SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

TOSHKENT SHAHRIDA RO‘Y BERAYOTGAN KIBERJINOYATLAR TURLARI VA ULARNING OLDINI OLISH ASOSLARI

Ergashev Javohir Alisher og’li

O‘zbekiston Respublikasi IIV Akademiyasi 3-o‘quv kursi kursanti

Toshkent sh.

https://doi.org/10.5281/zenodo.20569118

Annotatsiya: Ushbu maqolada raqamli iqtisodiyot va axborot texnologiyalari jadal rivojlanayotgan Toshkent shahrida sodir etilayotgan kiberjinoyatlarning zamonaviy turlari, ularning o‘ziga xos xususiyatlari hamda ijtimoiy xavfliligi kriminologik jihatdan tahlil qilingan. Tadqiqotda ijtimoiy injiniring, bank plastik kartalari bilan bog‘liq firibgarliklar, shuningdek, shaxsga qarshi qaratilgan virtual tahdidlar ko‘rib chiqilgan. Kiberjinoyatlarning oldini olish asoslari doirasida ichki ishlar organlarining huquqbuzarliklar profilaktikasini tashkil etishdagi yondashuvlari, yuqori texnologik vositalar (Face-ID, elektron ma'muriy bayonnomalar) orqali nazoratni o‘rnatish va Ma'muriy javobgarlik to‘g‘risidagi qonun hujjatlarini takomillashtirish masalalari bo‘yicha ilmiy asoslangan takliflar ishlab chiqilgan.

Kalit so‘zlar: kiberjinoyat, axborot xavfsizligi, firibgarlik, huquqbuzarliklar profilaktikasi, ma’muriy javobgarlik, ichki ishlar organlari, elektron bayonnoma, Face-ID, ijtimoiy injiniring.

Аннотация: В данной статье с криминологической точки зрения анализируются современные виды киберпреступлений, совершаемых в городе Ташкенте, где стремительно развиваются цифровая экономика и информационные технологии, а также их специфика и общественная опасность. В исследовании рассматриваются социальная инженерия, мошенничества, связанные с банковскими пластиковыми картами, а также виртуальные угрозы против личности. В рамках основ предотвращения

киберпреступлений разработаны научно обоснованные предложения по подходам органов внутренних дел к организации профилактики правонарушений, установлению контроля с помощью высокотехнологичных средств (Face-ID, электронные административные протоколы) и совершенствованию законодательства об административной ответственности.

Ключевые слова: киберпреступность, информационная безопасность, мошенничество, профилактика правонарушений, административная ответственность, органы внутренних дел, электронный протокол, Face-ID, социальная инженерия.

Abstract: This article provides a criminological analysis of the modern types of cybercrimes committed in Tashkent, a city with rapidly developing digital economy and information technologies, as well as their specific features and social danger. The study examines social engineering, fraud related to bank plastic cards, and virtual threats directed against individuals. Within the framework of the basics of cybercrime prevention, scientifically grounded proposals have been developed regarding the approaches of internal affairs bodies to organizing offense prevention, establishing control through high-tech tools (Face-ID, electronic administrative protocols), and improving legislation on administrative responsibility.

Keywords: cybercrime, information security, fraud, offense prevention, administrative responsibility, internal affairs bodies, electronic protocol, Face-ID, social engineering.

Raqamli texnologiyalar jamiyat hayotini qulaylashtirish bilan bir qatorda, huquqbuzarliklar va jinoyatchilikning yangi, transformatsiyalashgan shakllari yuzaga kelishiga ham sabab bo‘lmoqda. O‘zbekiston Respublikasining poytaxti Toshkent shahri mamlakatning eng yirik moliya, iqtisodiyot va IT-markazi sifatda

bu o‘zgarishlarning markazida turibdi. Fuqarolarning kundalik hayotida elektron to‘lov tizimlari, internet-do‘konlar, messenjerlar va davlat elektron xizmatlarining ommalashuvi oqibatida an’anaviy jinoyatlar (o‘g‘rilik, firibgarlik, tovlamachilik) virtual makonga ko‘chdi.

