KIBERJINOYAT VA KIBERTERRORIZM TUSHUNCHASI VA XUSUSIYATLARI

Egamov Orifjon Adilbekovich

“Yangi asr” unversiteti, Mumtoz sharq filologiyasi kafedrasi o‘qituvchisi

Annotatsiya: Bugungi rivojlanib borayotgan jamiyatimizda, turli xil tahdidlar va inson hayotiga tahdid soluvchi, tinchlik kabi ne’matlarning zavoli hisoblangan turli tuman tahdidlar yuzaga kelmoqda. Bu maqola shunday tahdidlardan biri kiberjinoyat va kiberterorizm tushunchalari va ularning xususiyatlarini yoritib beradi.

Kalit so‘zlari: Kiberjinoyat, jinoyat quroli, buzg’unchi-xakerlar, kiberterrorchi, Vinn shvartu, Jon Arquilla..

Kiberjinoyat — kompyuter va tarmoqning birgalikdagi aloqasi ostida sodir etiluvchi jinoyat turi[1]. Kompyuter jinoyat paytida maqsadli yo‘naltirilgan qurol vazifasini bajarib beradi. Kiberjinoyat kimningdir xavfsizligi va moliyaviy saviyasiga zarar yetkazish maqsadida sodir etiladi.[2]

Maxfiy ma’lumotlar qonuniy tarzda himoyalangan holatda yuz beruvchi kiberjinoyatlar bilan bog‘liq ko‘pgina jinoyatlar mavjud. Xalqaro miqyosda hukumat ham, nodavlat ham subyektlar kiberjinoyatlar, jumladan, josuslik, moliyaviy o‘g‘irlik va boshqa transchegaraviy jinoyatlar bilan shug‘ullanadi. Xalqaro chegaralarni kesib o‘tuvchi va kamida bitta milliy davlatning xatti-harakatlarini o‘z ichiga olgan kiberjinoyatlar ba’zan kiberurush deb ataladi. Uorren Baffet kiberjinoyatni „insoniyatning birinchi raqamli muammosi“[3] deb ta’riflaydi va „insoniyat uchun real xavf tug‘diradi“, deya qo‘shimcha qilib o‘tadi.[4]

2014-yilda chop etilgan hisobotda (McAfee homiyligida) jahon iqtisodiyotiga yetkazilgan yillik zarar 445 milliard dollarni tashkil qilgan.[5] Cybersecurity Ventures tomonidan 2016-yilgi hisobotda kiberjinoyatlar natijasida yetkazilgan global zararlar 2021-yilga kelib yiliga 6 trillion dollargacha, 2025-yilga kelib esa 10,5 trillion dollargacha ko‘tarilishi bashorat qilingan edi.[6]

2012-yilda AQShda onlayn kredit va debet kartalaridagi firibgarlik oqibatida taxminan 1,5 milliard dollar yo‘qotilgan[7] 2018-yilda Strategik va xalqaro tadqiqotlar markazi (CSIS) tomonidan McAfee bilan hamkorlikda o‘tkazilgan tadqiqot shuni ko‘rsatadiki, har yili global YaIMning qariyb bir foizi, ya’ni 600 milliard dollarga yaqini kiberjinoyatlar tufayli yo‘qoladi.[8] Jahon Iqtisodiy Forumi 2020 Global Risk hisobotida uyushgan kiberjinoyatlar idoralari jinoiy faoliyatni onlayn qilish uchun kuchlarni birlashtirayotganini tasdiqladi, shu bilan birga ularning aniqlash va jinoiy javobgarlikka tortilish ehtimoli AQShda 1 foizdan kamroqni tashkil qiladi.

[1] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime, " Cleveland, Mississippi: Anderson Publishing.

[2] *Bossler, Adam M.; Berenblum, Tamar (2019-10-20). „Introduction: new directions in cybercrime research“. Journal of Crime and Justice. 42-jild, № 5. 495–499-bet.*

[3] „BUFFETT: This is 'the number one problem with mankind'“. *Business Insider*.

[4] „Warren Buffett: 'Cyber poses real risks to humanity'“ (en-US). *finance.yahoo.com*.

[5] „Cyber crime costs global economy $445 billion a year: report“. *Reuters* (9-iyun 2014-yil).

[6] „Cybercrime To Cost The World 80.5 Trillion Annually By 2025“ (en-US). *Cybercrime Magazine* (4-mart 2018-yil).

[7] #Cybercrime— what are the costs to victims - North Denver News“. *North Denver News* (17-yanvar 2015-yil).

[8] Lewis, James (February 2018). „Economic Impact of Cybercrime - No Slowing Down“ (PDF).

Kiber-jinoyatchilik nisbatan yangi tushuncha bo'lsada, ko'plab davlatlar iqtisodiyotiga qimmatga tushayotgan muammo.

