IQRO JURNALI , IQRO JOURNAL, ИКРО ЖУРНАЛИ
ISSN:2181-4341| wordlyknowledge.uz/index.php/iqro
Volume 23. Issue 02. Sentabr, 2026

ТРАНСЧЕГАРАВИЙ КИБЕРМАКОНДА OSINT ВОСИТАЛАРИДАН ФОЙДАЛАНИШДАГИ ЮРИСДИКЦИЯ, ТАШКИЛИЙ-ТЕХНИК ТЎСИҚЛАР ҲАМДА ШАХСИЙ МАЪЛУМОТЛАР ДАХЛСИЗЛИГИ МАСАЛАЛАРИ

Жалолов Миркодир Мирхожиевич
Ҳуқуқни муҳофаза қилиш академияси
магистратура тингловсиси
https://doi.org/10.5281/zenodo.23080807

Аннотация. Мазкур тадқиқотда трансчегаравий кибермаконда очиқ манбалар асосидаги разведка (OSINT) воситаларидан фойдаланишнинг халқаро-ҳуқуқий ва криминалистик жиҳатлари, хусусан, миллий суверенитет, экстерриториал юрисдикция, ташкилий-техник тўсиқлар ҳамда шахсий маълумотлар дахлсизлигини таъминлаш муаммолари комплекс таҳлил қилинган.

Муаллиф томонидан анъанавий халқаро ҳуқуқий ёрдам (MLAT) механизмларининг рақамли ахборотларнинг ўта ўзгарувчанлиги (volatility) шароитидаги самарасизлиги кўрсатиб берилган ҳамда халқаро прецедентлар (Lotus, Benedik v. Slovenia, Roman Zakharov v. Russia) ва халқаро-ҳуқуқий ҳужжатлар (Будапешт конвенцияси ва унинг Иккинчи қўшимча протоколи, АҚШнинг CLOUD Act, ЕИнинг E-Evidence пакети, GDPR, Беркли протоколи) қиёсий ўрганилган. Шунингдек, веб-скрейпингга қарши тизимлар (Cloudflare, CAPTCHA), анонимлаштириш воситалари (VPN, Tor), Даркнет ҳамда ёпиқ API муҳитида OSINT ўтказишдаги процессуал чегаралар (провокация ва оператив эксперимент фарқи) ва мутаносиблик (proportionality) тамойили ёритиб берилган.

Калит сўзлар: кибермакон, OSINT, трансчегаравий юрисдикция, MLAT, рақамли далиллар, шахсий маълумотлар дахлсизлиги, Будапешт конвенцияси, E-Evidence, Беркли протоколи, SHA-256, 24/7 contact point.

Abstract. This study provides an in-depth analysis of the international legal, procedural, and forensic dimensions of utilizing Open Source Intelligence (OSINT) tools in cross-border cyberspace, addressing the core challenges of territorial sovereignty, extraterritorial jurisdiction, organizational-technical barriers, and data privacy rights. The author demonstrates the inefficiency of traditional Mutual Legal Assistance Treaties (MLAT) in dealing with volatile digital data and examines international jurisprudence (PCIJ Lotus case, ECHR cases of Benedik v. Slovenia and Roman Zakharov v. Russia) alongside contemporary regulatory frameworks, including the Budapest Convention and its Second Additional Protocol, the US CLOUD Act, the EU E-Evidence Regulation, GDPR, and the Berkeley Protocol.

The article explores technical countermeasures (web scraping blocks, CAPTCHA, Tor/VPN anonymization) and outlines the procedural boundary between passive OSINT gathering and active entrapment. Based on the findings, the author formulates concrete legislative and institutional recommendations (de lege ferenda) for the Republic of Uzbekistan: establishing dedicated statutory provisions for cross-border digital reconnaissance in the Law "On Operational-Search Activity", regulating digital evidence integrity via SHA-256 hashing in the Criminal Procedure Code, acceding to CETS No. 224, establishing a 24/7 National Point of

Contact integrated with Interpol/Europol, and implementing Privacy Impact Assessment guidelines under ISO/IEC 27037 standards.

Keywords: cyberspace, OSINT, cross-border jurisdiction, MLAT, digital evidence, data privacy, Budapest Convention, E-Evidence, Berkeley Protocol, SHA-256, 24/7 Point of Contact.

