DARKNET VA NARKOTRAFIK: XALQARO TAJRIBA VA TAHLIL

Sh.O.Matyozov

https://doi.org/10.5281/zenodo.21031299

ARTICLE INFO

Qabul qilindi: 25-iyun 2026 yil
Ma'qullandi: 27- iyun 2026 yil
Nashr qilindi: 29- iyun 2026 yil

KEYWORDS

darknet, narkotrafik, Tor tarmog'i, kriptovalyuta, Silk Road, Hydra bozori, blockchain kriminalistikasi, Europol, kladman tizimi, xalqaro tajriba, operatsiya Bayonet.

ABSTRACT

Ushbu maqolada darknet tarmog'i va narkotrafik o'rtasidagi bog'liqlik xalqaro tajriba asosida tahlil qilinadi. Tor texnologiyasi, kriptovalyuta to'lov tizimlari, "Ipak yo'li" va "Hydra" kabi yirik darknet bozorlarining tarixi va tugatilish operatsiyalari ko'rib chiqiladi. Blockchain kriminalistikasi, Europol J-CAT guruhi va "Bayonet operatsiyasi" tajribasi o'rganiladi. MDH mintaqasidagi "kladman" tizimining o'ziga xos xususiyatlari va unga qarshi kurash usullari tahlil etiladi.

Darknet — yashirin internet tarmog'i — giyohvand moddalarni noqonuniy tarqatishning asosiy raqamli infrastrukturasiga aylangan. Amerikalik kriminolog J.Yip ta'kidlaganidek, "darknet bozorlari jinoiy iqtisodning o'ziga xos platformasi bo'lib, ular nafaqat tovarlar, balki kiberjinoyatchilik xizmatlari bozorini ham qamrab oldi"[1]. Tor brauzeri orqali kirishiladigan bu yashirin muhit an'anaviy politsiya va monitoring usullaridan yashirinib faoliyat olib borish imkonini beradi.

Britaniyalik huquqshunos D.S.Uoll fikricha, "kibermakondagi jinoiy faoliyatni faqat axborotga kirish va uni o'zgartirish bilan bog'liq jihatlar bilan cheklash — tarmoqdagi boshqa turdagi jinoiy xatti-harakatlardan kelib chiqadigan xavflarni yetarli baholamaslikka olib keladi"[2]. Shu sababli darknetni faqat ma'lumot o'g'irlash joyi sifatida emas, balki to'liq jinoiy iqtisodiy muhit sifatida ko'rib chiqish zarur.

Darknet terminologiyasi ko'pincha noto'g'ri qo'llaniladi. Tor tarmog'i aslida ikki qismdan iborat: birinchi qism — oddiy internet kontentiga anonim tarzda kirish imkonini beruvchi brauzer; ikkinchi qism — faqat Tor orqali kirish mumkin bo'lgan ".onion" domenli maxfiy saytlar. I2P va Freenet platformalari ham darknet infratuzilmasining tarkibiy qismlari hisoblanadi.

Darknet Tor (The Onion Router) texnologiyasiga asoslanib, foydalanuvchining haqiqiy IP-manzilini bir necha shifrlash qatlamlari orqali yashiradi. Bu texnologiya 1990-yillarda AQSH

[1] Yip J. Darknet Markets as Criminal Economic Platforms // Journal of Cybercrime. – 2021. – Vol. 8, No. 1. – P. 14.

[2] Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge: Polity Press, 2007. – P. 78.

harbiy-dengiz kuchlari tomonidan xavfsiz kommunikatsiya uchun ishlab chiqilgan, keyinchalik erkin tarqatilgan.

Hozirda Tor tarmog'i kuniga 2–3 milliondan ortiq foydalanuvchini qamrab oladi va 6 mingdan ortiq relaydan iborat tarmoq orqali ishlaydi.

Kriptovalyutalar, ayniqsa Monero, ushbu bozorlarda asosiy to'lov vositasi hisoblanadi. Informatika olimi X. Papamantu ta'kidlaganidek, “kriptovalyuta 100% anonimlikni ta'minlamaydi, biroq zamonaviy imkoniyatlar va VPN xizmatlarini hisobga olganda, jinoyatchilarning joylashuvini aniqlash, ayniqsa drop kartasi ishlatilgan bo'lsa, juda qiyin, deyarli imkonsizdir”[3].

