SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

# KIBERJINOYATCHILIK VA KRIPTO-AKTIVLAR: RAQAMLI MAKONDA XAVFSIZLIK VA HUQUQIY TARTIBGA SOLISH MUAMMOLARI

**Ro’ziyev Javoxirbek Saidjon o’g’li**

*O’zbekiston Respublikasi IIV Akademiyasi kursanti*

*Toshkent. sh*

https://doi.org/10.5281/zenodo.20593298

**Annotatsiya:** Ushbu ilmiy maqolada raqamli makonda kriminogen barqarorlikni ta’minlash, xususan, "Darknet" yashirin tarmog‘ida keng tarqalgan kiber-ekstremizm va shaxsga doir ma’lumotlarning noqonuniy savdosiga qarshi kurashishning ma’muriy-huquqiy va texnik mexanizmlari kompleks tahlil qilingan. Kiberjinoyatchilar tomonidan qora bozorda xarid qilingan ma’lumotlar asosida amalga oshirilayotgan "SIM-swapping" (SIM-kartani almashtirish) kabi yuqori texnologik huquqbuzarliklarning yuridik tabiati ochib berilgan. Muammoni hal etishda AQSh, Buyuk Britaniya, Germaniya va Janubiy Koreya kabi rivojlangan xorijiy davlatlar tajribasi (xorij tajribasi) qiyosiy o‘rganilib, O‘zbekiston Respublikasi ichki ishlar organlari faoliyatiga "High-tech policing" (yuqori texnologik politsiya) konsepsiyasini va "E-Ma’muriy ish" tizimini chuqur integratsiya qilish yuzasidan ilmiy-amaliy takliflar ishlab chiqilgan.

**Kalit so‘zlar:** Darknet, kiber-ekstremizm, shaxsga doir ma’lumotlar, SIM-swapping, kriminogen barqarorlik, High-tech policing, ma’muriy huquqbuzarlik, xorij tajribasi, E-Ma’muriy ish.

**Аннотация:** В данной научной статье представлен комплексный анализ административно-правовых и технических механизмов обеспечения криминогенной стабильности в цифровом пространстве, в частности, борьбы с кибрэкстремизмом и незаконной торговлей персональными данными, широко распространенными в скрытой сети «Даркнет». Раскрыта юридическая природа таких высокотехнологичных правонарушений, как «SIM-swapping» (подмена SIM-карты), осуществляемых на основе данных, приобретенных киберпреступниками на черном рынке. Для решения проблемы проведен сравнительный анализ опыта развитых зарубежных стран, таких как США, Великобритания, Германия и Южная Корея, и разработаны научно-практические предложения по глубокой интеграции концепции «High-tech policing» (высокотехнологичная полиция) и системы «Е-Административное дело» в деятельность органов внутренних дел

Республики Узбекистан.

**Ключевые слова:** Даркнет, киберэкстремизм, персональные данные, SIM-swapping, криминогенная стабильность, High-tech policing, административное правонарушение, зарубежный опыт, Е-Административное дело.

**Abstract:** This scientific article provides a comprehensive analysis of the administrative, legal, and technical mechanisms for ensuring criminogenic stability in the digital space, specifically combating cyber-extremism and the illegal sale of personal data prevalent on the "Darknet" hidden network. The legal nature of high-tech offenses such as "SIM-swapping," carried out based on data purchased by cybercriminals on the black market, is revealed. To address the problem, a comparative analysis of the experience of advanced foreign countries such as the USA, UK, Germany, and South Korea was conducted, and scientific and practical proposals were developed for the deep integration of the "High-tech policing" concept and the "E-Administrative Case" system into the activities of the internal affairs bodies of the Republic of Uzbekistan.

**Keywords:** Darknet, cyber-extremism, personal data, SIM-swapping, criminogenic stability, High-tech policing, administrative offense, foreign experience, E-Administrative Case.

