SCIENTIFIC CONFERENCE OPEN PROCEEDINGS
Global Academic Knowledge Repository

АХБОРОТ ТЕХНОЛОГИЯЛАРИ СОҲАСИДАГИ ЖИНОЯТЛАРГА ҚАРШИ КУРАШИШДА ҲУҚУҚНИ МУҲОФАЗА ҚИЛУВЧИ ОРГАНЛАР ФАОЛИЯТИНИ ТАКОМИЛЛАШТИРИШНИНГ НАЗАРИЙ ВА АМАЛИЙ ЖИҲАТЛАРИ

Абдурасул Иминов

Ўзбекистон Республикаси ИИВ Академияси Рақамли технологиялар ва ахборот хавфсизлиги кафедраси бошлиғи, подполковник

Омонбоев Дилмурод Беккамол ўғли

Ўзбекистон Республикаси ИИВ Академияси 3-курс курсанти

Тошкент. ш

https://doi.org/10.5281/zenodo.20699555

Аннотация: Мазкур илмий мақолада ахборот технологиялари (IT) соҳасидаги жиноятларга қарши курашишда ҳуқуқни муҳофаза қилувчи органлар фаолиятининг назарий ва амалий муаммолари комплекс таҳлил қилинган. Кибер-макондаги жиноятларнинг трансмиллий табиати, рақамли далилларни тўплаш ва юридик баҳолашдаги назарий бўшлиқлар ҳамда тезкор-тергов амалиётидаги қийинчиликлар (анонимлик, криптография, электрон изларни йўқ қилиш) илмий асосланган. Кибержиноятчиликка қарши курашишда АҚШ (FBI Cyber Division), Эстония ва Интерпол (IGCI) каби халқаро ва хорижий тузилмаларнинг илғор тажрибаси қиёсий ўрганилиб, Ўзбекистон ҳуқуқни муҳофаза қилувчи органлари амалиётини, хусусан, кибер-криминалистика ва тезкор-қидирув фаолиятини такомиллаштириш юзасидан аниқ илмий-амалий таклифлар ишлаб чиқилган.

Калит сўзлар: ахборот технологиялари, кибержиноятчилик, ҳуқуқни муҳофаза қилувчи органлар, рақамли далил, OSINT, трансмиллий жиноят, киберхавфсизлик, хориж тажрибаси.

Аннотация: В данной научной статье проводится комплексный анализ теоретических и практических проблем деятельности правоохранительных органов по борьбе с преступлениями в сфере информационных технологий (ИТ). Научно обоснованы транснациональная природа преступлений в киберпространстве, теоретические пробелы в сборе и юридической оценке цифровых доказательств, а также трудности в оперативно-следственной практике (анонимность, криптография, уничтожение электронных следов). Изучен передовой зарубежный и международный опыт США (FBI Cyber Division), Эстонии и Интерпола (IGCI) в борьбе с киберпреступностью, разработаны конкретные научно-практические предложения по совершенствованию практики правоохранительных органов Узбекистана, в частности, киберкриминалистики и оперативно-розыскной деятельности.

Ключевые слова: информационные технологии, киберпреступность, правоохранительные органы, цифровое доказательство, OSINT, транснациональное преступление, кибербезопасность, зарубежный опыт.

Abstract: This scientific article provides a comprehensive analysis of the theoretical and practical problems of the activities of law enforcement agencies in combating crimes in the field of information technology (IT). The transnational nature of crimes in cyberspace, theoretical gaps in the collection and legal assessment of digital evidence, and difficulties in operational and investigative practice (anonymity, cryptography, destruction of electronic traces) are scientifically substantiated. The advanced foreign and international experience of the USA (FBI Cyber Division), Estonia, and Interpol (IGCI) in combating cybercrime was comparatively studied, and specific scientific and practical proposals were developed for improving the practice of law enforcement agencies of Uzbekistan, in particular, cyber forensics and operational-search activities.

Keywords: information technology, cybercrime, law enforcement agencies, digital evidence, OSINT, transnational crime, cybersecurity, foreign experience.

Жаҳон миқёсида ахборот-коммуникация технологияларининг (АКТ) жадал ривожланиши инсоният ҳаётини енгиллаштириш билан бирга, жиноят оламининг тўлиқ кибер-маконга кўчишига сабаб бўлди. Кибер-макон — жисмоний чегараларга эга бўлмаган, анонимлик ва тезкорлик ҳукмронлик қиладиган ҳудуддир. Бугунги кунда фирибгарлик, ўғрилик, гиёҳванд моддалар савдоси ва одам савдоси каби анъанавий жиноятлар ахборот технологиялари воситасида янгича, рақамли Modus Operandi (ишлаш услуби) касб этмоқда.

