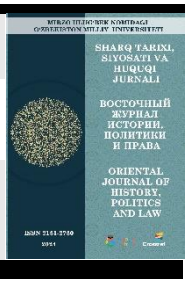
DOI: https://doi.org/10.37547/supsci-ojhpl-06-07-30 **Pages: 265-272**

Oriental Journal of History, Politics and Law

SUPPORT SCIENCE

ORIENTAL JOURNAL OF HISTORY, POLITICS AND LAW

journal homepage:
https://www.supportscience.uz/index.php/ojhpl



THE USE OF OPERATIONAL-SEARCH MEASURES IN COMBATING CYBERCRIMES

Timur Yusupjanovich Kamilov
Independent Researcher
Ministry of Internal Affairs of the Republic of Uzbekistan
Tashkent, Uzbekistan

ABOUT ARTICLE

Key words: cybercrime, operational-search measures, digital evidence, cybersecurity, information and communication technologies, operational-search activity, crime detection.

Received: 24.07.26
Accepted: 25.07.26
Published: 26.07.26

Abstract: This article examines the role and significance of operational-search measures in combating cybercrime. The legal and methodological foundations of organizing and conducting operational-search activities in the context of the growing use of information and communication technologies for criminal purposes are analyzed. The article considers the main operational-search measures used in detecting and investigating cybercrimes, the procedure for their conduct, issues of collecting and consolidating digital evidence, as well as foreign experience and existing problems in the legislation of the Republic of Uzbekistan in this area. Practical recommendations have been developed based on the research results.

КИБЕРЖИНОЯТЛАРГА ҚАРШИ КУРАШИШДА ТЕЗКОР-ҚИДИРУВ ТАДБИРЛАРИДАН ФОЙДАЛАНИШ

Тимур Юсупжанович Камилов
Ўзбекистон Республикаси ИИВ
мустақил изланувчиси
Тошкент, Ўзбекистон

МАҚОЛА ҲАҚИДА

Калит сўзлар: кибержиноят, тезкор-қидирув тадбирлари, рақамли далиллар, киберхавфсизлик, ахборот-коммуникация технологиялари, тезкор-қидирув фаолияти, жиноятни очиш.

Аннотация: Мазкур мақолада кибержиноятларга қарши курашишда тезкор-қидирув тадбирларининг ўрни ва аҳамияти тадқиқ этилади. Жиноий тарзда ахборот-коммуникация технологияларидан

фойдаланиш тобора кенг тус олаётган ҳозирги шароитда тезкор-қидирув фаолиятини ташкил этиш ва ўтказишнинг ҳуқуқий-методологик асослари таҳлил қилинади. Мақолада кибержиноятларни очиш ва тергов қилишда фойдаланиладиган асосий тезкор-қидирув тадбирлари, уларни ўтказиш тартиби, рақамли далилларни тўплаш ва мустаҳкамлаш масалалари, шунингдек, чет эл тажрибаси ва Ўзбекистон Республикаси қонунчилигида мазкур соҳадаги мавжуд муаммолар кўриб чиқилади. Тадқиқот натижалари асосида амалий тавсиялар ишлаб чиқилган.

ИСПОЛЬЗОВАНИЕ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Тимур Юсупжанович Камилов
Самостоятельный соискатель
Министерства внутренних дел Республики Узбекистан
Ташкент, Узбекистан

О СТАТЬЕ

Ключевые слова: киберпреступность, оперативно-розыскные мероприятия, цифровые доказательства, кибербезопасность, информационно-коммуникационные технологии, оперативно-розыскная деятельность, раскрытие преступлений.

Аннотация: В данной статье исследуются роль и значение оперативно-розыскных мероприятий в борьбе с киберпреступностью. В условиях стремительного роста преступного использования информационно-коммуникационных технологий анализируются правовые и методологические основы организации и проведения оперативно-розыскной деятельности. Рассматриваются основные оперативно-розыскные мероприятия, применяемые при выявлении и расследовании киберпреступлений, порядок их проведения, а также вопросы сбора, сохранения и закрепления цифровых доказательств. Кроме того, анализируются зарубежный опыт и существующие проблемы законодательства Республики Узбекистан в данной сфере. На основе результатов исследования разработаны практические рекомендации, направленные на повышение эффективности борьбы с киберпреступностью.