КИРИШ

Ахборот-коммуникация технологиялари ва глобал тармоқларнинг жадал тараққиёти натижасида кибермакон ҳудудий ва давлат чегараларидан холи бўлган алоҳида рақамли экотизим сифатида шаклланди[1]. Ушбу чегарасизлик ва трансчегаравийлик хусусияти традицион ҳуқуқ тизимларига, хусусан, миллий суверенитет ва юрисдикция тушунчаларига жиддий фундаментал чорловларни юзага келтирмоқда[2]. Анъанавий жиноят-процессуал ҳуқуқи муайян давлатнинг ҳудудий суверенитети (territorial sovereignty) принципига суянгани ҳолда, кибермаконда содир этиладиган жиноятлар ва уларнинг рақамли излари бир неча давлатлар юрисдикцияси бўйлаб тарқалиб кетади[3].

Халқаро ҳуқуқнинг умумий эътироф этилган принципларига кўра, ҳар бир суверен давлат ўз ҳудудида ҳуқуқни муҳофаза қилиш ва мажбурлов ваколатларини (jurisdiction to enforce) истисносиз амалга ошириш ҳуқуқига эга ҳисобланади[4]. Халқаро одил судлов судининг (Lotus иши бўйича) тарихий прецедентига мувофиқ, давлат бошқа бир суверен давлатнинг розилигисиз ёки халқаро шартномалар асосисиз хорижий ҳудудда ўз суверен ваколатларини амалга ошириши ман этилади[5]. Бироқ, очиқ интернет муҳитида OSINT (Open Source Intelligence) воситаларини қўллаш орқали хорижий серверларда жойлашган ахборотларни масофадан туриб тўплаш ҳудудийлик ва экстерриториаллик ўртасида коллизияларни келтириб чиқаради[6].

АСОСИЙ ҚИСМ

Давлат органлари ва оператив бўлинмаларнинг хорижий серверларда ёки булутли инфраструктураларда (cloud computing) сақланаётган очиқ маълумотларни тўплаш ваколатларининг ҳуқуқий чегараси трансчегаравий суриштирувларнинг энг баҳсли масалаларидан биридир[7]. Маълумотнинг оммавий очиқлиги (public accessibility) уни тўплаётган давлатга хорижий давлатнинг рақамли суверенитетини бузиш ҳуқуқини берадими ёки йўқми деган савол халқаро ҳуқуқшунослар ўртасида қизғин мунозараларга сабаб бўлмоқда[8]. Муайян юрисдикциядаги сервердан маълумот олиш хорижий давлат суверенитетига аралашув сифатида баҳоланиши хавфи мавжуд[9].

Трансчегаравий рақамли далиллар ва ахборотларни олишда анъанавий равишда Халқаро ҳуқуқий ёрдам (Mutual Legal Assistance Treaties – MLAT) механизмларидан фойдаланиб келинган[10]. Бироқ, амалиёт таҳлили шуни кўрсатадики, MLAT механизмлари ўта бюрократиялашган, секин ва кўп вақт талаб этадиган (ўртача 6 ойдан 2 йилгача) тартиб-қоидаларга эга бўлиб, рақамли маълумотларнинг ўта ўзгарувчанлиги (volatility) шароитида мутлақо самарасиз бўлиб қолмоқда[11].

Оператив-қидирув ва криминалистик фаолиятда OSINT усулларининг асосий афзаллиги уларнинг реал вақт режимида (real-time) ва тезкор ахборот тўплаш имкониятидир, бу эса секин ишловчи MLAT механизмлари билан зиддиятга келади[12]. MLAT бўйича расмий сўров юборилгунга қадар хорижий сервердаги ёки ижтимоий тармоқдаги очиқ маълумотлар жиноятчилар томонидан ўчириб ташланиши ёки

ўзгартирилиши мумкин[13]. Ушбу вақт омили оператив ходимларни MLAT тартиб-қоидаларини четлаб ўтиб, OSINT воситалари орқали масофадан туриб ахборот тўплашга мажбур қилмоқда[14].

Кибержиноятчилик тўғрисидаги Будапешт конвенциясининг 32-моддаси "a" банди хорижий юрисдикцияда сақланаётган оммавий очиқ (publicly available) компьютер маълумотларига бошқа давлатнинг розилигисиз бевосита трансчегаравий киришни легаллаштиради[15]. Бироқ, ушбу норма очиқ маълумотларнинг аниқ ҳуқуқий чегараларини ва қайси ҳолларда хорижий провайдер ёки сервер эгасининг розилиги талаб этилишини тўлиқ тартибга солмайди[16].

