

KIBERMAKONDA SODIR ETILAYOTGAN JINOYATLARGA QARSHI KURASH: MUAMMOLAR VA YECHIMLAR

To'xtayev Sardor Sulton o'g'li¹

¹Jahon iqtisodiyoti va diplomatiya universiteti

Xalqaro huquq fakulteti 2-kurs talabasi

Tashev Farrux Muzaffarovich²

Ilmiy rahbar

²Jahon iqtisodiyoti va diplomatiya universiteti

Xalqaro huquq kafedrasi katta o'qituvchisi

<https://doi.org/10.5281/zenodo.7317629>

Annotatsiya: Maqolada kibermakon, kiberjinoyat tushunchalari, uning mohiyati, unga qarshi kurash, muammolar, yechimlar haqida so'z boradi. Dunyo bo'yicha kuzatilayotgan holat, O'zbekistonda kiberjinoyatga qarshi qilinayotgan sa'y-harakatlar, bajarilishi lozim bo'lgan ishlar yoritiladi.

Kalit so'zlar: Kiberjinoyat, kodeks, muammo, internet, kompyuter, dastur.

Kiberjinoyat-taraqqiy etgan jamiyatdagi jinoyatning bir turi hisoblanadi. Jamiyat taraqqiy topishi bilan jinoyat turlari ham o'zgarib boraveradi. Bugungi kunda voyaga yetgan deyarli har bir inson internet resurslaridan foydalanadi. Bu jarayon esa o'ziga xos xavf-xatarga ega, ya'ni kiberjinoyat qurboniga aylanish hej gap emas. Kiberjinoyatning ko'plab turlari mavjud bo'lib, u nafaqat jismoniy shaxsga qaratilgan bo'lishi, balki ulkan davlat miqyosidagi moddiy va ma'naviy boyliklar talon-tarojiga qaratilgan bo'lishi ham mumkin. Bu bo'yicha davlatimizda qonun lohiyalari qayta ko'rib chiqilmoqda. Jumladan O'zbekiston Respublikasi Prezidentining 2018-yil 14-maydagi "Jinoyat va jinoyat-protsessual qonunchiligi tizimini tubdan takomillashtirish chora-tadbirlari to'g'risida"gi PQ-3723-sonli Qarorida "Texnologik taraqqiyot, jumladan kiberjinoyat bilan bog'liq jinoyat turlarining kengayganligini hisobga olgan holda axborot texnologiyalari sohasida javobgarlikni nazarda tutuvchi normalarni qayta ko'rib chiqish" nazarda tutilgan. Undan tashqari O'zbekiston Respublikasi Jinoyat kodeksining 278⁵-moddasiga ko'ra, o'zganing kompyuter uskunasi qasddan ishdan chiqarish, xuddi shuningdek kompyuter tizimini buzish (kompyuter sabotaji):

-3 yilgacha muayyan huquqdan mahrum qilib, 66 mln 900 ming so'mdan 89 mln 200 ming so'mgacha miqdorda jarima;

-2 yilgacha ozodlikni cheklash;

-2 yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

-shuningdek, mazkur harakatlarni guruh bo'lib, takroran yoki xavfli residivist tomonidan sodir etish 3 yilgacha ozodlikdan mahrum qilish bilan jazolashga sabab bo'lishi mumkin.

Kiberjinoyatlar axborot texnologiyalari sohasidagi jamoatchilik

munosabatlariga jiddiy tahdid soladi va shuning uchun zamonaviy sharoitda ularga qarshi kurashish davlat va fuqarolar uchun jiddiy muammoga aylandi. Davlatning huquqni muhofaza qilish organlari ularni zararsizlantirish bo'yicha qarshi choralarni ishlab chiqmoqda, kiberjinoyatlarga qarshi kurashish strategiyasi va taktikasini ishlab chiqmoqda.