Kiberjinoyatchilik bugungi kunda o‘ta yuqori darajadagi latentlikka, transmilliy xususiyatga va jamiyatga katta moddiy hamda ma'naviy zarar yetkazish salohiyatiga ega ekanligi bilan ajralib turadi. Ayniqsa, bunday huquqbuzarliklarga qarshi kurashishda qonunchilikning, birinchi navbatda, jinoyat va ma'muriy huquq normalarining doimiy ravishda zamon talablariga moslashtirib borilishi dolzarb ahamiyat kasb etadi. Ushbu jinoyatlarning faqat oqibatlari bilan kurashish samarasizdir; eng maqbul yo‘l – ularning barvaqt oldini olish (profilaktika) mexanizmlarini ilmiy-amaliy jihatdan kuchaytirishdir.

Mazkur maqolaning maqsadi – Toshkent shahrida sodir etilayotgan kiberjinoyatlarning asosiy turlarini tasniflash, jinoyatchilarning harakat usullarini kriminologik tahlil qilish hamda ushbu huquqbuzarliklarning oldini olishda ma'muriy-huquqiy choralarning va zamonaviy texnologiyalarning ahamiyatini ochib berishdan iborat.

TOSHKENT SHAHRIDA KIBERJINOYATLARNING O‘ZIGA XOS XUSUSIYATLARI VA TURLARI

Axborot texnologiyalari sohasidagi jinoyatlar tushunchasi O‘zbekiston qonunchiligida kompyuter texnikasi, axborot tizimlari va telekommunikatsiya tarmoqlaridan foydalangan holda yoxud ularga qarshi sodir etiladigan ijtimoiy xavfli qilmishlarni anglatadi. Poytaxt hududida huquqni muhofaza qiluvchi organlar amaliyotining tahlili quyidagi asosiy kiberjinoyat turlarini ajratib ko‘rsatish imkonini beradi.

1.1. Bank plastik kartalari va onlayn to‘lovlar bilan bog‘liq firibgarlik

Bugungi kunda mulkiy kiberjinoyatlarning eng salmoqli qismi aynan moliya sektoriga to‘g‘ri keladi. Toshkent shahrida plastik kartalardan pul o‘g‘irlashning quyidagi usullari keng tarqalgan:

- **Telefon firibgarligi (Vishing):** Jinoyatchilar o‘zini bankning xavfsizlik xizmati yoki to‘lov tizimlari ("Click", "Payme") xodimi deb tanishtirib, jabrlanuvchining ishonchiga kiradi. Ular IP-telefoniya yordamida rasmiy raqamlarga o‘xshash (spoofing) raqamlardan qo‘ng‘iroq qilib, "hisob raqamingizga hujum bo‘lyapti", "kredit rasmiylashtirilmoqda" degan vajlar bilan SMS orqali kelgan maxfiy kodni qo‘lga kiritadilar.
- **Fishing (Phishing) va zararli havolalar:** Telegram guruhlari va SMS xabarnomalar orqali davlat tomonidan moddiy yordam tarqatilayotgani, yirik savdo tarmoqlarida yutuqli o‘yinlar bo‘layotgani haqidagi soxta xabarlar tarqatiladi. Foydalanuvchi ko‘rsatilgan havolaga o‘tib, o‘z karta ma’lumotlarini kiritishi bilanoq pullaridan ayriladi.
- **Onlayn e'lonlar platformalaridagi sxemalar:** "OLX" va boshqa e'lonlar platformalarida o‘zini xaridor qilib ko‘rsatgan firibgarlar sotuvchiga pulni oldindan tashlab berishini aytib, karta tasdiqlanishi uchun soxta veb-saytga yo‘naltiradi. Sotuvchi o‘z ma'lumotlarini kiritgach, uning hisobi jinoyatchilar boshqaruviga o‘tadi.

1.2. Ijtimoiy tarmoqlar va messenjerlar orqali amalga oshiriladigan huquqbuzarliklar

Toshkent shahri yoshlari va aholisi o‘rtasida ommalashgan Instagram, Telegram kabi tarmoqlarda shaxs daxlsizligiga qarshi huquqbuzarliklar ortib bormoqda:

- **Akkauntlarni egallab olish:** Fuqarolarning messenjerlardagi akkauntlariga ruxsatsiz kirib (ikkitomonlama autentifikatsiyasi bo'lmagan profillarni buzish orqali), ularning nomidan qarindoshlari va do‘stlariga shoshilinch ravishda pul so‘rab xabar yuborish.