Динамик ва бўлинган булутли архитектура шароитида рақамли маълумотларнинг аниқ қайси географик ва миллий юрисдикцияда (data location) сақланаётганини аниқлаш мураккаб техник муаммога айланади[17]. Ахборот турли қитъалардаги серверлар бўйлаб бўлакланган (fragmented data) ҳолда сақланганда, ягона юрисдикциявий мансублик йўқолади, бу эса OSINT суриштирувларини амалга оширувчи орган учун мураккаб ҳуқуқий ноаниқликни юзага келтиради[18].

Натижада, сўров юборувчи давлат, маълумот жойлашган хорижий давлат ва глобал IT-платформалар (ISP/OSP) ўртасида уч томонлама юрисдикциявий зиддиятлар шаклланади[19]. Хорижий провайдерлар кўпинча ўзлари жойлашган давлатнинг шахсий маълумотларни ҳимоя қилиш қонунчилигига суянган ҳолда, хорижий тергов органларининг OSINT ёки тўғридан-тўғри сўровларига ахборот беришни рад этадилар[20].

Юрисдикциявий ва ҳуқуқий муаммолардан ташқари, трансчегаравий кибермаконда OSINT суриштирувларини амалга оширишда жиддий ташкилий-техник тўсиқлар юзага келмоқда[21]. Энг биринчи навбатда, йирик интернет-провайдерлар ва платформалар автоматик веб-скрейпинг ва сканерлаш воситаларига қарши махсус ҳимоя тизимларини қўллашмоқда[22].

Автоматик тарзда очиқ маълумотларни тўплашга қарши Cloudflare, CAPTCHA, rate limiting (сўровлар сонини чеклаш) ва IP-блоклаш каби техник чекловлар OSINT таҳлилчиларининг ва тергов органларининг очиқ ресурслардан самарали фойдаланишини чеклайди[23]. Ушбу техник тўсиқларни айланиб ўтиш учун автоматик парсерлар ёки махсус дастурий воситаларни қўллаш платформаларнинг фойдаланувчи келишувлари (Terms of Service) шартларини бузиши мумкин, бу эса олинган маълумотларнинг процессуал мақбуллигига путур етказади[24].

Жиноятчилар ва уюшган жиноий гуруҳлар ўзларининг рақамли изларини яшириш ва OSINT суриштирувларидан ҳимояланиш учун VPN (Virtual Private Network), Tor ва I2P каби анонимлаштирувчи ва шифрловчи тармоқлардан кенг фойдаланишмоқда[25]. Ушбу анонимлик воситалари IP-манзилларни ва тармоқ маршрутларини бир нечта хорижий серверлар орқали сохталаштириб (IP spoofing), ҳақиқий фойдаланувчи ва жиноят содир этилган жойни идентификация қилишга тўсқинлик қилади[26].

Қоронғи интернет (Dark Web) ва шифрланган мессенжерларда (Telegram, Signal) OSINT методикасини қўллаш махсус анонимлаштириш, де-анонимлаштириш ва крипто-аналитик воситаларни талаб қилади[27]. Бироқ, аноним тармоқларда фойдаланувчиларнинг ҳақиқий шахсини ва геолокациясини аниқлаш усуллари кўпинча пассив OSINT

доирасидан чиқиб, фаол ва техник жиҳатдан мураккаб оператив-техник тадбирлар билан туташиб кетади[28].

Сўнгги йилларда йирик ижтимоий тармоқлар ва онлайн платформалар (Facebook, X, Instagram, LinkedIn) ўзларининг очиқ API (Application Programming Interface) кириш сиёсатини кескин ёпишди ва маълумотларни тижоратлаштиришди[29]. Очиқ API платформаларининг ёпилиши тадқиқотчилар ва оператив ходимлар учун автоматик SOCMINT (ижтимоий тармоқлар разведкаси) воситаларидан фойдаланиш имкониятини жиддий чеклаб қўйди[30].

OSINT ўтказиш жараёнида фаол усуллар, хусусан, легендалаштирилган сохта аккаунтлар (sock puppets), ижтимоий инжиниринг усуллари ва автоматик ботлардан фойдаланишнинг қонуний чегаралари муҳим масаладир[31]. Сохта аккаунт орқали объект билан бевосита мулоқотга киришиш ёки ёпиқ гуруҳларга кириб бориш оператив эксперимент ёки провокация (entrapment) чегарасига яқинлашади, бу эса қатъий процессуал тартибга солишни талаб этади[32].

