KIBERMAKONDA SODIR ETILGAN FIRIBGARLIKLARDAN JABRLANGAN SHAXSLARNING KRIMINOLOGIK TAVSIFI

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 etilgan firibgarlik jinoyatlaridan jabrlangan shaxslarning kriminologik tavsifi kompleks tarzda tahlil qilingan. Tadqiqot davomida jabrlanuvchilarning ijtimoiy-demografik va psixologik xususiyatlari o‘rganilib, ularning viktimologik portreti shakllantirilgan. Shuningdek, kibermakonda firibgarlik jinoyatlarining o‘ziga xos xususiyatlari, ularning sodir etilish mexanizmlari hamda jabrlanuvchilarning jinoyatga duchor bo‘lishiga ta’sir etuvchi asosiy omillar aniqlangan. Maqolada jabrlanuvchilarning yosh, ijtimoiy mavqe, axborot savodxonligi darajasi kabi mezonlar asosida tasnifi amalga oshirilgan hamda ularning psixologik xususiyatlari — ishonuvchanlik, shoshqaloqlik va axborotni tekshirmaslik kabi jihatlar ilmiy asosda yoritilgan. Bundan tashqari, viktimologik omillar, jumladan axborot xavfsizligi qoidalariga rioya qilmaslik, shaxsiy ma’lumotlarni oshkor etish va ijtimoiy tarmoqlardagi ortiqcha faollikning salbiy oqibatlari tahlil etilgan.

Kalit so‘zlar: kibermakon, kiberfiribgarlik, kriminologik tavsif, jabrlanuvchi shaxs, viktimologiya, viktimologik omillar, raqamli viktimologiya, axborot xavfsizligi, ijtimoiy-demografik xususiyatlar, psixologik omillar, kiberjinoyat, profilaktika, ijtimoiy muhandislik, big data, sun’iy intellekt

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida jamiyat hayotining deyarli barcha sohalari raqamlashtirilmoqda. Bu jarayon ijobiy imkoniyatlar bilan bir qatorda yangi turdagi jinoyatchilik shakllarining, xususan, kibermakonda sodir etiladigan firibgarlik jinoyatlarining kengayishiga olib kelmoqda. Mazkur jinoyatlar o‘zining murakkabligi, transmilliy xarakteri va yuqori darajadagi yashirinligi bilan ajralib turadi.

Kibermakonda sodir etilgan firibgarliklar natijasida jabrlanuvchilar sonining ortib borishi, ularning ijtimoiy-demografik va psixologik xususiyatlarini o‘rganish zaruratini yuzaga keltirmoqda. Chunki jinoyatchilikka qarshi samarali kurash olib borishda nafaqat jinoyatchining shaxsini, balki jabrlanuvchining kriminologik tavsifini chuqur tahlil qilish muhim ahamiyat kasb etadi[1].

[1] https://cyberleninka.ru/article/n/kiber-jinoyatchilikka-qarshi-immunitet-hosil-qilish-masalalari

Mazkur maqolaning asosiy maqsadi — kibermakonda sodir etilgan firibgarlik jinoyatlaridan jabrlangan shaxslarning kriminologik tavsifini kompleks tarzda aniqlash, ularning tipologik xususiyatlarini ilmiy jihatdan asoslash hamda ushbu toifadagi jinoyatlarning oldini olishga qaratilgan profilaktika choralarini takomillashtirish yuzasidan amaliy ahamiyatga ega bo‘lgan ilmiy taklif va tavsiyalar ishlab chiqishdan iboratdir.

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi natijasida kibermakonda sodir etilayotgan firibgarlik jinoyatlari nafaqat son jihatdan ortib bormoqda, balki ularning sodir etilish mexanizmlari ham murakkablashib, yanada takomillashib bormoqda. Bu esa o‘z navbatida jabrlanuvchi shaxslarning xususiyatlarini chuqur o‘rganishni, ularning jinoyatga “nishon” bo‘lib qolish omillarini aniqlashni dolzarb ilmiy masalaga aylantirmoqda. Shu bois mazkur tadqiqotda jabrlanuvchilarning nafaqat tashqi (ijtimoiy-demografik), balki ichki (psixologik va xulqiy) omillari ham tizimli ravishda tahlil qilinadi.

