KIBERMAKONDA SODIR ETILGAN FIRIBGARLIKLARNING OLDINI OLISH YUZASIDAN VIKTIMOLOGIK CHORA-TADBIRLAR

Baxtiyorov Ixtiyor Baxtiyor o‘g‘li
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti magistratura tinglovchisi, kapitan
E-mail:ibaxtiyorov2007@gmail.com

Annotatsiya. Mazkur maqolada kibermakonda sodir etilayotgan firibgarlik jinoyatlarining viktimologik jihatlari kompleks tahlil qilinadi hamda ularning oldini olishga qaratilgan samarali chora-tadbirlar ishlab chiqiladi. Tadqiqot davomida jabrlanuvchilarning ijtimoiy-demografik, psixologik va xulq-atvor xususiyatlari o‘rganilib, ularning jinoyat sodir etilishidagi o‘rni ilmiy asosda yoritib beriladi. Shuningdek, raqamli savodxonlik darajasining pastligi, axborot xavfsizligi qoidalariga rioya qilmaslik hamda ijtimoiy muhandislik ta’siriga berilish kabi omillar viktimlik darajasini oshiruvchi asosiy determinantlar sifatida baholanadi. Maqolada xalqaro ilmiy manbalar va rasmiy statistik ma’lumotlarga tayangan holda individual, institutsional va davlat darajasida amalga oshirilishi lozim bo‘lgan profilaktik chora-tadbirlar tizimli ravishda asoslab berilgan. Shuningdek, kibermakondagi firibgarlik jinoyatlarining latentligi muammosi va uni kamaytirish yo‘llari ham alohida tahlil qilingan. Tadqiqot natijalari kibermakonda xavfsizlikni ta’minlash hamda jabrlanish xavfini kamaytirishga qaratilgan ilmiy-amaliy tavsiyalar ishlab chiqishga xizmat qiladi.

Kalit so‘zlar: kiberjinoyatchilik, firibgarlik, viktimologiya, jabrlanuvchi, ijtimoiy muhandislik, phishing, raqamli savodxonlik, kiberxavfsizlik, latentlik, profilaktika

Zamonaviy axborotlashgan jamiyat sharoitida kibermakonda sodir etilayotgan firibgarlik jinoyatlari jadal sur'atlarda rivojlanib, global miqyosdagi dolzarb muammolardan biriga aylanmoqda. Axborot-kommunikatsiya texnologiyalarining keng joriy etilishi natijasida iqtisodiy va ijtimoiy jarayonlarning raqamlashtirilishi yangi imkoniyatlar bilan bir qatorda yangi kriminogen xavflarni ham yuzaga keltirmoqda. Shu nuqtai nazardan, kibermakondagi firibgarlik jinoyatlarini faqat huquqiy yoki texnik jihatdan emas, balki viktimologik yondashuv asosida o'rganish zarurati yuzaga kelmoqda.

Mazkur tadqiqotning maqsadi - kibermakonda sodir etilayotgan firibgarlik jinoyatlarining viktimologik xususiyatlarini aniqlash va ularning oldini olishga qaratilgan samarali chora-tadbirlarni ishlab chiqishdan iborat.

Ilmiy adabiyotlarda kibermakondagi firibgarlik jinoyatlari ko'p jihatdan inson omiliga bog'liq ekanligi ta'kidlanadi. Xususan, Yar texnologik rivojlanish yangi jinoyat shakllarini yuzaga keltirishini qayd etadi. Leukfeldt kiberjinoyatchilikning tashkil etilishida ijtimoiy muhandislik muhim rol o'ynashini asoslaydi. Holtfreter va boshqalar esa firibgarlik jinoyatlarida jabrlanuvchilarning psixologik zaifliklari asosiy omil ekanini ta'kidlaydi.

Xalqaro tashkilotlar ma'lumotlariga ko'ra, kiberjinoyatlar soni global miqyosda ortib bormoqda. UNODC[1] va INTERPOL[2] hisobotlarida ayniqsa phishing va ijtimoiy muhandislik asosidagi firibgarliklarning keng tarqalayotgani qayd etilgan.