- **Kiber-tovlamachilik va Sextortion:** Jabrlanuvchining shaxsiy yozishmalari, foto yoki videolarini yashirin yo‘llar bilan qo‘lga kiritib, ularni ijtimoiy tarmoqlarda tarqatish bilan tahdid qilish va buning evaziga yirik miqdorda pul talab qilish. Ushbu jinoyat turi, ayniqsa, ma'naviy-psixologik jihatdan o‘ta og‘ir oqibatlarni (jumladan, jabrlanuvchining tushkunlikka tushishi va o‘z joniga qasd qilishi kabi holatlarni) keltirib chiqarishi mumkin.

1.3. Nolegal investitsion platformalar va moliyaviy piramidalar

Axborot makonida kriptovalyuta, qimmatli qog‘ozlar yoki valyuta birjalarida (Forex) "kofolatli daromad" va'da qiluvchi soxta platformalar faoliyati avj olmoqda. Aholining moliyaviy-huquqiy savodxonligi yetishmasligidan foydalangan jinoyatchilar yorqin reklamalar ostida fuqarolarning pullarini jalb qilib, qisqa muddatdan so‘ng resurslarni o‘chirib yuborishmoqda.

KIBERJINOYATLARNING OLDINI OLISH ASOSLARI: PROFILAKTIKA MEXANIZMLARI

Har qanday jinoyatni tergov qilib, jinoyatchini jazolagandan ko‘ra, uni sodir bo‘lishi uchun shart-sharoitlarni bartaraf etish jamiyat uchun ancha samarali va iqtisodiy jihatdan foydalidir. Kiberjinoyatlar profilaktikasi ko‘p qatlamli bo‘lib, u umumiy, maxsus va yakka tartibdagi profilaktik choralarni o‘z ichiga oladi.

2.1. Umumiy va ijtimoiy profilaktika: Raqamli immunitetni shakllantirish

Kriminologik izlanishlar shuni ko‘rsatadiki, aksariyat kiberjinoyatlar yuqori texnologik murakkablikka ega kompyuter dasturlari orqali emas, balki "Ijtimoiy injiniring" – inson psixologiyasini boshqarish orqali amalga oshiriladi. Shu sababli, oldini olishning eng asosiy poydevori aholining "raqamli gigiyena" madaniyatini yuksaltirishdir. Huquqni muhofaza qiluvchi organlar, ta'lim muassasalari va OAV hamkorligida aholini firibgarlarning yangi sxemalaridan tezkorlik bilan xabardor qilish mexanizmi yaratilishi kerak. Toshkent shahridagi har bir mahalla tizimida profilaktika inspektorlari faqatgina an'anaviy jinoyatlar haqida emas, virtual

xavfsizlik qoidalari (parollarni himoyalash, noma'lum havolalarga kirmaslik) bo‘yicha tushuntirish ishlarini olib borishi profilaktikaning birlamchi bosqichi hisoblanadi.

2.2. Maxsus-kriminologik va texnologik profilaktika (High-tech policing)

Kiberjinoyatchilikka qarshi kurashda Ichki ishlar organlari ilg‘or axborot texnologiyalaridan unumli foydalanishni yo‘lga qo‘ymoqda. Toshkent shahrida ushbu yo'nalishda amaliyotga tatbiq etilayotgan va takomillashtirilayotgan bir necha asosiy yo‘nalishlarni qayd etish mumkin:

- **Face-ID va intellektual videokuzatuv orqali "dropper"larni aniqlash:** Kiberjinoyatlarni sodir etuvchilar asosan pulni naqdlashtirish uchun vositachilardan ("dropper"lardan) foydalanadi. Ular jabrlanuvchining pulini vaqtincha ochilgan kartalarga o‘tkazib, shahardagi turli bankomatlardan naqd pul yechib oladi. "Xavfsiz shahar" tizimi va bankomatlardagi kameralarni sun'iy intellekt hamda Face-ID texnologiyalariga integratsiya qilish orqali jinoyat vositachilarining shaxsini sanoqli soniyalarda aniqlash imkoniyati yuzaga keldi. Bu nafaqat jinoyatni issiq izidan ochishga, balki jinoyatchilar orasida "baribir topib olishadi" degan qo‘rquvni uyg‘otish orqali profilaktik effekt (tiyib turish) beradi.
- **Raqamli izlarni (Digital footprint) tahlil qilish:** OSINT (ochiq manbalar razvedkasi) texnologiyalari orqali tarmoqda shubhali havolalar, noqonuniy xizmatlarni taklif etuvchi guruhlarni yopib borish va domenlarni bloklash bevosita jinoyat qurbonlari sonining kamayishiga olib keladi.

HUQUQBUZARLIKLAR PROFILAKTIKASINING MA'MURIY-HUQUQIY MEXANIZMLARI VA ULARNI TAKOMILLASHTIRISH

Jinoyat huquqi sohasidagi eng muhim aksiomalardan biri shuki, ma'muriy huquqbuzarlik va jinoyat o‘rtasida nozik chegara mavjud bo‘lib, ko‘pincha ma'muriy javobgarlikka tortilmagan, o‘z harakati uchun sanksiya olmagan huquqbuzar oxir-oqibat og‘ir jinoyatga qo‘l uradi. Shu sababli, kiberjinoyatlarning

oldini olish bevosita ma'muriy-huquqiy normalarni to‘g‘ri qo‘llashga borib taqaladi.

3.1. E-Ma'muriy ish: Elektron ma'muriy bayonnomalar amaliyoti

Huquqbuzarliklarni qayd etishning tezkorligi va jazo muqarrarligini ta'minlash maqsadida joriy etilgan "E-Ma'muriy ish" yagona axborot tizimi profilaktika ishlarida inqilobiy ahamiyatga ega. Huquqni muhofaza qiluvchi organ xodimlari tomonidan ijtimoiy tarmoqlardagi mayda bezoriliklar yoxud fuqarolarning osoyishtaligiga virtual makonda raxna soluvchi harakatlarni joyning o‘zida elektron planshetlar orqali bayonnoma rasmiylashtirish – sudga qadar ishlarni tezlashtirdi hamda raqamli dalillarning yo‘qolib ketishining oldini oldi. Bu tizim orqali qoidabuzar to‘g‘risidagi bazaviy ma’lumotlar yagona markazda to‘planib, kriminologik tahlil uchun muhim empirik baza vazifasini o‘tamoqda.

3.2. Ma'muriy javobgarlik to‘g‘risidagi kodeksini (MJtK) yangi voqelikka moslashtirish

Bugungi kunda qonunchilikda kiberjinoyatlarning muqaddimasi bo‘lib xizmat qiladigan qator xavfli harakatlar ma'muriy-huquqiy tartibga solinmagan. Kiberjinoyatlar profilaktikasini ma'muriy huquq doirasida mustahkamlash uchun quyidagi o‘zgartirishlarni kiritish talab etiladi:

1. **Fishing havolalarni va zararli kodlarni yaratish yoxud tarqatish uchun ma'muriy javobgarlik:** Amaldagi jinoyat qonunchiligi (JK 168-modda yoki XX-bob) qilmish oqibatida jiddiy moddiy zarar yuzaga kelishini nazarda tutadi. Biroq, biror shaxs ijtimoiy tarmoq guruhiga soxta bank havolasini tashlasa-yu, hali hech kim aldanmagan bo‘lsa, uni jinoyat ustida ushlash murakkab. Shuning uchun MJtKga "Axborot tizimlaridan firibgarlik maqsadida foydalanishga tayyorgarlik ko‘rish yoxud aldamchi elektron havolalar tarqatish" kabi modda kiritilishi profilaktik ahamiyatga ega bo‘ladi.