Maqsadga erishish uchun quyidagi vazifalar belgilab olindi:

kibermakonda firibgarlik tushunchasining nazariy-huquqiy asoslarini yoritish hamda uning kriminologik xususiyatlarini aniqlash;

mazkur turdagi jinoyatlardan jabrlangan shaxslarning ijtimoiy-demografik belgilarini (yoshi, jinsi, kasbi, ta’lim darajasi, ijtimoiy mavqei va boshqalar) tahlil qilish orqali ularning umumiy portretini shakllantirish;

jabrlanuvchilarning psixologik va xulq-atvor xususiyatlarini o‘rganish asosida viktimologik omillarni aniqlash va tizimlashtirish;

kibermakonda xavfsizlikni ta’minlashga qaratilgan mavjud profilaktika va himoya mexanizmlarini o‘rganish hamda ularni takomillashtirish bo‘yicha ilmiy asoslangan tavsiyalar ishlab chiqish.

Kriminologiya fanida jabrlanuvchi shaxsini o‘rganish viktimologiya yo‘nalishining muhim tarkibiy qismi hisoblanadi. Viktimologiya nafaqat jinoyat oqibatida zarar ko‘rgan shaxslarning holatini tahlil qiladi, balki ularning jinoyat sodir etilishidagi o‘rni va rolini ham ilmiy jihatdan asoslab beradi. Viktimologik yondashuvga ko‘ra, jinoyat sodir etilishida faqatgina jinoyatchining xatti-harakati emas, balki jabrlanuvchining xulq-atvori, ijtimoiy muhitdagi o‘rni, axborotdan foydalanish madaniyati ham muhim ahamiyat kasb etadi.

Xususan, kibermakonda sodir etiladigan firibgarlik jinoyatlarida jabrlanuvchi shaxsning roli yanada yaqqol namoyon bo‘ladi. Chunki bunday jinoyatlarda jinoyatchi ko‘pincha psixologik ta’sir o‘tkazish, ishonch qozonish, manipulyatsiya qilish kabi usullardan foydalanadi. Natijada jabrlanuvchi o‘z ixtiyori bilan shaxsiy ma’lumotlarini oshkor etadi yoki moliyaviy operatsiyalarni amalga oshiradi. Bu esa viktimologik omillarning ushbu turdagi jinoyatlarda alohida o‘rin tutishini ko‘rsatadi.

Shuningdek, zamonaviy ilmiy tadqiqotlar shuni ko‘rsatadiki, jabrlanuvchining raqamli savodxonlik darajasi, internetdan foydalanish madaniyati, axborot xavfsizligi qoidalariga rioya etish holati kabi omillar uning kiberjinoyatlarga duchor bo‘lish ehtimolini bevosita belgilaydi. Shu boisdan ham kibermakonda firibgarlikdan jabrlangan shaxslarni o‘rganish nafaqat nazariy, balki amaliy jihatdan ham muhim ahamiyat kasb etadi[2].

Mazkur yondashuv jinoyatchilikka qarshi kurashishda an’anaviy repressiv choralar bilan bir qatorda, profilaktik va preventiv mexanizmlarni kuchaytirish zarurligini ko‘rsatadi. Ayniqsa, aholi o‘rtasida axborot xavfsizligi madaniyatini shakllantirish, kiberxavfsizlik bo‘yicha bilimlarni oshirish hamda shaxsiy ma’lumotlarni himoya qilish ko‘nikmalarini rivojlantirish ustuvor vazifalardan biri sifatida e’tirof etiladi.

Kibermakonda firibgarlik — bu axborot-kommunikatsiya texnologiyalari, xususan internet tarmog‘i, mobil aloqa vositalari va turli raqamli platformalar orqali shaxsning mulkiga yoki mulkiy huquqlariga aldash, ishonchni suiiste’mol qilish yoxud ijtimoiy muhandislik (social engineering) usullaridan foydalanish orqali zarar yetkazishga qaratilgan g‘ayriqonuniy xatti-harakatlar majmuasidir. Mazkur turdagi jinoyatlar an’anaviy firibgarlikdan o‘zining amalga oshirish usullari, vositalari va ko‘lamining kengligi bilan farqlanadi.