Ўзбекистон Республикасида киберхавфсизликни таъминлаш ва IT соҳасидаги жиноятларга қарши курашиш давлат хавфсизлигининг ажралмас қисмига айланди. Бироқ, ҳуқуқни муҳофаза қилувчи органлар (ИИО, ДХХ, Прокуратура) фаолиятида жиноятчиларнинг юксак технологик қадамларига муносиб жавоб қайтаришда қатор назарий ва амалий муаммолар кўзга ташланмоқда. Бу эса тизимни кадрлар салоҳияти, техник таъминот ва ҳуқуқий база нуқтаи назаридан тубдан такомиллаштиришни тақозо этади.

Ахборот технологиялари соҳасидаги жиноятларни тергов қилишнинг ҳуқуқий механизмларида қатор назарий масалалар ҳал этилишини кутмоқда:

- **Рақамли далиллар муаммоси:** Жиноят-процессуал қонунчилигимизда "рақамли далил" (digital evidence) тушунчаси ва унинг мақоми тўлиқ очиб берилмаган. Кибержиноят жойи — бу серверлар, булутли технологиялар (Cloud) ёки мобиль қурилма хотирасидир. Электрон далилни нусхалаш, унинг асл нусха эканлигини исботлаш (хэш-суммага асосан) ва судда мақбул далил сифатида тан олиниши назарий жиҳатдан қатъий процессуал тартибга солиниши зарур.
- **Юрисдикция ва трансмиллий жиноятлар:** Кибержиноятчи чет элда туриб (масалан, Европа ёки Осиёда), серверни бошқа давлатда ижарага олган ҳолда, Ўзбекистон фуқаросига нисбатан жиноят содир этади. Бунда жиноят

содир этилган жой қайси давлат ҳисобланиши, қайси давлат қонунлари қўлланилиши борасида халқаро ҳуқуқ доирасида тергов юрисдикциясини аниқлаш катта назарий қийинчиликларни келтириб чиқармоқда.

Тезкор ходимлар ва терговчилар бевосита амалиётда қуйидаги тўсиқларга дуч келишмоқда:

- **Анонимлаштириш технологиялари (Darknet, VPN, Tor):** Жиноятчилар ўзларининг IP-манзилларини ва шахсини яшириш учун замонавий шифрлаш усулларидан фойдаланадилар. Ҳуқуқни муҳофаза қилувчи органларда аксарият ҳолларда занжирли прокси-серверларни бузиб кириш (де-анонимизация) учун кучли техник воситалар ва ҳисоблаш қувватлари етишмайди.
- **Халқаро IT корпорациялар билан ишлашдаги бюрократия:** Telegram, Meta (Facebook, Instagram), Google каби трансмиллий компаниялар серверларидан гумондор ҳақида маълумот олиш узоқ вақт олади ёхуд компаниялар ўз сиёсатини рўкач қилиб маълумот беришни рад этади. Жиноятни иссиқ изидан очишда эса ойлар давом этадиган расмий сўров хатлари тизимнинг самарадорлигини кескин пасайтиради.
- **Кадрлар етишмовчилиги:** Жиноят қидирув ходимлари асосан анъанавий тезкор ҳаракатларга ихтисослашган. Код ёзиш, кибер-ҳужумларни қайтариш ва криптовалюта транзакцияларини кузатиш (blockchain analytics) каби IT-компетенцияга эга бўлган "high-tech" тезкор ходимларга эҳтиёж юқори бўлиб қолмоқда.

Ривожланган давлатлар кибержиноятчиликка қарши ҳуқуқни муҳофаза қилиш тузилмаларини тўлиқ трансформация қилган:

- **АҚШ (FBI Cyber Division):** Америка Қўшма Штатлари Федерал Қидирув Бюросида "Cyber Action Teams" (Кибер тезкор ҳаракат гуруҳлари) мавжуд. Ушбу гуруҳ таркибига терговчидан ташқари, дастурчи, криптограф ва

хакерлик бўйича мутахассислар жалб қилинган. Шунингдек, хусусий сектор (банклар, IT-компаниялар) ва давлат ўртасида "InfraGard" тизими орқали реал вақт режимида шубҳали кибер-ҳаракатлар ҳақида маълумот алмашилади.

