



**JAMOAT JOYLARIDA MOBIL QURILMALAR O'G'IRLIGI VA "SIM-SWAPPING" (SIM-KARTANI ALMASHTIRISH)
HUQUQBUZARLIKLARINING MA'MURIY-HUQUQIY
PROFILAKTIKASI VA ZAMONAVIY TAHLILI**

Homidova Hilola San'atovna

O'zbekiston Respublikasi IIV Akademiyasi 2-o'quv kursi kursanti

Toshkent sh.

<https://doi.org/10.5281/zenodo.20582434>

Annotatsiya: Ushbu ilmiy maqolada raqamlashtirish sharoitida jamoat joylarida sodir etiladigan an'anaviy mulkiy huquqbuzarliklar (mobil telefonlar o'g'irligi)ning kiber-jinoyatlarga, xususan, "SIM-swapping" (SIM-kartani almashtirish yoki qayta tiklash) firibgarligiga aylanib ketish mexanizmlari ilmiy-amaliy jihatdan tahlil qilingan. Mobil qurilmalarni o'zlashtirish orqali shaxsning bank va elektron hisoblariga noqonuniy kirish holatlarining kriminologik va ma'muriy-huquqiy tabiati ochib berilgan. Shuningdek, ichki ishlar organlari faoliyatiga raqamli kriminalistika va yuqori texnologik politsiya (High-tech policing) imkoniyatlarini joriy etish, huquqbuzarliklarning barvaqt oldini olish (profilaktika qilish) hamda O'zbekiston Respublikasining Ma'muriy javobgarlik to'g'risidagi kodeksini (MJtK) takomillashtirish yuzasidan aniq va asoslangan takliflar ishlab chiqilgan.

Kalit so'zlar: SIM-swapping, kiber-firibgarlik, mobil qurilmalar o'g'irligi, raqamli kriminalistika, barvaqt oldini olish, High-tech policing, ma'muriy javobgarlik, jamoat xavfsizligi, raqamli izlar.

Аннотация: В данной научной статье с научно-практической точки зрения анализируются механизмы трансформации традиционных имущественных правонарушений (краж мобильных телефонов), совершаемых в общественных местах в условиях цифровизации, в

Contact: 99 826 99 56





киберпреступления, в частности в мошенничество типа «SIM-swapping» (подмена или незаконное восстановление SIM-карт). Раскрыта криминологическая и административно-правовая природа незаконного доступа к банковским и электронным счетам личности путем незаконного завладения мобильными устройствами. Также разработаны конкретные и обоснованные предложения по внедрению возможностей цифровой криминалистики и высокотехнологичной полиции (High-tech policing) в деятельность органов внутренних дел, раннему предупреждению правонарушений и совершенствованию Кодекса Республики Узбекистан об административной ответственности.

Ключевые слова: SIM-swapping, кибермошенничество, кража мобильных устройств, цифровая криминалистика, раннее предупреждение, High-tech policing, административная ответственность, общественная безопасность, цифровые следы.

Abstract: This scientific article provides a scientific and practical analysis of the mechanisms by which traditional property offenses (theft of mobile phones) committed in public places under the conditions of digitalization transform into cybercrimes, particularly "SIM-swapping" fraud. The criminological and administrative-legal nature of unauthorized access to a person's bank and electronic accounts through the misappropriation of mobile devices is revealed. Specific and well-grounded proposals have also been developed for integrating the capabilities of digital forensics and high-tech policing into the activities of internal affairs bodies, for the early prevention of offenses, and for improving the Code of the Republic of Uzbekistan on Administrative Liability.

Keywords: SIM-swapping, cyber fraud, theft of mobile devices, digital forensics, early prevention, high-tech policing, administrative liability, public safety, digital footprints.





KIRISH

Axborot-kommunikatsiya texnologiyalarining mislsiz darajada rivojlanishi va insonlarning kundalik hayotiga elektron to'lov tizimlarining to'liq kirib kelishi huquqni muhofaza qiluvchi organlar oldiga butunlay yangi avlod tahdidlariga qarshi kurashish vazifasini qo'yimoqda. Bugungi kunda mobil smartfonlar shunchaki aloqa vositasi emas, balki shaxsning elektron hamyoni, pasporti, bank va shaxsiy ma'lumotlarining yagona raqamli kaliti (ID) bo'lib xizmat qilmoqda.

