnologiyalarining maxfiyligini, yaxlitligini va mavjudligini saqlaydigan himoya strategiyasini ishlab chiqishga (ya’ni qarshi choralar) tegishli[5].

• **Maxfiylik** - bu ruxsatsiz shaxslar yoki tizimlarga ma’lumot oshkor qilinishining oldini olish uchun ishlatiladigan atama;

•**Butunlik** - bu ruxsatsiz tarzda har qanday o‘zgartirish yoki o‘chirishning oldini olish uchun ishlatiladigan atama;

•**Mavjudlik** - bu ma’lumotni yetkazib berish, saqlash va qayta ishlash uchun javobgar bo‘lgan tizimlar kerak bo‘lganda va ularga muhtoj bo‘lganlar foydalana olishlarini ta’minlash uchun ishlatiladigan atama.

Kiberxavfsizlik bo‘yicha ekspertlar zararli dastur kiberhujumda kiberxavfsizlikni buzish niyatida bo‘lgan zararli qurolni tanlashda asosiy vosita deb hisoblaydilar[6]. **Zararli dastur** - bu tizimga dushmanning foydasiga halaqit beradigan, odatda qonuniy egasining xabari bo‘lmagan holda, tizimga yuklangan hujumlarning keng sinfini anglatadi. Zararli dasturlarning ba’zi namunaviy sinflari orasida **viruslar, qurtlar**, **troyan otlari, shpion dasturlari** va **bot dasturlari** mavjud[7]. Zararli dastur zararli dasturlarni tarqatishda, foydalanuvchini sohta kerakli fayllarni ochish uchun undash yoki foydalanuvchilarni zararli dasturlarni tarqatuvchi veb-saytlarga kirishga majbur qilish uchun tizimlarni turli usullar bilan tarqatadi. Aniq dasturiy ta’minot

infektsiyasining aniq misollarida, zararli dastur o‘zini yuqtirgan qurilmaga o‘rnatilgan USB drayverga yuklashi va keyinchalik ushbu qurilma joylashtirilgan har qanday boshqa tizimiga joylashishi mumkin. Zararli dastur o‘rnatilgan tizim va hisoblash qobilyatini o‘z ichiga olgan qurilmalar va uskunalardan tarqalishi mumkin. Muxtasar qilib aytganda, zararli dasturni tizimning istalgan nuqtasiga kiritish mumkin. Zararli dasturlarning qurbonlari oxirgi foydalanuvchilar tizimlari, serverlar, tarmoq qurilmalari (ya'ni, marshrutizatorlar, kalitlar va boshqalar) va nazorat nazorati va ma’lumotlarni yig‘ish (SCADA) kabi jarayonlarni boshqarish tizimlaridan har qanday narsani qamrab olishi mumkin. Tez o‘sib borayotgan zararli dasturlarning tarqalishi va murakkabligi bugungi kunda Internetda katta qiziqish uyg‘otmoqda.

