KIBERJINOYATCHILIKKA QARSHI KURASHDA DAVLATLARNING XALQARO-HUQUQIY HAMKORLIGI

Mulla-Axunov Asadbek Botir o'g'li
Toshkent davlat yuridik universiteti
Magistratura bosqichi
Moliyaviy huquqiy monitoring yo'nalishi talabasi
ORCID: 0009-0007-5892-3392
mullaaxunovasadbek@gmail.com
https://doi.org/10.5281/zenodo.20044523

Annotatsiya: Ushbu maqolada kiberjinoyatchilikka qarshi kurashda davlatlarning xalqaro-huquqiy hamkorligi masalalari tadqiq etilgan. Kiberjinoyatchilikning transmilliy va chegarasiz tabiati uni global xavfsizlikka jiddiy tahdidga aylantirib, davlatlar, yuridik shaxslar hamda jismoniy shaxslarga katta miqdorda moddiy va ma'naviy zarar yetkazmoqda. Shu munosabat bilan Yevropa Kengashining 2001 yilgi Budapesht Konventsiyasi hamda 2025 yilda Xanoy shahrida imzolangan BMTning Kiberjinoyatchilikka qarshi Konventsiyasi xalqaro-huquqiy tartibga solishning asosiy manbalari sifatida tahlil qilingan. Tadqiqotda solishtirma-huquqiy, tizimli va tahliliy metodlardan foydalanilib, xalqaro konvensiyalar normalari, shuningdek, Yevropa Kengashi, BMT va UNODC ma'lumotlari o'rganilgan. Tahlil natijalariga ko'ra, 2025 yil holatiga Budapesht Konventsiyasiga 81 ta davlat a'zo bo'lib, BMTning yangi Konventsiyasiga esa 74 ta davlat imzo chekkanligi aniqlangan. Shu bilan birga, xalqaro hamkorlik samaradorligini oshirish uchun protsessual yordam mexanizmlarini takomillashtirish, elektron dalillar almashuvini soddalashtirish hamda davlatlar o'rtasida tezkor axborot almashuv tizimini mustahkamlash zarurligi asoslab berilgan. Tadqiqot natijalari kiberjinoyatchilikka qarshi kurashda xalqaro shartnomalar samaradorligini oshirishga xizmat qiladi.
Kalit so'zlar: kiberhuquqbuzarlik, xalqaro huquqiy hamkorlik, ekstraditsiya, o'zaro huquqiy yordam, elektron dalillar, mintaqararo tergov, xalqaro konvensiyalar

Аннотация: В данной статье исследуются вопросы международно-правового сотрудничества государств в борьбе с киберпреступностью. Транснациональный и безграничный характер киберпреступности превращает её в серьёзную угрозу глобальной безопасности, нанося значительный материальный и моральный ущерб государствам, юридическим и физическим лицам. В этой связи в качестве основных источников международно-правового регулирования проанализированы Будапештская конвенция Совета Европы 2001 года и Конвенция ООН по борьбе с киберпреступностью, подписанная в 2025 году в городе Ханой. В исследовании использованы сравнительно-правовой, системный и аналитический методы, изучены нормы международных конвенций, а также данные Совета Европы, ООН и UNODC. По результатам анализа установлено, что по состоянию на 2025 год участниками Будапештской конвенции являются 81 государство, а новую Конвенцию ООН подписали 74 государства. Вместе с тем обоснована необходимость совершенствования механизмов процессуальной помощи, упрощения обмена электронными доказательствами и укрепления системы оперативного обмена информацией между государствами для повышения эффективности международного сотрудничества. Результаты исследования способствуют повышению эффективности международных договоров в борьбе с киберпреступностью.
Ключевые слова: киберпреступность, международное сотрудничество, экстрадиция, международная правовая помощь, электронные доказательства, кибербезопасность, международные конвенции.

