SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

ДАРКНЕТДА СОДИР ЭТИЛАЁТГАН КИБЕРЖИНОЯТЛАР, УЛАРНИНГ ЮРИДИК ВА ТЕХНИК ЖИҲАТДАН ТАҲЛИЛИ

Рузиев Жавохирбек Сайиджон ўғли

Ўзбекистон Республикаси ИИВ Академияси курсанти

Тошкент ш.

https://doi.org/10.5281/zenodo.20592469

Аннотация: Мазкур илмий иш интернетнинг яширин сегменти ҳисобланган «Даркнет» (Darknet) муҳитида содир этилаётган кибержиноятларнинг юридик ва техник жиҳатларини комплекс таҳлил қилишга бағишланган. Тадқиқотда аноним тармоқларнинг техник архитектураси, хусусан Tor ва I2P протоколлари, криптографик маршрутизация ҳамда криптовалюталар орқали амалга ошириладиган ноқонуний молиявий транзакциялар механизми кўриб чиқилган. Юридик жиҳатдан, даркнетдаги жиноятларни квалификация қилиш, юрисдикция муаммолари, далиллар базасини тўплашнинг процессуал хусусиятлари ва халқаро ҳамкорлик масалалари таҳлил этилган. Иш якунида миллий қонунчиликни такомиллаштириш ва техник ҳимоя усулларини ривожлантириш бўйича таклифлар илгари сурилган.

Калит сўзлар: Даркнет, кибержиноятчилик, анонимлик, Tor тармоғи, криптовалюта, юридик таҳлил, рақамли далил, киберхавфсизлик, юрисдикция, пиёзли маршрутизация.

Аннотация: Данная научная работа посвящена комплексному анализу юридических и технических аспектов киберпреступлений, совершаемых в скрытом сегменте интернета — «Даркнете» (Darknet). В исследовании рассматриваются техническая архитектура анонимных сетей, в частности протоколы Tor и I2P, криптографическая маршрутизация и механизмы незаконных финансовых транзакций с использованием криптовалют. С

юридической точки зрения проанализированы проблемы квалификации преступлений в даркнете, вопросы юрисдикции, процессуальные особенности сбора цифровых доказательств и международное сотрудничество. В заключении выдвинуты предложения по совершенствованию национального законодательства и развитию методов технической защиты.

Ключевые слова: Даркнет, киберпреступность, анонимность, сеть Tor, криптовалюта, юридический анализ, цифровые доказательства, кибербезопасность, юрисдикция, луковая маршрутизация.

Abstract: This research paper is dedicated to a comprehensive legal and technical analysis of cybercrimes committed within the hidden segment of the internet, known as the "Darknet". The study examines the technical architecture of anonymous networks, specifically Tor and I2P protocols, cryptographic routing, and the mechanisms of illicit financial transactions conducted via cryptocurrencies. From a legal perspective, the paper analyzes the challenges of crime qualification in the Darknet, jurisdiction issues, procedural features of digital evidence collection, and international cooperation. The paper concludes with recommendations for improving national legislation and developing technical defense methods.

Keywords: Darknet, cybercrime, anonymity, Tor network, cryptocurrency, legal analysis, digital evidence, cybersecurity, jurisdiction, onion routing.

КИРИШ

1. Мавзунинг долзарблиги ва муаммонинг қўйилиши

XXI аср – глобал рақамлашиш ва ахборот технологияларининг мисли кўрилмаган даражада ривожланиши даври сифатида инсоният цивилизациясини бутунлай ўзгартирди. Бугунги кунда иқтисодиёт, сиёсат, ижтимоий ҳаёт ва давлат бошқаруви тизимлари тўлиқ электрон форматга

ўтмоқда. Бироқ, бундай шиддатли тараққиёт инсоният олдига янги ва ўта хавфли таҳдидларни ҳам кўндаланг қисди. Ушбу таҳдидларнинг энг мураккаб ва трансчегаравий кўриниши – кибержиноятчиликдир. Айниқса, анъанавий қидирув тизимлари ва оддий фойдаланувчилар кўзидан яширилган, махсус дастурий таъминотлар ёрдамида кириладиган «Даркнет» (яширин тармоқ) муҳити жиноят оламининг глобал марказига айланиб улгурди.

