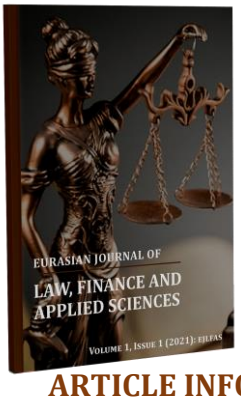
EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.961 www.in-academy.uz



KIBERJINOYATCHILIK YUZAGA KELTIRAYOTGAN JIDDIY TAHDIDLAR VA ULARGA QARSHI KURASHISH YO‘LLARI

Bexzod Rashidov
O‘zbekiston Respublikasi IIV Akademiyasi
kafedra boshlig‘i, y.f.d., professor
Aynura Sabirbayeva
O‘zbekiston Respublikasi IIV Akademiyasi
kafedra dotsenti, y.f.f.d, dotsent
https://doi.org/10.5281/zenodo.8166583

ARTICLE INFO

Received: 10th July 2023
Accepted: 15th July 2023
Online: 19th July 2023

KEY WORDS

Kiberxavfsizlik, kiberjinoyatchilik, kiberjinoyatchilik holati, fishing, kiberfiribgarlik, kiberjinoyatchilik sabablari, kiberjinoyatchilikning oldini olish.

ABSTRACT

Maqolada kiberjinoyatchilikning xavfi, bugungi holati, sodir etilish usullari va xususiyatlari, shuningdek kiberjinoyatchilikning oldini olish borasida qilinishi kerak bo‘lgan ishlar hamda kibermakonda sodir etilayotgan o‘zgalar mulkini talon-toroj qilish holatlarining oldini olish va jabrlangan shaxslarga yetkazilayotgan zararni qoplash uchun samarali bo‘lgan choralar haqida so‘z yuritilgan.

Bundan bir necha o‘n yillar oldin hech kim jinoyatning yangi “virtual” darajaga o‘tishini tasavvur qilmagan bo‘lsa kerak. Kiberjinoyat bilan bog‘liq filmlar ilmiy-fantastik janrga tegishli edi va u erda tasvirlangan narsa oddiy holatga aylanishini hech kim tasavvur qila olmasdi. Kiberjinoyat haqida gapirganda, avvalo bu nima ekanligini aniqlash kerak.

Aslida, kiberjinoyat bu jinoiy faoliyat bo‘lib, unda kompyuter, kompyuter tarmog‘i yoki tarmoq qurilmasi, aksariyat hollarda moliyaviy foyda olish maqsadida (asosan masofadan turib) foydalaniladi yoki hujum qilinadi. Qo‘llanilgan usul va maqsadlarga ko‘ra kiberjinoyatlarni quyidagi turlarga ajratish mumkin: moliyaviy yo‘naltirilgan; shaxsiy hayotga tajovuz qilish bilan bog‘liq; ijtimoiy va siyosiy.

Moliyaviy yo‘naltirilgan kiberjinoyatlarga quyidagilar kiradi: fishing, kiber tovlamachilik, kiberfiribgarlik. Kiber jinoyatlariga identifikatsiyani o‘g‘irlash, josuslik, yashirincha kirish, simsiz tarmoq hujumi, onlayn aldash, zararli elektron pochta, zararli veb-saytlar, zararli uskunalardan foydalanib sodir etiladigan harakatlarni misol qilib keltirish mumkin. Ijtimoiy va siyosiy motivli kiberjinoyatlar toifasiga kiberterrorizm kiradi.

An’anaviy turdagi jinoyatlar sodir etilganda, jinoyatchilar barmoq izlari yoki xakerlik izlari ko‘rinishida moddiy iz qoldirishi mumkin, kiberjinoyatlar jinoyatlar masofadan sodir etilganligi sababli izlarni topish va olish qiyin bo‘lishi mumkin. Jinoyat dunyoning boshqa qismida turib sodir etilishi mumkin. Bundan tashqari, kiberjinoyatning xavfi shundaki, ular nafaqat jismoniy shaxs yoki tashkilotga, balki butun davlatlarga ham katta zarar etkazishi mumkin.

Kiberxakerlar davlat xizmatlarining rasmiy veb-saytlariga kiberhujumlar uyushtirgan holatlarda, misol uchun, Albaniyadagi Axborot jamiyati milliy agentligi (AKSHI, NAIS) davomli

kiberhujumlardan keyin 2022-yilda hukumat onlayn xizmatlari va davlat veb-saytlarini yopishga majbur bo'ldi.

Cybercrime Magazine hisob-kitoblariga koʻra, kiberjinoyatlardan yetkazilishi mumkin boʻlgan zarar 2025-yilga kelib yiliga 10,5 trillion AQSh dollariga yetadi (Taqqoslash uchun 2015-yilda ushbu koʻrsatgich 3 trln. dollar boʻlgan). FBI Internet-firibgarlik hisoboti 2021-maʼlumotlariga koʻra, ushbu yoʻqotishlarning yarmidan koʻpi tovlamachilik, shaxsiy maʼlumotlarni oʻgʻirlash, maxfiy maʼlumotlarning sizib chiqishi, fishing (jumladan, vishing, smashing) va farming bilan bogʻliq.