**KIRISH**

Axborot-kommunikatsiya texnologiyalarining mislsiz darajada rivojlanishi jamiyat hayotining barcha sohalarini qamrab olishi bilan birga, jinoyatchilikning ham raqamli makonga (kiber-makonga) to‘liq ko‘chishiga sabab bo‘ldi. Bugungi kunda davlatning milliy xavfsizligi faqatgina an’anaviy geografik chegaralar bilan emas, balki kiber-makondagi barqarorlik bilan ham o‘lchanadi. Ushbu sharoitda "kriminogen barqarorlik" tushunchasi axborot xavfsizligini ta’minlash, turli kiber-tahdidlarning ommaviy tus olishiga yo‘l qo‘ymaslik va huquqbuzarliklarga qarshi zamonaviy IT-texnologiyalar asosida kurashishni anglatadi.

Jinoyat olamining eng asosiy va xavfli maydoni – bu "Darknet" (yashirin tarmoq) hisoblanadi. Oddiy qidiruv tizimlari (Google, Yandex) orqali kirib bo‘lmaydigan, maxsus brauzerlar (asosan Tor – The Onion Router) orqali ishlaydigan bu tarmoq mutlaq anonimlikni ta’minlashi tufayli kiberjinoyatchilarning asosiy markaziga aylangan. Darknet tarmog‘ida so‘nggi yillarda eng ko‘p kuzatilayotgan va davlat xavfsizligiga bevosita raxna soluvchi ikki katta tahdid – bu kiber-ekstremizm va fuqarolarning shaxsga doir ma’lumotlarining noqonuniy savdosidir. Ushbu jinoyatlarning yuridik tabiati murakkabligi va ularni fosh etish an’anaviy tergov

usullari bilan imkonsiz ekanligi ichki ishlar organlari faoliyatiga zudlik bilan "High-tech policing" (yuqori texnologik politsiya) yondashuvini joriy etishni taqozo qilmoqda.

## DARKNET VA KIBER-EKSTREMIZM: TEXNIK VA HUQUQIY TAHLIL

Ekstremistik va terroristik tashkilotlar o‘z g‘oyalarini targ‘ib qilish, yangi a’zolarni yollash va moliyaviy resurslarni yig‘ish maqsadida Darknetning anonimlik xususiyatlaridan keng foydalanmoqda.

**Texnik xususiyatlar:** Darknetda kiber-ekstremizm asosan yopiq forumlar, .onion domeniga ega maxfiy veb-saytlar va kriptovalyuta (Bitcoin, Monero) hamyonlari orqali amalga oshiriladi. Ekstremistik guruhlar qonuniy internet segmentida (Surface Web) bloklanishdan qochish uchun o‘zlarining o‘quv materiallari (portlovchi moddalar yasash bo‘yicha qo‘llanmalar, radikal adabiyotlar) va tashviqot videolarini bevosita Darknet serverlarida joylashtiradilar. Tor tarmog‘ining ko‘p qatlamli shifrlash (Onion routing) mexanizmi serverning qaysi davlatda ekanligini va foydalanuvchining IP-manzilini yashiradi.

**Yuridik va profilaktik muammolar:** Milliy qonunchiligimizda ekstremistik materiallarni tayyorlash, saqlash va tarqatish yuzasidan (Ma’muriy javobgarlik to‘g‘risidagi kodeksning 201-1-moddasi, Jinoyat kodeksining 244-1-moddasi) qat’iy javobgarlik belgilangan. Biroq, ushbu normalarni Darknet muhitiga qo‘llashda ashyoviy dalillarni to‘plash muammosi yuzaga keladi. Proksi-serverlar va VPN qatlamlari orqali yashiringan shaxsni identifikatsiya qilish uchun raqamli kriminalistika (Digital Forensics) asboblari va ochiq ma’lumotlar razvedkasi (OSINT) usullaridan foydalanish zarurati tug‘iladi.

Raqamlashtirishning yana bir salbiy oqibati sifatida fuqarolarning shaxsga doir ma’lumotlari "raqamli tovar"ga aylanganini aytish mumkin. Darknet bozorlarida har kuni millionlab insonlarning pasport nusxalari, bank karta raqamlari, login-parollari va biometrik ma’lumotlari noqonuniy savdoga qo‘yiladi.