Ташкилий жиҳатдан OSINT дастурий ва аппарат воситаларининг тезкор маънан эскириши, платформа алгоритмларининг тез-тез ўзгариши ҳамда тезкор ходимларнинг рақамли криминалистика ва киберхавфсизлик бўйича билим ва кўникмаларининг етишмаслиги амалий суриштирувлар самарадорлигини камайтирувчи омиллардир[33].

Инсон ҳуқуқлари ва инсон қадр-қиммати призмасида қараганда, очиқ манбалардан маълумот тўплаш жараёнида шахсий ҳаёт дахлсизлиги (right to privacy) ва шахсга доир маълумотларни ҳимоя қилиш масалалари марказий ўрин эгаллайди[34]. Ахборотнинг очиқ тармоқда жойлашганлиги давлат органларига ушбу маълумотларни чекловсиз ва назоратсиз тўплаш, сақлаш ва қайта ишлаш ҳуқуқини бермайди[35].

Инсон ҳуқуқлари бўйича Европа судининг (Benedik v. Slovenia) прецедент қарорига мувофиқ, полиция томонидан динамик IP-манзил бўйича фойдаланувчи тўғрисидаги маълумотларни очиқ ёки ярим-очиқ тармоқдан олиш ҳам Инсон ҳуқуқлари бўйича Европа конвенциясининг 8-моддасига (шахсий ҳаёт дахлсизлиги) аралашув ҳисобланади ва аниқ қонуний асослар ҳамда кафолатларни талаб этади[36].

ИҲЕСнинг Roman Zakharov v. Russia иши бўйича қарорида мустаҳкамланган "қонун сифати" (quality of law) принципига кўра, давлат томонидан рақамли маълумотларни тўплашга оид қонунчилик рамкаси ўта аниқ, олдиндан кўра билинадиган ва ўзбошимчаликдан ҳимоя қилувчи кафолатларга эга бўлиши шарт[37]. Кўпчилик давлатларда, шу жумладан миллий қонунчиликда OSINT воситалари орқали тизимли равишда рақамли маълумот тўплашни тартибга солувчи махсус нормаларнинг йўқлиги ушбу принципларга коллизия келтириб чиқаради[38].

Очиқ манбалардан маълумот тўплашда пропорционаллик (мутаносиблик) принципи (proportionality principle) талаб этилади (Bărbulescu v. Romania, López Ribalda v. Spain)[39]. Давлат органи томонидан амалга ошириладиган OSINT тадбирлари жиноятни фош этиш ва жамоат хавфсизлигини таъминлаш мақсадига мутаносиб бўлиши, ва жиноятга алоқаси бўлмаган учинчи шахсларнинг шахсий маълумотларига номутаносиб аралашувга йўл қўймаслиги лозим[40].

Европа Иттифоқининг Шахсга доир маълумотларни ҳимоя қилиш умумий регламенти (GDPR – Regulation (EU) 2016/679) ва "Полиция директиваси" (Directive (EU)

2016/680) рақамли ахборотларни қайд этишда "технологик нейтраллик" ва "маълумотларни минималлаштириш" (data minimisation) принципларини белгилайди[41]. Унга кўра, тергов органи фақат муайян жиноят иши учун зарур ва етарли бўлган ҳажмдаги шахсий маълумотларни тўплаши шарт[42].

Ўзбекистон Республикасининг "Шахсга доир маълумотлар тўғрисида"ги Қонуни (ЎРҚ-547) ва Вазирлар Маҳкамасининг 2026 йил 29 июлдаги 415-сонли қарори нормаларига кўра, шахсга доир маълумотларни трансчегаравий узатиш ва қайта ишлаш муайян режимларга бўйсунади[43]. Қонуннинг 3-моддасига мувофиқ, ҳуқуқни муҳофаза қилувчи органлар томонидан тезкор-қидирув ва жиноятчиликка қарши курашиш мақсадларида шахсга доир маълумотларни қайта ишлашга нисбатан алоҳида истиснолар белгиланган бўлса-да, бу истиснолар фундаментал конституциявий кафолатларни чекламаслиги лозим[44].

"Рақамли очиқ манбаларни суриштирув қилиш бўйича Беркли протоколи" (The Berkeley Protocol) OSINT ўтказишда инсон ҳуқуқлари ва ахборот дахлсизлигини таъминлашнинг халқаро стандарти сифатида манбаларни ҳимоя қилиш (source protection), зарар етказмаслик (do no harm) ва рақамли хавфсизлик кафолатларини мустаҳкамлайди[45]. Беркли протоколига кўра, очиқ манбалардан маълумот тўплашда гувоҳлар, жабрланувчилар ва учинчи шахсларнинг рақамли хавфсизлигини таъминлаш биринчи галдаги этик ва ҳуқуқий мажбуриятдир[46].

