



KIBERJINOYATCHILIKKA QARSHI KURASHISH: MILLIY QONUNCHILIK VA XALQARO HAMKORLIK

Yarashova Dilnoza Asrorovna

Toshkent davlat yuridik universiteti

3-bosqich talabasi

yarashovadilnoza27@gmail.com

<https://www.doi.org/10.5281/zenodo.8082838>

ARTICLE INFO

Received: 17th June 2023

Accepted: 25th June 2023

Online: 26th June 2023

KEY WORDS

Kiberxavfsizlik, kibermakon, kiberjinoyatlar, O'zbekiston Respublikasi Jinoyat kodeksi, vakolatli organ, xalqaro huquq hujjatlar.

ABSTRACT

Ushbu maqolada kiberjinoyat tushunchasi va bu kabi jinoyatlarni oldini olish maqsadida qabul qilingan milliy qonunchilik hujjatlari va xalqaro standartlar, shuningdek rivojlangan davlatlarda kiberxavfsizlik hodisalarini oldini olishga qaratilgan say-harakatlar haqida so'z yuritildi. O'zbekiston Respublikasi Jinoyat kodeksida belgilangan kiberjinoyatlar deb hisoblangan jinoyatlar qayd etildi va ularni obyekt jihatdan tasniflash to'g'ridagi olimlarning fikrlari o'rganildi.

XXI asrda axborot texnologiyalari hayotning har bir sohasi ya'ni ilm-fan, ishlab chiqarish, xizmat ko'rsatish va shuningdek, davlat boshqaruvida sezilarli o'sish va o'zgarishlarga sabab bo'ldi. Biroq, xuddi shu davrga kelib mazkur sohalarni kibermakonda sodir etilayotgan hujumlardan saqlash uchun, axborot va ma'lumotlarning xavfsizligini ta'minlash, kompyuter ma'lumotlarini turli xil virusli dasturlardan himoya qilish endigi muhim vazifaga aylandi. Shu sababli, so'nggi yillarda, kiberjinoyatchilikka qarshi kurashish g'oyasini keng ommaga tarqatish va fuqarolarning mazkur huquqbuzarliklarning jabrlanuvchilari bo'lib qolishlarini oldini olish uchun mamlakatimizda salmoqli ishlar amalga oshirib kelinmoqda.

Kiberjinoyatchilikka qarshi kurashish to'g'risida to'xtalishdan avval, kiberjinoyat atamasiga ta'rif beradigan bo'lsak, bunda O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonunining 3-moddasida belgilanishicha, "axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta'minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyat"¹ni tushunamiz, mazkur ta'rifdagi kibermakon so'zi esa axborot texnologiyalari yordamida yaratiladigan muhit ma'nosini anglatadi. Yana shuni ham ta'kidlab o'tishimiz joizki, "kiberjinoyat tushunchasi, bugungi kunda ommaviy ravishda qo'llaniladigan axborot texnologiyalari sohasidagi jinoyatlar va kompyuter jinoyatlariga nisbatan kengroq bo'lib, axborotlashtirish sohasidagi barcha jinoyatlarni qamrab oladi."² V.A.Nomokonov va T.L.Tropinaning yuqoridagi fikrlariga to'liq qo'shilgan holda shuni ayta olamizki, kiberjinoyat

¹ <https://lex.uz/uz/docs/-5960604> O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi O'zbekiston Respublikasining Qonuni 3-modda, 15.04.2022 yildagi O'RQ-764-son

² Номоконов В.А, Тропина Т.Л. Киберпреступность как новая криминальная угроза. // Криминология: вчера, сегодня, завтра. – 2012 г. – 1(24). – С47.



