ХОРИЖИЙ ДАВЛАТЛАР ҚОНУНЧИЛИГИДА РАҚАМЛИ МАКОНДАГИ ЎҒИРЛИКЛАРНИ ТЕРГОВ ҚИЛИШНИНГ ҚИЁСИЙ-ҲУҚУҚИЙ ТАҲЛИЛИ

Саидов Бобоқул Ёрикулович
Ўзбекистон Республикаси Бош прокуратураси Криминоген вазиятни таҳлил қилиш бошқармаси бошлиғи ўринбосари

АННОТАЦИЯ: *Ушбу илмий мақолада рақамли маконда содир этиладиган ўғирликлар ва трансчегаравий кибержиноятларни тергов қилишнинг моддий ва процессуал-ҳуқуқий жиҳатлари қиёсий-ҳуқуқий нуқтаи назардан таҳлил қилинган. Тадқиқотда АҚШ, Европа Иттифоқи мамлакатлари ва бошқа ривожланган давлатларнинг кибержиноятчиликка қарши курашиш қонунчилиги, электрон (рақамли) далилларни тўплаш, фиксация қилиш ҳамда OSINT (очиқ манбалардан разведка маълумотларини йиғиш) усулларини қўллаш тажрибаси атрофлича ўрганилган. Будапешт ва БМТнинг Кибержиноятчиликка қарши конвенциялари доирасидаги халқаро ҳамкорлик ва 24/7 тезкор алоқа тармоғининг роли очиб берилган.*

Калит сўзлар: *рақамли макондаги ўғирлик, кибержиноятчилик, электрон далиллар, рақамли излар, OSINT усуллари, Будапешт конвенцияси, БМТ Конвенцияси, ЖК 169-моддаси, киберэкспертиза, хеш-сумма.*

АННОТАЦИЯ: *В данной научной статье с сравнительно-правовой точки зрения анализируются материальные и процессуально-правовые аспекты расследования хищений и трансграничных киберпреступлений в цифровой сфере. В исследовании подробно изучен опыт США, стран Европейского Союза и других развитых государств в области законодательства по борьбе с киберпреступностью, сбора, фиксации электронных (цифровых) доказательств, а также применения методов OSINT (разведка на основе открытых источников). Раскрыта роль международного сотрудничества и круглосуточной сети 24/7 в рамках Будапештской конвенции и Конвенции ООН против киберпреступности.*

Ключевые слова: *хищение в цифровой сфере, киберпреступность, электронные доказательства, цифровые следы, методы OSINT, Будапештская конвенция, Конвенция ООН, статья 169 УК, киберэкспертиза, хеш-сумма.*

ABSTRACT: *This scientific article provides a comprehensive comparative legal analysis of the substantive and procedural aspects of investigating digital theft and transboundary cybercrimes. The study systematically examines the legislation*

and investigative practices of the United States, European Union member states, and other advanced jurisdictions regarding the collection, preservation, and authentication of electronic (digital) evidence, as well as the strategic deployment of OSINT (Open Source Intelligence) techniques. It highlights the mechanisms of international cooperation and 24/7 contact networks established under the Budapest Convention and the 2024 UN Convention against Cybercrime.

Keywords: *digital theft, cybercrime, electronic evidence, digital traces, OSINT techniques, Budapest Convention, UN Convention, Article 169 of CC, cyber forensics, hash value.*

1. КИРИШ

Жамият ҳаётининг барча соҳалари жадал рақамлашуви, банк-молия тизимининг масофавий хизмат кўрсатиш форматларига ўтиши, электрон ҳамёнлар, крипто-активлар ва булутли технологияларнинг кенг жорий этилиши анъанавий мулкий жиноятларнинг трансформациялашувига олиб келди. Бугунги кунда мулкка тажовуз қилувчи жиноятлар, хусусан, яширин равишда ўзганинг мулкини талон-торож қилиш — ўғирлик жинояти тобора виртуал ва рақамли маконга кўчмоқда. Агар илгари ўғирлик жинояти муайян моддий объектни жисмоний эгаликдан чиқариш орқали содир этилган бўлса, замонавий рақамли маконда у ахборот тизимларига рухсатсиз кириш, парол ва идентификация маълумотларини эгаллаш, банк ва тўлов иловалари алгоритмларига ноқонуний мудохала қилиш ҳамда электрон маблағларни масофадан туриб транзит ва 'дроп' ҳисобварақларига ўтказиш йўли билан амалга оширилмоқда.