Jinoyat quroli – internet va eng so’nggi raqamli texnologiyalar. Mamlakatning harbiy, strategik tarmoqlarini ishdan chiqarish salohiyatiga ega.

Buzg’unchi-xakerlarni topib jazolash esa oson ish emas, chunki ular davlatdan doimo bir qadam oldinda.

Bugungi hayotni zamonaviy texnologiyasiz tasavvur qilish qiyin. Uyali aloqa va internet dunyosidagi so’nggi kashfiyotlar uzoqni yaqin, og’irni yengil, biznes imkoniyatlarni esa kengaytirgan.

Biroq bu qulayliklar boshqa bir sohaga e’tibor qaratmoqda. Kiber-xavfsizlik har bir davlat uchun strategik masala. Avval asosan davlat sirlari va yuqori texnologiyalar nishonga olingan bo’lsa, hozir jinoyatchilar mo’ljalni kengroq olmoqda, deydi AQSh Federal Qidiruv Byurosi (FBR) rahbari Robert Myuller.
“*Google* qidiruv tizimiga bo’lgan hujumlardan bilamizki, nafaqat hukumatlar, balki xususiy kompaniyalar ham bu tahdid oldida ojiz. Global iqtisodiy integratsiya bizga ko’p eshiklarni ochib berdi, jinoyatchilarga esa yangi imkoniyatlarni”, - deydi Myuller.

Kiberjinoyat hodisa sifatida bir necha o‘n yillar oldin paydo bo‘lgan, biroq qisqa vaqt ichida axborot texnologiyalarining rivojlanishi bilan kibermakondagi noqonuniy xatti-harakatlar hodisasi global muammoga aylanib, nafaqat alohida foydalanuvchilarga, balki axborot xavfsizligiga ham xavf tug‘dirdi. Davlat internet orqali axborot almashinuviga kiritilgan paytdan boshlab, davlat va uning fuqarolari dunyoning istalgan nuqtasidan tajovuzlarga moyil bo'lib qoladi.

“Kiberjinoyat” atamasining ma’nosini kibermakonda sodir etilgan jinoyat deb ta’riflash mumkin. Kibermakon kompyuter tarmoqlari ishtirokida modellashtirilgan, internet orqali kengayib borayotgan ba'zi ma'lumotlarni saqlaydigan virtual axborot maydoni sifatida qaraladi. Ushbu ta'rifning ma'nosini tushunmasdan turib, kiberjinoyatga qarshi himoya choralarini qo'llash mumkin emasligi sababli, tadqiqotchilar ushbu hodisani batafsil o'rganib chiqib, unga qiziqarli ta'rif berdilar. Kiberjinoyat – kompyuter tizimlari yoki tarmoqlaridan foydalangan holda kibermakonda sodir etiladigan jinoyatlar majmuidir.[9]

Kiberterrorizm - bu kompyuter va kompyuter tizimlari tomonidan qayta ishlanadigan, inson hayoti yoki sog'lig'iga xavf tug'diradigan yoki boshqa og'ir oqibatlarga olib keladigan, agar bunday harakatlar jamoat xavfsizligini buzish maqsadida qilingan bo'lsa, qasddan, siyosiy sabablarga ko'ra hujum qilishda ifodalangan murakkab harakatdir.[10]

Hukumat amaldorlari va axborot texnologiyalari xavfsizligi bo‘yicha mutaxassislar 2001-yil boshidan buyon Internet muammolari va server firibgarliklarining sezilarli darajada oshganini hujjatlashtirdi. Federal Qidiruv Byurosi (FQB) va Markaziy razvedka boshqarmasi (CIA) kabi hukumat idoralari orasida bunday bosqinlar kiberterroristik tashqi razvedka xizmatlari yoki boshqa guruhlar tomonidan potentsial xavfsizlik teshiklarini xaritalash uchun uyushtirilgan sa’y-harakatlarning bir qismi ekanligidan xavotir ortib bormoqda. muhim tizimlar.[11]

Kiberterrorchi — bu hukumat yoki tashkilotni kompyuterlar, tarmoqlar yoki ularda saqlangan ma’lumotlarga qarshi kompyuter hujumi uyushtirish orqali o‘zining siyosiy yoki ijtimoiy maqsadlariga erishish uchun qo‘rqitadigan yoki majburlaydigan shaxs.