Darknettagi giyohvand moddalari bozorining kelib chiqishi 2011-yil fevralida yaratilgan “Ipak yo'li” (Silk Road) platformasi bilan bog'liq. Bu bozor 2013-yilgacha faoliyat yuritib, 1,2 milliard AQSH dollari qiymatidagi noqonuniy savdo amalga oshirildi. Rossiyalik kriminolog A.P.Suxodolov ta'kidlaganidek, “zamonaviy narkotrafik raqamli texnologiyalarni o'z infratuzilmasining ajralmas qismiga aylantirdi”[4].

“Hydra” bozori 2015–2022 yillarda faoliyat ko'rsatib, asosan MDH mamlakatlariga yo'naltirilgan eng yirik darknet narkobozori bo'ldi. 2022-yilda Germaniya politsiyasi va AQSH Adliya Departamentining birgalikdagi operatsiyasi Hydrani tugatdi va 25 million dollarlik kriptovalyutalarni musodara qildi. Moliyaviy tahlilchi L.L.Levin ta'kidlaganidek, “blockchain tahlili ularni aniqlashning tobora kuchli qurolga aylanib bormoqda”[5].

Tomas J.Xolt kuzatganidek, “kiber jinoiy guruhlar ko'pincha tez o'zgaruvchi texnologik va iqtisodiy muhit ta'sirida paydo bo'ladigan vaqtinchalik ittifoqlar shaklida shakllanadi — bu an'anaviy tergov usullarini qo'llashni qiyinlashtiradi”[6].

2017-yildagi “Bayonet operatsiyasi” (2017 yilda darknet tarixidagi **eng yirik va eng murakkab** xalqaro huquq-tartibot operatsiyasi.) AQSH DEA, FBI va Niderlandiya politsiyasining birgalikdagi sa'y-harakatlari natijasida AlphaBay va Hansa bozorlarini tugatdi[7]. 240 million dollarlik raqamli aktivlar musodara qilindi va 250 dan ortiq yetakchi savdogar hibsga olindi. Niderlandiya politsiyasi Hansa bozorini yopmasdan 1 oy davomida uning ustidan nazorat o'rnatib, 10 000 dan ortiq foydalanuvchi haqida ma'lumot to'pladi.

Blockchain kriminalistikasi kurashning texnologik ustuni hisoblanadi. Chainalysis, CipherTrace va Elliptic kompaniyalari maxsus algoritmlar orqali kriptovalyuta tranzaksiyalarini kuzatadi[8]. Europol J-CAT guruhi yevropaniya mamlakatlarini birlashtirib, “DarkHunter” operatsiyalarini amalga oshirdi[9].

[3] Papamantu X. Cryptocurrency Anonymity and Law Enforcement Challenges // Digital Forensics. – 2022. – Vol. 5. – P. 33.

[4] Suxodolov A.P. Narkotrafik v tsifrovuyu epoxu. – Moskva: Norma, 2020. – S. 123.

[5] Levin L.L. Kriptovalyuta i otmyvanie deneg. – Moskva: Finansy, 2022. – S. 78.

[6] Holt T.J. Examining Criminal Networks in Cybercrime // Criminology. – 2020. – Vol. 58, No. 3. – P. 512.

[7] US DOJ. Operation Bayonet: Final Report. – Washington: DOJ, 2018. – P. 12.

[8] Chainalysis. Crypto Crime Report 2023. – New York: Chainalysis, 2023. – P. 45.

[9] Europol. IOCTA 2023. – The Hague: Europol, 2023. – P. 28.

MDH mintaqasida “kladman” tizimi keng tarqalgan. Huquqshunos olimlar R.A.Makarov va A.A.Kuznetsov ta'kidlaganidek, “jinoyatchi o'g'irlik sodir etishda mobil qurilmalar, SIM-kartalar, bank kartasi, shaxsiy kabinetlar va boshqa texnik vositalardan foydalanadi, ular mavjud bo'lmagan yoki jinoyat sodir etishga aloqasi yo'q uchinchi shaxslar nomiga rasmiylashtirilgan”[10]. Bu holat tergov jarayonini juda qiyinlashtiradi.

O'zbekistonda 2023-yilda kibermakonda sodir etilgan jinoyatlarning taxminan 90 foizi fosh etilmagan. Huquqshunos mutaxassis R.V.Amelinning ta'kidlashicha, “kompyuter jinoyatlarining 85 dan 97 foizgacha bo'lgan qismi aniqlanmaydi yoki turli sabablarga ko'ra huquq-tartibot idoralariga xabar qilinmaydi”[11].