Кириш. Ҳозирги глобаллашув ва рақамлашув даврида ахборот-коммуникация технологияларини жамиятнинг барча соҳаларига кириб бориши жиноий ҳатти-ҳаракатлар учун принципиал янги шаклларнинг вужудга келишига олиб келди. Кибержиноятлар ўз кўлами, трансмиллий хусусияти ва аниқлашнинг мураккаблиги жиҳатидан ҳуқуқни муҳофаза қилувчи органлар учун жиддий синов бўлиб қолмоқда. Мазкур вазият тезкор-қидирув фаолиятини ташкил этишга нисбатан тамоман янги ёндашувларни шакллантиришни тақозо этади.

Муҳокама ва натижалар. Жаҳон миқёсида кибержиноятлардан келадиган зарар йилдан-йилга ортиб бормоқда. Халқаро экспертларнинг баҳолашига кўра, 2025 йилда глобал иқтисодиётга кибержиноятлар етказган зарар 8 трлн. доллардан ошди, 2027 йилга бориб 10,5 трлн. долларга етиши кутилмоқда. Ўзбекистон Республикасида ҳам рақамли трансформациянинг жадаллашуви билан бир қаторда киберхавфсизлик соҳасидаги таҳдидлар тобора кучайиб бормоқда.

Тезкор-қидирув тадбирлари (бундан кейин — ТҚТ) кибержиноятларни очиш, тергов қилиш ва олдини олишда асосий воситалардан бири бўлиб хизмат қилади. Бироқ анъанавий ТҚТ усуллари кибермуҳитнинг ўзига хос хусусиятлари, рақамли изларнинг ўчиб кетиш хавфи, шифрлаш технологиялари, анонимлаштириш воситалари ва трансмиллий юрисдикция муаммолари туфайли ўзгача ёндашувни тақозо этади.

Кибержиноят тушунчасини аниқлашда ҳуқуқ фанида бир неча ёндашув мавжуд. Кенг маънода кибержиноят деганда компьютер тизимлари, тармоқлар ёки рақамли маълумотларга нисбатан ёхуд уларнинг ёрдамида содир этиладиган барча жиноий қилмишлар тушунилади. Тор маънода эса бевосита ахборот-коммуникация тизимларини нишон қилиб олувчи жиноятлар назарда тутилади.

Бирлашган Миллатлар Ташкилотининг 2001 йилда қабул қилинган таснифига мувофиқ, кибержиноятлар қуйидаги гуруҳларга бўлинади:

1) компьютер тизимларига рухсатсиз кириш;

2) компьютер маълумотларига рухсатсиз таъсир кўрсатиш;

3) компьютер тизимларини суиистеъмол қилиш;

4) компьютер жиноятчилиги (фирибгарлик, сохталаштириш);

5) мазмун жиноятлари (болалар порнографияси ва б.);

6) муаллифлик ҳуқуқини бузиш.

Ўзбекистон Республикасининг Жиноят кодексида кибержиноятларга оид нормалар акс этган. Хусусан, XX1 боби Ахборот технологиялари соҳасидаги жиноятларга

бағишланган. Шу билан бир қаторда кибертехнологиялардан фойдаланилган ҳолда содир этиладиган аралаш жиноятлар (товламачилик, фирибгарлик, пул ювиш ва б.) ҳам алоҳида ўрин тутади.

Кибержиноятларнинг тезкор-қидирув фаолияти нуқтаи назаридан муҳим хусусиятлари қуйидагилардан иборат: биринчидан, жиноий изларнинг тезда йўқолиш хавфи; иккинчидан, жиноятчиларнинг кўпинча юрисдикцияларо тарзда фаолият юритиши; учинчидан, VPN, Tor каби анонимлаштириш воситалари ва криптовалюталарнинг кенг қўлланилиши; тўртинчидан, жиноятнинг виртуал муҳитда амалга оширилиши туфайли анъанавий гувоҳлик олишнинг чекланганлиги.

Ўзбекистон Республикасининг «Тезкор-қидирув фаолияти тўғрисида»ги Қонунида белгиланган ТҚТ тизимига кибержиноятлар контекстида ўзига хос тарзда ёндашиш талаб этилади. Амалиёт ва назария таҳлили асосида кибержиноятларни очишда қўлланиладиган тадбирларни бир неча гуруҳга ажратиш мумкин.