Kiberterrorizm, umuman olganda, kibermakon yoki kompyuter resurslaridan foydalanish orqali sodir etilgan terrorchilik harakati sifatida ta’riflanishi mumkin (Parker 1983). Shunday qilib, bayram kunlarida bombali hujumlar sodir bo‘lishi haqida Internetda oddiy targ‘ibot materiali kiberterrorizm

[9] A.V. Sokolov, O.M. Stepanyuk Kompyuter terrorizmidan himoya. Yordam yo‘riqnomasi
[10] E.V. Starostina, D.B. Frolov Kompyuter jinoyatlari va kiberterrorizmdan himoya qilish. Savol va Javob
[11] Laqueur, Walter. Cyberterrorism. Facts on File, 2002 — 52–53 bet.

deb hisoblanishi mumkin. Shuningdek, ayrim shaxslarga, oilalarga qaratilgan, tarmoqlar ichida guruhlar tomonidan tashkil etilgan, odamlar o‘rtasida qo‘rquv uyg‘otish, hokimiyatni namoyish etish, odamlar hayotini barbod qilish uchun zarur bo‘lgan ma’lumotlarni to‘plash, talonchilik, shantaj va hokazolarga qaratilgan xakerlik faoliyati ham mavjud.[12]

Shunday qilib, hozirda kiberterrorizm tahdidi juda jiddiy muammo hisoblanadi. Uning dolzarbligi axborot va telekommunikatsiya texnologiyalarining rivojlanishi va tarqalishi bilan ortadi.

Birinchi uchta maqsadni ajratib ko'rsatish kerak, chunki ular bir-biri bilan bog'liq va ularni alohida ko'rib chiqish qiyin. Infratuzilmaning jismoniy komponentlari kelishilgan va birlashtirilgan standartlarga muvofiq ishlaydigan apparat va dasturiy ta'minot to'plamidir. Shunday qilib, ushbu ob'ektlarni butun axborot tuzilmasining ishlashini ta'minlaydigan o'ziga xos xizmat ko'rsatish tuzilmasi sifatida ko'rib chiqish mumkin.[13]

Rendi Vikers AQSh Ichki xavfsizligi vazirligida shu masala bilan shug’ullanadi. Uning aytishicha, xuruj qayerda rejalanib, uni kim amalga oshirmoqda, buni aniqlash mushkul vazifa.

“Zarur resurslar bo’lmasa, qidiruv somon ichidan nina qidirish bilan barobar. Hukumat buyurtmasi asosida ishlayotgan maxsus xizmat bo’lishi mumkin, yoki zimdan ish yuritayotgan boshqa bir idora. Birovni devorga taqash qiyin”. Jumboq kaliti, deydi Vikers, jinoyatlarni bir-biriga qiyoslashda.

“Ma’lumotni bir joyga to’plab, tahlil qilib, jinoyatchini izidan axtarib boramiz. Juda mayda ish, tinimsiz surishtiruv talab qiladi. Bu ishda maqsadni aniqlash juda muhim. Bu bir guruh faollarmi yo hukumat? Yoki uyidan turib, mohirligini namoyish etayotgan bir talaba bo’lsachi?”

Prezident Barak Obama nazarida kiber-xavfsizlik XXI asrning eng dolzarb muammolaridan biri. Yadro va ommaviy qirg’in qurollaridan qolishmaydi.

Amerikadek, odamlar hayotini kompyutersiz tasavvur qila olmaydigan jamiyatda, internet xavfsizligi ham birinchi o’rinda. “Mustahkam tizim butun jamiyatga foyda, chunki internet texnologiyalar kirib bormagan soha-sanoatning o’zi yo’q”, - deydi internet xavfsizligi bo’yicha ekspert Larri Klinton. “Buzg’unchi virus-programmalar bir kompyuterdan ikkinchisiga ko’chib yurishi sir emas. Demak himoya tizimi barchani qamrab olishi kerak”.

Qo'shma Shtatlar internetdagi jinoyatlarga qarshi kurashga zo'r bermoqda, ammo bir paytning o'zida global tarmoqda erkinlikni ham targ'ib qilmoqda.

Kiberterrorizmga jamoatchilikning qiziqishi 1990-yillarning oxirida, bu atama Barri C. Kollin tomonidan kiritilgan paytda boshlangan.[14] 2000 yilga yaqinlashganda, qo'rquv va noaniqlik ming yillik xato kiber-terrorchilar hujumlari ehtimoli ham kuchaygan. Ming yillik xato hech qachon terroristik hujum yoki dunyo yoki AQShga qarshi fitna uyushtirmagan bo'lsa-da, lekin bu katta miqyosdagi halokatli kiberhujum qo'rquvini qo'zg'atishda katalizator vazifasini bajargan. Sharhlovchilar ta'kidlashlaricha, bunday hodisalarning aksariyat faktlari o'zgarganga o'xshaydi, aksariyat hollarda ommaviy axborot vositalarida bo'rttirilgan xabarlarda.

