2-TOM, 5-SON

KIBERTERRORIZMGA QARSHI KURASH STRATEGIYALARI

Shahzod Abdusattorov

Toshkent davlat yuridik universiteti magistraturasi talabasi

ANNOTATSIYA

XX asrning oxiri va XXI asrning boshlaridagi keng miqyosidagi globallashuv oqibatida mamlakatlar yangi muammolar bilan to'qnash keldi. Davlatlarning milliy xavfsizligiga nisbatan bo'ladigan xavflar doimiy ravishda mavjud bo'lishiga qaramay kompyuter texnologiyalari va internetning tezlik bilan rivojlanishi terrorizmning kuchayishiga sababchi bo'ldi. Ushbu tezisda Kiberterrorizm tahdidlari va uning zararlari haqida so'z yuritadi va kiberterrorizmga qarshi kurash borasida takliflar keltiriladi.

Kalit so'zlar: kiberterrorizm, kiberekstremizm, kiberjinoyat, kibertahdidlar

ANNOTATION

As a result of the large-scale globalization of the late 20th and early 21st centuries, countries faced new problems. Despite the constant presence of threats to the national security of states, the rapid development of computer technologies and the Internet has led to the increase of terrorism. This thesis discusses the threats and harms of cyber-terrorism and offers suggestions for combating cyber-terrorism.

Key words: cyber terrorism, cyber extremism, cyber crime, cyber threats.

АННОТАЦИЯ

В результате масштабной глобализации конца 20 – начала 21 веков страны столкнулись с новыми проблемами. Несмотря на постоянное наличие угроз национальной безопасности государств, бурное развитие компьютерных технологий и Интернета привело к росту терроризма. В этой тезисе обсуждаются угрозы и вред кибертерроризма и предлагаются предложения по борьбе с кибертерроризмом.

Ключевые слова: кибертерроризм, киберэкстремизм, киберпреступность, киберугрозы.

KIRISH

Hozirgi kunda texnologiyalar tezlik bilan rivojlanishi oqibatida davlatlar kibertahdidlarning turli xil shakllariga qarshi kurash borasida ko'plab muammoli vaziyatlar bilan to'qnash kelmoqda. Shu asnoda kiberjinoyatlarga qarshi kurash va uning oldini olish

dolzarb muammolardan biri bo'lib ulgurdi. Kiberxavfsizlik bu kompyuter tarmoqlari va internet tarmog'idan foydalana oladigan qurilamalarni xavfning turli xil ko'rinishlaridan xavfsizlikni taminlovchi turli xil vositalar jumladan strategiyalar, xavfsizlik kafolatlari, texnologiyalar orqali himoya qilish.

Shu o'rinda **Kiberxavfsizlik** va axborot xavfsizligi atamalari aksariyat holatlarda bir-birining o'rnida qo'llaniladi. Har ikki atama xavfsizlik va kompyuter tizimini tahdidlar va axborotlarga shikast yetishidan himoya qilishga mas'ul bo'lganligi uchun va kiberxavfsizlik va axborot xavfsizligi bir biriga o'zaro bog'liqligi yuzasidan sinonimdek ko'rinishi mumkin va shuning uchun sinonim sifatida qo'llaniladi. Qisqacha keltiradigan bo'lsak axborot xavfsizligi barcha yo'nalishlarda axborotning yaxlitligini saqlash va undan to'lqonli ravishda xavfsiz foydalana olishni taminlashga qaratilgan bo'lsa kiberxavfsizilik esa axborot xavfsizligining bir qismi sifatida faqat kibermakondagi xavfsizilikni taminlashdan iborat hisoblanadi.

Xalqaro darajda kiberjinoyatlarga bo'lgan e'tibor so'ngi yillarda keskin o'sdi buning sababi qilib shuni keltirish mumkinki sodir etilayotgan jinoyatlarning aksariyati an'anaviy usullardan vos kechgan holda yangi ko'rinishda yani kibermakonda sodir etilishi. Bu narsa firibgarlikdan tortib terroristik harakatlargacha uzaygan hisoblanadi. Shunday bo'lishiga qaramay haligacha xalqaro hamjamiyat tomonidan kibermakondagi jinoyatlarga nisbatan huquqiy tomonlama yondoshuvi yetarli darajada emas va shu bois ham kiberjinoyatlarga qarshi tura olish va sodir etilishi mumkin bo'lgan xavf va xatarlarga nisbatan hamkorlik qilishda to'siq bo'lib hizmat qiladi.