- **Эстония:** Кибер-хавфсизлик бўйича Европада етакчи. Эстония полициясида "Кибер-патруль" (Cyber Patrol) лойиҳаси доирасида махсус веб-констабллар фаолият юритади. Улар ижтимоий тармоқларда расмий профиль билан ўтириб, фуқароларга ёрдам беради, фирибгарликларни фош этади ва ёшлар ўртасида кибер-гигиенани тарғиб қилади.
- **Интерпол (IGCI - Сингапур):** Интерполнинг Сингапурдаги Глобал инновациялар мажмуаси (IGCI) кибержиноятчиликка қарши халқаро хаб бўлиб хизмат қилади. Бу марказ дунё бўйлаб полиция органларига Darknet тармоғидаги жиноятларни фош этишда ва рақамли далилларни экспертиза қилишда илғор технологик кўмак беради.

Мамлакатимиз ҳуқуқни муҳофаза қилувчи органларининг ахборот технологиялари соҳасидаги жиноятларга қарши курашиш фаолиятини тубдан такомиллаштириш ва замонавий талабларга мослаштириш мақсадида қуйидаги илмий-амалий таклифлар илгари сурилади:

Биринчидан, Ўзбекистон Республикасининг Жиноят-процессуал кодексига **"Электрон ва рақамли далиллар"** номли махсус боб киритиш. Бу бобда рақамли маълумотларни қидириш, нусха кўчириш, сақлаш (шифрланган ҳолда) ҳамда халқаро булутли серверлардаги маълумотларни қонуний далил сифатида эътироф этишнинг қатъий механизмларини белгилаш зарур.

Иккинчидан, Халқаро ҳуқуқий ҳамкорликни кенгайтириш мақсадида Ўзбекистон Республикасининг Европа Кенгашининг **"Кибержиноятчилик тўғрисида"ги Будапешт Конвенциясига** қўшилишини тезлаштириш. Бу орқали хорижий давлатлар, трансмиллий IT-компаниялар ва Ўзбекистон ИИО

ўртасида кибер-жиноятчиларга оид маълумотларни соатбай ва тезкор алмашишнинг қонуний платформаси шаклланади.

Учинчидан, ИИВ, ДХХ ва Бош прокуратура тизимида асосан дастурлаш, кибер-разведка (OSINT) ва криптовалюта трекингини мукаммал билувчи кадрлардан иборат **Ягона идоралараро Кибер-тергов (Cyber Investigation) марказини** ташкил этиш. Марказ ходимларига анъанавий ҳуқуқий билимлардан кўра кўпроқ техник ("High-Tech") билимларни берувчи халқаро сертификацияланган (CEH, CHFI) ўқув курсларини жорий қилиш.

Хулоса ўрнида шуни таъкидлаш керакки, ахборот технологиялари соҳасидаги жиноятлар интеллектуал салоҳиятли ва технологик қуролланган ҳуқуқбузарлар томонидан содир этилади. Бу урушда фақатгина "анъанавий" тергов ва оператив усуллар билан ғалаба қозониб бўлмайди. Ҳуқуқни муҳофаза қилувчи органлар тизимни тўлиқ рақамлаштириши, кибер-мутахассисларни тайёрлаши ва халқаро ахборот майдонида мустаҳкам интеграцияга эришиши бугунги куннинг кечиктириб бўлмас талабидир.

REFERENCES

1. Ўзбекистон Республикасининг "Киберхавфсизлик тўғрисида"ги Қонуни. 15.04.2022 йилдаги ЎРҚ-764-сон.
2. Ўзбекистон Республикасининг Жиноят ҳамда Жиноят-процессуал кодекслари. Электрон ресурс: https://lex.uz.
3. Худойбердиев А.А. "Маъмурий ишларни юритиш кафолатлари ва ҳуқуқни қўллаш амалиёти". Ўқув қўлланма. – Тошкент: ИИВ Академияси, 2024.
4. Ғофуров И., Каримов У. "Ахборот хавфсизлиги ва кибержиноятларга қарши курашиш асослари". – Тошкент: ИИВ Малака ошириш институти, 2022.
5. Federal Bureau of Investigation (FBI). "Internet Crime Report 2023: Cyber Division Strategies". U.S. Department of Justice, 2024.

6. Interpol. "Global Cybercrime Threat Assessment: Policing in the Digital Age". IGCI, Singapore, 2023.
7. Council of Europe. "Convention on Cybercrime" (Budapest Convention), ETS No. 185.