Kiberjinoyatlar muayyan sharoitlarda sodir etiladi, ularning sodir etilishiga yordam beradigan omillar mavjud. Ularni aniqlash va ilmiy tahlil asosida sud ekspertiza usulini, tegishli tergov harakatlarini o'tkazish taktikasini ishlab chiqish kerak.

Kibermakonda sodir etilgan ushbu jinoyatlar kompyuterlar, kompyuter dasturlari, kompyuter tarmoqlari faoliyatiga qonunga xilof ravishda aralashish, kompyuter ma'lumotlarini ruxsatsiz kirish, nusxa olish, o'zgartirish, shuningdek axborot-kommunikatsiya texnologiyalari, kompyuter tarmoqlari yordamida yoki ular orqali sodir etilgan boshqa noqonuniy ijtimoiy xavfli harakatlardir.

Ehtimol kiber tahdid manbalari nafaqat xakerlar yoki ularning guruhlar, balki alohida davlatlar, terroristik, jinoiy guruhlar ham hisoblanadi. Kiberjinoyatlarga qarshi kurashishda kurashish vositalari va usullarini ishlab chiqishdajinoyatning latentlikdarajasidan xabardor bo'lishi kerak. Mutaxassislar taxminiga ko'ra "kompyuter jinoyati"ning latentligi AQShda 80% ga, Buyuk Britaniyada - 85% ga, Germaniyada - 75% ga, Rossiyada - 90%ga ko'proqdir 1 . Symantec Security xalqaro kiberxavfsizlik xizmati ma'lumotlariga ko'ra, "har soniyada" dunyo bo'ylab 12 kishi kiberhujumga uchraydi va dunyoda har yili taxminan 556 mln kiberjinoyatlar sodir etiladi va buning natijasida 100 milliardAQSh dollardan ziyod zarar yetkaziladi.

Masalan, Qo'shma Shtatlarda, allaqachon faoliyat ko'rsatayotgan Milliy kiberxavfsizlik markazi bilan bir qatorda Qurolli Kuchlar Birlashgan Kiber Qo'mondonligi harbiy harakatlarni amalga oshirish paytida Pentagon tuzilmalari tegishli yordamni taqdim etadi. Bu global miqyosda barchaning sa'y-harakatlarini muvofiqlashtirib boradi. Fuqarolik federal institutlari va shunga o'xshash dasturiy ta'minot bilan o'zaro aloqadadir. Shu bilan birga, ushbu tashkilotlar qisman nazorat qilinadigan bo'limlardir, chunki «liy nazorat qiluvchi tuzilma "Kengashdir". Milliy xavfsizlik mas'uliyat sohasidagi qo'mitalar axborot strategiyasini amalga oshirishni o'z ichiga oladi. Kiberqurol dasturlari Buyuk Britaniyada rasmiylarning kiber kosmosdan kelib chiqadigan tahdidlarga qarshi turish qobiliyatini ta'minlashda amalga oshiriladi. Avstraliyada elektron pochta xavfsizligini muvofiqlashtirish guruhi tashkil etilgan bo'lib, ushbu guruhning asosiy vazifasi ham davlat, ham xususiy sektor uchun operasion makonni ishonchli himoyaelektron tizim yaratishdir. Kiberjinoyatlarning oldini olish

bo'yicha tadbirlar nafaqat alohida davlatlar tomonidan amalga oshiriladi, balki ularning bloklari, xususan NATO tomonidan amalga oshirilib kelinmoqda. Shunday qilib, so'nggi yillarda qabul qilingan barcha blok-yo'riq hujjatlarida aks ettirilgani ushbu muammoning ahamiyati ko'rsatib beradi. Strategik jihatdan birinchi marta NATO konsepsiyasida alyans faoliyatida qoidalar kiritilgan bo'lib harbiy sohaning yangi yo'nalishi sifatida kiber maydon paydo bo'lgan.

Bizning yurtimizda ham so'nggi paytlarda bir qator kiberjinoyatlar kuzatilmoqda.