METODOLOGIYA

Kiberterrorizm ma'nosi va uning aniq bir talqiniga to'xtaladigan bo'lsak bu turli davlatlarda turlicha aniq bir yakdil talqinga ega emas va hali ham bahsli mavzu hisoblanadi. Muhim infratuzilma ob'ektlari, tibbiyot muassasalari, davlat tashkilotlari, huquqni muhofaza qiluvchi organlar va davlat xavfsizlik organlarining internet tarmog'iga doimiy ravishda ulanishlarni kengayishi sababli kiberterroristik harakatlar ham o'z dolzarbligini bildirmoqda. Shu asosga ko'ra ko'pchilik olimlar tomonidan kiberterrorizm bu terrorizmni yangi bir turi sifatida ko'rib chiqishni ilgari surishmoqda o'ziga hos jihati shundan iboratki terrorchilik harakatlarning kibermakondan foydalangan olda amalga oshirilishi.

Kiberterrorizm – kiberterrorchilik maqsadlari yo'lida kompyuter va telekomunikatsiyalar texnologiyalari (asosan internet)dan foydalanish. Kiberterrorizm

shuningdek xaker dasturlari orqali kompyuter boshqaruvi tarmoqlarini egallab olish va kompyuter viruslari yordamida internet tarmog'ida terakt sodir etish.[1]

Demak V.A.Golubev va boshqa rossiyalik ekspertlar tomonidan kiberterrorizmni kompyuter ma'lumotlari, tizimi yoki tarmog'iga qasddan hujum, deb baholashadi. Maqsadi davlat va xalqaro xavfsizlikka tahdid yaratish, jamiyatni qo'rqitish yoki istalgan mintaqada harbiy mojaro qo'zg'atishdir [2]

A. A. Panenkov, M. A. Efremova, shuningdek, ko'plab xorijiy mualliflar, masalan, AQShdan IT mutaxassisi D. Denning fikricha, kiber terrorizm deganda kompyuter tizimlari, tarmoqlari yoki ulardagi ma'lumotlarga qaratilgan noqonuniy harakatlar tushunilishi kerak. siyosiy yoki ijtimoiy muammolarni hal qilishda hokimiyatga bosim o'tkazish maqsadi deb hisoblashadi.[3][4]

Markaziy Osiyo davlatlarida kiberterrorizmga bo'lgan aniq bir tushuncha hali yetarlicha shakllnaib bo'lmaganligi va bu borada ilmiy ishlar olib borilmaganligi sababli aniq bir nazariy ma'lumotlar topish bu borada juda qiyin. Shu sababli Yevropa va Osiyo davlatlari olimlari tomonidan olib borilgan izlanishlardagi yondoshuvlarga tayanish orqali talqin qilinadi ammo bu bir qator qarama qarshiliklarni keltirib chiqaradi.

Kiberterrorizmni tariflashda ikki xil ko'rinishda amalga oshirish mumkin;

Birinchi holatga ko'ra kiberterrorizmni terrorchi guruhlar yoki shaxslarni axborot texnologiyalridan foydalanishi yani bunda kompyuter tarmoqlarini buzish, turlicha viruslardan foydalanish, veb-saytlarni yo'q qilish kabi harakatlar.

Ikkinchi holatda esa mafkuraviy, diniy tahdidlarni amalga oshirish zo'ravonlikni amalga oshirish yoki aholi orasida qo'rquvni shakllantirish.

Kiberterrorizm iqtisodiy masalalar bilan bog'liq bo'lgan hujumlar yoki zararlarni qamrab olgan bo'lsa bu vaziyatda kiberjinoyatning boshqa shakliga kegishli hisoblanadi.