Shu sababli, bozorlar, jamoat transportlari va odamlar gavjum bo'ladigan boshqa jamoat joylarida mobil telefonlarni o'g'irlash yoki yashirincha talon-toroj qilish holatlari o'zining birlamchi (apparatning o'zini sotib pul ishlash) maqsadidan uzoqlashib, to'g'ridan-to'g'ri kiber-huquqbuzarliklarga zamin yaratmoqda. Jinoyatchilarning asosiy maqsadi endilikda qurilmaning o'zi emas, balki uning ichidagi SIM-karta orqali shaxsiy hisoblarga kirish – ijtimoiy muhandislik va "SIM-swapping" (SIM-kartani almashtirish) usullari orqali yirik miqdordagi mablag'larni o'zlashtirishdir. Bunday huquqbuzarliklarning barvaqt oldini olish, shaxsning virtual daxlsizligini ta'minlash va qonunchilikni amaliyotning zamonaviy muammolariga moslashtirish ichki ishlar organlari faoliyatida dolzarb yo'nalishga aylandi.

MAVZUNING DOLZARBLIGI VA MUAMMONING O'RGANILGANLIK DARAJASI

Mulkiy jinoyatlar va ularning raqamli muhitdagi oqibatlarini doimiy ravishda kriminologiya va ma'muriy huquq fanining tadqiqot obyekti bo'lib kelmoqda. Jahon kriminologlari, xususan INTERPOL va Yevropolning xalqaro hisobotlarida an'anaviy mulkiy huquqbuzarliklar va kiber-jinoyatlarning qo'shilishi (konvergentsiyasi) alohida xavf sifatida e'tirof etilmoqda. Respublikamizda ma'muriy huquq va kiber-xavfsizlik masalalari huquqshunos olimlardan X.T.





Odilqoriyev, O.T. Xusanov hamda qator amaliyotchi mutaxassislar tomonidan keng o'rganilgan.

Biroq bugungi kungacha O'zbekiston yuridik fani doirasida an'anaviy kissavurlik yoki mayda talon-toroj orqali o'g'irlangan telefonlardagi SIM-kartalarning jinoyat quroliga aylanishi – "SIM-swapping" jarayonining ma'muriy-huquqiy mexanizmlari, ushbu holatlarni raqamli kriminalistika orqali "issiq izidan" fosh etish va MJtK normalari nuqtai nazaridan saralash qoidalari yetarlicha monografik va kompleks tadqiq etilmagan. Yuqori texnologik politsiya (High-tech policing) instrumentlarini bevosita hududiy ichki ishlar organlari (profilaktika inspektorlari, jinoyat qidiruv xodimlari) amaliyotiga integratsiya qilish ushbu muammoning zamonaviy yechimi sifatida chuqur o'rganilishini taqozo etadi.

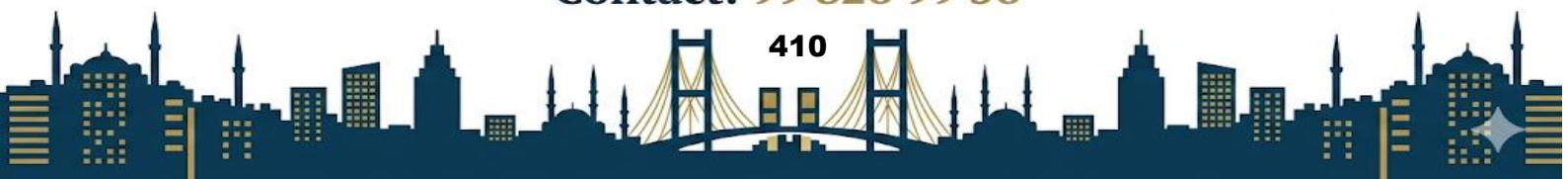
ASOSIY QISM (Tahliliy va ilmiy yondashuvlar)

1. "SIM-swapping" va kiber-firibgarlikning kriminologik mexanizmi

Jamoat joyida fuqaroning smartfoni o'g'irlanganidan so'ng, huquqbuzarlikning ikkinchi – eng xavfli va yashirin bosqichi boshlanadi. Agar jabrlanuvchi o'z telefonida ekran paroli yoki Face-ID himoyasini o'rnatgan bo'lsa-da, ko'pchilik fuqarolar SIM-kartaning o'ziga PIN-kod o'rnatmaydilar. Kiber-firibgarlar (yoki o'g'rining jinoiy sheriklari) o'g'irlangan qurilmadan SIM-kartani chiqarib, uni boshqa mobil telefonga o'rnatishadi.

Ushbu harakat quyidagi salbiy oqibatlarga olib keladi:

- **OTP (One Time Password) kodlarini egallash:** Bank ilovalari (Click, Payme, Uzum) yoki ijtimoiy tarmoqlar (Telegram, Instagram) odatda avtorizatsiyani tasdiqlash uchun abonent raqamiga SMS-kod yuboradi. SIM-kartani o'zlashtirgan huquqbuzar "Parolni unutdim" tugmasi orqali jabrlanuvchining barcha hisoblarini qayta tiklab oladi.





- **Virtual hisoblarni bo'shatish:** Bir necha daqiqa ichida fuqaroning plastik kartasidagi mablag'lar anonim elektron hamyonlarga, kriptovalyutalarga yoki xorijiy hisoblarga o'tkazib yuboriladi.