Xususan, Samarqand viloyatida bir guruh shaxslar tomonidan «OLTINYUL.UZ» va «E-SUM.UZ» veb-saytlari orqali fuqarolarni mulkiy manfaatga qiziqtirib, «Moliyaviy piramida» loyihasi tuzilgan.

Shu asosda 8 200 nafardan ziyod fuqarodan jami 450 mln. so'mdan ortiq pul mablag'lari yig'ilib, ushbu guruh tomonidan o'zlashtirilgan.

Holat yuzasidan IIV huzuridagi Tergov departamenti tomonidan N.R. va uning sheriklariga nisbatan O'zbekiston Respublikasi Jinoyat kodeksining 188(1)-moddasi 2-qismi bilan jinoyat ishi qo'zg'atilgan.

Bundan tashqari, 2018 yil 23 iyul kuni Toshkent shahrida 5 ta avtotransport vositasi davlat raqamlari o'g'irlanib, jabrlanuvchilardan davlat raqamlarini qaytarish evaziga Internet tarmog'idagi "QIWI" va "WEB money" elektron tizimlari orqali pul talab qilgan. Ko'rilgan choralar natijasida ushbu jinoyatni Toshkent shahar Bektemir tumanida yashovchi 19 yoshli fuqaro sodir etganligi aniqlanib, qo'lga olingan.

Shuningdek, 2018 yilning 4 oktabr kuni Internet tarmog'idagi "Telegram" messenjeridagi 374 mingdan ortiq a'zolari bo'lgan kanaldan telefon va kompyuter vositalariga zarar keltiruvchi dasturlar tarqatilgan. Ko'rilgan choralar natijasida ushbu jinoyatni Farg'ona viloyatida yashovchi M.V. sodir etganligi aniqlanib, qo'lga olingan.

Kiberjinoyatchilikka qarshi Budapesht konvensiyasi 2001 yil 23-noyabr', Internet va komp'yuter jinoyati (kiberjinoyat)larni uyg'unlashtirish orqali milliy qonunlar, tergov usullarini takomillashtirish va xalqlar o'rtasidagi hamkorlikni oshirish yuzasidan imzolangan. Konvensiya va uning izohli ma'ruzasi Yevropa Kengashi Vazirlar qo'mitasi 2001 yil 8-noyabrdagi 109-sessiyasida imzolash uchun Budapeshtda ochilgan va 2001 yil 23-noyabrda kuchga kirgan. 2019 yil sentyabr' oyiga qadar 64 davlat ushbu konvensiyani ratifikatsiya qildi, yana to'rtta davlat konvensiyani imzoladi, ammo uni tasdiqlamadi. U kuchga kirgandan buyon Braziliya va Hindiston kabi muhim davlatlar Konvensiyani ishlab chiqishda qatnashmaganliklari sababli qabul qilishdan bosh tortdilar. Bu kiberjinoyatchilikni tartibga soluvchi birinchi ko'p tomonlama huquqiy majburiy

vositadir. 2018 yildan boshlab, Hindiston kiberjinoyatchilik kuchayganidan keyin Konvensiyadagi pozitsiyasini qayta ko'rib chiqmoqda, ammo chet el agentliklari bilan ma'lumot almashish xavotirlari uni ratifikatsiya qilishdan saqlab qolmoqda.

2006 yil 1 martda Kiberjinoyatchilik to'g'risidagi konvesiyaga qo'shimcha protokol kuchga kirdi. Qo'shimcha protokolni ratifikatsiya qilgan davlatlar irqchi va ksenofobik kompyuter tizimlari orqali material, shuningdek, irqchilik yoki ksenofobiya tomonidan tahdid va haqorattarqatishni jinoiy javobgarlikka tortishlari shartligi belgilandi.