---

[1] *Кибертерроризм как новая разновидность терроризма URL: https://papers.ssrn.com/sol3 / papers.cfm?abstract_ id=3927791*

[2] *Голубев В. А. Кибертерроризм — угроза национальной безопасности [Электронный ресурс] / Центр исследования проблем компьютерной преступности. URL: http://www.crimeresearch.ru/articles/Golubev_ Cyber_Terrorism/ (дата обращения: 15.04.2020).*

[3] *Ефремова М. А. Уголовно-правовое обеспечение кибербезопасности // Информационное право. 2015. № 5. С. 10–13. .*

[4] *Паненков А. А. Кибертерроризм как реальная угроза национальной безопасности России // Право и кибербезопасность. 2018. № 1. С. 12–19*

Muhokama

Davlatlarning internet tezligi va internet tarmog'laridan foydalanish bo'yicha xalqaro reyting darajasida nechinchi o'rinda turishidan qat'iy nazar kiberjinoyatlar barcha davlatlar uchun bir xil xavf solidi. Kiberterrorizm bu terrorizmning yangi ko'rinishi bo'lib bunda eski usullardan qisman vos kechilgan holda turli xil texnologiyalar orqali zarar berishga qaratilgan. Bir qancha sabablarga ko'ra bu turdagi jinoyatga qarshi kurash olib borishqiyinchiliklarni keltirib chiqaradi.

Birinchidan yuqorida takidlaganimizdek kiberterrorizmning umumiy tushunchasi mavjud emasligi va xar bir davlatda turlicha talqin etilishi;

Ikkinchidan, Har bir mamalakat fuqarolarini himoya qilish, ularga tinch va farovon hayot tarzini taqdim etish uchun har bir sohada kompyuter internet tarmoqlaridan foydalanadi ammo buning qanchalik muhim ekanligi haqida har bir shaxs yetarlicha ma'lumotga ega emas. Terrorchilik harakatlarini sodir etishda kibermakondan foydalangan holda **atom** yoki **elektrenergiya stansiyalari**ga hujumlar orqali millionlab aholiga zarar keltirishi mumkin.

2018 yil oxirida BMT Bosh Assambleyasi 119 davlat tomonidan imzolangan "Xalqaro xavfsizlik kontekstida axborot va telekommunikatsiya sohasidagi yutuqlar" rezolyutsiyasini qabul qildi. O'z o'rnida ushbu qabul qilingan rezolyutsiya kiberjinoyatlarga qarshi kurashda asosiy hujjatlardan biri hisoblanadi.

Shu maqsadda xalqaro konvensiyalarga asoslangan holda bir qancha davlatlar kiberterrorizm bo'yicha bandlarni milliy qonunchilida mustahkamlaydi. Bunga misol qilib Gruziya davlatining Jinoyat kodeksi 324-moddasiga kiberterrorizm sodir etganlik uchun javobgarlik 2006 yil o'zgartirishlar natijasida kiritiladi. Moddaning talqiniga ko'ra aholini qo'rquvga solish yoki jamoatchilikka ta'sir o'tkazishni maqsad qilib qonunchilik orqali qo'riqlanadigan kompyuter axborotlarini noqonuniy egallab olish, foydalanish yoki foydalanish tahdidi, og'ir oqibatlarga sababchi bo'lsa bu kiberterrorizm hisoblanadi.

Xitoy Xalq Respublikasining "XXRning davlat xavfsizlik xizmati to'g'risida"gi Qonuni "Kiberxavfsizlik to'g'risida"gi Qonuni va "Terrorizmga qarshi kurashish to'g'risida"gi Qonunlari orqali mamlakatda kiberjinoyatlarga nisbatan qarshi qaratilgan chora-tadbirlar olib borilmoqda va yuqorida keltirilgan qonunlarda kiberterrorizm sodir etilishini oldini olish shuningdek axborot telekomunikatsiyasining terrorizm bilan bog'liqligi haqida keltirib o'tiladi.

Ukrayina davlatining 2017 yildagi №2163-VIII-sonli "Kiberxavfizlikni ta'minlashning asosiy tamoyillari to'g'risida"gi qonunining 1-moddasiga ko'ra kiberterrorizm kiberfazoda yoki undan foydalangan holda terroristik faoliyatni amalga oshiradigan faoliyat hisoblanadi.[5]

Shu o'rinda AQSh, Ukraina, Gollandiya, Ispaniya, Avstriya, Buyuk Britaniya, Rossiya, Gruziya, Qozog'iston, Estoniya va boshqa mamlakatlarda kiberjinoyatchilik va kiberterrorizmga qarshi kurashish masalasida qonunlar mavjud yoki qonunchikda tegishli bandlar kiritilgan.