Abstract: This article examines the issues of international legal cooperation among states in combating cybercrime. The transnational and borderless nature of cybercrime makes it a serious threat to global security, causing significant material and moral damage to states, legal entities, and individuals. In this context, the 2001 Budapest Convention of the Council of Europe and the United Nations Convention against Cybercrime signed in Hanoi in 2025 are analyzed as the main sources of international legal regulation. The research applies comparative legal, systemic, and analytical methods, studying the provisions of international conventions as well as data from the Council of Europe, the United Nations, and UNODC. The analysis shows that as of 2025, 81 states are parties to the Budapest Convention, while 74 states have signed the new UN Convention. At the same time, the study substantiates the need to improve procedural assistance mechanisms, simplify the exchange of electronic evidence, and strengthen the system of оперативе information exchange between states in order to enhance the effectiveness of international cooperation. The results of the study contribute to improving the effectiveness of international treaties in combating cybercrime.

Keywords: Cybercrime, International legal cooperation, Extradition, Mutual legal assistance, Electronic evidence, Cybersecurity, International conventions.

KIRISH

Bugungi globallashuv va raqamli texnologiyalar jadal rivojlanib borayotgan davrda kiberjinoyatchilikka qarshi kurashish xalqaro darajadagi eng dolzarb muammolardan biri bo‘lib qolmoqda. Axborot-kommunikatsiya texnologiyalarining davlat boshqaruvi, bank-moliya tizimi, elektron tijorat, transport, sog‘liqni saqlash va boshqa strategik sohalarga keng joriy etilishi bilan bir qatorda, ushbu tizimlarga noqonuniy aralashuv, ma’lumotlarni o‘g‘irlash, moliyaviy firibgarlik, zararli dasturlar tarqatish, phishing, ransomware va boshqa turdagi kiberjinoyatlar soni ham ortib bormoqda. Kiberjinoyatchilik XXI asrda xavfsizlikka jiddiy tahdid solib, odatiy jinoyatlarni ham kiber elementlari orqali amalga oshirishga imkon yaratmoqda. Internetning chegaralarsizligi tufayli jinoyatchilar bir nechta davlatda bir vaqtning o‘zida harakat qilishi, shu bilan birga ma’lumot va mulkka zarar yetkazishi mumkin.[1] Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi, internet tarmog‘ining kengayishi hamda raqamli xizmatlarning kundalik hayotga chuqur kirib borishi natijasida jinoyatchilikning yangi shakllari yuzaga keldi. Endilikda an’anaviy jinoyatlar, jumladan firibgarlik, tovlamachilik, o‘g‘rilik, shaxsga doir ma’lumotlarni noqonuniy egallash, moliyaviy firibgarlik va hatto terroristik faoliyat ham kiber makon orqali sodir etilmoqda. Bu esa jinoyatlarning ko‘lamini kengaytirib, ularni aniqlash va oldini olishni yanada murakkablashtirmoqda. Internetning transchegaraviy va markazlashmagan tabiati kiberjinoyatchilikni boshqa jinoyat turlaridan ajratib turadi. Jinoyatchi bir davlat hududida turib, boshqa davlatdagi serverlarga hujum qilishi, uchinchi davlat fuqarolarining ma’lumotlarini o‘g‘irlashi va zarar yetkazilgan mablag‘larni to‘rtinchi davlat bank tizimi orqali noqonuniy aylantirishi mumkin. Bunday holatlarda jinoyat sodir etilgan joyni aniqlash, vakolatli yurisdiksiyani belgilash hamda jinoyatchini javobgarlikka tortish murakkablashadi. Shu sababli faqat milliy qonunchilik doirasida kiberjinoyatchilikka qarshi samarali kurash olib borish yetarli emas.

Bundan tashqari, kiberhujumlar nafaqat alohida shaxslar yoki tijorat tashkilotlariga, balki davlatlarning strategik infratuzilmalariga ham jiddiy zarar yetkazmoqda. Energetika tizimlari, bank-moliya sektori, sog‘liqni saqlash, transport, davlat boshqaruvi va mudofaa tizimlariga qilingan hujumlar milliy xavfsizlikka bevosita tahdid tug‘diradi. Ayniqsa, ransomware hujumlari, davlat sirlarini o‘g‘irlash, saylov jarayonlariga noqonuniy aralashuv va kritik axborot infratuzilmasiga qilingan hujumlar xalqaro xavfsizlik masalasiga aylangan.