MUHOKAMALAR

An’anaga ko‘ra, zararli dasturlarga qarshi hujumlar har bir jabhada mavjud dizayn va amalga oshirishning zaif tomonlaridan foydalangan holda, apparat uskunalari, dasturiy ta’minot qismlari yoki tarmoq darajasida bitta joyida amalga oshiriladi. Kiber hujumlarni aniqlashda bir qancha hayotiy misollarga to‘xtalish mumkin. Bularga **ijtimoiy media**, **yashirin hisoblash, smartfonlar tehnologiyasi va muhim infratuzilma kiradi**. Masalan, ijtimoiy tarmoqlar va bloglar kabi axborot tarmoqlari bugungi kunda bizning turmush tarzimizning ajralmas qismidir, chunki ijtimoiy tarmoqlarda ko‘p odamlar o‘zlarining hayotiy voqealari haqida yozmoqdalar, yangiliklar almashmoqdalar, shuningdek do‘stlar orttirmoqdalar. Bir vaqtning o‘zida millionlab odamlarni bog‘lash imkoniyatini anglagan holda, dushmanlar ijtimoiy tarmoqdagi akkauntlardan foydalanib, jabrlanuvchining do‘stlariga **spam** yuborish uchun transport vositasi sifatida foydalanishadi. Yashirin hisoblash paradigmasi foydalanuvchiga faqat oldindan xarajatlarni to‘lamasdan yoki murakkab hisoblash infratuzilmasini boshqarish ko‘nikmalarini talab qilmasdan foydalanish uchun to‘laydigan kommunal dasturlar kabi kompyuter resurslaridan foydalanishga imkon beradi. Yashirin saqlash xizmatlarida to‘plangan ma’lumotlar soni bugungi kunda tajovuzkorlarni o‘ziga jalb qilmoqda. 2012-yil iyun oyida tajovuzkorlar uyali aloqa foydalanuvchilari uchun AT & T ning ovozli pochta xizmatidagi kamchiliklardan foydalangan holda CloudFlare-da Distribution Denial of Service (DDoS) yumshatish xizmatini buzishdi; shunga o‘xshash Google-ning Gmail foydalanuvchilari uchun hisobni tiklash xizmati[8]. 2015-yilga kelib smartfonlarning foydalanuvchisining 2 milliardga o‘sishi bilan, so‘ngi paytlarda mobil zararli dasturlarning sezilarli darajada ko‘payishi kuzatilmoqda. Masalan, 2012-yil davomida Android uchun zararli dasturlarning noyob aniqlanishi dunyo miqyosida o‘tgan yilga nisbatan 17 marta oshdi. Terrorizm, axborot urushida foydalanishi mumkin bo‘lgan elektr tarmoqlari va

sog‘liqni saqlash tizimlari kabi muhim infratuzilmaning kiber-tahdidlari haqida ham havotirlar kuchaymoqda.

Kiber hujumlarning deyarli barchasi moddiy manfaatga asoslanadi. Axborot tehnologiyalaridan foydalanib siyosiy, diniy va idealogik maqsadni amalga oshirish uchun ma’lumot uzatiladigan ob’yektlarni yo‘q qilish bilan ham insonlarni havotirga solmoqda. Bular orasida xakkerlar asosiy o‘rinni egallaydi. Xakkerlar korxona yoki tashkilotlarning mablag‘larini o‘zlashtirish orqali katta zarar yetkazadi. Tashkilotlarga xavfli hisoblangan asosiy tizim bu ma’lumotlar ombori hisoblanadi. Viruslarga qarshi dasturlar ishlab chiqaradigan McAfee kompaniyasi ma’lumotlariga qaraganda dunyo bo‘ylab kompyuter tizimlarini ishdan chiqaradigan kunig 60 ming virus ishlab chiqarilgan. Bu tahdidlar dunyoni tashvishga solib qo‘ymoqda.

XULOSA

Kiberhujumlarni bartaraf etish texnologik jihatdan olib qaraydigan bo‘lsak katta mablag‘ talab etadigan jarayondir. Buning uchun O‘zbekiston o‘zining Internet tarmog‘ini yaratishi zarur. Bu juda katta mablag‘ talab etsada nafaqat axborot hujumlarini bartaraf etishda balki kiber tahdidlarga qarshi kurashishning eng samarali yechimidir. Shuningdek, ta’lim tizmida axborot texnologiyalariga oid kurslar tashkil etish, turli xil targ‘ibot tashviqot ishlarini olib borish lozim. Chora-tadbirlarni amalga oshirish mexanizimiga ko‘ra bosqichma-bosqich tizimlashtirish lozim.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Aminova D. O'zbekiston milliy jurnalistikasining mafkuraviy asoslari. O'quv qo'llanma.

Toshkent:; “Turon-Iqbol”, 2013.B.44.

2. Muhammad Amin Yahyo. Internetdagi tahdidlardan himoya. Yordamchi o‘quv qo‘llanma. –Toshkent: Movorounahr nashryoti, 2016, B.158.
3. Internet Security Threats Report. Symantec http://www.symantec.com/threatreport/last accessed: June 2013
4.]http://www.maawg.org/, last accessed: June 2013.
5. Goodman S.E., Lin H.S. (Eds.), Toward a Safer and More Secure Cyberspace, The Nat'l Academics Press (2007)
6. Australian Parliament the report of the inquiry into Cyber Crime http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf

7. DHS S&TRoadmap for cybersecurity researchJan. 2009 http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf
8. R.C. NewmanComputer Security: Protecting Digital Resources (first edition), Jones & Bartlett Publishers (February 20, 2009)