Konvensiya Internet va boshqa kompyuter tarmoqlari orqali sodir etilgan jinoyatlar bo'yicha birinchi xalqaro shartnomadir, xususan mualliflik huquqining buzilishi, kompyuter bilan bog'liq firibgarlik, bolalar pornografiyasi, tahdid jinoyatlariva tarmoq xavfsizligi jinoyatlarigi o'z ichiga oladi. Shuningdek, u kompyuter tarmoqlarini qidirish va qonuniy ushlashga doir qator vakolatlar va protseduralarni o'z ichiga oladi. Uning muqaddimasida keltirilgan asosiy maqsadi jamiyatni himoya qilishga qaratilgan umumiy jinoyat siyosatini olib borishdir. Shuningdek, kiberjinoyatlargadoir tegishli qonunlarni qabul qilish va joriy etish orqali xalqaro hamkorlikni targ'ib etadi.

Konvensiya asosan quyidagilarga qaratilgan:

- Kiberjinoyatchilik sohasidagi huquqbuzarliklar va ular bilan bog'liq qoidalarni ichki jinoyat moddiy-huquqiy elementlarini uyg'unlashtirish;

- Ichki jinoyat-protsessual qonunchiligini tergov qilish va jinoiy javobgarlikka tortish uchun zarur bo'lgan vakolatlarni, shuningdek, elektron tizimda bo'lgan kompyuter tizimi yoki dalillar yordamida sodir etilgan boshqa huquqbuzarliklarni ta'minlash.

- Xalqaro hamkorlikning tezkor va samarali rejimini o'rnatish

Konvensiya tomonidan quyidagi huquqbuzarliklar belgilangan: noqonuniy kirish, noqonuniy yo'l bilan tutish, ma'lumotlarga aralashish, tizimga aralashish, qurilmalardan noto'g'ri foydalanish, kompyuter bilan bog'liq qalbakilashtirish, kompyuter bilan bog'liq firibgarlik, bolalar pornografiyasiva mualliflik huquqi va qo'shni huquqlar bilan bog'liq huquqbuzarliklardir.

Darhaqiqat, ko'rishimiz mumkinki butun dunyo ushbu turdagi jinoyatlarga kurashayotgan bir davrda MDH mamlakatlari ham bundan chetda turmadi. 2018 yil 28 sentabr kiberjinoyatlarni tergov qilishda hamkorlik qilish masalasini tartibga soluvchi ixtisoslashtirilgan hujjatlardan biri hisoblanmish Mustaqil Davlatlar Hamdo'stligiga a'zo davlatlar o'rtasida axborot texnologiyalari sohasida jinoyatlarga qarshi kurashish bo'yicha Bitim imzolandi. Ozarbayjon Respublikasi, Armaniston Respublikasi, Belorusiya, Qozog'iston, Qirg'iziston

Respublikasi, Rossiya Federatsiyasi, Moldova Respublikasi, Tojikiston, Turkmaniston, O'zbekiston va Ukraina ushbu Bitim qatnashchilaridir. O'zbekiston Respublikasi Prezidentining 13.02.2019 yildagi PQ-4188-sonli qarori bilan 2018 yil 28 sentyabrda MDH davlatlari rahbarlari kengashining majlisida imzolangan Mustaqil Davlatlar Hamdo'stligiga a'zo davlatlar o'rtasida axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurashish sohasida hamkorlik to'g'risidagi Bitimni tasdiqladi. Ushbu Bitimni amalga oshirish bo'yicha vakolatli organlar sifatida O'zbekiston Respublikasi Ichki ishlar vazirligi, Davlat xavfsizlik xizmati va Axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo'yicha davlat inspeksiyasi belgilandi. Qonunchiligimizda kompyuter axboroti sohasidagi jinoiy harakatlar, ma'lumki, O'zbekiston Jinoyat kodeksining XX1-bobi "Axborot texnologiyalari sohasidagi jinoyatlar" (2781-2787-moddalar)da o'z aksini topgan. Ushbu jinoyatlarning xususiyatlari axborot-kommunikatsiya texnologiyalaridan qonunga xilof ravishda foydalanish bilan bog'liq ijtimoiy xavfli qilmishlarning kichik bir qismiga taalluqlidir. Qayd etish joizki, O'zbekiston Respublikasi Jinoyat kodeksida unga berilgan izohlarda axborotni to'plash, to'plash va tarqatishning axborot-kommunikatsiya usullari va vositalaridan foydalanish masalalari keng o'z aksini topmagan. Demak, DDos hujumlari, fishing va kiberjinoyatlarni sodir etishning boshqa vositalari va usullaridan foydalanish, ayniqsa, internet-banking sohasida O'zbekiston Respublikasi Jinoyat kodeksida alohida aks ettirilmagan. Hozirgi vaqtda jinoyat qonunchiligi oldida kiberjinoyatlarga qarshi kurashish sohasidagi qonunchilikni o'z vaqtida takomillashtirish zarurati bilan bog'liq vazifalar turibdi.