Халқаро ва қиёсий-ҳуқуқий тажрибани таҳлил қилганда, Кибержиноятчилик тўғрисидаги Будапешт конвенцияси (ETS No. 185) ва унинг Иккинчи қўшимча протоколи (CETS No. 224) трансчегаравий электрон далилларни олиш ва юрисдикциявий низоларни ҳал этишнинг энг илғор халқаро-ҳуқуқий механизми ҳисобланади[47]. Иккинчи қўшимча протоколнинг 6 ва 7-моддалари хорижий провайдерлардан домен номлари ва абонент маълумотларини (subscriber information) тўғридан-тўғри олишнинг тезкор тартибини назарда тутади[48].

БМТнинг Кибержиноятчиликка қарши бўлажак Конвенцияси (United Nations Convention against Cybercrime) бўйича олиб борилаётган глобал мунозараларда давлатларнинг суверен юрисдикциясини ҳурмат қилиш ва трансчегаравий рақамли далилларни олиш механизмлари ўртасидаги мувозанат марказий баҳс мавзусига айланди[49]. Традицион давлатчилик позициясини ҳимоя қилувчи давлатлар масофадан туриб очиқ ва ярим-очиқ маълумотларни тўплашда суверен розилик талабини илгари сурмоқда, бу эса глобал консенсусга эришишни мураккаблаштирмоқда[50].

АҚШ томонидан қабул қилинган CLOUD Act (Clarifying Lawful Overseas Use of Data Act) модели хорижий серверларда сақланаётган рақамли маълумотларга экстерриториал юрисдикцияни қўллашнинг ўзига хос намунасидир[51]. Ушбу ҳужжат АҚШ тергов органларига АҚШ юрисдикциясидаги IT-компаниялар хорижий серверларда сақлаётган маълумотларни тўғридан-тўғри талаб қилиш ҳуқуқини беради, бу эса хорижий давлатларнинг суверенитети ва GDPR нормалари билан ҳуқуқий коллизияни юзага келтиради[52].

Европа Иттифоқининг E-Evidence пакети (Regulation (EU) 2023/1543) эса ЕИга аъзо давлатлар ўртасида трансчегаравий электрон далилларни сақлаш ва олиш учун Европа олиш ва сақлаш ордерларини (EPOC ва EPOC-PR) жорий этди[53]. Бу механизм аъзо

давлатларнинг тергов органларига хорижий провайдерларга 10 кун ичида (фавқулодда ҳолатларда 8 соатда) маълумот бериш мажбуриятини юклайди ва традицион MLAT'га нисбатан инқилобий қадам ҳисобланади[54].

Ривожланган хорижий давлатлар (Германия, Буюк Британия, Франция) амалиётида суверен юрисдикцияни ҳурмат қилган ҳолда OSINT воситаларидан фойдаланишнинг "интеллектуал ва мақсадли суриштирув" (targeted investigation) моделлари қўлланилади[55]. Бунда оммавий очиқ ахборотларни тўплаш учун суд санкцияси талаб этилмайди, бироқ тизимли мониторинг ва шахсий маълумотларни чуқур қайта ишлаш устидан мустақил назорат органи (Data Protection Authority) назорати ўрнатилган[56].

Халқаро полиция ҳамкорлиги ташкилотлари (Интерпол, Европол) таркибидаги SIRIUS ва J-CAT платформалари трансчегаравий OSINT суриштирувлари ва провайдерлар билан тўғридан-тўғри мулоқотни мувофиқлаштирувчи глобал хаб вазифасини ўтамоқда[57]. Ушбу платформалар орқали очиқ манба маълумотлари ва рақамли излар халқаро даражада тезкор ва хавфсиз каналлар орқали алмашилади[58].

Юқоридаги халқаро тажриба ва назарий манбаларни умумлаштириш шуни кўрсатадики, трансчегаравий кибермаконда OSINT'дан фойдаланишнинг ҳуқуқий механизми уч устунга таяниши лозим: суверен юрисдикция чегараларини ҳурмат қилиш, рақамли далилларнинг процессуал кафолатлари ва инсон ҳуқуқлари дахлсизлиги[59].

