ISSN 3060-4567

KIBER MAKON, KIBER TERRORIZM, KIBER ZO'RAVONLIK (CYBERBULLYENG)TUSHUNCHALARINING MOHIYATI

Azamova Sitora Ayonovna
SHDPI Ijtimoiy fanlar kafedrasi o'qituvchisi
Narzullayeva Durdona
Shahrisabz davlat pedagogika instituti
maktagacha ta'lim yo'nalishi 2-kurs talabasi

***Annotatsiya**: Ushbu maqolada Kiber makon,kiber terrorizm tushunchalarining mohiyati va hozirgi kunda yurtimizda bo'layotgan kiber zo'ravonlikning oldini olish unga qarshi kurashish haqida so'z boradi. Hukumat va ommaviy axborot vositalarida kiber terrorizmning yetkazilishi mumkin bo'lagan havotirlar haqida so'z boradi.*

***Kalit so'zlar**: Kiber makon ,kiber terrorizm, kiber zo'ravonlik, tahdid, qo'rqitish, kompyuter qurtlari, feshing, zararli dasturlar, kiber jinoyat, buzg'unchilik.*

Kibermakon kompyuter tarmoqlari orqali amalga oshiriladigan muloqot maydonini ifodalovchi voqelik sifatida 1990 yildan boshlab keng miqyosida rivojlanib, takomillashib kelmoqda. Kibermakon tushunchasini dastlab kanadalik yozuvchi Uilyam Gibson 1982 yil «Sojjenie Xrom» («Burning Chrome») nomli hikoyasida yozadi. Keyinchalik, Gibsonning 1990 yilda yozib tugatgan "Neuromancer" (o'zbek tilida tarjimasi "Asabli manzaralar tasvirlovchisi", rus tilida «Nervo-sochinitel») nomli texno-utopik fantastik trilogiyasida qo'llagan. Bu asardagi kibermakon tushunchasi millionlab odamlarning jamoaviy sarob, xayolparastlikning o'ziga xos ko'rinishi sifatida tasvirlangan. Bu erda jamoaviy sarob yoki xayolparastlik inson ongida sub'ektiv psixologik holat sifatida namoyon bo'ladi. Ijtimoiy nuqtai-nazardan kibermakon deganda kompyuter tarmog'i orqali bir-biri bilan bog'langan va bir vaqtning o'zida turli geografik