2. **Kiber-bezorilik (Cyberbullying) va Kiber-ta'qib (Cyberstalking) qilmishlarini tartibga solish:** MJtKning 41-moddasi (Haqorat qilish) va 183-moddasi (Mayda bezorilik) virtual makondagi tajovuzlarni to‘liq qamrab olmaydi. Shaxsni ijtimoiy tarmoqda doimiy ta'qib qilish, o‘z akkauntlaridan uning nomiga doimiy ravishda tahdidli xabarlar yuborish kabi harakatlar uchun maxsus ma'muriy javobgarlik belgilanmas ekan, bu harakatlar jinsiy erkinlikka yoki mulkka qarshi jinoyatlarga aylanib ketish xavfi saqlanib qoladi.

3. **Sim-kartalar va bank hisoblaridan noqonuniy (vositachi sifatida) foydalanish:** Bugungi kunda "dropper"lar (o‘z kartasini ma'lum haq evaziga firibgarlarga ijaraga beruvchilar) o‘zini jabrlanuvchi qilib ko‘rsatib javobgarlikdan qutulib qolmoqda. O‘ziga tegishli bo‘lgan elektron to‘lov vositalari (kartalar) va aloqa vositalarini qonunga xilof harakatlar amalga oshirilishini bila turib uchinchi shaxslarga berganlik uchun qat'iy ma'muriy javobgarlik kiritilishi qora bozorning "qon tomiri"ni kesishga xizmat qiladi.

XORIJIY TAJRIBA VA MILLIY AMALIYOT INTEGRATSIYASI

Toshkent shahrida huquqbuzarliklar profilaktikasini kuchaytirishda muvaffaqiyatli xorijiy modellarni o‘rganish maqsadga muvofiqdir. Masalan, Singapur va Janubiy Koreya davlatlarida moliya institutlari va huquq-tartibot idoralari o‘rtasidagi "API" (dasturiy interfeys) integratsiyasi to‘liq yakunlangan. Agar fuqaroning hisobidan g‘ayrioddiy manzildan, g‘ayrioddiy vaqtda yirik miqdorda pul ko‘chirilayotgan bo‘lsa, tizim buni shubhali operatsiya deb baholaydi va tranzaksiyani muzlatib, avtomatik ravishda fuqaroning telefoniga ovozli yoki biometrik tasdiq yuboradi.

Shuningdek, Estoniyada qo‘llaniladigan "E-Police" tizimi orqali patrul politsiyasi hududdagi har qanday IP-manzildan yuborilayotgan xavfli so‘rovlarni

onlayn tahlil qila oladi. O‘zbekiston sharoitida ham bank sirini saqlagan holda, shubhali tranzaksiyalar (xususan, VPN orqali xorijdan turib boshqarilayotgan IP-manzillar orqali kartaga kirish) to‘g‘risida Ichki ishlar organlarining axborot tizimiga tezkor (inson omilisiz) avtomatlashtirilgan xabarnoma yuborish protokolini tasdiqlash muhim ahamiyatga ega.

XULOSA

Xulosa qilib ta’kidlash lozimki, Toshkent shahrida sodir etilayotgan kiberjinoyatlar – bu an'anaviy jinoyatchilikning raqamli muhitga ko‘chgan formati bo‘lib, o‘zining yuqori tashkilotiyligi, moslashuvchanligi va masofaviyligi bilan ajralib turadi. Ijtimoiy injiniring, onlayn firibgarlik va kiber-tovlamachilik poytaxt aholisining asosiy huquqiy va iqtisodiy xavfsizligiga tahdid soluvchi ochiq xavfga aylangan.

Ushbu muammoga qarshi faqat jazolash instituti orqali kurashib bo‘lmaydi. Kriminologik tadqiqotlar nuqtai nazaridan yondashganda, ushbu jarayonda davlatning asosiy e'tibori jinoiy qilmishlarni erta bosqichda to‘xtatishga, ya'ni huquqbuzarliklar profilaktikasiga va ma'muriy-huquqiy preventiv choralarga qaratilishi lozim.