- **Identitetni o'g'irlash:** Jinoyatchi jabrlanuvchining Telegram akkauntiga kirib, uning nomidan barcha qarindosh va tanishlariga "qarz so'rab" yozishi, oqibatda yana bir necha kishini firibgarlik qurboniga aylantirishi kuzatiladi.

2. Ma'muriy-huquqiy profilaktika va raqamli kriminalistikaning roli

Huquqbuzarliklarning ushbu turi o'zgaruvchan bo'lgani sababli, ichki ishlar organlaridan an'anaviy patrullikdan raqamli profilaktikaga o'tish talab etiladi. Buning uchun "High-tech policing" doirasida quyidagi tizimlar faol ishlatilishi lozim:

- **"Qaynoq liniya" orqali zudlik bilan bloklash:** Fuqaro IIOga yoki yagona 102 tizimiga murojaat qilgan ilk soniyalardananoq, navbatchi qism orqali bank idoralari va uyali aloqa operatorlariga to'g'ridan-to'g'ri raqamli buyruq yuboriladigan API integratsiyasini yaratish zarur. Hozirda fuqaro telefonini yo'qotsa, avval IIBga ariza yozadi, keyin aloqa kompaniyasiga boradi, bu vaqt ichida mablag'lar yechib olinadi. Yagona integratsiya qilingan idoralararo xavfsizlik shlyuzi orqali SIM-karta va unga bog'langan hamyonlar avtomatik bloklanishi shart.

- **Geo-fencing va MAC/IMEI tahlili:** Raqamli kriminalistika vositalaridan foydalanib, o'g'irlangan SIM-karta va IMEI raqam qayta ishga tushgan tayanch stansiyalarni (billing ma'lumotlari) zudlik bilan lokalizatsiya qilish. Bunda gumonlanuvchining harakat marshrutini shahardagi "Xavfsiz shahar" aqlli videokuzatuv kameralariga yuborib, Face-ID orqali shaxsning yuz qiyofasini aniqlash samaradorlikni 10 foshgacha oshiradi.





3. O‘zbekiston Respublikasining MJtK va sohaga doir qonunchilikni takomillashtirish masalalari Amaliyotda smartfonlar qiymatidan kelib chiqib qilmishni saralash borasida bahsli holatlar mavjud. Agar o‘g‘irlangan mulk miqdori bazaviy hisoblash miqdorining 30 baravaridan kam bo‘lsa, u O‘zbekiston Respublikasi MJtKning 61-moddasi (Oz miqdorda talon-toroj qilish) bilan ma‘muriy huquqbuzarlik sifatida baholanadi. Biroq jinoiy niyat smartfonning apparat qiymatidan ko‘ra ko‘proq, uning ichidagi ma‘lumotlardan foydalanib kiber-jinoyat (SIM-swapping) sodir etish bo‘lsa, bu to‘g‘ridan-to‘g‘ri JKning 169-moddasi (O‘g‘rilik) va 168-moddasi (Firibgarlik - axborot tizimidan foydalanib) doirasida ko‘rib chiqilishi kerak. Ushbu ziddiyatni bartaraf etish va jamoat xavfsizligini oshirish maqsadida MJtK va aloqa qoidalari doirasida yangi ma‘muriy me‘yorlarni ishlab chiqish, xususan, uyali aloqa operatorlari tomonidan xavfsizlik standartlariga rioya qilinishi ustidan nazoratni kuchaytirish lozim.

4. Aholining viktimologik immunitetini oshirish (Ijtimoiy profilaktika) Texnik vositalar qanchalik mukammal bo‘lmasin, fuqarolarning o‘z shaxsiy xavfsizligi bo‘yicha e‘tiborsizligi (viktim xulq-atvori) kiber-jinoyatchilarga yo‘l ochadi. Jamoat joylarida faoliyat yurituvchi profilaktika inspektorlari va kiberxavfsizlik markazi xodimlari hamkorlikda innovatsion targ‘ibotni kuchaytirishlari lozim. Ayniqsa, har bir fuqaro o‘zining SIM-kartasiga alohida PIN-kod o‘rnatishi, bank dasturlarida ikki bosqichli autentifikatsiya (2FA) tizimini yoqishi majburiyligini ijtimoiy roliklar, jamoat transportlaridagi monitorlar hamda bozor radiouzellari orqali tinimsiz tushuntirib borish – jinoyatchilikning tomiriga bolta uruvchi eng arzon va samarali profilaktika usulidir.