Ma’lumotlarning sizib chiqishi (Data breach) asosan yirik korporatsiyalar, banklar yoki tibbiyot muassasalarining serverlariga qilingan xakerlik hujumlari natijasida yuzaga keladi. O‘zbekiston Respublikasining "Shaxsga doir ma’lumotlar to‘g‘risida"gi Qonuni ushbu ma’lumotlarning daxlsizligini kafolatlasa-da, transmilliy xakerlik guruhlari uchun bu to‘siq bo‘la olmayapti.

Darknetda olingan shaxsiy ma’lumotlar keyinchalik murakkab moliyaviy va kiberjinoyatlarni sodir etish uchun tayanch baza bo‘lib xizmat qiladi. Buning eng yorqin va xavfli namunasi – bu "SIM-swapping" amaliyotidir.

## "SIM-SWAPPING" JINOYATLARINING TEXNIK VA MA’MURIY-HUQUQIY MEXANIZMLARI

SIM-swapping (SIM-kartani almashtirish yoki o‘g‘irlash) – bu kiberjinoyatchi jabrlanuvchining shaxsiy ma’lumotlaridan foydalanib, uyali aloqa operatorini aldagani holda jabrlanuvchining mobil raqamini o‘ziga tegishli bo‘lgan yangi SIM-kartaga ko‘chirib o‘tkazish jarayonidir.

**Jinoyatning ishlash mexanizmi:**

1. **Ma’lumotlarni yig‘ish:** Jinoyatchi Darknetdan jabrlanuvchining pasport ma’lumotlari, yashash manzili va bank rekvizitlarini sotib oladi.
2. **Ijtimoiy muhandislik:** Uyali aloqa kompaniyasining ofisiga qo‘ng‘iroq qilib yoki soxta pasport orqali borib, "telefonimni yo‘qotdim" degan vaj bilan abonent raqamini yangi SIM-kartaga tiklashni so‘raydi. Olingan shaxsiy ma’lumotlar yordamida u abonent ekanligini tasdiqlaydi.
3. **Hisoblarni egallash:** Yangi SIM-karta faollashgach, jabrlanuvchining telefoni tarmoqdan uziladi. Jinoyatchi esa SMS orqali keladigan barcha tasdiqlash kodlarini (OTP – One Time Password) o‘ziga qabul qiladi. Bu orqali u qisqa muddat ichida bank ilovalariga (Click, Payme, Uzcard) kirib, barcha mablag‘larni o‘zlashtiradi, shuningdek Telegram kabi messenjerlarni buzib kirib, boshqalardan firibgarlik yo‘li bilan pul undiradi.

**Ma’muriy-huquqiy masalalar:** SIM-swapping muammosining yuridik yechimi nafaqat jinoyatchini topishda, balki xizmat ko‘rsatuvchi subyektlarning javobgarligini ta’minlashda yotadi. Aloqa operatorlari tomonidan fuqaroni to‘liq identifikatsiya qilmasdan (masalan, Face-ID yordamisiz) SIM-kartalarni tiklab berish holatlari uchun Ma’muriy javobgarlik to‘g‘risidagi kodeksda qat’iy sanksiyalar, litsenziya talablarini buzganlik uchun yirik miqdordagi jarimalar kiritilishi maqsadga muvofiqdir.

## XORIJ TAJRIBASI (XORIJ TAJRIBASI): AQSH, BUYUK BRITANIYA, GERMANIYA VA JANUBIY KOREYA

Raqamli kriminogen tahdidlarga qarshi kurashishda qator rivojlangan xorijiy davlatlar qonunchiligi va amaliyoti o‘ziga xos ahamiyatga ega:

- **Amerika Qo‘shma Shtatlari (AQSh):** AQShda Darknet va kiber-ekstremizmga qarshi kurashish CISA (Kiberxavfsizlik va infratuzilmani himoya qilish agentligi) va FBI tarkibidagi maxsus "Darknet Task Force" tomonidan olib boriladi. SIM-swapping bo‘yicha AQSh Federal Aloqa Komissiyasi (FCC) operatorlar uchun qat’iy qoidalarni o‘rnatgan bo‘lib, abonent ma’lumotlarini o‘zgartirishdan oldin xavfsiz autentifikatsiyani amalga oshirmagan kompaniyalarga millionlab dollar jarimalar qullanadi.
- **Buyuk Britaniya (UK):** Buyuk Britaniya Milliy Jinoyat Agentligi (NCA) qoshida "National Cyber Crime Unit" (NCCU) faoliyat yuritadi. Shaxsga doir ma’lumotlar himoyasi qat’iy tarzda GDPR standartlari (Information Commissioner's Office - ICO) asosida tartibga solinadi. Ekstremistik kontentni Darknetdan izlash va proaktiv bloklash uchun sun’iy intellektga asoslangan "High-tech policing" usullari keng qo‘llaniladi.
- **Germaniya:** Germaniya Federal Jinoyat Politsiyasi (BKA) kiberjinoyatlarni tergov qilish bo‘yicha dunyoda eng ilg‘or davlatlardan biridir. Germaniya Jinoyat kodeksida Darknetda noqonuniy savdo maydonchalarini yaratish va boshqarish (Operating criminal trading platforms on the internet) uchun maxsus jinoiy javobgarlik moddasi mavjud. Bu bevosita platforma ma’murlarini nishonga olishga yordam beradi.
- **Janubiy Koreya:** Kiber-barqarorlik bo‘yicha dunyoda yetakchi bo‘lgan Janubiy Koreya Milliy Politsiya Agentligi (KNP Cyber Bureau) yuqori darajadagi axborot texnologiyalariga tayanadi. Janubiy Koreyada internetda anonimlik deyarli yo‘q qilingan, fuqarolar muhim xizmatlardan foydalanishda raqamli ID va Face-ID tizimlari orqali avtorizatsiyadan o‘tishi shart. Bu SIM-swapping kabi ijtimoiy muhandislikka asoslangan jinoyatlarni minimal darajaga tushirgan.

## HIGH-TECH POLICING VA "E-MA’MURIY ISH" TIZIMI DOIRASIDA ISLOHOTLAR

O‘zbekiston Respublikasida kriminogen barqarorlikni raqamli makonda ta’minlash Ichki ishlar organlarining huquqbuzarliklar profilaktikasi va tergov faoliyatini to‘liq raqamlashtirishni, ya’ni "High-tech policing" modellariga o‘tishni talab etadi.

**E-Ma’muriy ish integratsiyasi:** Axborot texnologiyalari sohasidagi huquqbuzarliklar (ma’lumotlar daxlsizligini buzish, aloqa tarmoqlaridan noqonuniy foydalanish) bo‘yicha ishlarni yuritish "E-Ma’muriy ish" tizimiga bevosita biriktirilishi lozim. Agar fuqaro o‘z SIM-kartasi o‘zlashtirilgani yoki ma’lumotlari o‘g‘irlangani bo‘yicha IIOga elektron murojaat qilsa, "E-Ma’muriy ish" tizimi avtomatik ravishda Markaziy bank bazasi va aloqa operatorlari bazasi

bilan integratsiyalashgan holda shaxsning bank kartalarini bloklashi va SIM-karta lokatsiyasini aniqlab berishi kerak. Bunday tezkorlik firibgarlikning oxiriga yetishiga to‘sqinlik qiladi.

**Politsiya ta’limi:** Ichki ishlar organlari kadrlari, ayniqsa profilaktika inspektorlari va tezkor xodimlar uchun kiber-gigiyena, raqamli izlarni (digital footprints) tahlil qilish, kriptovalyuta tranzaksiyalarini (OSINT orqali) aniqlash bo‘yicha simulyatsion mashg‘ulotlar tizimini yaratish zarur. Maxsus hududiy kiber-guruhlar jinoyatchilarning Darknetdagi xatti-harakatlarini tahlil qila oladigan IT mutaxassislari darajasida tayyorlanishi shart.

## XULOSA VA ILMIY-AMALIY TAKLIFLAR

Olib borilgan tahlillar shuni ko‘rsatadiki, Darknet muhitida kiber-ekstremizm va shaxsiy ma’lumotlar savdosi davlatning kriminogen barqarorligiga to‘g‘ridan-to‘g‘ri tahdid solmoqda. Ushbu huquqbuzarliklarning yashirinligini inobatga olgan holda, faqatgina High-tech policing va zamonaviy ma’muriy-huquqiy vositalar orqaligina jamoat xavfsizligini ta’minlash mumkin.