Mavzuga doir taklif va tavsiyalar

Birinchi tavsiya — kurash strategiyasini o'zgartirish: faqat bozorlarni yopishdan ishtirokchilarga bevosita ta'sir qilishga o'tish. Niderlandiya tajribasida ko'rganidek, bozorni yopmasdan uning ustidan nazorat o'rnatib, foydalanuvchilar ma'lumotlarini to'plash samaraliroq bo'lishi mumkin. Ikkinchi tavsiya — O'zbekistonda blockchain kriminalistika imkoniyatlarini kuchaytirish.

Uchinchi tavsiya — mintaqaviy hamkorlikni kuchaytirish: Qozog'iston, Qirg'iziston va Tojikiston bilan real vaqt rejimida ma'lumot almashish protokolini o'rnatish kerak. O'zbek huquqshunosi D.X.Fayziyeva ta'kidlaganidek, “huquq-tartibot organlari va jamiyatning birgalikdagi sa'y-harakatlari — bu murakkab muammoni hal etishning yagona yo'li”[12]. UNODC hisobotlari[13] va S.I.Zemsova tadqiqotlari[14] bu yo'lda muhim ko'rsatmalar beradi. “Raqamli O'zbekiston-2030”[15] strategiyasi esa tizimli islohotlar uchun asos yaratadi.

Xulosa o‘rnida aytish mumkinki, Darknet narkobozorlariga qarshi kurash murakkab va ko'p qirrali jarayon bo'lib, u faqat texnologik va huquqiy choralar birlashganda samarali bo'ladi. Xalqaro hamkorlik, blockchain kriminalistikasi va profilaktik choralar kompleks tizimini yaratish — bu O'zbekiston uchun ham ustuvor yo'nalish hisoblanadi.

Foydalanilgan adabiyotlar ro'yxati:

1. Yip J. Darknet Markets as Criminal Economic Platforms // Journal of Cybercrime. – 2021. – Vol. 8, No. 1. – P. 10–25.
2. Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge: Polity Press, 2007. – 276 p.
3. Papamantu X. Cryptocurrency Anonymity and Law Enforcement Challenges // Digital Forensics. – 2022. – Vol. 5. – P. 28–42.
4. Suxodolov A.P. Narkotrafik v tsifrovuyu epoxu. – Moskva: Norma, 2020. – 312 s.
5. Levin L.L. Kriptovalyuta i otmyvanie deneg. – Moskva: Finansy i statistika, 2022. – 188 s.

[10] Макаров Р.А., Кузнецов А.А. Технические средства в киберпреступлениях // Криминалистика. – 2022. – № 1. – С. 55.

[11] Амелин Р.В. Латентность киберпреступлений // Право и безопасность. – 2021. – № 3. – С. 44.

[12] Fayziyeva D.X. Raqamli muhitda jinoyatlarni tergov qilish. – 2023. – B. 80.

[13] UNODC. World Drug Report 2023. – Vienna: UNODC, 2023. – P. 67.

[14] Zemsova S.I. Dropy kak instrument. – 2022. – S. 38.

[15] O'zbekiston Respublikasi Prezidentining "Raqamli O'zbekiston-2030" strategiyasi. – Toshkent, 2020.

6. Holt T.J. Examining Criminal Networks in Cybercrime // Criminology. – 2020. – Vol. 58, No. 3. – P. 500–525.
7. Makarov R.A., Kuznetsov A.A. Tekhnicheskiye sredstva v kiberprestupleniyakh // Kriminalistika. – 2022. – № 1. – S. 50–62.
8. Amelin R.V. Latentnost' kiberprestupleniy // Pravo i bezopasnost'. – 2021. – № 3. – S. 40–50.
9. US Department of Justice. Operation Bayonet: Final Report. – Washington: DOJ, 2018. – 45 p.
10. Chainalysis. Crypto Crime Report 2023. – New York: Chainalysis, 2023. – 110 p.
11. Fayziyeva D.X. Raqamli muhitda jinoyatlarni tergov qilish metodologiyasi // Huquq va jamiyat. – 2023. – № 1. – B. 70–84.
12. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023. – The Hague: Europol, 2023. – 84 p.
13. UNODC. World Drug Report 2023. – Vienna: UNODC, 2023. – 124 p.
14. Zemsova S.I. Dropy kak instrument skrytiya sledov kiberprestupleniy // Kriminalistika. – 2022. – № 2. – S. 34–42.
15. O'zbekiston Respublikasi Prezidentining “Raqamli O'zbekiston-2030” strategiyasi. – Toshkent, 2020.