Kibermakonda sodir etiladigan firibgarlik jinoyatlarining asosiy xususiyati shundaki, ular bevosita jismoniy aloqasiz, ya’ni virtual muhitda amalga oshiriladi. Bu esa jinoyatchiga keng imkoniyatlar yaratib, uni aniqlash va javobgarlikka tortish jarayonini murakkablashtiradi. Shu bilan birga, ushbu jinoyat turi global xarakterga ega bo‘lib, u milliy chegaralar bilan cheklanmaydi va ko‘pincha transmilliy xususiyat kasb etadi.

Ushbu jinoyat turi quyidagi asosiy belgilar bilan tavsiflanadi:

Anonimlik darajasining yuqoriligi.

Kiberjinoyatchilar turli texnik vositalar (VPN, proksi serverlar, anonim akkauntlar va boshqalar) yordamida o‘z shaxsini yashirish imkoniyatiga ega. Natijada jinoyatchining haqiqiy shaxsini aniqlash qiyinlashadi, bu esa jinoyatlarni fosh etish va tergov qilish jarayoniga salbiy ta’sir ko‘rsatadi. Anonimlik omili jinoyatchilarda jazodan qochib qolish hissini kuchaytirib, ularni bunday jinoyatlarni sodir etishga undovchi muhim kriminogen omil sifatida namoyon bo‘ladi.

Masofaviy sodir etilishi.

Kibermakonda firibgarlik jinoyatlari geografik jihatdan uzoq masofalarda joylashgan shaxslar o‘rtasida sodir etilishi mumkin. Jinoyatchi va jabrlanuvchi turli

[2] https://cyberleninka.ru/article/n/kiberjinoyatlar-va-ularning-mahalla-darajasida-profilaktikasi-axborot-savodxonligi-va-internet-xavfsizligini-ta-minlash

davlatlarda bo‘lishiga qaramay, internet orqali oson aloqa o‘rnatiladi. Bu holat jinoyatning transchegaraviy xususiyatini kuchaytiradi hamda huquqni muhofaza qiluvchi organlar o‘rtasida xalqaro hamkorlikni zarur etadi.

Tezkorlik va ko‘lamdorlik.

Raqamli texnologiyalar yordamida qisqa vaqt ichida juda ko‘p sonli shaxslarga ta’sir o‘tkazish imkoniyati mavjud. Masalan, ommaviy xabarlar, phishing elektron pochta yoki ijtimoiy tarmoqlar orqali bir vaqtning o‘zida minglab foydalanuvchilarga firibgarlik mazmunidagi xabarlar yuborilishi mumkin. Bu esa jinoyatning ommaviy tus olishiga va katta miqdordagi moddiy zarar yetkazilishiga olib keladi[3].

Psixologik manipulyatsiyaga asoslanganligi.

Kiberfiribgarlikning eng muhim jihatlaridan biri — bu jabrlanuvchining ongiga psixologik ta’sir o‘tkazish orqali uni muayyan harakatni amalga oshirishga majbur qilishdir. Jinoyatchilar odatda ishonch uyg‘otish, qo‘rqitish, shoshiltirish yoki yolg‘on va’dalar berish orqali jabrlanuvchini chalg‘itadi. Masalan, bank xodimi sifatida o‘zini tanishtirib, shaxsiy ma’lumotlarni talab qilish yoki yutuq va’da qilish orqali pul o‘tkazishga undash keng tarqalgan usullardan hisoblanadi.

Shuningdek, kibermakonda firibgarlik jinoyatlari doimiy ravishda evolyutsiyalanib boradi, ya’ni jinoyatchilar yangi texnologiyalar va usullardan foydalanib, o‘z faoliyatini takomillashtirib boradi. Bu esa ushbu jinoyat turiga qarshi kurashishda innovatsion yondashuvlar, zamonaviy texnologiyalar va kompleks profilaktik choralarni qo‘llash zarurligini taqozo etadi.

Umuman olganda, kibermakonda firibgarlik jinoyatlari o‘zining yuqori darajadagi ijtimoiy xavfliligi, yashirinligi va murakkabligi bilan ajralib turadi. Shu boisdan ham ularni chuqur kriminologik tahlil qilish, ayniqsa jabrlanuvchi shaxsning o‘rni va rolini o‘rganish, mazkur jinoyatlarga qarshi samarali kurash strategiyasini ishlab chiqishda muhim ilmiy-amaliy ahamiyat kasb etadi. Tadqiqotchilar (masalan, Yarochkin, Grabosky) ta’kidlaganidek, “kiberfiribgarliklarda jabrlanuvchi ko‘pincha o‘z xatti-harakati orqali jinoyat sodir etilishiga bilvosita sharoit yaratadi”.