Даркнет феномени фақатгина техник муаммо эмас, балки замонавий ҳуқуқ тизими учун жиддий чақириқдир. Ушбу яширин маконда гиёҳванд моддаларнинг ноқонуний айланмаси, қурол-яроғ савдоси, инсон аъзолари ва одам савдоси, порнографик материалларнинг тарқатилиши, шунингдек, давлат ва хусусий секторларга қарши йўналтирилган вайронкор киберҳужумлар хизмати (Cybercrime-as-a-Service) очиқчасига таклиф этилмоқда. Муаммонинг асосий илдизи шундаки, даркнет ўзининг табиатига кўра фойдаланувчиларга мутлақ анонимлик ва кузатувдан холи бўлиш имконини беради. Бу эса жиноятчиликка қарши курашувчи анъанавий ҳуқуқни муҳофаза қилувчи органларнинг фаолиятини сезиларли даражада чеклаб қўймоқда.

Ўзбекистон Республикасида ҳам рақамли иқтисодиёт ва электрон давлат хизматлари кенг жорий этилаётган ҳозирги даврда, миллий кибермакон хавфсизлигини таъминлаш устувор вазифалардан бири ҳисобланади. Ҳукуматимиз томонидан киберхавфсизлик соҳасига оид қатор қонун ҳужжатлари қабул қилинаётган бўлса-да, даркнет сингари глобал ва криптографик ҳимояланган тармоқлардаги жиноятларни аниқлаш ва уларга ҳуқуқий баҳо бериш механизмлари ҳали тўлиқ шаклланмаган. Ушбу тадқиқот иши даркнетдаги кибержиноятларнинг ички техник тузилишини ва

уларни жиноят-ҳуқуқий жиҳатдан квалификация қилишдаги бўшлиқларни илмий асосда таҳлил қилишга қаратилганлиги билан ўта долзарбдир.

2. Тармоқнинг техник тузилиши: Клиент-сервер архитектурасидан анонимликкача

Даркнетни тушуниш учун аввало интернетнинг уч қатламли тузилишини техник жиҳатдан фарқлаб олиш зарур. Биринчи қатлам – бу «Юзаки веб» (Surface Web) бўлиб, унга Google, Yandex, Bing каби оддий қидирув тизимлари орқали кириладиган барча очиқ сайтлар киради. Иккинчи қатлам – «Чуқур веб» (Deep Web) деб аталади ва у қидирув тизимлари томонидан индекс қилинмайдиган, пароль ёки махсус рухсатнома талаб қилувчи маълумотлар базалари, корпоратив тармоқлар, тиббий карталар ва банк тизимларини ўз ичига олади. Учинчи ва энг яширин қатлам эса «Даркнет» (Darknet) бўлиб, у нафақат индекс қилинмайди, балки унга кириш учун стандарт браузерлар (Chrome, Safari, Edge) мутлақо ярамайди.

Даркнетнинг техник асосини Onion (Пиёзли) ва Garlic (Саримсоқли) маршрутизация протоколлари ташкил этади. Энг оммабоп тармоқ ҳисобланган **Tor (The Onion Router)** тармоғи маълумотларни узатишда уларни бир неча қатламли криптографик шифрлаш (худди пиёз пўстлоғидек) билан ҳимоялайди. Фойдаланувчи сўрови марказий серверга эмас, балки бутун дунё бўйлаб жойлашган учта ихтиёрий тугун (node) – кириш, оралиқ ва чиқиш тугунлари орқали йўналтирилади:

1. **Кириш тугуни (Entry Node):** Фойдаланувчининг реал IP-адресини кўради, лекин узатилаётган маълумот мазмунини ва якуний манзилни билмайди.
2. **Оралиқ тугун (Middle Node):** Маълумотни фақат занжир бўйлаб ўтказади, у на жўнатувчини ва на қабул қилувчини билади.