faqatgina kompyuterlar orqali emas, balki jahon axborot tarmog'iga ulana oladigan vositalar, masalan mobil telefon apparati orqali ham sodir etilishi mumkin. Shuningdek, kiberjinoyat tushunchasiga rus olimlaridan bo'lgan I.V.Ramanov – Internet tarmog'iga kirishi mumkin bo'lgan har qanday vosita orqali davlatga yoki jismoniy va yuridik shaxslarga iqtisodiy, siyosiy, ma'naviy, madaniy va boshqa shaklda zarar yetkazish maqsadidagi ijtimoiy xavfli harakat yoki harakatsizlik deb ta'rif bergan.³

Amaldagi qonunchiligimizga ko'ra, kiberxavfsizlik va axborot texnologiyalari bilan bog'liq jinoyat turlari sifatida O'zbekiston Respublikasi Jinoyat kodeksining 103-modda 2-qismi "g" bandi, 103¹-modda 2-qismi "v" bandi, 139-modda 2-qismi, 140-modda 2-qismi, 141¹-modda, 141²-modda, 158-modda 3-qismi, 159-modda 1-qismi, 160-modda, 162-modda, 165-modda, 167-modda 3-qismi "g" bandi, 168-modda 2-qismi "v" bandi, 169-modda 3-qismi "b" bandi, 177-modda, 188¹-modda, 189-modda, 191-modda, 192-modda, 194-modda, 215-modda, 216-modda, 216¹-modda, 216²-modda, 217-modda, 228-modda, 229²-modda, 230¹-modda, 230²-modda, 237-modda, 239-moddam 244¹-modda 3-qismi "g" bandi, 244⁵-modda, 278-modda 3-qismi hamda ushbu kodeksga 2007-yilda kiritilgan XX¹-bob ya'ni axborot texnologiyalari sohasidagi jinoyatlarni o'z ichiga oluvchi 278¹-278⁷-moddalari nazarda tutiladi. N.S.Salayev va R.N.Ro'ziyevlar o'z monografiyalarida Jinoyat kodeksidagi kompyuter texnologiyasidan foydalanib sodir etiladigan jinoyatlarni obyektiga nisbatan shartli ravishda 11 turga bo'lib o'rganishni nazarda tutishgan.⁴

Axborot texnologiyalari sohasidagi jinoyatlarning ijtimoiy xavflilik darajasi yuqori bo'lganligi tufayli, ularning oldini olish va unga qarshi kurashish uchun butun davlatimiz siyosati darajasida e'tibor berilib, axborotni muhofaza qilish va uni kiberhujumlardan saqlash maqsadida o'nlab normativ-huquqiy hujjatlar, shu jumladan, O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni (2003), "Elektron hujjat aylanishi to'g'risida"gi Qonuni (2004), "Kiberxavfsizlik to'g'risida"gi Qonuni (2022), "Davlat sirlarini saqlash to'g'risida"gi Qonuni (1993), O'zbekiston Respublikasi Prezidentining "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi PQ-4452-sonli qarori (2019), O'zbekiston Respublikasi Prezidentining "Raqamli O'zbekiston – 2030" strategiyasini tasdiqlash va uni samarali amalga oshirish to'g'risida"gi PF-6079-sonli farmoni (2020) kabi o'nga yaqin qonun hujjatlari qabul qilindi.

Yuqorida keltirilgan normativ-huquqiy hujjatlar ichida sohani tartibga solishga qaratilgan maxsus qonun hujjati bu 2022-yil 15-aprelda qabul qilingan hamda mazkur yilning 17-iyulida kuchga kirgan "Kiberxavfsizlik to'g'risida"gi O'zbekiston Respublikasining O'RQ 764-sonli Qonunidir. Ushbu Qonunga muvofiq kiberxavfsizlikni ta'minlashda "qonuniylik, kibermakonda shaxs, jamiyat va davlat manfaatlarining ustunligi, kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokinining ustuvorligi hamda O'zbekiston Respublikasining kiberxavfsizlikni ta'minlashda xalqaro hamkorlik uchun ochiqligi kabi

