

VIRTUAL MAKONDA SODIR ETILAYOTGAN KIBERJINOYATLARGA QARSHI

KURASHISH: MUAMMOLAR VA YECHIMLAR

Rashidxo'jayev Muxriddinxo'ja Muxsinxo'ja o'g'li

Toshkent davlat yuridik universiteti

Davlat boshqaruvi kafedrasasi xodimi

mukhriddinkhujarashidkhujaev@gmail.com

+998911704751

<https://doi.org/10.5281/zenodo.10618589>

ANNOTATSIYA

Bugungi kunda jahonda virtual makonda sodir etilayotgan kiberjinoyatlar hajmi tobora kengaymoqda. Ushbu maqolada kiberjinoyatchilikning vujudga kelish omillari, uni oldini olish, kiberjinoyatlarga nisbatan jazo tizimini takomillashtirish hamda davlatimizda kiberjinoyatchilikka qarshi kurashishning samarali usullari yoritib berilgan.

Kalit so'zlar: Virtual makon, virtual firibgarlik, kiberjinoyatchilik, kibertahdid, kiberxavfsizlik, ijtimoiy tarmoq, kiberjinoyatlar uchun jazo qo'llash tizimi.

Bugungi kunda jamiyatda axborot texnologiyalarning rivojlanishi, insonlarning kundalik hayotida internet tarmog'idan keng foydalanishi barobarida jamiyat hayotiga salbiy ta'sir ko'rsatuvchi huquqbuzarliklar soni hamda turlari tobora ortib bormoqda. Axborot texnologiyalari xususan internet tarmog'i orqali virtual makonda sodir etilayotgan jinoyatlar bugungi kunda kiberjinoyat sifatida butun dunyoga keng tarqalmoqda. Ushbu turdagi jinoyatlar o'zining xususiyatiga ko'ra boshqa turdagi jinoyatlardan tubdan farq qiladi. Kiberjinoyatlar boshqa jinoyatlar kabi zamon, makon va vaqt tanlamaydi. Ushbu turdagi jinoyatlar asosan internet tarmog'i orqali web sahifalar, web dasturlar yordamida amalga oshiriladi. Bunga misol qilib hacking ni keltirishimiz mumkin. Hacking ni amalga oshiruvchi shaxslar hakerlar hisoblanib, ular tomonidan ma'lum bir tashkilot yoki hukumatga tegishli web saytni buzib kirilishi va undagi maxfiy ma'lumotlarni o'g'irlash, o'chirib yuborish yoki soxta ma'lumotlar joylash orqali katta zarar yetkazishlari mumkin.

Bugungi kunda hakerlar hujumi natijasida juda ko'plab hukumat idoralari, korporatsiyalar, biznes kompaniyalar katta miqdorda zarar ko'rishgan. Kiberjinoyatlarni tasniflash asnosida har bir jinoyatning ajlalmas qismlari bo'lgan obyekt, subyekt, obyektiv tomoni, subyektiv tomoni hamda predmeti va belgilari haqida toxtalib o'tamiz.

Kiberjinoyatning obyekt bevosita kiberhujum natijasida zarar keltirilishi mumkin bo'lgan kibermakondagi munosabatlar, web sahifalar, hukumat portallari va shunga o'xshash kiber olamni tashkil etuvchi obyektlardir.

Kiberjinoyatning subyektlari esa ushbu jinoyatni amalga oshiruvchi shaxslar, ko'p hollarda ularni hakerlar deb atash mumkin. Albatta kiberjinoyatlar salmog'i yuldan yilga ortib borayotganligini ko'rishimiz mumkin. Dunyo bo'yicha 2022 yilning o'zida davlatlar kiberjinoyatlar natijasida 4,4 trln dollar zarar ko'rgani aytilmoqda. Bu summa yanada ortib borishi va mutaxassislar tomonidan 2023 yilda 11.4 trln dollar bo'lishi kutilmoqda [1]. Kiberjinoyatlarning dunyo davlatlari iqtisodiyotiga keltirayotgan zararlari ushbu jinoyatlarning xalqaro maydonda ortib borishi ushbu jinoyatlarning oldini olish bo'yicha huquqiy ta'sir chorasini ishlab chiqish talab etilmoqda.