2001 yil 11 sentyabrda Qo'shma Shtatlardagi shov-shuvli teraktlar va undan keyingi voqealar Terrorizmga qarshi urush AQSh tomonidan keyingi yillarda kiberterrorizmning yuzaga kelishi mumkin bo'lgan tahdidlari to'g'risida ommaviy axborot vositalarida ko'proq ma'lumot berishga olib keldi. Ommaviy axborot vositalarida ko'pincha inson hayotini xavf ostiga qo'yish yoki milliy miqyosda buzilishga olib keladigan yoki to'g'ridan-to'g'ri yoki milliy iqtisodiyotni buzish uchun

[12] „Cybercriminals Need Shopping Money in 2017, too! - SentinelOne“ (en-US). sentinelone.com (28-dekabr 2016-yil).
[13] Vasenin V.A. Muhim ob'ektlar va kiberterrorizm. 2-qism. Qarshi choralarni dasturiy ta'minotni amalga oshirish aspektlari
[14] William L. Tafoya, Ph.D.,"Cyber Terror", FBI Law Enforcement Bulletin (FBI.gov), November 2011

muhim infratuzilmani sabotaj qilish uchun kompyuter tarmoqlaridan foydalangan holda katta hujum qilish ehtimoli muhokama qilinadi.[15]

Kabi mualliflar Vinn Shvartau va Jon Arquilla ma'lumotlarga ko'ra, kiberterrorizm oqibatida yuzaga kelgan mayhemning taxminiy ssenariylari tasvirlangan kitoblarni sotishda katta moliyaviy yutuqlarga erishilgan. Ko'pgina tanqidchilar ushbu kitoblar tasvirlangan hujumlar (masalan, yadroviy eritmalar va kimyoviy zavodlarning portlashlari) mumkinmi yoki yo'qligini baholashda haqiqiy emas deb da'vo qilmoqdalar. Tanqidchilar kiberterror-shov-shuv sifatida qabul qiladigan narsalar orasida keng tarqalgan mavzu – bu qalbakilashtirish; ya'ni bashorat qilingan falokatlar ro'y bermasa, bu nazariyani qoralashdan ko'ra, shu paytgacha qanchalik omadli ekanligimizni ko'rsatib beradi.

2016 yilda Adliya vazirligi birinchi marta Ardit Feriziyni kiberterrorizmda aybladi. U harbiy veb-saytni buzib kirishda va davlat va harbiy xizmatchilarning ismlari, manzillari va boshqa shaxsiy ma'lumotlarini o'g'irlab, IShIDga sotishda ayblanmoqda.[16]

Boshqa tomondan, shuningdek, kiberterrorizm bo'yicha jiddiy tadqiqotlar olib borilganiga qaramay, adabiyotlar to'plami hanuzgacha tahdidning realistik bahosini taqdim eta olmaydi, deb ta'kidlashadi.Masalan, elektrostansiya yoki aviakompaniyani buzish orqali jamoat infratuzilmasiga kiberterror hujumi uyushtirilgan taqdirda, uning muvaffaqiyati to'g'risida noaniqlik mavjud, chunki bunday hodisalar haqidagi ma'lumotlar cheklangan.[17]

Darhaqiqat, bunday tahdidlar va jinoyatlar insoniyat tomonidan emg xavfli deb topilayotgan davrda bu borasidagi aniq ishlangan materiallar va adabiyotlar taqdim qilish ilmiy faoliyat bilan shug‘ullanuvchilar uchun eng dolzarb va muammoli mavzuligicha qolavermoqda. Bu borasida aniq ishlangan materiallar taqdi qilish xavsizlig uchun assosiy, va hal qilinishni kutayotgan sohadir.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. A. U. Anorboyev Kiberjinoyatchilik, unga qarshi kurashish muammolari va kiberxavfsizlikni ta’minlash istiqbollari. Monografiya. –T. : Milliy gvardiya instituti. 2020.
2. S. K. Ganiyev, A. A. Ganiyev, Z. T. Xudoyqulov Kiberxavfsizlik asoslari. O‘quv qo‘llanma. –T. : “Toshkent” 2020.
3. Salayev N.S., Ro`ziyev R.N Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya ., – T.: TDYU, 2018
4. Нестерович С.А. Проблемы расследования преступлений, которые стоят пред сотрудниками следственных органов.//Вестник науки и образования. №8. 2018.
5. A.V. Sokolov, O.M. Stepanyuk Kompyuter terrorizmidan himoya. Yordam yo‘riqnomasi

[15] "White House shifts Y2K focus to states, CNN (February 23, 1999)". CNN. 23 February 1999. Retrieved 25 September 2011.
[16] http://www.washingtontimes.com, The Washington Times. "Ardit Ferizi, hacker who aided Islamic State, sentenced for helping terror group with 'kill list'". Washington Times.
[17] C, Reich, Pauline (2012). Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization: Cyberterrorism, Information Warfare, and Internet Immobilization. Xersi, Pensilvaniya: Axborot fanlari bo'yicha ma'lumotnoma. p. 354.