Kelgusida Toshkent shahrida kiberjinoyatchilikning oldini olish samaradorligini oshirish uchun quyidagi ustuvor vazifalarni amalga oshirish taklif etiladi:

1. **Qonunchilikni takomillashtirish:** O‘zbekiston Respublikasining Ma'muriy javobgarlik to‘g‘risidagi kodeksiga zararli axborotlarni tarqatish, ruxsatsiz portlarni skanerlash, fishing, shuningdek, shaxsiy kartalardan uchinchi shaxslarga jinoyat sodir etishi uchun foydalanishga ruxsat berganlik uchun tegishli normalarni kiritish;
2. **Raqamli vositalarni kengaytirish:** Huquqni muhofaza qiluvchi organlar amaliyotiga raqamli politsiya (High-tech policing)

usullarini keng joriy etish, xususan, "E-Ma'muriy ish" tizimiga sun'iy intellekt modulini o‘rnatib, ehtimoliy huquqbuzarlarning psixologik-ijtimoiy portretini yaratish, Face-ID orqali shubhali bankomat operatsiyalarini onlayn bloklash tizimini moliya tashkilotlari bilan birgalikda ishlab chiqish.

3. **Idoralararo hamkorlik:** Ichki ishlar vazirligi akademiyasi kursantlari va amaliyot xodimlarini kiberxavfsizlik va axborot texnologiyalari sohasidagi malakasini muttasil oshirib borish, elektron dalillarni yig‘ish va tahlil qilish bo‘yicha amaliy mashg‘ulotlarni zamonaviy trenajerlar yordamida olib borish.

4. **Aholining raqamli huquqiy savodxonligi:** Ommaviy axborot vositalari va ta'lim maskanlarida maxsus ijtimoiy roliklar va darsliklar orqali jamiyatda xavfsiz internet madaniyatini shakllantirish profilaktikaning asosi bo‘lib qolishi shart.

Ushbu vazifalarning kompleks amalga oshirilishi Toshkent shahrida raqamli muhitning xavfsizligini kafolatlashga, fuqarolarning huquqlari va mol-mulkini kiberjinoyatchilar xurujlaridan samarali himoya qilishga hamda qonun ustuvorligini mustahkamlashga xizmat qiladi.

REFERENCES:

1. **O‘zbekiston Respublikasi Konstitutsiyasi.** – T.: "O‘zbekiston", 2023.
2. **O‘zbekiston Respublikasining Jinoyat kodeksi.** (01.01.2024 yil holatiga ko‘ra). Qonunchilik ma'lumotlari milliy bazasi - Lex.uz.
3. **O‘zbekiston Respublikasining Ma'muriy javobgarlik to‘g‘risidagi kodeksi.** Qonunchilik ma'lumotlari milliy bazasi - Lex.uz.
4. O‘zbekiston Respublikasining 2022-yil 15-apreldagi "Kiberxavfsizlik to‘g‘risida"gi O‘RQ-764-son Qonuni.

5. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi "Raqamli O‘zbekiston — 2030" strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida"gi PF-6079-son Farmoni.
6. **Rustamboyev M.H.** O‘zbekiston Respublikasi Jinoyat huquqi kursi. Maxsus qism. Darslik. – T.: ILM ZIYO, 2018.
7. **Ismoilov I., Ziyodullayev M.Z.** Huquqbuzarliklar profilaktikasi va jinoyatchilikka qarshi kurashishning nazariy-huquqiy muammolari. – T.: IIV Akademiyasi, 2019.
8. **Odilov N.K.** Axborot texnologiyalari sohasidagi jinoyatlarni tergov qilish metodikasi. – T.: IIV Akademiyasi nashriyoti, 2021.
9. **Mavlonov N.** Kiber makonda huquqbuzarliklar profilaktikasini tashkil etishning ma'muriy-huquqiy mexanizmlari: muammo va yechimlar. (Ilmiy maqola). // Huquq va burch, 2023-yil.
10. **Broadhurst, R.** (2021). *Cybercrime: Criminological and Legal Perspectives*. International Journal of Law and Technology.
11. **Nomozov, A.** Kiberjinoyatchilikning oldini olishda raqamli texnologiyalar (Face-ID va OSINT) imkoniyatlari. // O‘zbekiston qonunchiligi tahlili. – T., 2023. № 4.
12. "Scientific Conference Open Proceedings" (SCOP) materials on Administrative Responsibility and Modern Law Enforcement Strategies. Tashkent, 2026. (OJS-indexed).