Hozirgi kunda virtual olamda keng tarqalgan jinoyat turi firibgarlikdir. Ulardan eng keng

tarqalganlaridan biri bu Plastik karta foydalanuvchilarining hisoblaridan pul o'g'irlashdir. Respublikamizda so'ngi paytlarda bank plastik kartalaridan pul o'g'irlash holatlarining ko'p uchrayotganini kuzatish mumkin. Bunday virtual firibgarlik jinoyati "Fishing" deb nomlanadi. "Fishing" ya'ni "baliq ovi" usuli bo'lib, bunda firibgarlar tomonidan sohta xabarlar jo'natish orqali o'zga shaxslarni karta raqami va kodlarini olishga urinishi yoki ijtimoiy tarmoqalra orqali viruslar, linklar yuborish orqali karta ma'lumotlarini qo'lga kiritish orqali amalga oshiriladi. Afsuski, firibgarlar odamlarning ishonuvchanligidan foydalangan holda, o'zini bankdan, Click, Payme yoki boshqa to'lov xizmatlari tashkiloti xodimi ekanini aytib fuqarolarni aldab, ushbu ma'lumotlarni so'raganda, plastik karta egalari bu ma'lumotlarni berib yuborish holatlari ko'p kuzatilmoqda. Firibgarlar mana shunday vaziyatlardan foydalanib odamlarning plastik kartalaridan pullarini yechib olib ularga juda katta molyaviy zararlar yetkazmoqda. Ushbu vaziyatda firibgarlarning tuzog'iga tushib qolmaslik uchun shaxsiy bank kartalaringizdagi parol va kodlarini hech kimga bermaslik hamda karta bo'yicha SMS ogohlantirish xizmatini ulashi lozim. O'zingiz bilmagan noma'lum saytlar va linklardan foydalanmaslik zarur, shundagina firibgarlar tuzog'iga tushib qolish ehtimolingiz ancha kamayadi.

"Cybersecurity Ventures" ma'lumotlariga ko'ra, kiberjinoyatlarning moliyaviy zarari ko'rsatkichi 2022-yilda 6 trillion dollardan oshiq deya baholangan bo'lsa, 2025-yilga kelib bu ko'rsatkich 10,5 trillion dollarga yetishi prognoz qilinmoqda [2]. Qayd qilingan kiberjinoyatlarning 80 foizi yuqorida aytib o'tganimizdek odatda fishing hujumlari bilan bog'liq ekani aytiladi.

Kiberjinoyatlar statistikasi shuni ko'rsatadiki, FQBning internet jinoyatlari qaydlariga ko'ra, 2022-yilda 800 944 ta shikoyat ro'yxatga olingan. 2023-yilda 33 milliardga yaqin akkaunt buzilgan bo'lib, bu buzilishlar qiymati 8 trillion dollarni tashkil etadi. Shu o'rinda kiberjinoyatlarning qancha vaqt oralig'ida sodir etiladi degan savol tug'iladi. Buni quyidagi statistikada ko'rishimiz mumkin. 2023-yilda 33 milliardga yaqin akkaunt buzilgan bo'lib, bu kuniga 2328 ta, soatiga 97 ta kiberjinoyat sodir etilganini anglatadi. Jami 800 000 kiberhujum qayd etilgan va bu o'rtacha har 39 soniyada xakerlar hujumi sodir etilganini bildiradi [3]. Ushbu statistikalar shuni ko'rsatadiki, virtual makonda sodir etilayotgan kiberjinoyatlar tobora havfli tus olayotganligini va buni oldini olish yuzasidan huquqiy ta'sir chorasini kuchaytirish lozimligini ko'rsatmoqda.

Bugungi kunda har kuni virtual makonda 2328 ga yaqin kiberjinoyatlar sodir etiladi. 2001 yildan 2021 yilgacha bo'lgan so'nggi 21 yil ichida kamida 6,5 million yaqin insonlar kiberjinoyatlar qurboni bo'lgan va shu davrgacha taxminan 26 milliard dollar zarar yetkazilgan.