ХУЛОСА

Олиб борилган тадқиқот натижасида шундай илмий хулосага келиш мумкинки, трансчегаравий кибермаконда OSINT суриштирувларини амалга оширишнинг амалдаги миллий ва халқаро-ҳуқуқий базаси технологик тараққиёт ва кибержиноятчилик таҳдидларидан ортда қолмоқда, бу эса миллий қонунчиликни тизимли такомиллаштиришни талаб этади[60].

Биринчи илмий-амалий таклиф – Ўзбекистон Республикасининг "Тезкор-қидирув фаолияти тўғрисида"ги Қонунига "Трансчегаравий рақамли ахборот маконида тезкор маълумотлар тўплаш (OSINT)" моддасини киритиш. Унда оператив бўлинмалар томонидан хорижий серверлардаги ва очиқ манбалардаги маълумотларни тўплашнинг юрисдикциявий чегараларини, пассив ва фаол усуллардан фойдаланиш шартларини ва анонимлик кафолатларини мустаҳкамлаш зарур[61].

Иккинчи таклиф – Ўзбекистон Республикаси ЖПКга "Трансчегаравий рақамли маълумотларни олиш ва легаллаштириш" номли янги норма киритиш. Ушбу нормада хорижий манбалардан OSINT орқали олинган рақамли маълумотларни халқаро ҳуқуқий ёрдам (MLAT) ва тўғридан-тўғри сўровлар орқали процессуал мустаҳкамлаш, уларнинг SHA-256 хэш-қийматларини қайд этиш ҳамда ЖПК 95-1-моддасига мувофиқ мақбуллигини таъминлаш механизмларини назарда тутиш[62].

Учинчи таклиф – Ўзбекистон Республикасининг Кибержиноятчилик тўғрисидаги Будапешт конвенциясига ҳамда унинг Иккинчи қўшимча протоколига (CETS No. 224) қўшилиши бўйича ташкилий-ҳуқуқий чора-тадбирларни амалга ошириш. Бу миллий ҳуқуқни муҳофаза қилувчи органларга хорижий провайдерлардан абонент ва домен маълумотларини тўғридан-тўғри ва тезкор олиш имконини беради[63].

Тўртинчи таклиф – Ҳуқуқни муҳофаза қилувчи органлар ва ИИВ, ДХХ, Бош прокуратура тузилмасида "Трансчегаравий OSINT ва рақамли далиллар бўйича 24/7

марказлаштирилган миллий контакт пункти"ни (24/7 Network POC) ташкил этиш. Ушбу пункт Интерпол ва Европол (SIRIUS) каналлари орқали хорижий провайдерлар билан тезкор алоқани ва ахборот ушлаб туриш (expedited preservation) сўровларини таъминлайди[64].

Бешинчи таклиф – Беркли протоколи ва ISO/IEC 27037:2017 стандартлари асосида "Трансчегаравий кибермаконда OSINT суриштирувларини амалга оширишда шахсий маълумотлар дахлсизлигини таъминлаш ва пропорционалликни баҳолаш (Privacy Impact Assessment – PIA) бўйича идоралараро методик қўлланма"ни тасдиқлаш ва амалиётга жорий этиш[65].

Хуллас калом, трансчегаравий кибермаконда OSINT воситаларини қўллашнинг таклиф этилаётган ҳуқуқий ва ташкилий-техник механизмлари миллий суверенитет ва инсон ҳуқуқлари кафолатларини мустаҳкамлаган ҳолда, трансчегаравий ва кибержиноятларни тергов қилиш ҳамда фош этиш самарадорлигини сифат жиҳатидан янги босқичга кўтаришга хизмат қилади[66].

ГОСТ УСЛУБИДАГИ БИБЛИОГРАФИК МАНБАЛАР РЎЙХАТИ

1. Böhm R., Lolagar S. Defining OSINT in the Criminal Investigation Context // Balkan Journal of Interdisciplinary Research. – 2026. – Vol. 12, No. 1. – P. 15–28.

2. United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime. – Vienna: UNODC, 2013. – 320 p.

3. Osula A-M. Transborder Access and Territorial Sovereignty // Computer Law & Security Review. – 2015. – Vol. 31. – P. 719–735.

4. Shaw M. N. International Law. – 8th ed. – Cambridge: Cambridge University Press, 2017. – 1034 p.

5. Permanent Court of International Justice. The Case of the S.S. "Lotus" (France v. Turkey). PCIJ Series A, No. 10. – The Hague: PCIJ, 1927. – 45 p.

6. Council of Europe Cybercrime Convention Committee (T-CY). Transborder access to data and jurisdiction: Options for further action. – Strasbourg: Council of Europe, 2014. – 42 p.