Kibermakondagi firibgarlik jinoyatlarida jabrlanuvchilarning xulq-atvori muhim rol o'ynaydi. Tadqiqotlar shuni ko'rsatadiki, axborotni tanqidiy baholash ko'nikmasining pastligi, tezkor qaror qabul qilishga moyillik va ortiqcha ishonuvchanlik kabi xususiyatlar viktimlik darajasini oshiradi.

[1] https://www.unodc.org
[2] https://www.interpol.int

Raqamli savodxonlikning yetarli emasligi ham asosiy omillardan biri hisoblanadi. O‘zbekiston sharoitida internet foydalanuvchilari sonining ortishi bilan birga xavfsizlik madaniyati yetarli darajada shakllanmagan[3].

Shuningdek, kibermakondagi jinoyatlarning yuqori darajadagi latentligi ham muhim muammo hisoblanadi. Ko‘plab jabrlanuvchilar huquqni muhofaza qiluvchi organlarga murojaat qilmaydi, bu esa real statistikani aniqlashni qiyinlashtiradi.

Viktimologik chora-tadbirlar: Quyida keltirilgan viktimologik chora-tadbirlar tizimi kibermakonda sodir etilayotgan firibgarlik jinoyatlarining oldini olishga qaratilgan kompleks yondashuvni ifodalaydi. Mazkur chora-tadbirlar individual, institutsional hamda davlat darajasida o‘zaro uyg‘un holda amalga oshirilgandagina samarali natija beradi.

Individual daraja: Kibermakondagi firibgarlik jinoyatlarining oldini olishda eng muhim bo‘g‘inlardan biri - bu foydalanuvchining o‘zi hisoblanadi. Shu sababli, avvalo aholining raqamli savodxonligini tizimli ravishda oshirish zarur. Bu jarayon faqatgina texnik bilimlarni berish bilan cheklanmasdan, balki axborot xavfsizligi madaniyatini shakllantirishni ham o‘z ichiga olishi lozim. Foydalanuvchilarda shubhali xabarlar, havolalar va takliflarni tanib olish ko‘nikmalarini rivojlantirish, ijtimoiy muhandislik usullariga nisbatan immunitet hosil qilish muhim ahamiyat kasb etadi. Shu bilan birga, axborotni tanqidiy baholash qobiliyatini shakllantirish - ya’ni har qanday kelayotgan ma’lumotni tekshirish, uning manbasini aniqlash va mantiqiy tahlil qilish - viktimlik darajasini sezilarli darajada kamaytiradi.

Bundan tashqari, foydalanuvchilarning texnik himoya choralariga amal qilishi ham zarur. Xususan, murakkab va noyob parollardan foydalanish, ularni muntazam yangilab borish, ikki yoki ko‘p bosqichli autentifikatsiya tizimlarini joriy etish, shuningdek, shaxsiy qurilmalarni antivirus va xavfsizlik dasturlari bilan himoyalash muhim hisoblanadi. Ommaviy Wi-Fi tarmoqlaridan ehtiyotkorlik bilan foydalanish,

[3] https://stat.uz

shaxsiy ma’lumotlarni ijtimoiy tarmoqlarda ortiqcha oshkor qilmaslik ham individual darajadagi asosiy profilaktik choralar qatoriga kiradi.

Institutsional daraja: Kibermakondagi firibgarlik jinoyatlarining oldini olishda moliyaviy institutlar, axborot texnologiyalari kompaniyalari va onlayn platformalarning roli alohida ahamiyatga ega. Avvalo, banklar va to‘lov tizimlari tomonidan xavfsizlik infratuzilmasini kuchaytirish zarur. Bu jarayonda zamonaviy texnologiyalar, jumladan sun’iy intellekt va “big data” tahlili asosida firibgarlik operatsiyalarini real vaqt rejimida aniqlash tizimlarini joriy etish muhimdir. Shubhali tranzaksiyalarni avtomatik bloklash, foydalanuvchini darhol xabardor qilish mexanizmlarini yaratish firibgarlik oqibatlarini kamaytirishga xizmat qiladi.