2. Muammo tahlili

Kibermakonda firibgarlikdan jabrlangan shaxslarning kriminologik tavsifini tizimli ravishda o‘rganish ularni muayyan mezonlar asosida tasniflashni taqozo etadi. Bunday yondashuv nafaqat jabrlanuvchilarning umumiy portretini shakllantirish, balki jinoyat sodir etilishiga imkon beruvchi viktimologik omillarni aniqlashda ham muhim ilmiy-amaliy ahamiyat kasb etadi. Shu nuqtai nazardan, jabrlanuvchilarning

[3] https://finlit.uz/uz/articles/payments-and-transfers/finlituz-termins

kriminologik tavsifi, avvalo, ularning ijtimoiy-demografik va psixologik xususiyatlari asosida tahlil qilinadi[4].

Ijtimoiy-demografik tavsif

O‘tkazilgan ilmiy tahlillar shuni ko‘rsatadiki, kibermakonda firibgarlik jinoyatlaridan jabrlanuvchi shaxslar turli ijtimoiy-demografik guruhlarga mansub bo‘lsa-da, ularni ayrim umumiy belgilar asosida guruhlash mumkin.

Birinchi navbatda, yoshlar (18–30 yosh) alohida guruhni tashkil etadi. Ushbu toifa vakillari internet tarmoqlari va ijtimoiy platformalardan eng faol foydalanuvchilar hisoblanadi. Ular ko‘pincha onlayn savdo, elektron to‘lovlar, kriptovalyuta operatsiyalari va turli mobil ilovalar orqali moliyaviy faoliyat yuritadi. Biroq, yuqori darajadagi raqamli faollik bilan bir qatorda, xavfsizlik choralariga yetarlicha e’tibor bermaslik, shuningdek, yangi texnologiyalarga ortiqcha ishonch bildirish ularni firibgarlik qurboniga aylanish ehtimolini oshiradi.

Ikkinchi guruh — o‘rta yoshdagilar (30–55 yosh) bo‘lib, ular asosan moliyaviy barqarorlikka ega shaxslar hisoblanadi. Mazkur toifa vakillari bank operatsiyalari, investitsiya faoliyati va onlayn xizmatlardan keng foydalanadi. Shu sababli ular firibgarlar uchun “maqsadli auditoriya” sifatida ko‘riladi. Ayniqsa, kredit olish, investitsiya kiritish yoki biznes bilan bog‘liq takliflar orqali ularni aldash holatlari keng tarqalgan.

Uchinchi guruh — keksalar, ya’ni yoshi katta shaxslar bo‘lib, ular ko‘pincha axborot-kommunikatsiya texnologiyalaridan foydalanish ko‘nikmalarining yetarli darajada shakllanmaganligi bilan ajralib turadi. Axborot savodxonligining pastligi, yangi texnologiyalarga moslashishdagi qiyinchiliklar hamda ishonuvchanlik darajasining yuqoriligi ularni firibgarlik jinoyatlariga nisbatan eng zaif qatlamga aylantiradi.

Statistik ma’lumotlar shuni ko‘rsatadiki, so‘nggi yillarda kiberfiribgarlik qurbonlarining sezilarli qismi — 60 foizdan ortig‘i — aynan internet orqali moliyaviy operatsiyalarni amalga oshiruvchi shaxslarga to‘g‘ri keladi. Bu holat raqamli iqtisodiyotning kengayishi bilan bir qatorda, axborot xavfsizligi madaniyatining yetarli darajada shakllanmaganligini ham ko‘rsatadi.

Psixologik xususiyatlar

Kibermakonda firibgarlikdan jabrlangan shaxslarning psixologik portreti ham muhim kriminologik ahamiyatga ega. Tadqiqotlar shuni ko‘rsatadiki, jabrlanuvchilarning aksariyatida quyidagi psixologik xususiyatlar kuzatiladi:

ishonuvchanlik — notanish manbalardan kelgan axborotlarga tanqidiy yondashmaslik, rasmiy ko‘rinishdagi xabar va takliflarga tez ishonish;

[4] https://journalss.org/index.php/tal/article

shoshqaloqlik — qaror qabul qilishda yetarlicha tahlil qilmaslik, tezkor harakat qilishga moyillik;

tez foyda olish istagi — qisqa muddat ichida katta daromad olishga intilish, bu esa firibgarlar tomonidan keng qo‘llaniladigan “investitsiya tuzoqlari”ga tushib qolish xavfini oshiradi;

axborotni tekshirmaslik odati — manbaning ishonchliligini tekshirmasdan, yuborilgan havola yoki ma’lumotlarga ishonish.