Soʻnggi yillarda kiberjinoyatchilik bilan bogʻliq jinoiy vaziyat yomonlashdi va milliy muammoga aylanmoqda. Tergov bilan bogʻliq muammolar, mutaxassislarning, shuningdek kiberjinoyatlarga qarshi kurash boʻyicha zamonaviy dasturlar yetishmasligi virtual makonda jinoyatlar sonining bir necha barobar ortishiga sharoit yaratadi. Kiberhujumchilar faol va huquqni muhofaza qiluvchi organlardan bir necha qadam oldinda. Kiberjinoyatchilarning bitta sxemasini toʻxtatishga urinishlar yangi, hatto kattaroq va xavfliroq sxemalarning paydo boʻlishiga olib kelishi mumkin.

Kiberjinoyatlar miqyosi shu darajaga yetdiki, ularni xalqaro xavfsizlikka tahdid deb atash mumkin. Birlashgan Millatlar Tashkilotining 71-sessiyasi kiberjinoyatchilikka qarshi kurashish masalalariga bagʻishlangani bejiz emas, unda dunyoning aksariyat davlatlari virtual makonda jinoyatlar soni ortib borayotganidan xavotir bildirdilar. Dunyo davlatlari yagona jinoyat qonunchiligining yoʻqligi (ayrim mamlakatlarda jinoyat qonunchiligida kiberjinoyatning ayrim turlarini sodir etganlik uchun javobgarlik nazarda tutilmagan), qogʻozbozlik, davlatlar oʻrtasida kelishuvlarning yoʻqligi va boshqa sabablar tufayli boshqa mamlakatlarning huquqni muhofaza qiluvchi organlaridan qonuniy yordam olish qiyinligi bilan bogʻliq kiberjinoyatlarni tergov qilishning milliy muammolari haqida soʻz yuritildi.

Mamlakatimizda, masalan, Toshkent shahrida axborot texnologiyalari sohasidagi jinoyatlar soni 2022-yilda qariyb ikki baravarga oshgan. Agar 2020-yilda ichki ishlar organlari xodimlari tomonidan kibermakonda 106 ta jinoyat qayd etilgan boʻlsa, 2021-yilda ularning soni 2281 taga yetdi. 2022-yilda 4332 ta shunday faktlar aniqlandi. Kiberjinoyatlarning asosiy qismini bank kartalaridan pul oʻgʻirlash tashkil etadi – 2747 ta holat, kiber giyohvandlik bilan bogʻliq holatlari 625 ta. Federal qidiruv byurosining kompyuter jinoyati boʻyicha milliy boʻlimi maʼlumotlariga koʻra, kiberjinoyatlarning 85-97 foizi fosh etilmaydi.

Hozirgi vaqtda kiberjinoyatlarning eng keng tarqalgan turlaridan biri bu kiberfiribgarlikdir. IIV Kiberxavfsizlik markazi maʼlumotlariga koʻra, 34% hollarda kiberfiribgarlar foydalanuvchilarni soxta saytlarga ulardan karta maʼlumotlarini olish maqsadida moddiy yordam takliflari, onlayn kreditlar yoki yutuq haqidagi xabarlar bilan jalb qilgan (fishing); 17% karta egalariga oʻzlarini banklarning xavfsizlik xizmati yoki toʻlov xizmati (vishing) xodimlari sifatida tanishtirib karta maʼlumotlarini telefon orqali olishga erishgan.

Zamonaviy texnologiyalarga qaramay, jabrlanuvchining oʻzi bank kartasi maʼlumotlarini yoki tasdiqlash kodlarini uchinchi shaxslarga berishda davom etsa, bu jarayonni toʻxtatish juda qiyin boʻladi. Har safar tasdiqlash kodini olganingizda, “*hech kimga aytmang, ular firibgar boʻlishi mumkin*” degan xabar paydo boʻladi. Ammo e’tiborsizlik, jaholat yoki insonning ochkoʻzligi jinoyatchilar tomonidan shaxsiy maʼlumotlarni, shu jumladan pulni egallashlariga olib keladi.

Kiberjinoyatlarni aniqlash va tergov qilishda yetarlicha muammolar mavjud. Shunday qilib, kiberjinoyat statistikasi bir necha sabablarga ko‘ra ob’ektiv vaziyatni aks ettirmaydi: jabrlanuvchi kiberhujum va to‘langan to‘lov haqida to‘lov dasturini yashirganligi sababli jinoyat aniqlanmasligi, zararning kam ahamiyatliligi sababli jabrlanuvchining ichki ishlar organlariga murojaat qilishdan bosh tortishi, zararni qoplash mumkinligiga ishonch yo‘qligi, tashkilotlar jamoatchilikning ijobiy fikrini saqlab qolish uchun kiberhujum faktini xabar qilmasligi mumkin. Bundan tashqari, agar bir jinoyatchi tomonidan bir nechta kiberhujum sodir etilgan bo‘lsa va bitta jinoyat ishi qo‘zg‘atilganligi sababli, bu ishda 100 ta holat bo‘lsa ham, statistikada bitta holat sifatida namoyon bo‘ladi.