nuqtada kesishuvchi har qanday mavjud kompyuterning grafik sifatidagi ma’lumotlariga o‘ralashib qolgan kishilar jamoasi tushuniladi. **Kiberterrorchilik** – bu tahdid yoki qo‘rqitish orqali, internetdan foydalangan holda, siyosiy yoki mafkuraviy muvaffaqiyatga erishish maqsadida uyushtiriluvchi kiber hujumlardir. Kompyuter viruslari, kompyuter qurtlari, fishing, zararli dasturlar, apparat usullari, dasturlash skriptlari kabi vositalar yordamida kompyuter tarmoqlarini, xususan, Internetga ulangan shaxsiy kompyuterlarni qasddan, keng miqyosda buzish harakatlari internet terrorizmining ko‘rinishi bo‘lishi mumkin. Kiberterrorizm munozarali atamadir. Ba’zi mualliflar ma’lum terroristik tashkilotlar tomonidan signalizatsiya, vahima yoki jismoniy buzilishlarni yaratish maqsadida axborot tizimlariga qarshi hujumlarni buzish bilan bog‘liq juda tor ta’rifni tanlaydilar. Boshqa mualliflar esa kiberjinoyatni o‘z ichiga olgan kengroq ta’rifni afzal ko‘rishadi. Kiberhujumda ishtirok etish, hatto zo‘ravonlik bilan amalga oshirilmagan bo‘lsa ham, terror tahdidi idrokiga ta’sir qiladi. Ba’zi ta’riflarga ko‘ra, onlayn faoliyatning qaysi holatlari kiberterrorizm yoki kiberjinoyat ekanligini farqlash qiyin bo‘lishi mumkin. Kiberterrorizmni shaxsiy maqsadlar yo‘lida vayron qilish va zarar yetkazish uchun kompyuterlar, tarmoqlar va ommaviy internetdan qasddan foydalanish sifatida ham e’tirof etish mumkin. Tajribali kiberterrorchilar, buzg‘unchilik bo‘yicha juda malakali bo‘lganlar hukumat tizimlariga katta zarar yetkazishi va keyingi hujumlardan qo‘rqib, mamlakatni tark etishi mumkin. Bunday terrorchilarning maqsadlari siyosiy yoki mafkuraviy bo‘lishi, bu esa terrorning bir ko‘rinishi deb hisoblanishi mumkin. Hukumat va ommaviy axborot vositalarida kiberterrorizm yetkazilishi mumkin bo‘lgan ziyon haqida xavotirlar talaygina. Bu esa Federal Qidiruv Byurosi (FQB) va Markaziy Razvedka Boshqarmasi (CIA) kabi davlat idoralarini kiberhujumlar va kiberterrorizmga chek qo‘yishga unday boshladi.Kiberterrorizmning bir necha asosiy va kichik holatlari bo‘lgan. Al-Qoida internetdan tarafdorlari bilan muloqot qilish va hatto yangi a’zolarni yollash uchun foydalangan. Estoniya, Boltiqbo‘yi mamlakati, texnologiya jihatidan rivojlanib borishmoqda, 2007-yil aprel oyida Estoniya poytaxti Tallinda joylashgan Ikkinchi Jahon urushi davridagi sovet

haykali ko‘chirilishi bilan bog‘liq tortishuvlardan so‘ng kiberterror uchun kurash maydoniga aylanib qoladi. ***Umumiy ko’rinishi:*** Kiberterrorizm ko‘lamining asosiy ta’rifi bo‘yicha munozaralar mavjud. Ushbu ta’riflar tor bo‘lishi mumkin, masalan, Internetdagi boshqa tizimlarga hujum qilish uchun Internetdan foydalanish, bu odamlar yoki mulkka nisbatan zo‘ravonlikka olib keladi. Ular, shuningdek, axborotni texnologiyalari infratuzilmalariga odatiy hujumlar uchun terrorchilar tomonidan Internetdan foydalanishning har qanday shaklini o‘z ichiga olgan keng bo‘lishi mumkin. Ishda motivatsiya, maqsadlar, usullar va kompyuterdan foydalanishning markaziyligi bo‘yicha malakaning o‘zgarishi mavjud. AQSh davlat idoralari ham turli xil ta’riflardan foydalanadilar va ularning hech biri hozirgacha o‘z ta’sir doirasidan tashqarida majburiy bo‘lgan standartni joriy etishga urinmagan. Kontekstga qarab, kiberterrorizm kiberjinoyat, kiberurush yoki oddiy terrorizm bilan sezilarli darajada mos kelishi mumkin. Kasperskiy laboratoriyasi asoschisi Yevgeniy Kasperskiy hozirda“kiberterrorizm”,“ kiberurush” dan ko‘ra aniqroq atama ekanligini his qilmoqda. Uning ta’kidlashicha, bugungi hujumlar bilan siz buni kim qilgani yoki ular yana qachon zarba berishini bilmaysiz. Bu kiber-urush emas, balki kiberterrorizmdir”. U, shuningdek, o‘z kompaniyasi kashf etgan Flame Virus va NetTraveler Virus kabi keng ko‘lamli kiber qurollarni biologik qurollarga tenglashtirib, bir-biriga bog‘langan dunyoda ular bir xil darajada halokatli bo‘lish potentsialiga ega ekanligini ta’kidlaydi. Agar kiberterrorizmga an’anaviy terrorizmga o‘xshash munosabatda bo‘lsa, u faqat mulk yoki hayotga tahdid soladigan hujumlarni o‘z ichiga oladi va jismoniy, haqiqiy zarar yoki jiddiy buzilishlarni keltirib chiqarish uchun maqsadli kompyuterlar va ma’lumotlardan, xususan, Internet orqali foydalanish infratuzilmasi sifatida ta’riflanishi mumkin. Terrorizmni o‘rganish bo‘yicha ixtisoslashgan ko‘plab akademiklar va tadqiqotchilar kiberterrorizm mavjud emasligini va haqiqatan ham xakerlik yoki axborotni urushi masalasi ekanligini ta’kidlamoqda. Hozirgi hujum va himoya texnologiyalarini hisobga olgan holda, elektron vositalardan foydalangan holda aholida qo‘rquv, jiddiy jismoniy zarar yoki o‘lim paydo bo‘lishi ehtimoli yo‘qligi