Mazkur psixologik omillar kiberfiribgarlik mexanizmlarida muhim o‘rin tutadi. Chunki jinoyatchilar aynan inson psixologiyasining zaif jihatlaridan ustalik bilan foydalanadi. Masalan, “tez boyib ketish” yoki “katta yutuq qo‘lga kiritish” haqidagi reklama va xabarlar jabrlanuvchining qiziqishini uyg‘otadi va uni tezkor qaror qabul qilishga undaydi. Xuddi shuningdek, bank yoki davlat organlari nomidan yuborilgan soxta xabarlar ishonch uyg‘otish orqali shaxsiy ma’lumotlarni qo‘lga kiritishga xizmat qiladi.

Bundan tashqari, qo‘rquv va xavotir omillaridan foydalanish ham keng tarqalgan usullardan biridir. Masalan, “hisobingiz bloklandi” yoki “zudlik bilan ma’lumotlarni tasdiqlang” kabi xabarlar jabrlanuvchini shoshiltirib, uni o‘ylamasdan harakat qilishga majbur etadi.

Umuman olganda, kibermakonda firibgarlikdan jabrlangan shaxslarning ijtimoiy-demografik va psixologik xususiyatlarini kompleks o‘rganish, ularning viktimologik portretini shakllantirishga imkon beradi. Bu esa o‘z navbatida, jinoyatchilikka qarshi kurashishda samarali profilaktika choralarini ishlab chiqish va aholining kiberxavfsizlik darajasini oshirishda muhim ilmiy asos bo‘lib xizmat qiladi[5].

Viktimologik omillar: Kibermakonda sodir etiladigan firibgarlik jinoyatlarida jabrlanuvchining o‘rni va roli alohida ahamiyat kasb etadi. Viktimologik yondashuv nuqtai nazaridan qaralganda, jinoyat sodir etilishida nafaqat jinoyatchining faol harakatlari, balki jabrlanuvchining xulq-atvori, ehtiyotsizligi yoki yetarli bilimga ega emasligi ham muhim omil sifatida namoyon bo‘ladi. Shu boisdan, kibermakonda firibgarlik qurboniga aylanish ehtimolini oshiruvchi asosiy viktimologik omillarni aniqlash va tizimlashtirish ilmiy va amaliy jihatdan muhimdir.

Avvalo, axborot xavfsizligi qoidalariga rioya qilmaslik eng keng tarqalgan omillardan biri hisoblanadi. Ko‘plab foydalanuvchilar oddiy xavfsizlik choralariga, masalan, murakkab parollar yaratish, ikki bosqichli autentifikatsiyadan foydalanish yoki dasturiy ta’minotni muntazam yangilab borish kabi talablarni e’tibordan chetda qoldiradi. Natijada ularning shaxsiy akkauntlari va moliyaviy resurslari kiberjinoyatchilar uchun oson nishonga aylanadi.

[5] https://cyberleninka.ru/article/n/kiber-jinoyatchilikka-qarshi-immunitet-hosil-qilish-masalalari

Ikkinchi muhim omil — shaxsiy ma’lumotlarni oshkor etishdir. Ijtimoiy tarmoqlar va turli onlayn platformalarda foydalanuvchilar o‘zlari haqidagi ortiqcha ma’lumotlarni (telefon raqami, yashash manzili, bank kartasi rekvizitlari va boshqalar) e’lon qilib qo‘yishi ko‘p uchraydi. Bunday holatlar jinoyatchilarga jabrlanuvchining shaxsiy profilini shakllantirish va unga nisbatan individual firibgarlik sxemalarini ishlab chiqish imkonini beradi.