Замонавий криминалистик тадқиқотлар кўрсатишича, ҳозирда деярли барча анъанавий ва юқори технологик жиноятлар таркибида у ёки бу кўринишдаги рақамли таркибий қисм (digital component) ва рақамли излар мавжуддир. ФБРнинг Интернетда содир этилган жиноятлар бўйича шикоятларни қабул қилиш маркази (IC3) маълумотларига кўра, кибермаконда содир этиладиган жиноятлар ва улар натижасида етказиладиган молиявий зарар миқдори йилдан-йилга геометрик прогрессияда ортиб бормоқда. Бундай жиноятларнинг асосий хусусиятлари сифатида уларнинг анонимлиги, экстерриториаллиги (жиноятчи бир давлатда, сервер ва платформа иккинчи давлатда, жабрланувчи эса учинчи давлатда жойлашиши) ҳамда электрон далилларнинг ўта таъсирчанлиги ва тез йўқолувчанлиги намоён бўлади.

Ўзбекистон Республикасида ҳам киберхавфсизликни таъминлаш, ахборот-коммуникация технологиялари ёрдамида содир этиладиган жиноятларга қарши курашиш масаласи давлат сиёсатининг стратегик устувор

йўналишига айланди. Хусусан, 'Киберхавфсизлик тўғрисида'ги Қонун, Президентнинг 2025 йил 30 апрелдаги ПҚ–153-сон 'Ахборот технологиялари ёрдамида содир этиладиган жиноятларга қарши курашиш фаолиятини янада кучайтиришга қаратилган чора-тадбирлар тўғрисида'ги Қарори ҳамда 2022 йил 19 октябрдаги ЎРҚ–794-сон Қонуни билан Жиноят кодексининг 169-моддаси учинчи қисми 'б' бандига 'қонунга хиллоф равишда (рухсатсиз) ахборот тизимига кириб ёки ундан фойдаланиб' содир этилган ўғирлик учун махсус квалификацияловчи белгининг киритилиши ҳуқуқий базани мустаҳкамлашга хизмат қилмоқда.

Бироқ, тергов амалиётида рақамли изларни аниқлаш, олиш ва процессуал расмийлаштириш, хорижий сервер ва провайдерлардан маълумот олиш, шунингдек, киберўғирликни ахборот тизимларидан фойдаланиб содир этиладиган фирибгарлик (ЖК 168-моддаси) ёки компютер ахборотига рухсатсиз кириш (ЖК 278^2-моддаси) жиноятларидан тўғри чегаралаш борасида қатор муаммолар сақланиб қолмоқда. Шу сабабли ривожланган хорижий давлатлар (АҚШ, Европа Иттифоқи аъзолари) қонунчилиги ва тергов амалиётини қиёсий-ҳуқуқий таҳлил қилиш ҳамда уларнинг илғор усулларини миллий ҳуқуқий тизимга имплементация қилиш долзарб илмий ва амалий аҳамият касб этади.

2. АСОСИЙ ҚИСМ

2.1. Хорижий давлатлар (АҚШ, ЕИ) қонунчилиги ва амалиётида рақамли макондаги ўғирликларнинг ҳуқуқий квалификацияси

Хорижий давлатларнинг жиноят қонунчилигини ўрганиш шуни кўрсатадики, рақамли макондаги мулкий жиноятларни ва компютер тизимлари орқали содир этиладиган ўғирликларни квалификация қилишда икки асосий ҳуқуқий тизим — англо-саксон ва романо-герман ҳуқуқ оилалари ўзига хос ёндашувларни намойиш этади.