Tadqiqot natijalariga ko‘ra, kiberfiribgarlar ko‘pincha yengil bosim orqali jabrlanuvchining hushyorligini zaiflashtirishga e’tibor beradilar. Masalan, “TEZKOR! 1 SOAT QOLDI! BITTASINING NARXIGA 2 TA IPHONE 14 OLING! TELEFON SONI CHEKLANGAN!”. Shunday qilib, ular ochko‘z fuqarolarni tuzoqqa tushiradilar.

Bunday jinoiy usullarga qarshi kurashish uchun yagona markaz va zamonaviy texnologiyalarning yo‘qligi yana bir muammoni yuzaga keltiradi. Masalan, kiber jinoyatni to'xtatish uchun Sberbank (uning Bi.Zone kiberxavfsizlik kompaniyasi bor) telefon firibgarlarining “ovozlari kutubxonasi”ni jamlaydi, uning yordamida mijozlarga qo‘ng‘iroqlarni kuzatib boradi va hisobvaraqlardan mablag‘larni yechib olinisihni bloklaydi. Bank firibgar kimgadir qo‘ng‘iroq qilganini bilgach, call-markaz qo‘ng‘iroq qiluvchining raqamiga qayta qo‘ng‘iroq qiladi: agar u firibgarligi ma’lum bo‘lsa, “robotlar hisobdan hisob raqamiga mumkin bo‘lgan operatsiyani avtomatik ravishda to‘xtatib qo‘yadi yoki bloklaydi”. Tizim tajovuzkor bank mijozimi yoki yo‘qligiga ahamiyat bermaydi. Ushbu tizimning joriy etilishi ko‘payib borayotgan vishing (buzg‘unchilar o‘zlarini bank xodimlari sifatida ko‘rsatib, shaxsiy ma’lumotlarni olish) hujumlarining oldini olishga xizmat qilgan bo‘lardi. Yagona markazning joriy etilishi amalga oshirilayotgan kiberhujumlar soni oshishsining oldini olish masalasini hal qilishda asosiy bo‘g‘in bo‘lishi mumkin. Chunki mazkur yagona markaz telekommunikatsiya kompaniyalari, banklar, axborot xavfsizligi kompaniyalari, internet-provayderlar, shuningdek huquqni muhofaza qiluvchi idoralarni birlashtirishi kerak, bu esa eng so‘nggi innovatsiya texnologiyalarini amaliyotda tezkorlik bilan qo‘llash, jinoyatchilikka chek qo‘yish, yetkazilgan zarar qoplanishini ta’minlash, shuningdek huquqbuzarliklarga samarali qarshi kurashish imkonini beradi.

Kiberjinoyatlar, xususan, kiberfiribgarlik, ijtimoiy muhandislikdan foydalanadi va psixologik bosim (vaqt tig‘izligi, ochko‘zlik) ostida jabrlanuvchini shaxsiy ma’lumotlarni berishga majbur qiladi. Pul mablag‘larini hisobdan chiqarishda, jabrlanuvchi bankka firibgarlik sodir bo‘lganligi to‘g‘risida ariza bilan murojaat qilsa ham, banklar pul mablag‘larini ularga qaytarmaydilar, chunki ma’lumotlarni uchinchi shaxslarga oshkor qilish banklar zimmasidan javobgarlikni soqit qiladi (ular tasdiqlash kodini yuborganda, bu firibgarlar bo‘lishi mumkinligi haqida ogohlantiradilar). Banklar firibgarlik alomatlarini (jabrlanuvchining bayonoti) ko‘rsalar, bir yoki ikki ish kuni ichida o‘tkazilgan mablag‘larni qaytarib yechib olish huquqi mavjud bo‘lgan tizim joriy etilishi ushbu muammoning yechimi bo‘lishi mumkin. “Shubhali” tranzaktsiyalar bank tomonidan (jo‘natuvchi bank va oluvchi bank sifatida) o‘tkazmalar asosida tekshirilishi kerak, ammo bu holda mijozning roziligi talab qilinmaydi. Bu

kiberjinoyatlar sodir etilishini bir necha baravarga kamaytiradi va yangi jinoyatlar sodir etilishining oldini oladi, jinoyatlarni fosh etish va huquqbuzarlarni topishga yordam beradi. Kiberjinoyatchilik ham xususiy, ham davlat sektorida yetkazilgan zarar ko‘lami bo‘yicha katta xavf hisoblanadi, shuning uchun ularga qarshi kurashish borasidagi chora-tadbirlarni kuchaytirish huquqni muhofaza qiluvchi organlar faoliyatida ustuvor bo‘lishi kerak.