Shuningdek, mijozlarni muntazam ravishda xabardor qilish va ogohlantirish tizimini yo‘lga qo‘yish ham muhim profilaktik choradir. Banklar va platformalar o‘z foydalanuvchilariga yangi firibgarlik sxemalari haqida tezkor ma’lumot berib borishi, xavfsizlik bo‘yicha tavsiyalarni muntazam yetkazishi lozim. Bundan tashqari, foydalanuvchi autentifikatsiyasini kuchaytirish, biometrik identifikatsiya vositalarini keng joriy etish, shuningdek, platformalarda xavfsizlik standartlarini xalqaro talablar darajasiga olib chiqish zarur.

Institutsional darajada yana bir muhim yo‘nalish - bu kadrlar tayyorlash va ichki xavfsizlik tizimini takomillashtirishdir. Tashkilot xodimlarining o‘zi ham ijtimoiy muhandislik hujumlariga nisbatan zaif bo‘lishi mumkinligi sababli, ular uchun muntazam treninglar o‘tkazish muhim ahamiyat kasb etadi.

Davlat darajasi: Davlat darajasida kibermakondagi firibgarlik jinoyatlariga qarshi kurashish tizimli va strategik yondashuvni talab etadi. Avvalo, normativ-huquqiy bazani zamonaviy tahdidlarga mos ravishda takomillashtirish zarur. Kiberjinoyatlar uchun javobgarlik choralarini aniqlashtirish, transmilliy jinoyatlarga qarshi kurashishda xalqaro huquqiy mexanizmlarni joriy etish muhim ahamiyatga ega.

Shu bilan birga, milliy kiberxavfsizlik strategiyalarini ishlab chiqish va ularni amaliyotga tatbiq etish davlat siyosatining ustuvor yo‘nalishlaridan biri bo‘lishi lozim. Bu strategiyalar doirasida axborot infratuzilmasini himoyalash, davlat organlari va xususiy sektor o‘rtasida hamkorlikni kuchaytirish, shuningdek, tezkor axborot almashish tizimlarini yaratish ko‘zda tutiladi.

Aholi o‘rtasida keng ko‘lamli targ‘ibot va tushuntirish ishlarini olib borish ham davlat darajasidagi muhim vazifalardan biridir. Ommaviy axborot vositalari, ta’lim muassasalari va ijtimoiy tarmoqlar orqali axborot xavfsizligi madaniyatini shakllantirish, fuqarolarda xavfsiz xulq-atvor ko‘nikmalarini rivojlantirish zarur. Bundan tashqari, jabrlanuvchilarni qo‘llab-quvvatlash tizimini yaratish, murojaat qilish jarayonlarini soddalashtirish hamda anonim murojaat imkoniyatlarini kengaytirish latentlik darajasini kamaytirishga xizmat qiladi.

Umuman olganda, yuqorida keltirilgan viktimologik chora-tadbirlar tizimi o‘zaro integratsiyalashgan holda amalga oshirilgandagina kibermakondagi firibgarlik jinoyatlarining oldini olishda yuqori samaradorlikka erishish mumkin. Latentlik darajasini kamaytirish kibermakondagi firibgarlik jinoyatlariga qarshi kurashish samaradorligini oshirishda muhim strategik yo‘nalishlardan biri hisoblanadi. Shu nuqtai nazardan, anonim murojaat tizimlarini joriy etish alohida ahamiyat kasb etadi, chunki ko‘plab jabrlanuvchilar o‘z shaxsini oshkor etishdan cho‘chishi, ijtimoiy bosim yoki uyat hissi tufayli huquqni muhofaza qiluvchi organlarga murojaat qilmaydi. Anonim platformalar orqali murojaat qilish imkoniyatining yaratilishi esa fuqarolarning ishonchini oshirib, jinoyatlar haqida xabar berish darajasini sezilarli ravishda ko‘paytiradi. Bunday tizimlar nafaqat murojaatlarni qabul qilishni soddalashtiradi, balki tezkor javob qaytarish, dastlabki tahlilni amalga oshirish va zarur choralarni ko‘rish imkonini ham kengaytiradi.