Америка Қўшма Штатлари (АҚШ) қонунчилигида рақамли макондаги мулкий жиноятлар ва ахборот тизимларига ноқонуний кириш орқали маблағларни эгаллаш алоҳида комплекс федерал қонунлар билан тартибга солинади. Асосий норматив-ҳуқуқий ҳужжат — Компютер фирибгарлиги ва суиистеъмоллиги тўғрисидаги қонун (Computer Fraud and Abuse Act - CFAA, 18 U.S.C. § 1030) ҳисобланади. Ушбу қонун ҳар қандай ҳимояланган компютер ёки тармоққа ваколатсиз (рухсатсиз) киришни ёки белгиланган кириш ваколатларидан четга чиққан ҳолда қимматли маълумотларни, молиявий ресурсларни эгаллашни жиноят деб баҳолайди ва бунда технология турига чеклаб қўйилмайди. Бундан ташқари, Электрон алоқа махфийлиги тўғрисидаги қонун (Electronic Communications Privacy Act -

ECPA) ва Сақланаётган алоқалар тўғрисидаги қонун (Stored Communications Act - SCA) орқали рақамли маълумотлар, электрон почта ва трафик маълумотларини олиш ва терговда фойдаланиш тартиби қатъий белгиланган. АҚШда рақамли макондаги ўғирлик ва фирибгарлик ишлари бўйича тергов ҳаракатлари АҚШ Адлия вазирлиги (DOJ) ва ФБР (FBI) таркибидаги махсус кибержиноятчиликка қарши курашиш гуруҳлари ҳамда CISA томонидан олиб борилади. IC3 тизими эса бутун мамлакат бўйича рақамли талон-торожларга оид аризаларни марказлаштирилган ҳолда тўплаб, улар ўртасидаги технологик ва молиявий боғланишларни автоматлаштирилган тарзда аниқлайди.

Буюк Британияда 1990 йилдаги Компютердан ноқонуний фойдаланиш тўғрисидаги қонун (Computer Misuse Act 1990) ва 2006 йилдаги Фирибгарлик тўғрисидаги қонун (Fraud Act 2006) амал қилади. Компютер материалларига, трафик маълумотларига ва ахборот тизимларига ҳар қандай мақсадда рухсатсиз кириш ёки уларни ўзгартириш орқали мулкий манфаат олиш технологик жиҳатдан нейтрал тарзда жазоланади.

Европа Иттифоқи (ЕИ) мамлакатларида (Германия, Франция, Австрия, Болгария, Нидерландия) рақамли ўғирлик ва компютер фирибгарлиги романо-герман жиноят-ҳуқуқий доктринаси асосида квалификация қилинади. Масалан, **Германия Жиноят кодексининг (Strafgesetzbuch - StGB) 263a-моддаси** ('Компютер фирибгарлиги') компютер дастурини нотўғри шакллантириш, ёлғон ёки тўлиқ бўлмамаган маълумотларни киритиш, маълумотлардан рухсатсиз фойдаланиш ёки ахборотни қайта ишлаш жараёнига ноқонуний аралашиш орқали бошқа шахснинг мулкига зарар етказишни жиноий жавобгарликка сабаб бўлишини белгилайди. Германия қонунчилиги ўрнатилган техник ҳимоя воситаларини бузиб, электрон маълумотларга киришни жуда кенг қамровда қамраб олади. **Франция ва Австрия** жиноят қонунчилигида ҳам электрон тўлов воситаларидан фойдаланиб содир этилган талон-торожликлар ва авторизация чекловларини бузиш алоҳида оғирлаштирувчи ҳолат сифатида қаралади.

Қиёсий таҳлил шуни кўрсатадики, хорижий қонунчиликда рақамли макондаги ўғирликни квалификация қилишда **'технологик нейтраллик' (technological neutrality)** принципига таянилади. Яъни, жиноят қонуни муайян бир дастурий таъминот ёки қурилма брендига боғланмайди, балки қилмишнинг ҳуқуқий ва техник моҳиятига — ахборот тизимига ноқонуний кириш, маълумотларни модификация қилиш ва мулкдорнинг иродасига зид равишда активларни ўзлаштириш фактларига баҳо беради.

2.2. Рақамли изларни йиғиш, OSINT усуллари ва махсус дастурий-аналитик воситалардан фойдаланиш тажрибаси

Рақамли маконда содир этиладиган ўғирликларни аниқлаш ва тергов қилиш анъанавий процессуал ҳаракатлардан фарқ қилиб, махсус тактик ва оператив-техник усулларни талаб этади. Хорижий давлатлар тергов амалиётида асосий эътибор рақамли изларни марказлаштирилган ҳолда йиғиш ва **OSINT (Open Source Intelligence - очиқ манбалар орқали разведка қилиш)** усулларига қаратилган.