7. Velasco C. Jurisdictional Aspects of Cloud Computing and Cybercrime Investigations // Council of Europe Octopus Conference Publications. – Strasbourg: CoE, 2010. – P. 12–28.

8. Daskal J. The Un-Territoriality of Data // Yale Law Journal. – 2015. – Vol. 125, No. 2. – P. 326–398.

9. Bazzell M. Open Source Intelligence Techniques: A Practical Guide to Online Intelligence. – 9th ed. – AuthorHouse, 2023. – 670 p.

10. Abrahams H. H. Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives // International Journal of Law and Information Technology. – 2021. – Vol. 29, No. 2. – P. 118–153.

11. Europol. SIRIUS EU Electronic Evidence Situation Report 2025. – The Hague: European Union Agency for Law Enforcement Cooperation, 2025. – 58 p.

12. Internet & Jurisdiction Policy Network. Cross-Border Access to Electronic Evidence: Operational Workflows. – Paris: IJPN, 2023. – 34 p.

13. FATF/OECD. Countering Ransomware Financing. – Paris: FATF/OECD, 2023. – 68 p.

14. Crawford-Holland S., Smith P. B., Williams A. Law's capture of human rights focused open-source investigation // London Review of International Law. – 2025. – Vol. 13, No. 1. – P. 93–112.

15. Council of Europe. Convention on Cybercrime (ETS No. 185). – Budapest: Council of Europe, 2001. – 24 p.

16. Council of Europe Cybercrime Convention Committee (T-CY). Guidance Note #3 on Transborder Access to Data (Article 32 Budapest Convention). – Strasbourg: Council of Europe, 2013. – 14 p.

17. Svantesson D., van Zwieten J. Law Enforcement Access to Evidence in the Cloud // Computer Law & Security Review. – 2016. – Vol. 32, No. 4. – P. 521–538.

18. Reidenberg J. R. Technology and Data Privacy Choices in Cyberspace // Stanford Law Review. – 2005. – Vol. 58. – P. 1951–1974.

19. Koops B-J., Brenner S. W. Cybercrime and Jurisdiction: A Global Survey. – Hague: T.M.C. Asser Press, 2006. – 348 p.

20. ReedSmith Legal Guides. Understanding the Scope of the e-Evidence Regulation and Directive. – London: ReedSmith LLP, 2023. – 18 p.

21. Europol. Internet Organised Crime Threat Assessment (IOCTA 2024). – The Hague: European Union Agency for Law Enforcement Cooperation, 2024. – 86 p.

22. Stoykova R. A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings // Computer Law & Security Review. – 2024. – Vol. 55. – Art. 106040.

23. Bazzell M. Open Source Intelligence Techniques: A Practical Guide to Online Intelligence. – 9th ed. – AuthorHouse, 2023. – 670 p.

24. Mason S., Seng D. Electronic Evidence and Electronic Signatures. – 5th ed. – London: Institute of Advanced Legal Studies, 2021. – 540 p.

25. Kleijssen J., Perri P. Cybercrime, Evidence and Territoriality: Issues and Options // Information & Communications Technology Law. – 2017. – Vol. 26. – P. 148–173.

26. Davies G. Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers // The Journal of Criminal Law. – 2020. – Vol. 84, No. 5. – P. 407–426.

27. International Anti-Corruption Academy (IACA). AI-Driven Asset Tracing in Stolen Asset Recovery. – Laxenburg: IACA Publishing, 2024. – 48 p.

28. Office of the United Nations High Commissioner for Human Rights (OHCHR) & UC Berkeley Human Rights Center. Berkeley Protocol on Digital Open Source Investigations. – New York and Geneva: United Nations, 2022. – 108 p.

29. Murray D. et al. Open Source Investigations and International Criminal Law // Journal of Human Rights Practice. – 2022. – Vol. 14, No. 2. – P. 554–578.

30. Koenig A. Digital Investigations of Systematic and Conflict-Related Sexual Violence // Chicago Journal of International Law. – 2025. – Vol. 26, No. 1. – P. 185–204.

31. United Nations Office on Drugs and Crime (UNODC). Using Open-Source Intelligence in Criminal Investigations. – Vienna: UNODC, 2024. – 52 p.

32. Gillett M., Fan W. Expert evidence and digital open source information: Bringing online evidence to the courtroom // Journal of International Criminal Justice. – 2023. – Vol. 21, No. 4. – P. 661–693.