Virtual makonda sodir etilayotgan jinoyatlar hajmi ham davlatlarning axborot kommunikatsiya sohasida rivojlanishiga mutanosib ravishda oshib bormoqda. Jumaladan, AQSH, Fransiya, Angliya, Germaniya, Belgiya, Lyuksemburg kabi rivojlangan davlatlarda virtual olamdagi jinoyatlar ko'rsatkichi ushbu davlatlardagi umumiy jinoyatchilikning 60-65 foizini tashkil etmoqda. O'zbekistonda ham so'nggi uch yilda bu turdagi jinoyatlar 8,3 baravarga ko'payib, hozirda umumiy jinoyatchilikning qariyb 5 foizdan ortig'ini tashkil etmoqda. Jahonning 38 foiz yoshlari esa shafqatsizlik, zo'ravonlikni targ'ib etuvchi materiallar ta'siriga tushib qolayotgan bo'lsa, yana bir qanchasi o'z joniga qasd qilishni targ'ib qiluvchi 9 mingdan ziyod saytlar orqali osongina jon taslim qilish "dars" larini o'rganishmoqda [4].

Ushbu turdagi jinoyatlarning virtual makonda sodir etilishi va o'zidan ko'p hollarda iz qoldirmasligi ularni kim sodir etganligini aniqlashni murakkablashtirmoqda. Ko'p holatlarda fishing orqali sodir etilayotgan virtual firibgarliklarni kim sodir etganligi noma'lumligicha qolib ketmoqda.

Respublikamizda kiberxavfsizlikni ta'minlash va virtual makonda sodir etilayotgan jinoyatlarni vaqtda aniqlash, oldini olish choralari ko'rish maqsadida O'zbekiston Respublikasi Prezidentining 2019-yil 16-sentyabrdagi "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish oid qo'shimcha chora-tadbirlari to'g'risida"gi PQ-4052-son qarori asosida "Kiberxavfsizlik markazi" tashkil etildi va Davlat xavfsizlik xizmati tarkibiga kiritildi [5]. Shuningdek 2022-yil 15-aprelda "Kiberxavfsizlik to'g'risida"gi qonun ham qabul qilindi. Ushbu qonun kiberxavfsizlik munosabatlarini tartibga solishga qaratilgan hisoblanadi [6].

O'zbekiston Respublikasi amaldagi jinoyat kodeksining XX¹ bobi Axborot texnologiyalari sohasidagi jinoyatlarga bag'ishlangan, shuningdek bir qator maxsus normalarning (139, 140, 141², 141³, 168 va boshqalar) bandlarida axborot kommunikatsiya texnologiyalari va internet tarmog'idan foydalanib sodir etilgan jinoyatlarga nisbatan jazo chorasi belgilab berilgan. Lekin jazo choralari belgilanganligi va kiberjinoyatlarga qarshi kurash chora-tadbirlari olib borilayotganligiga qaramasdan ushbu turdagi jinoyatlar tobora avj olib bormoqda. Bizning nazarimizda bunga sabab quyidagi omillar hisoblanadi:

Aholining virtual makonda sodir etiladigan jinoyatlar haqida yetarli darajada tushunchaga ega emasligi;

Aholining internet, OAK texnologiyalari, ijtimoiy tarmoqlardan to'g'ri foydalanish qoidalarini bilmasligi va amal qilmasligi;

Aholining ushbu sohadagi huquqiy madaniyati va huquqiy ongi yetarli darajada emasligi;

Mamlakatimizda kiberxavfsizlik sohasida malakali mutaxassislarning yetishmasligi va kiberxavfsizlik sohasida ta'limning yetarli darajada yo'lga qo'yilmaganligi;

Huquqiy jihatdan vujudga kelayotgan yangi munosabatlarning kiberjinoyatga olib kelishi mumkin bo'lgan jihatlari to'la qonuniy tartibga solinmaganligi kabi muammolarni ko'rishimiz mumkin.