АҚШ олимлари ва криминалистлари томонидан кибержиноятларни тергов қилишда қуйидаги 3 та бирламчи ва фундаментал метод ажратиб кўрсатилади:

1. **Оммага очиқ бўлган онлайн маълумотларни тўплаш (OSINT):** Ижтимоий тармоқлар, домен номлари реестрлари (WHOIS), очиқ серверлар, IP-манзиллар базалари, BGP-маршрутлаш қайдлари, форумлар ва ахборот платформаларидан жиноятчининг рақамли профилини аниқлаш;
2. **Онлайн хизмат кўрсатувчи провайдерлар (ISP) ва платформаларга сўровлар юбориш:** Ҳостинг провайдерлар, IT-платформалар, электрон почта ва мессенжер хизматларидан фойдаланувчиларнинг IP-логи, вақт кўрсаткичлари (timestamps) ва транзакция қайдларини олиш;
3. **Ахборот тизимлари ва қурилмаларни криминалистик кўздан кечириш (Digital Forensics):** Олиб қўйилган компютер ва телекоммуникация қурилмаларидаги тизим журналлари (system logs), аудиторлик текшируви ёзувлари (audit logs) ҳамда вақтинчалик файлларни криминалистик нусхалаш орқали ўрганиш.

Ривожланган давлатларда рақамли изларни таҳлил қилишда йирик автоматик дастурий-аналитик мажмуалар кенг қўлланилмоқда:

- **“Log Management” ва SIEM тизимлари (Splunk, ELK Stack):** АҚШ ва ЕИ ҳуқуқ-тартибот идораларида тармоқ трафиги, сервер журналлари ва фойдаланувчиларнинг ҳаракатларини реал вақт режимида мониторинг қилиш ҳамда маълумотлар сизиб чиқиши ёки рухсатсиз кириш изларини марказлаштирилган тартибда таҳлил қилиш учун қўлланилади.
- **Крипто-активлар ва блокчейн аналитикаси дастурлари (Chainalysis, CipherTrace Scout, Bitfury Crystal):** Нидерландия ва АҚШ тергов органлари ўғирланган электрон пуллар ва криптовалюталарнинг каскадли ўтказмаларини, 'дроп' ҳамёнлар занжирини ва ноқонуний накдлаштириш нуқталарини транзакциялар графиги орқали визуаллаштириш ва кузатиш учун айнан ушбу аналитик платформалардан фойдаланадилар.
- **Рақамли тактикани аниқлаш тизимлари:** АҚШ ФБР томонидан қўлланиладиган махсус аналитик тизимлар жиноятчи

гуруҳларнинг хусусий кодини ва қўллайдиган зарарли дастурий таъминотини автоматик аниқлаб, жиноятчиларнинг шахсини ва жойлашган жойини ўрнатишга хизмат қилади.

- **Шифрланган тармоқларда тергов ўтказиш усуллари:** Махсус муҳитларда содир этиладиган оғир ва трансчегаравий жиноятларни фош этишда махсус дастурий-техник тергов усуллари қўлланилади.

2.3. Рақамли далиллар билан ишлашнинг процессуал тартиби ва халқаро ҳамкорлик механизмлари

Рақамли далиллар (digital/electronic evidence) анъанавий ашёвий далиллардан ўзининг физик шаклга эга эмаслиги, осон ўзгарувчанлиги, тез ўчириб юборилиши ва нусхаланганда асли билан нусхаси ўртасида фарқ қолмаслиги каби специфик хусусиятлари билан ажралиб туради. Шу сабабли, рақамли далилларни олиш ва судда мақбул далил деб топиш учун хорижий процессуал қонунчиликда қатъий стандартлар ўрнатилган.

Бу борада асосий тамойил **'Chain of Custody' (Далилларни сақлаш ва кузатиш занжири)** деб аталади. Ушбу тамойилга кўра, рақамли маълумот аниқланган вақтдан бошлаб судда далил сифатида баҳолангунга қадар унинг яхлитлиги ва ўзгармаганлиги технологик жиҳатдан исботланиши лозим. Хорижий амалиётда бу жараён **хеш-сумма (SHA-256, MD5 алгоритмлари)** ёрдамида таъминланади. Рақамли манбадан форензик нусха олинганда, унинг хеш-коди ҳисоблаб чиқилади ва баённомага киритилади. Агар судда тақдим этилган маълумотнинг хеш-коди дастлабки кўрсаткичга мос келса, далилнинг мақбуллиги ва дахлсизлиги тан олинади.