[1] Reitano, T.; Oerting, T.; Hunter, M. (2015). *Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT)*. Global Initiative Against Transnational Organized Crime. (Feb 2015)

Shu bois kiberjinoyatchilikka qarshi kurash davlatlarning o‘zaro xalqaro-huquqiy hamkorligini kuchaytirishni talab etadi. Elektron dalillarni tezkor almashish, jinoyatchilarni ekstraditsiya qilish, qo‘shma tergov olib borish, xalqaro konvensiyalar asosida yagona huquqiy mexanizmlarni shakllantirish zamonaviy davrning muhim vazifalaridan biri hisoblanadi. Aynan shu jihatlar kiberjinoyatchilikka qarshi kurashda xalqaro-huquqiy hamkorlikning dolzarbligini belgilaydi. Bunda milliy huquqiy chora-tadbirlar yetarli bo‘lmay qoladi. Global muammoni hal etish uchun davlatlar o‘rtasida tartiblar bir xil yo‘lga qo‘yilishi zarur. Masalan, OAV ma’lumotlariga ko‘ra, zamonaviy jinoiy guruhlar tarmoqlarni buzish, bank va shaxsiy ma’lumotlarni o‘g‘irlash, pul talash kabi transmilliy jinoyatlar bilan shug‘ullanadi, bu esa faqat xalqaro miqyosda hamkorlik orqali aniqlanishi va oldi olinishi mumkin. Shuning uchun kiberjinoyatchilikka qarshi kurashda xalqaro-huquqiy mexanizmlar, jumladan konvensiya va kelishuvlar katta ahamiyat kasb etadi[2]. Masalan, bir guruh jinoyatchilar bir mamlakatda turib boshqa davlat bank tizimiga zararli dastur yuborishi, uchinchi davlatdagi serverlardan foydalanishi va noqonuniy olingan mablag‘larni to‘rtinchi davlat moliyaviy tizimi orqali yashirishi mumkin. Bunday murakkab sxemalarda jinoyat sodir etilgan hududni aniqlash, dalillarni to‘plash, aybdor shaxslarni topish va javobgarlikka tortish faqat bitta davlat imkoniyatlari bilan amalga oshirilishi qiyin. Ayniqsa, elektron dalillarning tez yo‘qolishi, serverlarning turli yurisdiksiyalarda joylashgani va qonunchilikdagi farqlar tergov jarayonini murakkablashtiradi.

Shu sababli kiberjinoyatchilikka qarshi samarali kurash faqat xalqaro miqyosdagi hamkorlik orqali amalga oshirilishi mumkin. Davlatlar o‘rtasida tezkor axborot almashinuvi, elektron dalillarni taqdim etish, jinoyatchilarni ekstraditsiya qilish, qo‘shma tergov guruhlarini tashkil etish hamda protsessual yordam mexanizmlarini yo‘lga qo‘yish zarur hisoblanadi. Aynan shu ehtiyoj xalqaro-huquqiy mexanizmlarning ahamiyatini oshiradi.

Xususan, Yevropa Kengashining Budapesht Konventsiyasi, BMTning kiberjinoyatchilikka qarshi yangi Konventsiyasi hamda ikki va ko‘p tomonlama xalqaro bitimlar davlatlar o‘rtasida yagona huquqiy asos yaratishga xizmat qiladi. Ushbu hujjatlar jinoyat tarkiblarini uyg‘unlashtirish, tergov jarayonlarini soddalashtirish va xalqaro hamkorlik samaradorligini oshirishga qaratilgan. Demak, kiberjinoyatchilikka qarshi kurashda xalqaro-huquqiy mexanizmlar nafaqat huquqiy zarurat, balki global xavfsizlikni ta’minlashning muhim sharti hisoblanadi.

Maqolaning maqsadi va muammoni asoslash.

Maqolaning asosiy maqsadi kiberjinoyatchilikka qarshi kurashda davlatlar o‘rtasidagi xalqaro-huquqiy hamkorlikning mazmuni, ahamiyati va amaliy samaradorligini chuqur tahlil qilishdan iborat. Xususan, mazkur tadqiqotda xalqaro konvensiyalar, ikki va ko‘p tomonlama bitimlar, ekstraditsiya institutlari, o‘zaro huquqiy yordam mexanizmlari hamda elektron dalillar almashinuvi kabi vositalarning huquqiy asoslari o‘rganiladi. Shuningdek, mavjud xalqaro institutlar, jumladan Yevropa Kengashi, Birlashgan Millatlar Tashkiloti va boshqa xalqaro tuzilmalar faoliyatining samaradorligi baholanadi.