Aholiga xavfsiz turmish tarzi yaratib berish har bir davlat siyosatining asosiy vazifasi hisoblanadi. Kiberterrorizmga qarshi kurash olib borishda mamlakatimizda qonuniy asosi mavjud bo'lishi lozim va bu jinoyatni to'laligicha qamrab olishi lozim. O'zbekiston Respublikasida bu turdagi jinoyatlarni sodir etganlik uchun javobgarlik masalasi to'laligicha qamrab olinmagan shu sababli kompyuter texnikasi vositalari orqali terrorchilik harakatlarini sodir etganlik uchun JKning 155-moddasida javobgarlik belgilash va "**Terrorizmga qarshi kurash to'g'risida**"gi qonunga kiritish lozim hisoblanadi. Ushbu moddaga kiberterrorizm, yani kompyuter texnikasi vositasi tizimlari yoki xalqaro internet tarmog'idan foydalagan holda terrorchilik harakatlarini sodir etish va terrorchilik harakatlariga insonlarni targ'ib qilish qismini qo'shish lozim.

XULOSA

Xulosa o'rnida shuni alohida ta'kidlaymizki, milliy huquq tizimlarini asosiy tushunchalar bo'yicha yaqinlashtirish shuningdek kiberjinoyatlar uchun javobgarlik kabi chora-tadbirlarni amalga oshirish natijasida muvaffaqiyatli xalqaro hamkorlik qilish mumkin. Kompyuter hujumlariga qarshi kurashuvchi davlat tuzilmalarini va vositalar to'g'risida ma'lumotlar almashinuvi; axborot resurslarini monitoring qilish, terrorchilikka oid veb-saytlar mazmunini qidirish va kuzatish bo'yicha tajriba va amaliyot almashish va hokozolar. Faqat yuqoridagi mexanizmlarni kompleks tatbiq etish va bu jarayonda har bir ishtirokchi davlatning ishtirokigina kiberterrorizmga qarshi kurashda xalqaro hamkorlikni samarali qiladi.

Foydalanilgan adabiyotlar:

[5] *Закон от 05.10.17 г. № 2163-VIII "Об основных принципах обеспечения кибербезопасности Украины". https://uteka.ua/publication/news-14-delovye-novosti-36-osnovnye-principy-obespecheniya kiberbezopasnostiukrainy.*

1. *Odilqoriyev X., Ochilov B. Hozirgi zamon xalqaro huquqi. Darslik. -T.: JIDU, 2002.*
2. *Rustamboev M.X. O'zbekiston Respublikasining Jinoyat kodeksiga sharh. Maxsus qism. – T.: "Adolat" nashriyoti. 2016 y*
3. *Кибертерроризм как новая разновидность терроризма URL: https://papers.ssrn.com/sol3 / papers.cfm?abstract_ id=3927791*
4. *Голубев В. А. Кибертерроризм — угроза национальной безопасности [Электронный ресурс] / Центр исследования проблем компьютерной преступности. URL: http://www.crimeresearch.ru/articles/Golubev_ Cyber_Terrorism/ (дата обращения: 15.04.2020).*
5. *Ефремова М. А. Уголовно-правовое обеспечение кибербезопасности // Информационное право. 2015. № 5. С. 10–13.*
6. *Паненков А. А. Кибертерроризм как реальная угроза национальной безопасности России // Право и кибербезопасность. 2018. № 1. С. 12–19*

Normativ huquqiy hujjatlar:

1. *O'zbekiston Respublikasi Konstitusiyasi. – T.: O'ZBEKISTON, 2023.*
2. *O'zbekiston Respublikasi "Kiberxavfsizlik to'g'risidagi qonuni"*
3. *O'zbekiston Respbulikasi Jinoyat kideksi*
4. *Закон от 05.10.17 г. № 2163-VIII "Об основных принципах обеспечения кибербезопасности Украины". https://uteka.ua/publication/news-14-delovye-novosti-36-osnovnye-principy-obespecheniya kiberbezopasnostiukrainy*