Shu bilan birga, jabrlanuvchilarni qo‘llab-quvvatlash mexanizmlarini rivojlantirish ham muhim viktimologik chora hisoblanadi. Bu borada huquqiy, psixologik va axborotiy yordam ko‘rsatish tizimini yo‘lga qo‘yish zarur. Xususan,

jabrlanuvchilarga bepul yuridik maslahat berish, ularning huquqlarini tushuntirish, moliyaviy zararlarni qoplash mexanizmlarini ishlab chiqish, shuningdek, psixologik reabilitatsiya xizmatlarini tashkil etish muhim ahamiyatga ega. Bundan tashqari, murojaat qilish jarayonlarini soddalashtirish, byurokratik to‘siqlarni kamaytirish va onlayn platformalar orqali tezkor ariza topshirish imkoniyatlarini yaratish ham latentlik darajasini pasaytirishga xizmat qiladi.

Xulosa va takliflar: Kibermakonda sodir etilayotgan firibgarlik jinoyatlari murakkab, dinamik va ko‘p omilli xarakterga ega bo‘lib, ularni samarali oldini olish uchun kompleks va tizimli yondashuv zarur. Viktimologik yondashuv ushbu jarayonda alohida o‘rin tutadi, chunki u jabrlanuvchilarning xulq-atvori, psixologik xususiyatlari, ijtimoiy holati hamda raqamli muhitdagi faoliyatini chuqur tahlil qilish imkonini beradi. Mazkur yondashuv asosida jinoyatlarning nafaqat oqibatlari, balki ularni yuzaga keltiruvchi sabab va shart-sharoitlar ham aniqlanadi.

Tadqiqot natijalari shuni ko‘rsatadiki, jabrlanuvchilarning axborotni tanqidiy baholash ko‘nikmalarining yetarli darajada rivojlanmaganligi, raqamli savodxonlik darajasining pastligi hamda ijtimoiy muhandislik ta’siriga moyilligi ularning viktimlik darajasini oshiruvchi asosiy omillar hisoblanadi. Shu bois, aholining raqamli savodxonligini oshirish, xavfsiz xulq-atvor madaniyatini shakllantirish va axborot xavfsizligi bo‘yicha tizimli targ‘ibot ishlarini olib borish ustuvor vazifalardan biri bo‘lishi lozim.

Bundan tashqari, kibermakondagi firibgarlik jinoyatlarining yuqori darajadagi latentligi ularning real ko‘lamini aniqlashni murakkablashtiradi hamda samarali profilaktika choralarini ishlab chiqishga to‘sqinlik qiladi. Shu sababli anonim murojaat tizimlarini joriy etish, jabrlanuvchilarni qo‘llab-quvvatlash infratuzilmasini rivojlantirish hamda fuqarolarning huquqni muhofaza qiluvchi organlarga bo‘lgan ishonchini mustahkamlash muhim ahamiyat kasb etadi.

Yakuniy xulosa sifatida aytish mumkinki, kibermakonda firibgarlik jinoyatlariga qarshi kurashish faqat texnik yoki huquqiy choralar bilan cheklanib

qolmasligi, balki inson omiliga qaratilgan viktimologik yondashuv bilan uyg‘unlashtirilishi zarur. Aynan shu yondashuv asosida ishlab chiqilgan kompleks profilaktika tizimi jamiyatda raqamli xavfsizlikni ta’minlash va jabrlanish xavfini sezilarli darajada kamaytirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Yar, M. (2005). The novelty of cybercrime. European Journal of Criminology.
2. Leukfeldt, R. (2014). Cybercrime and social engineering.
3. Holtfreter, K., Reisig, M., Pratt, T. (2008). Fraud victimization.
4. UNODC (2023). https://www.unodc.org
5. INTERPOL (2023). https://www.interpol.int
6. ENISA (2022). https://www.enisa.europa.eu
7. FBI IC3 (2023). https://www.ic3.gov
8. stat.uz (2023). https://stat.uz