33. INTERPOL. Global Cyberthreat Assessment Report 2026. – Lyon: INTERPOL General Secretariat, 2026. – 64 p.

34. European Court of Human Rights. Case of Benedik v. Slovenia (Application no. 62357/14). Judgment of 24 April 2018. – Strasbourg: ECHR, 2018. – 28 p.

35. European Court of Human Rights. Case of Roman Zakharov v. Russia (Application no. 47143/06). Judgment of 4 December 2015. – Strasbourg: ECHR, 2015. – 42 p.

36. European Court of Human Rights. Case of Benedik v. Slovenia (Application no. 62357/14). Judgment of 24 April 2018. – Strasbourg: ECHR, 2018. – 28 p.

37. European Court of Human Rights. Case of Roman Zakharov v. Russia (Application no. 47143/06). Judgment of 4 December 2015. – Strasbourg: ECHR, 2015. – 42 p.

38. Stoykova R. Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence // Computer Law & Security Review. – 2021. – Vol. 42. – Art. 105575.

39. European Court of Human Rights. Case of Bărbulescu v. Romania (Application no. 61496/08). Judgment of 5 September 2017. – Strasbourg: ECHR, 2017. – 36 p.; Case of López Ribalda and Others v. Spain (Applications nos. 1874/13 and 8567/13). Judgment of 17 October 2019. – Strasbourg: ECHR, 2019. – 30 p.

40. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR) // Official Journal of the European Union. – 2016. – L 119. – P. 1–88.

41. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities // Official Journal of the European Union. – 2016. – L 119. – P. 89–131.

42. Ibid.

43. Ўзбекистон Республикаси Вазирлар Маҳкамасининг "Шахсга доир маълумотлар ҳимоя қилинишининг етарлилик даражасини таъминловчи хорижий давлатлар рўйхатини тасдиқлаш тўғрисида"ги Қарори, 2026 йил 29 июль, 415-сон // lex.uz – Ўзбекистон Республикаси Қонунчилик маълумотлари миллий базаси.

44. Ўзбекистон Республикасининг "Шахсга доир маълумотлар тўғрисида"ги Қонуни, 2019 йил 2 июль, ЎРҚ-547-сон // lex.uz.

45. Office of the United Nations High Commissioner for Human Rights (OHCHR) & UC Berkeley Human Rights Center. Berkeley Protocol on Digital Open Source Investigations. – New York and Geneva: United Nations, 2022. – 108 p.

46. Ibid.

47. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). – Strasbourg: Council of Europe, 2022. – 28 p.

48. Ibid.

49. United Nations. Draft United Nations Convention against Cybercrime. – New York: UN, 2024. – 45 p.

50. Ibid.

51. Daskal J. Law Enforcement Access to Data Across Borders: The US CLOUD Act Framework // Yale Law Journal. – 2019. – Vol. 128. – P. 562–598.

52. Ibid.

53. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 27 November 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings // Official Journal of the European Union. – 2023. – L 191. – P. 1–38.

54. Ibid.

55. Europol. SIRIUS EU Electronic Evidence Situation Report 2025. – The Hague: European Union Agency for Law Enforcement Cooperation, 2025. – 58 p.

56. Ibid.

57. Ibid.

58. Ibid.

59. Office of the United Nations High Commissioner for Human Rights (OHCHR) & UC Berkeley Human Rights Center. Berkeley Protocol on Digital Open Source Investigations. – New York and Geneva: United Nations, 2022. – 108 p.

60. Böhm R., Lolagar S. Defining OSINT in the Criminal Investigation Context // Balkan Journal of Interdisciplinary Research. – 2026. – Vol. 12, No. 1. – P. 15–28.

61. Ўзбекистон Республикасининг "Тезкор-қидирув фаолияти тўғрисида"ги Қонуни, 2012 йил 25 декабрь, ЎРҚ-344-сон // lex.uz.

62. Ўзбекистон Республикасининг Жиноят-процессуал кодекси. 1994 йил 22 сентябрь (амалдаги таҳрири) // lex.uz.

63. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). – Strasbourg: Council of Europe, 2022. – 28 p.

64. INTERPOL. Global Cyberthreat Assessment Report 2026. – Lyon: INTERPOL General Secretariat, 2026. – 64 p.

65. O‘z DSt ISO/IEC 27037:2017. Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Рақамли исботларни идентификация қилиш, йиғиш, олиш ва сақлаш. – Тошкент: Ўзстандарт агентлиги, 2017. – 65 б.

66. Ibid.