3. **Чиқиш тугуни (Exit Node):** Шифрни охирги қатламини ечади ва сўровни сайтга юборади, лекин сўров эгаси кимлигини кўрмайди.

Бундан ташқари, **I2P (Invisible Internet Project)** тармоғи мавжуд бўлиб, унда маълумотлар «саримсоқли шифрлаш» асосида, бир вақтнинг ўзида бир нечта пакетларга бўлиниб, турли йўналишлар бўйлаб ҳаракатланади. Бундай децентрализациялашган (марказлаштирилмаган) ва тўлиқ шифрланган техник муҳит фойдаланувчининг рақамли изини (digital footprint) бутунлай яширади. Жиноятчилар мана шу техник мукаммалликдан фойдаланиб, ўзларининг ноқонуний веб-сайтлари ва серверларини яширадилар, натижада провайдерлар ёки махсус хизматлар кимнинг қайси сайтга кираётганини кузата олмайди.

3. Даркнетдаги кибержиноятларнинг таснифи ва иқтисодий модели

Даркнет муҳитида содир этилаётган жиноятлар ўз миқёси ва характерига кўра бир нечта йирик гуруҳларга бўлинади. Биринчи ва энг кенг тарқалган тури – бу **ноқонуний савдо майдончалари (Darknet Marketplaces - DNMs)** ҳисобланади. Илгари машҳур бўлган "Silk Road", кейинчалик "AlphaBay", "Hydra" ва ҳозирги кунда уларнинг ўрнини эгаллаган янги синдикатлар худди оддий "Amazon" ёки "AliExpress" каби ишлайди. Фарқи шундаки, у ерда сотиладиган маҳсулотлар қонун билан тақиқланган. Харидорлар ва сотувчилар ўртасидаги ишончни таъминлаш учун «Эскроу» (Escrow) тизими – яъни маҳсулот харидорга етиб бормагунча маблағни ушлаб турувчи учинчи мустақил томон (автоматлаштирилган тизим) фаолият кўрсатади.

Иккинчи хавфли йўналиш – **«Кибержиноятчилик хизмат сифатида» (Cybercrime-as-a-Service - CaaS)** моделидир. Бугунги кунда даркнетда профессионал хакер бўлиш шарт эмас; етарлича маблағ эвазига исталган давлат органи ёки банк тизимига DDoS-ҳужум уюштириш, мураккаб

Ransomware (товламачилик-вируслари) дастурларини сотиб олиш ёки маълум бир корхонанинг маълумотлар базасини бузиб киришни буюртма қилиш мумкин.

Уччиндаги йўналиш – **шахсий ва корпоратив маълумотлар савдоси**. Бу ерда миллионлаб фойдаланувчиларнинг паспорт маълумотлари, кредит карта рақамлари, тиббий сирлари ва тижорат сирлари пакет шаклида жуда арзон нархларда сотилади. Бу маълумотлар кейинчалик фишинг ҳужумлари ва ижтимоий инженерия орқали фуқароларнинг маблағларини ўғирлаш учун хомашё вазифасини ўтайди.

Ушбу жиноий иқтисодиётнинг яшаб қолишини таъминловчи асосий восита – **криптовалюталардир**. Bitcoin (BTC) тармоғи нисбатан шаффоф бўлгани сабабли, замонавий кибержиноятчилар мутлақ анонимликни таъминловчи **Monero (XMR)** ёки **Dash** каби криптоактивлардан фойдаланишмоқда. Бундан ташқари, транзакциялар изини йўқотиш учун «Крипто-миксерлар» (Crypto Mixers ёки Tumblers) ишлатилади. Бу тизим юзлаб фойдаланувчиларнинг маблағларини битта умумий «қозон»да аралаштириб, кейин майда қисмларга бўлиб бошқа манзилларга жўнатади, бу эса блокчейн тармоғида пулнинг асл эгасини аниқлашни техник жиҳатдан имконсиз қилади.