³ Романов И.В. Понятие киберпреступлений и его значение для расследование. // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. – С.106

⁴ Salayev N.S., Ro'ziyev R.N. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya – Toshkent.: TDYU, 2018. – 36-b



asosiy tamoyillarga asosan ish yuritiladi.”⁵ Qonun bilan kiberxavfsizlik sohasidagi vakolatli organ etib O'zbekiston Respublikasining Davlat xavfsizlik xizmati belgilandi va organga kiberxavfsizlik hodisalarini oldini olish, kiberxavfsizlik hodisalari yuzasidan tezkor-qidiruv tadbirlarini, tergovga qadar tekshiruvlarni va tergov harakatlarini amalga oshirish hamda kiberxavfsizlik sohasida tadqiqotlar o'tkazilishi va monitoringini tashkil etish kabi bir qator muhim vazifa va vakolatlar belgilandi.

Kiber makondagi jinoyatlarning oldini olish va ularga qarshi kurashish kiberjinoyatchilik avj olib borayotgan bugungi kun uchun juda muhim o'rin tutadi. “Axborot texnologiyalari sohasidagi jinoyatlarning oldini olish chora-tadbirlarini amalga oshirishda, eng avvalo, bu sohada maxsus vakolatli organlarning faoliyati mavjudligi, huquqni muhofaza qiluvchi organlar tizimi qanday tashkil etilganini, uning ijro etuvchi hokimiyat organlari va jamoatchilik bilan aloqalarini hisobga olish lozim.”⁶ Hozirgi kunda mamlakatimizda kiberxavfsizlik hodisalarini oldini olishga qaratilgan say-harakatlarning ko'lami kengligi va huquqni muhofaza qiluvchi organlar ayniqsa kiberjinoyatchilikka qarshi kurashuvchi maxsus vakolatli organ O'zbekiston Respublikasi Davlat xavfsizlik xizmati mavjudligi, bu kabi jinoyatlarni oldini olishda albatta ijobiy ta'sirga ega, ammo bu kabi jinoyatlarning yashirin usulda sodir etilishi ularning oldini olishga qaratilgan chora-tadbirlarni yo'qqa chiqarishi ehtimoldan holi emas.

Kiberjinoyatchilikka qarshi kurashda ushbu turdagi jinoyatlarning bir nechta o'ziga xos xususiyatlarini hisobga olish muhim ahamiyat kasb etadi. Shu jumladan, kiberjinoyatlar alohida hududni talab etmaydi, ular kibernakonning istalgan hududida amalga oshirilishi mumkin, shuning uchun ham jinoyatchining ijtimoiy xavfli qilmishni qayerdan turib bajarayotganini aniqlash qiyin bo'ladi, kiberjinoyatchilik natijasida asosan axborotlarga nisbatan mulkchilik huquqi yo'qotiladi, bu esa muayyan shaxsning mulk huquqi buzilishiga nisbatan ijtimoiy jihatdan xavfli hisoblanadi va shuningdek, kiberjinoyatlar odatda kech aniqlanganligi sababli ularni oldini olish va ularga qarshi samarali kurash olib borish deyarli imkonsiz hisoblanadi.

Kiberjinoyat haqida so'z yuritganda, uning yuqorida ta'kidlanganidek, chegara bilmas ekanligi yana bir bora aytishimiz joizdir. Bu orqali biz, kiberjinoyatlar faqatgina muayyan bir davlatning ichida sodir etilmasligini bildirib o'tmoqdamiz. Ya'ni mazkur ijtimoiy xavfli qilmishni sodir etayotgan shaxs milliy chegaralarni kesib o'tib, jahon tarmog'iga ulangan boshqa mamlakatlardagi kompyuterlarning axborot tarmog'iga kirib ham kiber hujumni amalga oshirish imkoniyatiga egadir. Bu esa globallashuv jarayonida, dunyo hamjamiyati a'zolarini yakka o'zi emas balki boshqa davlatlar bilan birgalikda harakat qilish, kiber tahdidlarni oldini olishda murosaga kelib, muammolarga birgalikda yechim topishga undaydi. S.Tojiyev ta'kidlaganidek, “bunday sharoitda xalqaro hamkorlikni kengaytirish, kiberjinoyatchilikka qarshi birgalikda harakat qilish va uni tekshirish borasida tegishli organlar faoliyatini tartibga solish hamda o'zaro hamkorlikning huquqiy mexanizmlarini ishlab chiqish yagona yo'ldir.”⁷