Кибержиноятларга қарши курашишда энг кенг қўлланиладиган ТҚТ турларидан бири ахборот тизимлари ва тармоқлар фаолиятини кузатишдир. Интернет-трафикни мониторинг қилиш, зарарли IP-манзилларни аниқлаш, шубҳали домен номларини ўрганиш шу гуруҳга киради. Ўзбекистон Республикасида телекоммуникация операторлари ва интернет-провайдерлар ҳуқуқни муҳофаза қилувчи органлар сўровига биноан фойдаланувчилар ҳақидаги маълумотларни тақдим этишга мажбурдир.

Шубҳали шахсларнинг онлайн-фаолиятини, ижтимоий тармоқлардаги ҳатти-ҳаракатларини ва рақамли алоқаларини қонун доирасида кузатиш ТҚТнинг муҳим кўриниши ҳисобланади. Бундай кузатув амалга оширилганда Ўзбекистон Республикаси Конституциясида кафолатланган шахсий дахлсизлик ҳуқуқи ва хат-хабарлар сирини сақлаш принципига риоя этилиши шарт. Суд санкцияси олинмасдан амалга оширилган ТҚТ натижалари суд муҳокамасида далил сифатида тан олинмайди.

Кибержиноятларни очишда махфий агентлар фойдаланиладиган тадбирлар ҳам муҳим ўрин тутади. Dark Web платформаларида жиноий гуруҳларга кириш, суиистеъмолчилик материалларини тарқатувчи тармоқларни аниқлаш, молиявий жиноятларда пул кетишини кузатиш («пул йўлини топиш») шу тоифадаги тадбирлар жумласига киради. Бироқ, бундай тадбирларни ўтказишда провокацияни истисно этиш принципи қатъий сақланмоғи лозим.

Рақамли қурилмалар компьютер, смартфон, маршрутизатор (роутер) ва бошқаларни қидириш, судга қадар олиб қўйиш, экспертиза тайинлаш орқали рақамли далилларни сақлаш тадбирлари кибержиноятларга қарши куришишнинг ажралмас қисмини ташкил

этади. «Рақамли криминалистика» методологиясига мувофиқ барча далиллар ишончли сақлаш занжири (chain of custody) асосида тўпланиши зарур.

Кибержиноятлар кўпинча молиявий манфаатни кўзлаб содир этилади. Шу сабабли криптовалюта транзакцияларини кузатиш, Blockchain таҳлили, шубҳали молиявий операцияларни аниқлаш ва молиявий разведкани амалга ошириш тезкор-қидирув фаолиятида тобора кенг қўлланилмоқда.

Рақамли далиллар кибержиноятларга қарши курашишда марказий ўринни эгаллайди. Жиноят-процессуал қонунчиликда рақамли далилларнинг мавқеини аниқлаштириш муҳим илмий ва амалий аҳамият касб этади. Ўзбекистон Республикаси ЖПК нормалари умумий хусусиятга эга бўлиб, рақамли далилларнинг ўзига хос жиҳатларини тўлиқ қамраб олмайди.

Халқаро стандартлар нуқтаи назаридан рақамли далилларга нисбатан ACPO (Association of Chief Police Officers) принциплари кенг эътироф этилган. Хусусан:

1) рақамли далилларга ўзгартириш киритилмаслиги;

2) зарурий ҳолларда нусха ноутентик материалга таъсир қилиш эвазига олиниши;

3) ҳамма рақамли материаллар ишончли сақлаш занжири (chain of custody) асосида сақланиши;

4) далил сифатида тақдим этиладиган барча материаллар мустақил экспертиза воситасида текширилиш имконига эга бўлиши.

Юридик нуқтаи назардан рақамли далиллар тезкор-қидирув фаолияти доирасида тўпланганда, уларни жиноят-процессуал далилга айлантирилиш тартиби аниқ белгиланмоғи лозим. Тезкор-қидирув фаолияти натижалари жиноят ишига қўшиш, «легаллаштириш» жараёнини талаб этади, бунда тергов ҳатти-ҳаракатлари орқали (тинтув, кўздан кечириш, тиклаб олиш) тезкор-қидирув фаолияти натижалари расмийлаштирилиши зарур.

Хориж тажрибасига кўра, АҚШда рақамли далиллар бўйича илмий ишчи гуруҳи (SWGDE) ишлаб чиққан стандартлар, Европа Кенгашининг Будапешт конвенциясига мувофиқ ўрнатилган тартиблар, шунингдек, ISO/IEC 27037:2012 халқаро стандарти рақамли далилларни тўплаш ва сақлашга нисбатан методологик асос бўлиб хизмат қилади.