4. Ҳуқуқий муаммолар: Юрисдикция ва далиллар базасини шакллантириш

Даркнетде содир этиладиган жиноятларни тергов қилиш ва уларга ҳуқуқий баҳо беришда дунё ҳамжамияти, жумладан, Ўзбекистон Республикаси суд-ҳуқуқ тизими бир нечта жиддий юридик тўсиқларга дуч келмоқда. Биринчи ва энг катта муаммо – **юрисдикция (ҳудудий тегишлилик) инқирозидир**. Анъанавий жиноят ҳуқуқи давлатнинг суверенитети ва ҳудудий чегараларига асосланади. Жиноят содир этилган жой қонунчиликни қўллашда бош мезон ҳисобланади. Аммо даркнетда

жиноятчи Тошкентда ўтириб, АҚШдаги сервер орқали Германия фуқаросига Германияда тақиқланган моддани сотиши мумкин, сервернинг ўзи эса Панамада жойлашган бўлади. Бундай вазиятда жиноий иш қайси давлат қонунчилиги бўйича ва ким томонидан қўзғатилиши кенг муҳокамали савол бўлиб қолмоқда.

Иккинчи юридик муаммо – **рақамли далилларни (digital evidence) тўплаш ва уларнинг процессуал мақомидир**. Жиноят-процессуал кодекси талабларига кўра, ҳар қандай далил қонуний йўл билан олинган, ўзгармас ва ишончли бўлиши шарт. Бироқ, рақамли маълумотлар ўта динамик бўлиб, уларни масофадан туриб сониялар ичида бутунлай ўчириб ташлаш ёки ўзгартириш мумкин. Масалан, ҳуқуқни муҳофаза қилувчи органлар томонидан даркнетдаги сотувчининг сервери масофадан туриб хакерлик усули билан бузиб кирилиб, маълумотлар олинса, ушбу маълумотлар судда қонуний далил сифатида тан олинадими ёки йўқми? Кўплаб давлатлар қонунчилигида прокурор ёки суд санкциясисиз, виртуал маконда ўтказилган «рақамли тинтув» натижалари далил сифатида қабул қилинмайди.

Учинчидан, **жиноий субъектни идентификация қилиш** муаммоси. Даркнетда фақат виртуал никнеймлар (псевдонимлар) ва крипто-ҳамён рақамлари мавжуд бўлади. Жиноят кодекси бўйича жавобгарликка фақат муайян жисмоний шахс тортилиши мумкин. Виртуал никнейм орқали ҳаракат қилган шахс айнан ўша айбланувчи эканлигини, унинг компьютеридан бошқа одам (масалан, оила аъзоси ёки тармоқни бузиб кирган бошқа хакер) фойдаланмаганини судда исботлаш ўта мураккаб процессуал жараёндир.

5. Халқаро тажриба ва Миллий қонунчилик таҳлили

Даркнетнинг трансчегаравий табиати унга қарши фақат бир давлат доирасида курашиб бўлмаслигини кўрсатмоқда. Халқаро амалиётда Европол

(Europol), ФБР (FBI) ва Интерпол каби ташкилотларнинг ҳамкорликдаги махсус операциялари (масалан, "Operation Bayonet", "Operation Trojan Shield") натижасида энг йирик даркнет бозорлари йўқ қилинган. Бунда асосан "кибер-тузоқ" (honeypot) усули ишлатилади: махсус хизматлар даркнет сайтининг серверидаги техник хатоликни топиб, уни ўз назоратига олади, лекин сайтни дарҳол ёпмайди. Бир неча ой давомида ундан фойдаланаётган барча харидор ва сотувчиларнинг маълумотларини тўплаб, кейин бутун дунё бўйлаб бир вақтда ҳибсга олишлар амалга оширилади.

Ўзбекистон Республикасининг жиноий ва киберхавфсизлик қонунчилиги таҳлил қилинганда, бу борада ижобий қадамлар ташланганини кўриш мумкин. Хусусан, «Киберхавфсизлик тўғрисида»ги Қонуннинг қабул қилиниши, Жиноят кодексининг XX Кора боби («Ахборот технологиялари соҳасидаги жиноятлар») мавжудлиги ҳуқуқий базани ташкил этади. Бироқ, амалдаги Жиноят кодексида «Даркнет», «Аноним тармоқлар», «Крипто-миксерлар орқали жиноий даромадларни легаллаштириш» каби тушунчалар ва уларни оғирлаштирувчи ҳолат сифатида малакалаш нормалари мавжуд эмас.