sababli uni terrorizm deb belgilashga rozi emaslar. Umuman kiberjinoyatda bo‘lgani kabi, kiberterrorizm aktlarini amalga oshirish uchun talab qilinadigan bilim va ko‘nikmalar chegarasi erkin foydalanish mumkin bo‘lgan xakerlik to‘plamlari va onlayn kurslar tufayli doimiy ravishda pasayib bormoqda. Bundan tashqari, jismoniy va virtual olamlar jadal sur’atlar bilan birlashib, yana ko‘plab imkoniyatlar maqsadlariga erishmoqda, buni Stuxnet, 2018-yildagi Saudiya neft-kimyosi sabotaj urinishi va boshqalar kabi e’tiborga molik kiberhujumlar tasdiqlaydi. Hozirgi davrda fan, texnika va asosan kompyuter taraqqiyoti mahsuli bo‘lgan kibermakon va uning boshqaruvchi qiyofasi “superkorporatsiya” texnologiyalarning insoniylikdan begonalashuvi natijasida din niqobidagi ijtimoiy va madaniy buzg‘unchilikni sodir etishga bo‘lgan urinishlar tobora kuchayib bormoqda. Jumladan, bugungi kunda kiberterrorchilik tuzilmalari o‘z g‘arazli maqsadlari yo‘lida axborot-kommunikatsiya texnologiyalaridan keng foydalanishga urinmoqda. Bu borada O‘zbekiston Respublikasi Birinchi Prezidenti I.A.Karimovning “Yuksak ma’naviyat-engilmas kuch” asarida quyidagicha ta’kidlaangan: “Taassufki, ba’zan islom dini va diniy aqidaparastlik tushunchalarini bir-biridan farqlay olmaslik yoki g‘arazli maqsadda ularni teng qo‘yish kabi holatlar ham ko‘zgatashlanmoqda. Shu bilan birga, islom dinini niqob qilib, manfur ishlarni amalga oshirayotgan mutaassib kuchlar hali ongi shakllanib ulgurmagan, tajribasiz, g‘o‘r yoshlarni o‘z tuzog‘iga ilintirib, bosh-ko‘zini aylantirib, ulardan o‘zining nopok maqsadlari yo‘lida foydalanmoqda. Bunday nojo‘ya harakatlar avvalo muqaddas dinimizning sha’niga dog‘ bo‘lishini, oxir-oqibatda esa ma’naviy hayotimizga salbiy ta’sir ko‘rsatishini barchamiz chuqur anglab olishimiz va shundan xulosa chiqarishimiz zarur”. Bu xususida Xalqaro press-klubda Mintaqaviy aksilterror tuzilma (MAAT) Ijroiya qo‘mitasi direktori Evgeniy Sisoevning so‘zlariga ko‘ra, MAAT O‘zbekiston bilan o‘zaro ishonch va yordamga asoslangan aloqalarni o‘rnatgan. Xalqaro Press-klubda bo‘lib o‘tgan ko‘p tomonlama hamkorlik masalalariga bag‘ishlangan navbatdagi yig‘ilish zamonaviy tahdidlar sharoitida asosiy masalalardan biri axborot xavfsizligi, kiberxavfsizlik masalasi ekanini ta’kidladi.