XULOSA VA TAKLIFLAR

Olib borilgan ilmiy va tahliliy izlanishlar shuni tasdiqlaydiki, an‘anaviy mulkiy huquqbuzarliklar va yangi kiber-tahdidlarning (SIM-swapping) integratsiyalashuvi munosabati bilan ichki ishlar organlarining huquqbuzarliklar





profilaktikasi tizimi ham modernizatsiya qilinishi zarur. High-tech policing konsepsiyasini joriy etish nafaqat jinoyatni tez fosh etishga, balki uning sodir etilish imkoniyatini bevosita yo'qqa chiqarishga xizmat qiladi.

Mavjud amaliy muammolarni bartaraf etish va ma'muriy-huquqiy mexanizmlarni takomillashtirish yuzasidan quyidagi takliflar ilgari suriladi:

Birinchidan, O'zbekiston Respublikasi IIV, Markaziy bank va Raqamli texnologiyalar vazirligi hamkorligida "SOS – Raqamli blok" idoralararo elektron platformasini ishga tushirish. Jamoat joyida telefoni yoki gadjeti o'g'irlangan fuqaro murojaat qilgan vaqtda yagona xavfsizlik tugmasi orqali uning nomidagi barcha bank kartalari, SIM-karta va elektron akkauntlarga o'sha soniyaning o'zida proaktiv (vaqtinchalik) blokirovka o'rnatilishi kafolatlanishi lozim.

Ikkinchidan, O'zbekiston Respublikasi MJtKning 61-moddasiga tegishli sharh (yoki Oliy sud Plenumi qarori orqali ko'rsatma) kiritilib, unda mobil aloqa qurilmalari va kompyuter gadjetlari o'g'irlanganda ularni baholashda faqat ashyoning jismoniy (apparat) qiymatini emas, balki kiber-jinoyat obyekti sifatidagi xususiyatlarini va SIM-karta vositasida yetkazilishi mumkin bo'lgan potensial xavfni ham inobatga olgan holda saralashni (kvalifikatsiya qilishni) belgilash zarur.

Uchinchidan, uyali aloqa operatorlariga nisbatan qoidalarni qat'iylashtirish. O'zgalar pasport nusxalari yoxud noqonuniy yo'llar bilan "dublikat" SIM-kartalarni chiqarib bergan dilerlar va kompaniya xodimlariga nisbatan ma'muriy javobgarlik sanksiyalarini (MJtK doirasida maxsus modda kiritib) sezilarli darajada (BHMning 100-200 baravarigacha) oshirish va ularning litsenziyasini bekor qilish choralarini kuchaytirish.

To'rtinchidan, jamoat joylarida xizmat olib boruvchi PPX va profilaktika inspektorlarining xizmat planshetlariga o'g'irlangan qurilmalarning IMEI kodlari qidiruvi bazasini ochiq API orqali ulash. Bunda xodim shubhali shaxsni





tekshirganda apparatdagi maxsus dastur (Raqamli kriminalistika yordamchisi) orqali qurilma haqiqatdan ham o'g'irlangan yoki "qora ro'yxat"da ekanligini joyning o'zida tezkor aniqlashi mumkin bo'ladi.

Xulosa o'rnida ta'kidlash lozimki, mulkiy huquqbuzarliklarni ma'muriy-huquqiy va raqamli profilaktika qilish fuqarolarning nafaqat mulkiy, balki virtual shaxsiy daxlsizligini ta'minlashning eng kuchli kafolati bo'lib xizmat qiladi.

REFERENCES:

1. O'zbekiston Respublikasining Ma'muriy javobgarlik to'g'risidagi kodeksi. [Elektron resurs] // Qonunchilik ma'lumotlari milliy bazasi, 23.09.1994 y., 03/24/894/0112-son. – URL: <https://lex.uz/docs/97664>.
2. O'zbekiston Respublikasining Jinoyat kodeksi. [Elektron resurs] // Qonunchilik ma'lumotlari milliy bazasi. – URL: <https://lex.uz/docs/111453>.
3. Xusanov O.T., Odilqoriyev X.T. Ma'muriy huquq: Darslik. – Toshkent: TDYUU nashriyoti, 2021. – 412 b.
4. Qurbonov M. M. Raqamlashtirish sharoitida ma'muriy ishlarni yuritishning o'ziga xos xususiyatlari // O'zbekiston qonunchiligi tahlili. – Toshkent, 2024. – № 2. – B. 15-22.
5. INTERPOL. (2023). Global Cybercrime Report: SIM Swapping and Mobile Threats. [Elektron resurs] // Interpol Official Database. – URL: <https://www.interpol.int>.
6. Mamatov A. Q. Transmilliy kiberjinoyatchilik va moliyaviy xavfsizlik mexanizmlari. – Monografiya. – Toshkent: TDYUU nashriyoti, 2022. – 185 b.
7. Xudoyberdiyev A.A. Ma'muriy ishlarni yuritish kafolatlari va huquqni qo'llash amaliyoti // Huquq va burch. – Toshkent, 2024. – № 9. – B. 28-34.