⁵ <https://lex.uz/uz/docs/-5960604> “Kiberxavfsizlik to'g'risida”gi O'zbekiston Respublikasining Qonuni 4-modda

⁶ Алексеев А. И., Герасимов С. И., Сухарев А.И. Криминологическая профилактика: теория, опыт, проблемы. – М. 2001, - С 68

⁷ Tojiyev S. Kiberjinoyatchilik – shaxs va jamiyat xavfsizligiga tahdid. // www.uza.uz



Jahon miqyosda yuqoridagi maqsadlarni amalga oshirish uchun bir necha o'nlab xalqaro konferensiyalar tashkil etildi va shuningdek, xalqaro shartnomalar, pakt hamda rezolutsiyalar qabul qilinib, ularga a'zo bo'ladigan davlatlarning soni hanuz ortib bormoqda. Ularga misol sifatida keltiriladigan bo'lsak, Yevropa parlamentining "Informatika sohasidagi taraqqiyot munosabatlari bilan shaxs huquqlarini himoya qilish to'g'risida"gi Rezolutsiya (1979), Yevropa Ittifoqi Axborotni himoya qilish to'g'risidagi Konvensiya (1981), kompyuter jinoyatchiligi profilaktikasi hamda unga qarshi kurashishga bag'ishlangan BMT Bosh Assambleyasining VIII kongressiga qo'shimcha sifatida Gavana simpoziumi (1991), BMT Bosh Assambleyasi kiberjinoyatchilik, kiberterrorizm va kiberurushga taalluqli rezolutsiya (1998), Global axborot jamiyati xartiyasi (2000), Internet va kompyuter tarmoqlari, axborot texnologiyalaridan foydalanib, sodir etilayotgan jinoyatlarga qarshi kurashish bo'yicha Budapesht konvensiyasi (2001), Kiberjinoyatchilik muammolarini o'rganish instituti ko'magida kiberjinoyatchilik muammolariga bag'ishlangan birinchi xalqaro sammit (2003), Qohira shahrida Kiberhuquqda axborot xavfsizligi va maxfiyligiga bag'ishlangan konferensiya (2008), MDH ga a'zo davlatlarning kiberjinoyatlar holatlarida qo'llaniladigan Tallin ko'rsatmalari⁸ (2013) kabilar kiberxavfsizlik hodisalarini oldini olishda muhim o'rin tutib kelmoqda.