Ўзбекистон Республикасида кибержиноятларга қарши курашишда тезкор-қидирув фаолиятини ташкил этишда бир қатор муаммолар мавжуд. Жумладан, Ўзбекистон Республикасининг «Тезкор-қидирув фаолияти тўғрисида»ги (2012 й.) ва «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги (2002 й.) қонунлари кибержиноятлар билан боғлиқ барча ҳолатларни тўлиқ тартибга солмайди. Жумладан, онлайн-провокация,

шифрланган маълумотларни тиклаш, трансмиллий кибержиноятлар бўйича тезкор ҳамкорлик механизмлари ноаниқ қолмоқда.

Кибержиноятларни тергов қилиш юқори малакали техник мутахассисларга эҳтиёжни кучайтирмоқда. Ҳуқуқни муҳофаза қилувчи органларда ахборот хавфсизлиги мутахассислари, рақамли криминалист аналитик таҳлилчилар ва кибеpразведка соҳасидаги кадрлар етарли эмаслиги амалиётдаги асосий камчиликлардан бири сифатида кўрсатилмоқда. Ички ишлар вазирлиги Академиясида тегишли йўналишлар ривожлантирилаётган бўлса-да, кадрлар тайёрлашни янада тезлаштириш зарурати мавжуд.

Кибержиноятларни аниқлаш ва тергов қилиш учун замонавий техник воситалар, компьютер криминалистика комплекслари (Cellebrite, Oxygen Forensic, EnCase ва б.), трафик таҳлили тизимларига эҳтиёж ортиб бормоқда.

Кибержиноятларнинг 70 фоизга яқини трансмиллий хусусиятга эгалиги туфайли (Europol, 2022) давлатлараро ҳуқуқий ҳамкорлик механизмлари ниҳоятда муҳим. МДҲ ва Интерпол орқали IGCI (Interpol Global Complex for Innovation) билан ҳамкорлик мавжуд бўлса-да, тезкор маълумот алмашинуви ва рақамли далилларни танишиш муаммолари бартараф этилмаган.

Ривожланган мамлакатлар тажрибаси шуни кўрсатадики, кибержиноятларга қарши самарали курашиш учун махсус ташкилий-ҳуқуқий механизмлар яратиш зарур.

АҚШ тажрибаси. Федерал қидирув бюроси (ФҚБ) кибержиноятлар бўлинмаси (Cyber Division) 2002 йилда тузилган бўлиб, ФҚБ ва Ички хавфсизлик вазирлиги (DHS) ўртасидаги ҳамкорлик асосида ишлайди. 2016 йилда қабул қилинган Компьютерни суиистеъмол қилиш ва жиноят тўғрисидаги қонун (CFAA) кенг тушунтириш имкониятларини беради. National Cyber Investigative Joint Task Force (NCIJTF) тизими орқали барча федерал идоралар кибержиноятларга қарши курашда координация қилинади.

Европа Иттифоқида Европол қошидаги EC3 (European Cybercrime Centre) 2013 йилдан буён ЕИ мамлакатларида кибержиноятларга қарши ягона тезкор-қидирув маркази сифатида фаолият юритади. Будапешт конвенцияси (2001) доирасида тезкор маълумот алмашиш, «24/7» тармоғи орқали ёрдам сўраш ва электрон далилларни трансмиллий тарзда тўплаш имконияти мавжуд. ЕИда GDPR (General Data Protection Regulation) доирасида ТҚТ ва конфиденциаллик ўртасидаги мувозанат масаласи алоҳида тартибга солинган.

Россия ИИВ тизимида «К» бош бошқармаси ва ФХХнинг ахборот хавфсизлиги маркази кибержиноятларни тергов қилишда асосий субъектлар ҳисобланади. СОРМ (Система оперативно-розыскных мероприятий) тизими орқали телекоммуникация

операторлари тезкор-қидирув органларига техник имконият беришга мажбур. Мазкур тажриба Ўзбекистон ҳуқуқ тизимига мосроқ бўлиб, уни ўрганиш мақсадга мувофиқ.

Сингапурнинг Компьютер жиноятлари тўғрисидаги қонуни (Computer Misuse Act, 1993, кейинги таҳрирлар) ва Кибергуруҳ (Cybersecurity Agency, 2015) кибержиноятларни олдини олиш ва жавобгарликка тортишда самарали механизм ярата олган. Хусусий сектор ва давлат ўртасидаги public-private partnership (давлат-хусусий ҳамкорлик) модели Осиё-Тинч океани минтақасида намунали тажриба сифатида тан олинган.