Шунингдек, Жиноят-процессуал кодексида рақамли далилларни олиш, уларни криптографик хэш-рақамлар (hash-values) орқали муҳрлаш ва сақлашнинг аниқ процессуал регламенти етарлича очиб берилмаган. Бу эса даркнетда содир этилган жиноят ишлари судга етиб борганда, далиллар базасининг заифлиги сабабли ишнинг бузилишига олиб кириши мумкин.

6. Тадқиқотнинг мақсади ва вазифалари

Юқорида баён этилган муаммо ва зиддиятлардан келиб чиққан ҳолда, мазкур тадқиқот ишининг асосий **мақсади** – даркнет муҳитида содир этилаётган кибержиноятларнинг техник механизмларини очиб бериш ва уларга қарши курашишнинг жиноят-ҳуқуқий ва жиноят-процессуал

тизимини такомиллаштириш бўйича илмий асосланган таклиф ва тавсиялар ишлаб чиқишдан иборат.

Ушбу мақсадга эришиш учун қуйидаги тизимли **вазифалар** белгилаб олинди:

1. Даркнет ва унинг таркибий қисмлари (Tor, I2P, Freenet) архитектурасини техник ва криптографик жиҳатдан тадқиқ этиш;
2. Яширин тармоқлардаги иқтисодий жиноятлар, жумладан криптовалюталар воситасидаги ноқонуний айланмалар ва пул ювиш схемаларини аниқлаш;
3. Даркнетдаги жиноятларни квалификация қилишдаги миллий ва халқаро ҳуқуқий муаммоларни (юрисдикция, субъект, объектив томон) аниқлаш;
4. Рақамли далилларни тўплаш, текшириш ва баҳолашнинг процессуал жиҳатларини таҳлил қилиш ва Ўзбекистон Республикаси Жиноят-процессуал кодексига тегишли ўзгартиришлар киритиш бўйича таклифлар тайёрлаш;
5. Кибермакон хавфсизлигини таъминлашда сунъий интеллект (AI) ва катта маълумотлар (Big Data) технологияларини қўллашнинг техник имкониятларини баҳолаш.

Ушбу тадқиқот иши техник билимлар билан юридик нормаларни интеграция қилган ҳолда, миллий киберхавфсизлик стратегиясини янги босқичга олиб чиқишга хизмат қилади.

REFERENCES:

1. Ўзбекистон Республикасининг Қонуни. **«Киберхавфсизлик тўғрисида»** ЎРҚ-764-сон. 2022 йил 15 апрель.

2. Ўзбекистон Республикасининг **Жиноят кодекси** (махсус қисм, XX Кора боб).
3. Ўзбекистон Республикасининг **Жиноят-процессуал кодекси** (рақамли далиллар билан ишлаш қисми).
4. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd Edition. Wiley.
5. Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival: Global Politics and Strategy*, 58(1), 7-38.
6. Europol. (2025). *Internet Organised Crime Threat Assessment (IOCTA 2025)*. Enforcement report. The Hague.
7. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Whitepaper.
8. Калмыков, Д. А. (2022). Юридический и технический анализ преступности в сети Даркнет. *Журнал российского права*, №4, 112-125.
9. Джураев, А. Х. (2023). Рақамли макондаги кибержиноятчилик ва унга қарши курашишнинг процессуал хусусиятлари. *Юридик фанлар ахборотномаси*, 3(2), 45-51.
10. Finklea, K. (2017). *Dark Web*. Congressional Research Service Report for Congress.
11. Jardine, E. (2018). The Dark Web: Dilemmas of a dual-use technology. *Global Commission on Internet Governance*, Paper No. 41.
12. Сухаренко, А. Н. (2024). Transnational cybercrime: new challenges and methods of counteraction. *Право и кибербезопасность*, №1, 18-24.