Tadqiqotning muhim vazifalaridan biri kiberjinoyatchilikning transmilliy xususiyati sababli yuzaga kelayotgan huquqiy va amaliy muammolarni aniqlash hamda ularni bartaraf etish bo‘yicha ilmiy asoslangan takliflar ishlab chiqishdir. Chunki zamonaviy sharoitda kiberjinoyatlar bir vaqtning o‘zida bir nechta davlat hududiga ta’sir ko‘rsatishi, jinoyatchilar esa turli yurisdiksiyalardan foydalanib javobgarlikdan qochishga harakat qilishi mumkin. Bu esa milliy huquqiy mexanizmlarning o‘zi yetarli emasligini ko‘rsatadi.

Bugungi global kiber tahdidlar sharoitida tezkor axborot almashinuvi, qo‘shma tergov harakatlarini tashkil etish, elektron dalillarni qisqa muddatda olish va jinoyatchilarni

[2] Nigmatullin, R.V. (2025). Mezhdunarodnoe sotrudnichestvo gosudarstv v bor’be s kiberprestupnost’yu. *Mezhdunarodnoe publichnoe i chastnoe parvo*

ekstraditsiya qilish masalalari alohida dolzarb ahamiyat kasb etmoqda. Ayniqsa, bank firibgarligi, shaxsiy ma'lumotlarni o'g'irlash, ransomware hujumlari va davlat axborot infratuzilmasiga qarshi hujumlar xalqaro hamkorliksiz samarali bartaraf etilishi qiyin bo'lgan jinoyatlar sirasiga kiradi.

Shu sababli maqolada xalqaro-huquqiy hamkorlikning mavjud mexanizmlarini takomillashtirish, davlatlar o'rtasida ishonchli va tezkor hamkorlik tizimini yaratish hamda xalqaro konvensiyalarning ijrosini kuchaytirish bo'yicha amaliy tavsiyalar ishlab chiqish ko'zda tutilgan. Mazkur tadqiqot natijalari kiberjinoyatchilikka qarshi kurash samaradorligini oshirishga xizmat qiladi. Shu munosabat bilan xalqaro huquqiy instrumentlar (masalan, Budapesht Konventsiyasi, 2025-yilgi BMT Konvensiyasi) hamda mintaqaviy kelishuvlar (SHA miqyosidagi shartnomalar, Afrika Ittifoqi konvensiyasi) o'rganildi.[3] Bir qancha huquqshunoslar bu borada tadqiqot olib bordi: Klevtsov (2020) ruhiy va yalpi huquq yordam va ekstraditsiya orqali hamkorlik qilishga urg'u berib, tinchlik va xavfsizlikka doir global hujjatlarni tahlil qilgan.[4] Nigmatullin (2025) esa yangi BMT Konvensiyasining qabul qilinishi va ikki tomonlama bitimlar zarurligini ko'rsatdi.

Mazkur masala bo'yicha bir qancha nazariy va amaliy ishlanmalar mavjud. Klevtsov (2020) kiberjinoyatchilikka qarshi xalqaro hamkorlikni o'rganib, CoEning Budapeşht Konventsiyasi va mintaqaviy kelishuvlar (SHA, Arab Ittifoqi) orqali ekstraditsiya va huquqiy yordam mexanizmlarini taqdim etadi. Shuningdek, u ham kuchli davlatlarning ba'zilari ushbu konventsiyalarga qo'shilmagani (masalan, RF Buda¬peştni ratifikatsiya qilmagan) va undan keyin kompaniya usullardan foydalanishga majbur ekanini ta'kidlagan. UNODC va CoE manbaalarida xalqaro hamkorlik zarurligi va unga to'siq bo'luvchi omillar tahlil qilingan. Masalan, UNODC ta'kidicha, agar so'rov davlatning inson huquqlari majburiyatlari bilan ziddiyatli bo'lsa, MDH rad etilishi mumkin[5]. Global Initiative tahlili esa Yevropada J-CAT kabi tuzilmalarni misol qilib, "millatlar o'rtasida sezilarli hamkorlik" bo'lmasa, "19-asr qurollari bilan 21-asr jinoyatlari bilan" kurash qilishga to'g'ri kelishini ko'rsatadi.[6] Shu tarzda, pustkiy hujjatlar va amaliyot tahlili maqsadga muvofiq tarzda xalqaro hamkorlik tizimini konseptual jihatdan yaxshiroq anglash imkonini beradi.