Shuningdek, shubhali havolalarga kirish va noma’lum manbalardan yuborilgan fayllarni ochish ham yuqori xavf tug‘diradi. Phishing, smishing va boshqa ijtimoiy muhandislik usullari orqali foydalanuvchilar zararli dasturlarni o‘z qurilmalariga o‘rnatib qo‘yishi yoki maxfiy ma’lumotlarini firibgarlarga topshirib qo‘yishi mumkin. Bu esa ko‘pincha foydalanuvchining yetarli darajada ehtiyotkorlik qilmasligi bilan bog‘liq.

Bundan tashqari, ijtimoiy tarmoqlarda ortiqcha faollik ham viktimologik xavf omillaridan biri sifatida e’tirof etiladi. Foydalanuvchining doimiy ravishda o‘z joylashuvi, moliyaviy holati yoki kundalik faoliyati haqida ma’lumot berib borishi jinoyatchilar uchun muhim axborot manbai bo‘lib xizmat qiladi. Ayniqsa, ommaviy sahifalarda shaxsiy hayot tafsilotlarini ochiq e’lon qilish firibgarlik xavfini sezilarli darajada oshiradi.

Umuman olganda, yuqoridagi viktimologik omillar kibermakonda jinoyat sodir etilishiga qulay sharoit yaratib beruvchi muhim determinantlar hisoblanadi. Ularni bartaraf etish esa profilaktika choralarining samaradorligini oshirishga xizmat qiladi.

3. Zamonaviy yondashuvlar

Zamonaviy kriminologiya fanida kibermakonda sodir etiladigan jinoyatlarni, xususan, firibgarlik holatlarini o‘rganishda kompleks va tizimli yondashuvlar qo‘llanilmoqda. Ushbu yondashuvlar nafaqat jinoyatchilikni aniqlash va fosh etishga, balki uning oldini olishga, ya’ni preventiv choralarni ishlab chiqishga qaratilganligi bilan ahamiyatlidir[6].

Birinchi navbatda, raqamli viktimologiya konsepsiyasi alohida e’tiborga loyiqdir. Ushbu yondashuv doirasida shaxslarning raqamli muhitdagi xulq-atvori, internetdan foydalanish odatlari, axborot bilan ishlash madaniyati tahlil qilinadi. Mazkur tahlillar asosida foydalanuvchilarning xavf darajasi baholanadi hamda ular uchun individual xavfsizlik strategiyalari ishlab chiqiladi. Raqamli viktimologiya nafaqat jabrlanuvchining hozirgi holatini, balki uning potensial xavf ostida ekanligini ham oldindan aniqlash imkonini beradi.

Ikkinchi muhim yo‘nalish — profilaktik modellashtirish hisoblanadi. Zamonaviy axborot texnologiyalari, xususan sun’iy intellekt va katta ma’lumotlar (big data) tahlili yordamida firibgarlik xavfi yuqori bo‘lgan holatlar va shaxslar aniqlanadi.

[6] https://kti.iiv.uz/storage/journal/files

Maxsus algoritmlar orqali shubhali tranzaksiyalar, noodatiy xatti-harakatlar yoki xavfli onlayn faoliyat avtomatik tarzda aniqlanib, tegishli choralar ko‘riladi. Bu esa jinoyat sodir etilishidan oldin uning oldini olish imkonini yaratadi.

Shuningdek, huquqiy mexanizmlarni takomillashtirish ham muhim ahamiyat kasb etadi. So‘nggi yillarda ko‘plab davlatlarda kiberjinoyatlarga qarshi kurashni kuchaytirishga qaratilgan maxsus normativ-huquqiy hujjatlar qabul qilinmoqda. Xususan, Yevropa Ittifoqida qabul qilingan Umumiy ma’lumotlarni himoya qilish reglamenti (GDPR) shaxsiy ma’lumotlarning xavfsizligini ta’minlashda muhim vosita bo‘lib xizmat qilmoqda. Mazkur hujjat orqali foydalanuvchilarning shaxsiy ma’lumotlarini qayta ishlash tartibi qat’iy tartibga solingan hamda ma’lumotlarni noqonuniy foydalanish uchun javobgarlik kuchaytirilgan.

Bundan tashqari, xalqaro hamkorlikni rivojlantirish, kiberjinoyatlarga qarshi kurashuvchi maxsus bo‘linmalar faoliyatini takomillashtirish va aholining huquqiy ongini oshirish ham zamonaviy yondashuvlarning ajralmas qismi hisoblanadi.