Dunyoning bir qancha mamlakatlari ham yuqorida keltirilgan xalqaro hujjatlarda belgilangan hamda ko'p sonli davlatlar tomonidan qabul qilingan xalqaro huquqning normalariga amal qilgan holda, kiberjinoyatchilikka qarshi kurashda o'ziga xos uslublarni ishlab chiqqanlar. Xususan, "bugungi kunda dunyoning 50 dan ziyod mamlakatlarida "Virtual olamdagi jinoyatlar va jazo" kabi va shunga o'xshash maxsus qonunlar qabul qilingan."⁹ Rivojlangan davlatlardan biri bo'lgan AQShning bu boradagi tajribasini o'rganadigan bo'lsak, AQShda 1978-yildayoq "Kompyuter jinoyatlari to'g'risida"gi akt qabul qilingan edi va shu orqali kiberjinoyatlarning keltirishi mumkin bo'lgan ulkan zararlar haqida asosli taxminlar qilingan edi. Kanadada ham kiberjinoyatlarning bir nechta turlari shu jumladan, ma'lumotlarga zarar yetkazish, kompyuterdan ruxsatsiz foydalanish kabi jinoyatlar mazkur davlatning Jinoyat kodeksidan o'rin olgan. Germaniya Federativ Respublikasining Jinoyat kodeksiga 1986-yilda kompyuter jinoyatlari uchun javobgarlikni belgilovchi normalar kiritilgan va ular uchun nisbatan qattiqroq javobgarlik nazarada tutilgan. Fransiya Jinoyat kodeksiga kiritilgan kiberjinoyatchilik bilan bog'liq normalar ularning obyektiga qarab ya'ni shaxsga, mulkka, shuningdek millat va davlat manfaatlariga qarshi kompyuter vositasidan foydalanib sodir etiladigan jinoyatlar kabi toifalarga ajratilgan. Rossiya Federatsiyasida 1995-yildayoq "Axborotlashtirish va axborotlarni muhofaza qilish to'g'risida"gi federal qonun qabul qilingan bo'lib, axborot resurslaridan foydalanish, ularni yaratish, yig'ish, qayta ishlash, tarqatish kabi munosabatlarni tartibga soladi.

Xulosa o'rnida shuni aytishimiz mumkinki, hozirda ko'p davlatlar qatorida bizning mamlakatimizda ham, kiberxavfsizlikni ta'minlash va kiberjinoyatchilik holatlarini oldini olishga qaratilgan qonunchilik hujjatlari yetarli hamda bu borada ulkan islohotlar ham amalga oshirib kelinmoqda. Biroq shunday bo'lsada, mazkur toifadagi jinoyatlarning yashirin usulda

⁸ The Tallinn administration on the international law applicable in case of cyberlaw // www.Cambridge.org/9781107024434

⁹ Расулев А.К. Компьютерные преступления: уголовно-правовые и криминологические аспекты. Автореф.дисс... кан.юрид.наук. – Ташкент, 2006. – С27.



va kibermakonda sodir etilishi tufayli o'zidan iz qoldirmasligi, umuman olganda amalga oshirilayotgan islohotlarning yetarli darajada samarali bo'lishiga to'sqinlik qilib kelmoqda. Fikrimizcha, avvalo bu kabi jinoyatlarning qurboniga aylanib qolmaslik uchun, har bir fuqarolarimizdan ogohlik talab etiladi. Zero, agar shaxs kompyuterida saqlanayotgan axborotlar xavfsiligini ta'minlash choralari ko'rishi va shaxsiy ma'lumotlarini ishonchli tarzda saqlash imkoniyatiga egadir.

References:

1. "Kiberxavfsizlik to'g'risida"gi O'zbekiston Respublikasining Qonuni <https://lex.uz/uz/docs/-5960604>
2. Salayev N.S., Ro'ziyev R.N. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya – Toshkent.: TDYU, 2018.
3. Номоконов В.А, Тропина Т.Л. Киберпреступность как новая криминальная угроза. // Криминология: вчера, сегодня, завтра. – 2012 г. – 1(24).
4. Романов И.В. Понятие киберпреступлений и его значение для расследование. // Сибирские уголовно-процессуальные и криминалистические чтения. 2016.
5. Алексеев А. И., Герасимов С. И., Сухарев А.И. Криминологическая профилактика: теория, опыт, проблемы. – М. 2001.
6. Tojiyev S. Kiberjinoyatchilik – shaxs va jamiyat xavfsizligiga tahdid. // www.uza.uz
7. The Tallinn administration on the international law applicable in case of cyberlaw // www.Cambridge.org/9781107024434
8. Расулев А.К. Компьютерные преступления: уголовно-правовые и криминологические аспекты. Автореф.дисс... кан.юрид.наук. – Ташкент, 2006.