Трансчегаравий киберўғирликларни тергов қилишда халқаро-ҳуқуқий ҳамкорлик ҳал қилувчи аҳамиятга эга. Боиси, жиноят излари хорижий серверларда сақланади, анъанавий дипломатик сўровлар (MLAT) эса ойлаб вақт олади, ваҳоланки кибермаконда далиллар бир неча дақиқада йўқ қилиниши мумкин.

Дунё тажрибасида бу муаммони ҳал қилишнинг 2 та асосий глобал конвенциявий механизми мавжуд:

1. **Европа Кенгашининг Кибержиноятлар тўғрисидаги Будапешт конвенцияси (2001 йил 23 ноябрь):** Кибержиноятчиликка қарши курашдаги илк халкаро ҳужжат бўлиб, компютер маълумотларини ва трафикни тезкор сақлаб қўйиш (expedited preservation), провайдерлардан маълумот олиш, тизимларни тинтув қилиш ва энг муҳими — **24/7 режигида ишлайдиган миллий алоқа нуқталари тармоғини** яратишни назарда тутади. 2022 йилда қабул қилинган 2-Илова Протокол эса электрон далилларга трансчегаравий тўғридан-тўғри кириш имкониятини янада кенгайтирди.

2. **БМТнинг Кибержиноятчиликка қарши Конвенцияси (2024 йил 24 декабрь):** Глобал миқёсда жиддий жиноятлар бўйича электрон далиллар билан алмашиш ва халқаро ҳуқуқий ёрдам кўрсатишнинг универсал қоидаларини белгилаб берди.

3. ХУЛОСА ВА ТАКЛИФЛАР

Олиб борилган қиёсий-ҳуқуқий таҳлил, хорижий давлатларнинг қонунчилиги ва тергов амалиётини ўрганиш натижалари асосида, Ўзбекистон Республикасида рақамли макондаги ўғирликлар ва кибержиноятларни тергов қилиш самарадорлигини ошириш, шунингдек, миллий қонунчиликни такомиллаштириш бўйича қуйидаги **аниқ ва илмий асосланган таклифлар** илгари сурилади:

1. **Ўзбекистон Республикаси Жиноят кодексининг 169-моддасини такомиллаштириш ва диспозициясини аниқлаштириш:** ЖК 169-моддаси учинчи қисми 'б' бандидаги 'ахборот тизимига кириб ёки ундан фойдаланиб' содир этилган ўғирлик ва ЖК 168-моддаси учинчи қисми 'г' бандидаги ахборот тизимидан фойдаланиб содир этилган фирибгарлик нормалари ўртасидаги чегарани қатъий белгилаш лозим. Олий суд Пленумининг тегишли қарорларида (хусусан, 2023 йил 23 июндаги 17-сон қарорида) компютер тизимига ноқонуний кириб, алгоритмларни ўзгартириш ёки паролларни ғайриқонуний эгаллаш орқали мулкдорнинг иродасига зид равишда пулларни олиб чиқиб кетиш айнан **электрон ўғирлик (ЖК 169-моддаси)** сифатида квалификация қилиниши, инсонни алдаш ва ишончини суиистеъмол қилиш ҳолатлари эса **фирибгарлик (ЖК 168-моддаси)** сифатида баҳоланиши шартлиги аниқ шарҳлаб берилиши керак.

2. **Жиноят-процессуал кодексида 'Рақамли далиллар' тўғрисидаги алоҳида бобни ва мустақил процессуал нормаларни мустаҳкамлаш:** АҚШ ва ЕИ тажрибасидан келиб чиқиб, ЖПКга 'Рақамли далиллар' тушунчаси, уларни тўплаш, олиб қўйиш, кўздан кечириш ва сақлаш тартибини тартибга солувчи нормаларни киритиш лозим. ЖПКга хеш-суммаларни (SHA-256) баённомада қайд этиш, форензик нусха олиш ҳамда далилларни сақлаш ва кузатиш занжирини (Chain of Custody) мажбурий расмийлаштириш қоидалари киритилиши рақамли далилларнинг судда мақбуллигини тўлиқ кафолатлайди.