Ushbu sohadagi qonunchilik va amaliyotni takomillashtirish yuzasidan quyidagi takliflar ilgari suriladi:

1. **Qonunchilikni takomillashtirish:** O‘zbekiston Respublikasining Jinoyat hamda Ma’muriy javobgarlik to‘g‘risidagi kodekslariga "Axborot-kommunikatsiya tarmoqlarining yashirin segmentida (Darknet) qonunga xilof ravishda virtual xizmatlar ko‘rsatish va ma’lumotlar savdosi" bo‘yicha maxsus javobgarlik moddalarini kiritish.
2. **Operatorlar mas’uliyatini oshirish:** Ma’muriy javobgarlik to‘g‘risidagi kodeksda SIM-swapping jinoyatlarining oldini olish maqsadida, uyali aloqa operatorlari tomonidan abonentga dublikat SIM-kartani berish tartibini qo‘pol ravishda buzganlik uchun yuridik shaxslarga nisbatan yirik miqdorda moliyaviy sanksiyalar (jarimalar) qo‘llash tizimini joriy etish.
3. **Identifikatsiyani kuchaytirish:** Barcha uyali aloqa kompaniyalari filiallari va dilerlarida shaxsni biometrik (Face-ID) identifikatsiya qilish uskunalari mavjudligini litsenziya talabi sifatida qat’iy belgilash.
4. **Idoralararo integratsiya:** "E-Ma’muriy ish" bazasini Kiberxavfsizlik markazlari va Markaziy Bankning "Antifrod" (firibgarlikka qarshi) tizimlari bilan yagona himoyalangan tarmoq (API) orqali bog‘lash, bu orqali shubhali kiber-tranzaksiyalarni onlayn monitoring qilish va oldini olishni yo‘lga qo‘yish.

Xulosa qilib aytganda, raqamli makonda kriminogen barqarorlikni ta’minlash doimiy evolyutsiyani talab qiladigan jarayondir. Ilg‘or xorijiy tajribani o‘zlashtirib, amaliyotda yuqori texnologik yondashuvlarni qo‘llash orqali huquqni muhofaza qiluvchi organlar nafaqat jinoyatlarni fosh etishi, balki ularning ildizini qirqishga to‘liq qodir bo‘ladi.

## REFERENCES:

1. O‘zbekiston Respublikasining Konstitutsiyasi. – Toshkent: O‘zbekiston, 2023.
2. O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksi. [Elektron resurs] // Qonunchilik ma’lumotlari milliy bazasi, https://lex.uz.
3. O‘zbekiston Respublikasining "Shaxsga doir ma’lumotlar to‘g‘risida"gi Qonuni. 02.07.2019-yildagi O‘RQ-547-son.
4. Xudoyberdiyev A.A. "Ma’muriy ishlarni yuritish kafolatlari va huquqni qo‘llash amaliyoti". O‘quv qo‘llanma. – Toshkent: IIV Akademiyasi, 2024.
5. Europol. "Internet Organised Crime Threat Assessment (IOCTA)". The Hague: European Union Agency for Law Enforcement Cooperation, 2023.
6. Mamatov A.Q. "Transmilliy kiberjinoyatchilik: yuridik va texnik tahlil". Monografiya. – Toshkent: TDYUU, 2022.
7. Interpol. "Global Cybercrime Report: SIM Swapping and Darknet Threats". Lyon, France, 2023.
8. Lee, H., & Kim, J. "High-tech policing and proactive cyber-threat detection in South Korea". Asian Journal of Criminology, 15(3), 245-261, 2020.
9. "Budapesht konvensiyasi: Kiberjinoyatlar bo‘yicha xalqaro standartlar va implementatsiya muammolari". Xalqaro hujjatlar to‘plami.
10. Federal Communications Commission (FCC). "Data Breach Reporting Requirements and SIM Swapping Fraud Prevention". Washington, D.C., 2023.