Mamlakatimiz Jinoyat kodeksida axborot texnologiyalari sohasiga oid yetti moddasida va boshqa qonun hujjatlarida axborot tizimlari, internet tarmog'idagi axborotdan foydalanuvchilar, provayderlar, ommaviy axborot vositalarining va boshqalarning javobgarligi to'g'risidagi ayrim qoidalarining yetishmasligidir. Shu sababli O'zbekiston Respublikasi Jinoyat kodeksiga o'zgartishlar (o'zgartirish va qo'shimchalar)ni ishlab chiqish va belgilangan tartibda kiritishning real zarurati vujudga keldi. Jinoyat kodeksiga o'zganing mulkini o'g'irlash (o'g'irlik, firibgarlik, tovlamachilik), aloqa tarmoqlari, shu jumladan Internet bilan bog'liq jinoyatlarni tartibga solish bo'yicha axborot tizimi va ma'lumotlarga ruxsatsiz kirish, plastik va kredit kartalar orqali pul mablag'larini yechib olish bilan bog'liq ma'lumotlarni qo'shib, o'zgartirish va qo'shimchalar kiritish maqsadga muvofiq, deb hisoblayman.

Zamonaviy voqelikni hisobga olgan holda "kiberjinoyat"ning kompleks tushunchasini belgilash uchun ushbu jinoyatlarning asosiy elementlarini

aniqlash bo'yicha ilmiy tadqiqotlar olib borish va ushbu ijtimoiy xavfli qilmishlarni tergov qilish metodologiyasini ishlab chiqish zarur.

Adabiyotlar:

- 1.Salayev N.S., Ro'ziyev R.N Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya ., – T.: TDYU, 2018, 139-b.
- 2.Карпова Д.Н. Киберпреступность: глобальная проблема и её решение. //Власть. №8. 2014. С. 46-50
- 3.Anorboyev A.U Kiberjinoyatchilik, unga qarshi kurashish muammolari va kiberxavfsizlikni ta'minlash istiqbollari. Monografiya – T.: Milliy gvardiya instituti, 2020. – 324 b.
- 4.Нестерович С.А. Проблемы расследования преступлений, которые стоят пред сотрудниками следственных органов. // Вестник науки и образования. №8. 2018. С. 46-49.
- 5.Karpova D.N. Cybercrimes: a global issue and its solution. Vlast'= The Power no. 8, pp. 46–50. (In Russian).
- 6.Berd K. A war with many unknown quantities. Computerra, 2009, no. 20, pp. 26– 29. (In Russian).
- 7.Zav'yalov S. International experience in fighting the propaganda of terrorism in the Internet. Zarubezhnoevoennoeobozrenie = Foreign Military Review, 2014, no. 4, pp. 34–39. (In Russian).
- 8.Convention on cybercrime, opening of the treaty: Budapest, 23/11/2001. URL: www.coe.int/en/web/cybercrime/the-budapest-convention
www.lex.uz
www.norma.uz
<https://advokatnews.uz/>