Ушбу тажрибалар асосида миллий аалиётга қуйидагиларни жорий этилиши мақсадга мувофиқ:

Биринчидан, ИИВ тизимидаги кибержиноятларга ихтисослашган тезкор-қидирув бўлинмасини кучайтириш ва унинг ваколатларини аниқ белгилаш;

иккинчидан, «Тезкор-қидирув фаолияти тўғрисида»ги Қонунга кибержиноятлар бўйича ТҚТнинг ўзига хос тартибини белгиловчи алоҳида боб киритиш;

учинчидан, рақамли далилларни тўплаш, сақлаш ва тақдим этишнинг процессуал стандартларини кодификациялаштириш;

тўртинчидан, Будапешт конвенциясига қўшилиш ёки тегишли иккитомонлама шартномалар тизимини кенгайтириш;

бешинчидан, ҳуқуқни муҳофаза қилувчи органлар ходимлари учун рақамли криминалистика, киберразведка ва техник тадқиқот бўйича мунтазам малака ошириш курсларини ташкил этиш.

Ўтказилган тадқиқот натижалари шуни кўрсатадики, кибержиноятларга қарши курашишда тезкор-қидирув тадбирларидан самарали фойдаланиш учун ҳуқуқий, ташкилий, техник ва кадрлар борасидаги чоралар тизимини шакллантириш зарур.

Ҳуқуқий жиҳатдан кибержиноятлар учун ихтисослашган ТҚТ тартибини белгиловчи норматив-ҳуқуқий базани такомиллаштириш, рақамли далилларнинг жиноят-процессуал мавқеини аниқлаштириш ва халқаро ҳамкорлик механизмларини ривожлантириш асосий устувор вазифалар сирасига киради.

Хулоса. Умуман олганда, кибержиноятларга қарши курашишда тезкор-қидирув фаолиятини такомиллаштириш Ўзбекистон Республикасини рақамли иқтисодиётни ривожлантиришга йўналтирилган Янги Ўзбекистон тараққиёт стратегиясининг таркибий қисми бўлмоғи зарур. Хавфсиз рақамли муҳитни таъминлаш иқтисодий ривожланиш, инвестициялар жалб қилиш ва фуқаролар манфаатларини ҳимоя қилишнинг зарурий шарти ҳисобланади.

Фойдаланилган адабиётлар рўйхати:

1. Ўзбекистон Республикасининг Жиноят кодекси. 22.09.1994 й. — Тошкент, 1994. — 451 б.

2. Ўзбекистон Республикасининг Жиноят-процессуал кодекси. 22.09.1994 й. — Тошкент, 1994.

3. Ўзбекистон Республикасининг «Тезкор-қидирув фаолияти тўғрисида»ги Қонуни. 25.12.2012 й., № ЎРҚ-343.

4. Ўзбекистон Республикасининг «Киберхавфсизлик тўғрисида»ги Қонуни. 15.04.2022 й., № ЎРҚ-764.

5. Будапешт конвенцияси: Компьютер жиноятлари тўғрисидаги конвенция. Будапешт, 23.11.2001 й. — Европа Кенгаши, ETS № 185.

6. Аверьянова Т.В., Белкин Р.С. Криминалистика: учебник. — Москва: Норма, 2019. — 990 б.

7. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. — Москва: Право и закон, 2016. — 182 б.

8. Касенова М.Б. Киберпреступность и уголовное преследование. — Алматы: ВШП «Адилет», 2018. — 224 б.

9. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология. — 2013. — № 1. — Б. 45–54.

10. Раджабов Б.А. Жиноят процессида исботлаш. Монография. 2021. — 168 б.

11. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2022. — The Hague: Europol, 2022. — 76 p.

12. Interpol. Cybercrime: COVID-19 Impact. — Lyon: Interpol, 2020. — 28 p.

13. Casey E. Digital Evidence and Computer Crime. 3rd ed. — London: Academic Press, 2011. — 840 p.

14. Kosseff J. Cybersecurity Law. 2nd ed. — Hoboken: Wiley, 2020. — 688 p.

15. ISO/IEC 27037:2012. Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. — Geneva: ISO, 2012.

16. UNODC. Comprehensive Study on Cybercrime. — Vienna: United Nations, 2013. — 320 p.

17. Cybersecurity Ventures. 2023 Official Cybercrime Report. — Sausalito: Cybersecurity Ventures, 2023. — 64 p.