3. **Рақамли излар билан ишлашда IT-мутахассиси иштирокини мажбурий этиб белгилаш ва 'Киберэкспертиза' институтини ривожлантириш:** Тергов ҳаракатлари давомида (тинтув, кўздан кечириш, олиб қўйиш) рақамли ташувчилардан маълумотларни олишда IT-мутахассиси ва киберкриминалист иштирокини ЖПКда мажбурий қилиб белгилаш зарур.

Шунингдек, мутахассис томонидан олинган рақамли далилларни баҳолаш учун мустақил 'Суд-киберэкспертизаси' институтини қонунчилик асосида мустаҳкамлаш тавсия этилади.

4. **Тергов органлари фаолиятига SIEM, Log Management ва OSINT аналитик тизимларини кенг жорий этиш:** АҚШнинг ICЗ ва ЕИнинг кибермарказлари тажрибаси асосида, Ҳуқуқни муҳофаза қилувчи органлар таркибида ягона марказлаштирилган 'Log Management' ва SIEM тизимларини ҳамда махсус OSINT аналитик бўлинмаларини ташкил этиш лозим. Бу интернет-провайдерлар, банклар, тўлов тизимлари ва крипто-биржалар логларини реал вақт режимида cross-referencing (ўзаро солиштириш) орқали 'дроп' ҳисобварақларини ва жиноятчиларнинг шахсини тезкор аниқлаш имконини беради.

5. **Халқаро ҳамкорлик ва 24/7 тезкор алоқа тармоқларига интеграциялашувни жадаллаштириш:** Трансчегаравий киберўғирликларга қарши курашишда ва хорижий серверлардаги электрон далилларни музлатиб қўйиш (expedited preservation) учун Будапешт конвенциясининг 24/7 алоқа нуқталари механизмидан унумли фойдаланиш, шунингдек БМТнинг 2024 йилги Кибержиноятчиликка қарши конвенцияси доирасидаги халқаро процессуал ҳамкорликни миллий амалиётга фаол татбиқ этиш зарур.

4. ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. Ўзбекистон Республикасининг Жиноят кодекси // Қонунчилик маълумотлари миллий базаси.
2. Ўзбекистон Республикасининг Жиноят-процессуал кодекси // Қонунчилик маълумотлари миллий базаси.
3. Ўзбекистон Республикасининг 'Киберхавфсизлик тўғрисида'ги 2022 йил 15 апрелдаги ЎРҚ–764-сон Қонуни // Қонунчилик маълумотлари миллий базаси.
4. Ўзбекистон Республикаси Президентининг 'Ахборот технологиялари ёрдамида содир этиладиган жиноятларга қарши курашиш фаолиятини янада кучайтиришга қаратилган чора-тадбирлар тўғрисида'ги 2025 йил 30 апрелдаги ПҚ–153-сон Қарори.
5. Ўзбекистон Республикаси Олий суди Пленумининг 'Фирибгарликка оид ишлар бўйича суд амалиёти тўғрисида'ги 2023 йил 23 июндаги 17-сон қарори.

6. Атемов Б.У. Киберфирибгарлик билан курашиш: миллий муаммолар ва халқаро амалиёт // Modern Science and Research. – 2026. – Vol. 5, Issue 10. – Б. 148-155.

7. Закурлаев А.К. Тезкор-қидирув фаолиятида рақамли далиллардан фойдаланишнинг процессуал ва криминалистик муаммолари // Тергов амалиёти. – 2023. – № 4 (20). – Б. 151-155.

8. Cernomoreț S., Nastas A. Comparative Analysis of Cybercrime in the Criminal Law System // ADJURIS – International Journal of Law and Social Sciences. – 2023. – Vol. 12, Issue 1. – Pp. 33-82.

9. Council of Europe. Convention on Cybercrime (Budapest Convention), ETS No. 185, Budapest, 23.XI.2001.

10. United Nations Office on Drugs and Crime (UNODC). United Nations Convention against Cybercrime: Strengthening international cooperation. – Vienna: UN, 2024.

11. FBI Internet Crime Complaint Center (IC3). Internet Crime Report 2020. – Washington D.C.: Federal Bureau of Investigation, 2021.