Material va metodlar

Tadqiqotda asosan xalqaro huquqiy hujjatlar (konvensiyalar, bitimlar), intervyu va hisobotlar hamda ilmiy maqolalardan foydalanildi. Masalan, CoE Buda¬peşt Konventsiyasi, CIS bitimi (kiberjinoyatchilik bo'yicha), Afrika Ittifoqining Malabo konvensiyasi kabi hujjatlar ko'rib chiqildi.[7] Bundan tashqari, UNODC, Europol, FBI kabi xalqaro tashkilotlarning keskin xatarlarga doir hisobotlari va ko'rsatmalari talqin qilindi. Tadqiqotda so'ngi 5-10 yildagi ma'lumotlar ustuvorlashtirilib, Web of Science va Scopus indeksli jurnallardan olingan nashrlar ham tahlil qilindi. Matnli tahlil uchun CoE va BMTning rasmiy veb-saytlari, shuningdek rasmiy hujjatlar to'plamlari (elektron shaklda) manba sifatida ishlatildi. Tadqiqot jarayonida kiberjinoyatchilikka qarshi kurash bo'yicha davlatlar amaliyotini qiyosiy tahlil qilishga alohida e'tibor qaratildi. Xususan, turli mamlakatlarning ekstraditsiya, elektron dalillarni olish va tezkor axborot almashinuvi bo'yicha tajribasi o'rganilib, ularning xalqaro standartlarga mosligi baholandi. Shuningdek, mavjud xalqaro-huquqiy mexanizmlarning samaradorligi va amaliy

[3] International Cooperation in the Fight Against Cybercrime: Current State and Development Prospects
[4] Klevtsov, K. (2020). International Cooperation in the Fight Against Cybercrime: Current State and Development Prospects. SSRN Electronic Journal.
[5] United Nations Office on Drugs and Crime (2019). Cybercrime: University Module Series (Module 7, International Cooperation).
[6] Reitano, T.; Oerting, T.; Hunter, M. (2015). Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT). Global Initiative Against Transnational Organized Crime.
[7] African Union (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).

qo‘llanishida uchraydigan muammolar aniqlanib, ularni bartaraf etish bo‘yicha ilmiy-amaliy takliflar ishlab chiqildi.

Maqolada huquqiy taqqoslash, tarixiy-tahliliy va abstraktsiyalash metodlari asos qilib olindi. Chet el tajribasi hamda me’yoriy-huquqiy asoslarni solishtirib, butun dunyo bo‘ylab qabul qilingan normalarga nisbatan mamlakatimiz qonunchiligini ko‘zdan kechirganmiz. Shuningdek, statistik va eksperimental tadqiqot elementlari sifatida konvensiyalarga qo‘shilgan davlatlar soni, ular o‘rtasidagi muzokaralar holati, ko‘plab jahon rasmlarini ko‘rsatadigan konferensiyalar (masalan, Octopus) ma’lumotlari ham ko‘rilgan. Ta’lim metodologiyasidan kelib chiqib, huquqiy masalalarga «gunohni aniqlash va yechimini taklif etish» usuli qo‘llanib, mavjud normalarning qo‘llanish amaliyoti va ularning samaradorligi tahlil qilindi.

Tadqiqot natijalari

Tahlil ko‘rsatdiki, xalqaro miqyosda cyberjinoyatchilik bo‘yicha quyidagi asosiy shartnomalar faoliyat ko‘rsatmoqda:

Instrument	Qabul yili	Imzolovchilar / A’zolar	Asosiy mazmuni
Budapest Konventsiyasi (CoE)	2001	97 mamlakat (81 tasdiqlangan)	Kiberjinoyatlarni jinoyat deb tan olish, *ex parte* saqlash (ma’lumotni saqlash) va izlanish, ekstraditsiya va o‘zaro huquqiy yordam (MLA)[1][4].
UN Konvensiyasi (Hanoi)	2025	74 ta davlat (imzolagan)	Keng qamrovli huquqiy yordam, elektron dalillar almashinuvi; BMT doirasida global hamkorlikni mustahkamlash[2][13].
SHA (MDH) bitimi (kompyuter jinoyatlari)	2001	SHA davlatlari (bitim taraflari)	Computer va axborot jinoyatlari bo‘yicha ekstraditsiya va huquqiy yordam[7].
Afrika Ittifoqi konvensiyasi (Malabo Konv.)	2014	Amalga kiritish jarayoni	Kiberxavfsizlik va shaxsiy ma’lumotlarni himoya qilish, jamiyatni hujumga qarshi majburiy choralar bilan ta’minlash. (Litsenziya bo‘yicha)[12][5].

Ushbu jadvaldan ko‘rinib turibdiki, asosan kiberjinoyatga aloqador jinoyatlar bo‘yicha aniq ekstraditsiya va huquqiy yordam qoidalari qabul qilingan. Masalan, CoE Konventsiyasi 29-moddasiga binoan, ayrim vaziyatlarda elektron ma’lumotlarni saqlashni talab qilish uchun ikki tomonlama jinoyat mavjudligi talab qilinmaydi[14]. Boshqa tomondan, ko‘plab davlatlar: Rossiya, AQSh kabi yirik davlatlar hali Buda¬peşt konventsiyasiga qo‘shilmaganligi sababli, ular bilan asosiy muloqot bilateral shartnomalar asosida, reciproklik prinsipi bo‘yicha amalga oshiriladi[9][15]. Shuningdek, Interpol va Europol kabi tashkilotlar Yevropa mamlakatlari va boshqalar o‘rtasida tezkor axborot almashish uchun tizimlar yaratgan.

Tadqiqotdan olingan natijalar shuni ko‘rsatdiki, o‘rganilgan hujjatlarning normativ komponenti kiberjinoyatchilik bilan kurashga keng imkoniyatlar beradi. Masalan, Buda¬peşt Konventsiyasida elektron ma’lumotlarni saqlash va qidirish bo‘yicha to‘g‘ridan-to‘g‘ri tartiblar, shuningdek ma’lumotlarni tezkor razmiyot qilish mexanizmlari nazarda tutilgan[8]. UN Konvensiyasi esa global hamkorlikni kuchaytirish va zamonaviy jinoyat turlari bo‘yicha birdek

[8] United Nations Office on Drugs and Crime (2019). Cybercrime: University Module Series (Module 7, International Cooperation). Vienna: UNODC E4J Programme

javob berishni ko‘zda tutadi. Tajribada, birga tergov o‘tkazish va ma’lumot almashish natijasida jinoyatlarni fosh etish tezlashdi: masalan, J-CAT tadqiqotlari ko‘p davlatlarni jalb qilib kattaroq jinoyat tarmoqlarini ochishda muhim rol o‘ynagan.[9] Shuningdek, rivojlangan davlatlar o‘zaro ma’lumot platformalarini keng joriy qilmoqda: BMT ma’lumotlariga ko‘ra, tezkor ma’lumotni talab qilish va elektron dalillarni berish bo‘yicha standartlar tizimi takomillashtirilmoqda. Maqola muallifi ish davomida, ayniqsa, hujjatlarda nazarda tutilgan jamiyatlararo ishonchni oshirish va sud-huquqiy idoralar o‘rtasida doimiy aloqani yo‘lga qo‘yish zarurligini aniqladi.