Virtual makondagi jinoyatlarni eng keng tarqalgani "fishing" firibgarlik jinoyati hisoblansa demak ushbu turdagi jinoyatlarni oldini olish uchun avvalo aholining huquqiy ongini rivojlantirishimiz zarur. Ularning hakerlarning tuzog'iga tushib qolmasliklari uchun ularning ongida virtual jinoyatlarning turlari, qanday sodir etilishi, ular uchun jinoiy javobgarlik asoslari, bank ilovalaridan to'g'ri foydalanish, shaxsiy hisob qaydnomalarini to'g'ri himoya qilish usullarini o'rgatishimiz lozim. Virtual makonda sodir etilayotgan jinoyatlarning ya'na bir salbiy oqibati shundaki, Respublikamizda virtual olamdagi qonunbuzilishlarning aksariyati 16-23 yosh oralig'idagi o'smir-yoshlar tomonidan sodir qilinmoqda. Bundan ko'rinib turibdiki, kiberxavfsizlikni ta'minlash masalasi bugun har qachongidan ham dolzarb ahamiyat kasb etmoqda [7].

Virtual makondagi kiberjinoyatlarni huquqiy jihatdan tasniflash va jinoiy jazo tayinlashda bir qator muhim jihatlarga e'tibor berish lozim. Har qanday aybli ijtimoiy xavfli qilmish jinoyat deb topilishi uchun 4 ta zaruriy belgisi ya'ni jinoyatning obykti, obyektiv tomoni, subykti, subyektiv tomoni bo'lishi zarur. Aynan kiberjinoyatlarda subyektini aniqlash masalasi ancha murakkab hisoblanadi. Chunki kiberjinoyatni sodir etgan shaxs odatda soxta hisob raqam

yoki xabarlardan foydalangan holda moliyaviy firibgarliklarni juda katta miqdorda amalga oshirishi va o'zidan iz qoldirmaslik holatlari ko'p uchramoqda, bu esa jinoyatlarni ochilmasdan qolib ketishiga sabab bo'lmoqda. Bularni oldini olish uchun esa insonlarni shaxsga doir ma'lumotlarini va bank operatsiyalarini amalga oshirish bilan bog'liq jarayonlarni xavfsizlik tizimini takomillashtirish zarur.

Xulosa o'rnida shuni aytishimiz mumkinki, so'nggi bir necha yil davomida virtual olamdagi kiberjinoyatlar soni bir necha baravarga oshib ketganini kuzatishimiz mumkin. Mazkur jarayon bilan bir qatorda, yaratilayotgan raqamli texnologiyalar va axborot tizimlarining xavfsizligini ta'minlash muammosi ham mavjud, albatta. Bu eng dolzarb masalardan biri-kiberxavfsizlikni ta'minlash, sodir etilishi mumkin bo'lgan virtual olamdagi jinoyatlarning oldini olish va unga qarshi kurashish masalasi hisoblanadi.

Yuqoridagi statistik ma'lumotlar shuni ko'rsatadiki agar biz virtual olamdagi jinoyatchilikka qarshi kurashmasak va uning sodir etilishining oldini olmasak bu raqamlar ortsa ortadiki lekin kamaymaydi. Shuning uchun biz virtual makonda ijtimoiy tarmoqlardan, internet tarmog'idan va online savdo platformalaridan foydalanishda ehtiyot bo'lishimiz va iloji boricha o'z xavfsizligimizni ta'minlashga intilishimiz kerak. Virtual makonda sodir etadigan har bir harakatimizni kiberxavfsizlik qoidalariga amal qilgan holda bajarishimiz kerak.

References:

1. N.Kenjayeve, X.Mo'ydinova. "Virtual olamdagi jinoyatlar" Buxoro Davlat Universiteti «Научный Фокус» 01.05.2023.
2. www.statista.com
3. U.Muxsimov. "Kiberjinoyatchilik va unga qarshi kurash" Golden Brain journal, september, 2023.
4. Adam M. Bossler & Tamar Berenblum "Introduction: new direction in cybercrime research" Georgia Southern university, journal "Crime and justice", 2019 .
5. O'zbekiston Respublikasi Prezidentining 2019-yil 16-sentyabrdagi "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish oid qo'shimcha chora-tadbirlari to'g'risida"gi PQ-4052-son qarori
6. "Kiberxavfsizlik to'g'risida"gi O'zbekiston Respublikasi qonuni 15.04.2022 O'RQ 764-son.
7. Do'stmurodov "Yoshlar o'rtasidagi virtual jinoyatlar" Guliston davlat universiteti. 02.03.2023.