«Kibermaydonlar xalqaro terrorchi tashkilotlar a’zolarining o‘z maqsadlariga erishish uchun qulay imkoniyatlar yaratmoqda. Bu yo‘nalishda ko‘p ishlarni amalga oshiryapmiz, bu borada hamkorlik chora-tadbirlari ishlab chiqilgan. Biz terrorchilikka qarshilik qilish maqsadida aksilterror o‘quv mashqlarini o‘tkazyapmiz. Xitoy tomon bu masalalarga katta e’tibor qaratmoqda va ko‘plab qiziq takliflar kiritmoqda. Aprel oyida Shanxayda ajoyib seminar bo‘lib o‘tdi. Undakiberterrorizm masalasiga bag‘ishlangan uchrashuvlar o‘tkazildi. Bu mazmunda janob Mirziyoevning takliflari juda o‘rinli», — qo‘shimcha qiladi E.Sisoev. “Kibermakon”da din niqobidagi “kiberhujum”lar tahdidi: din niqobi ostidagi ekstremistik saytlarda asosan davlat to‘ntarilishi va xunrezlik urushlari haqida gap boradi. Bugungi kunda dunyoda eng katta xavf solib turgan ISHID guruhining internet kibermakonidagi axborot hujumi va tahdidi to‘g‘risida Aydarbek Tulepov o‘zining “ISHID fitnasi” kitobida quyidagi ma’lumotlarni beradi. ISHID o‘zining internet orqali go‘yo Islom yo‘lida “qurbon” bo‘layotgani aks etgan videolavhalari va fotosuratlari “al-Hayot” media studiyasida tayyorlanadi va internetga joylashtiriladi

Kiber makon va kiber terrorizm tushunchalari hozirgi kunda texnologik inqilobning ajralmas qismi hisoblanadi. Kiber makon axborot almashinuvi, biznes va ta'lim kabi sohalarda ijobiy rol o'ynashiga qaramasdan, u noxush oqibatlarga olib kelishi mumkin. Kiber terrorizm esa uning xavfli tomonini tashkil qiladi. Shunday qilib, kiber xavfsizlikni ta'minlash va kiber terrorizmga qarshi kurashish uchun davlatlar va tashkilotlar o'rtasida hamkorlik zarur. Bu esa global xavfsizlikni ta'minlashga yordam beradi.

FOYDALANILGAN ADABIYOTLAR

1. Abduqayumov, T. (2021). Kiber xavfsizlik va uning zamonaviy tahdidlari. Toshkent: Akademiya nashriyoti.

2. Khalilov, A. (2020). Kiber makon: Xavf va imkoniyatlar. Tashkent: O'zbekiston xalqaro munosabatlar akademiyasi.

3. O'zbekiston Respublikasi Kiber Xavfsizlikni Ta'minlashning Milliy Strategiyasi. (2018). O'zbekiston Respublikasi Hukumatining qarori.

4. Suleymanov, M. (2022). Kiber terrorizm va uning global xavfsizlikka ta'siri. Journal of Cybersecurity Studies, 5(3), 45-57.

5. Global Forum on Cybersecurity (2019). Kiber terrorizmga qarshi kurashish: Xalqaro tajribalar va istiqbollar.

6. Berge, M. (2017). Cybersecurity in the modern world: Challenges and Strategies. New York: TechBooks.

7. Shulgin, V. (2020). Kiber makon va davlatlar xavfsizligi. Moskva: Akademiya nashriyoti.

8. International Telecommunication Union (ITU). (2021). Cybersecurity and the challenges of the digital age. Geneva: ITU Report.