Xulosa qilib aytganda, kibermakonda firibgarlikka qarshi kurashishda zamonaviy yondashuvlar kompleks xarakterga ega bo‘lib, ular texnologik, huquqiy va ijtimoiy mexanizmlarning uyg‘unlashuvi asosida amalga oshiriladi. Bu esa mazkur turdagi jinoyatlarning oldini olishda samaradorlikni oshirishga xizmat qiladi.4. Amaliy tajriba

Amaliyot shuni ko‘rsatadiki, kiberfiribgarliklarning asosiy turlari quyidagilardan iborat:

phishing (soxta saytlar orqali ma’lumot olish);

smishing (SMS orqali firibgarlik);

vishing (telefon orqali aldash);

onlayn savdo firibgarligi.

Masalan, bank nomidan yuborilgan soxta havola orqali foydalanuvchi o‘z karta ma’lumotlarini kiritadi va natijada mablag‘lar yechib olinadi.

O‘zbekiston amaliyotida ham so‘nggi yillarda kiberjinoyatlar soni sezilarli darajada oshgan bo‘lib, bu esa profilaktika choralarini kuchaytirishni talab etadi.

Tadqiqot natijalariga ko‘ra, kibermakonda firibgarlikdan jabrlangan shaxslarning kriminologik tavsifi murakkab va ko‘p omilli xarakterga ega ekanligi aniqlandi. Jabrlanuvchilarning ijtimoiy-demografik, psixologik va xulqiy xususiyatlari jinoyat sodir etilishida muhim rol o‘ynaydi: jabrlanuvchilarning axborot savodxonligi pastligi asosiy omillardan biridir; psixologik manipulyatsiya kiberfiribgarlikning asosiy vositasidir; raqamli muhitda xavfsizlik madaniyati yetarli darajada shakllanmagan.

Takliflar: Aholining raqamli savodxonligini oshirish bo‘yicha tizimli dasturlar joriy etish; kiberxavfsizlik bo‘yicha majburiy o‘quv kurslarini tashkil etish; bank va moliyaviy tizimlarda qo‘shimcha himoya mexanizmlarini joriy etish; kiberjinoyatlar

profilaktikasida viktimologik yondashuvni keng qo‘llash; huquqni muhofaza qiluvchi organlar faoliyatida zamonaviy texnologiyalardan foydalanishni kengaytirish.

Yakuniy xulosa sifatida aytish mumkinki, kibermakonda sodir etiladigan firibgarliklarning oldini olishda faqatgina jinoyatchiga qarshi kurash yetarli emas, balki jabrlanuvchini himoya qilish va uning xulq-atvorini to‘g‘ri shakllantirish ham muhim ahamiyatga ega.

Foydalanilgan adabiyotlar:

1. Yarochkin V.I. Kiberjinoyatchilik asoslari. – Moskva: Akademiya, 2018. – 256 b.
2. Grabosky P. Cybercrime: The Nature and Impact of Computer Crime. – London: Routledge, 2016. – 192 p.
3. Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge: Polity Press, 2015. – 240 p.
4. Leukfeldt E.R., Yar M. Cybercrime and Cybervictimization: An Introduction. – London: Routledge, 2020. – 210 p.
5. Holt T.J., Bossler A.M., Seigfried-Spellar K.C. Cybercrime and Digital Forensics: An Introduction. – New York: Routledge, 2018. – 310 p.
6. Akhmedov B.A. Kiberjinoyatlar va ularga qarshi kurashish muammolari. – Toshkent: TDYU nashriyoti, 2021. – 180 b.
7. O‘zbekiston Respublikasi Jinoyat kodeksi. – Toshkent: Adolat, 2023.
8. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuni. – Toshkent, 2003 (oxirgi o‘zgartirishlar bilan).
9. O‘zbekiston Respublikasi “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. – Toshkent, 2019.
10. European Union. General Data Protection Regulation (GDPR). – Brussels, 2016.
11. INTERPOL. Global Cybercrime Report. – Lyon, 2022.
12. UNODC (United Nations Office on Drugs and Crime). Comprehensive Study on Cybercrime. – Vienna, 2021.
13. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – New York: Wiley, 2020. – 640 p.
14. Kaspersky Lab. Cybersecurity and Cybercrime Statistics Report. – 2023.
15. Cisco. Annual Cybersecurity Report. – 2022.