Tadqiqot natijalari tahlili

Tahlil shuni ko‘rsatdiki, samarali hamkorlik davlatlarning normativ base bir xilligi va ishonch mexanizmlariga bog‘liq. Kiberjinoyat jinoyatchilari ko‘p hollarda uzluksiz boshqariluvchi infratuzilmadan foydalanganligi sababli (masalan, botnetlar), mamlakatlar o‘rtasida tezkor reaksiya yo‘lini topish muhim[3][11]. Mazkur tadqiqot doirasida muallif boshqa tadqiqotlar bilan solishtirganda, BMTning yangi konvensiyasi yirik davlatlarni ham sohadagi hamkorlikka chorlayotgani ta’kidlandi[8][2]. Biroq amalda ayrim davlatlar (masalan, AQSh) ekstraditsiya bo‘yicha an’anaviy ikki tomonlama bitimlarga tayanadi[15]. Tadqiqot natijalariga ko‘ra, yosh davlat huquqiy tizimlari uchun Buda¬peşt Konventsiyasidagi mansublik va uni ichki qonunchilikka qo‘shish ustuvor vazifa hisoblanadi, biroq barchaga majburiy emas (85% davlat bundan ilhomlanmoqda[17]). Shu asosda muallif fikricha, texnologik va ijtimoiy yutuqlardan kelib chiqib kelgusida kelishuv shartlarini yangilab borish, shuningdek, elektron dalillarni olish va saqlashga oid yangi mexanizmlar ishlab chiqish lozim.

To‘siqlar va cheklovlar.

Xalqaro hamkorlikni murakkablashtiruvchi omillar turli qonunchiliklar, texnologik tafovutlar va suverenitet muammolari hisoblanadi. Hujjatlarda ma’lumki, so‘rovnoma ko‘rilishi inson huquqlariga zid bo‘lsa, davlat uni bajarishdan bosh tortishi mumkin[10]. Shuningdek, ba’zi davlatlarda shifrlash amaliyoti kuchli bo‘lib, cheklovlarsiz ma’lumot olish deyarli mumkin emas (bu esa qonuniy maqsad bilan ham qiyinchiliklar tug‘diradi). Avvalo, jinoyat darajasi to‘g‘risida adolatli baho berish uchun double criminality (ikki marta jinoyat) prinsipi talab qilinadi; bu esa ba’zi hollarda hamkorlikni qiyinlashtiradi (masalan, TXD qonuniy bo‘lmagan so‘rovlar holati). Shuningdek, ba’zi mintaqalarda kadrlar salohiyati, texnika va byudjet cheklovlari sababli xalqaro hamkorlikni amalga oshirishga tayyorlik past bo‘lishi mumkin. Mana shunday to‘siqlarni bartaraf etish uchun davlatlar qonunlarini moslashtirish, xalqaro standartlarga integratsiya qilish va zudlik bilan informatsiya almashishga yo‘l qo‘yuvchi mexanizmlarni mustahkamlashi lozim.

Avvalgi tadqiqotlar bilan taqqoslaganda, bu maqolada an’anaviy bitimlar o‘rniga yangi global tashabbuslar (masalan, 2025 yildagi BMT Konventsiyasi) ahamiyatli ekanligi ko‘rsatilgan. Klevtsov (2020) ham xuddi shunday xulosaga kelib, “ko‘p tomonlama konvensiyalarga imzo chekmaydigan davlatlar an’anaviy ikki tomonlama va reciproklik mexanizmlaridan foydalanishi kerak” degan fikrni ilgari surgan.[11] Bundan tashqari, ba’zi tadqiqotlarda Interpol va Europol tizimlarining ham hamkorlikda roli e’tiborga olingan; masalan, Europolning J-CAT tuzilmasi ham innovatsion yondashuv sifatida ko‘rib chiqilgan (u «fanat, birgalikda tergov olib borish imkonini beruvchi samarali platforma» ekanligi ta’kidlangan). Bu tadqiqotda esa kiberjinoyatchilik sohasida davlat nazariyasidan amaliy natijalarga o‘tish uchun aniqlik kiritilib, ayniqsa tezkor muomala va dalillarni integratsiyalash

[9] Reitano, T.; Oerting, T.; Hunter, M. (2015). Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT). Global Initiative Against Transnational Organized Crime
[10] United Nations Office on Drugs and Crime (2019). Cybercrime: University Module Series
[11] https://www.researchgate.net/publication/348653930_International_Cooperation_in_the_Fight_Against_Cybercrime_Current_State_and_Development_Prospects

bo‘yicha ma’lumot platformalarining muhimligi qayd etildi. Boshqacha aytganda, sheriklik formati muammo yechimi sifatida samaradorligi jihatidan boshqa tadqiqotlar bilan mos keladi, ammo undan ham so‘ng, kooperatsiyaning huquqiy-ta’limiy mexanizmlari kengaytirilishi kerak.

Xulosalar va takliflar

Xorijiy va mahalliy manbalarni tahlil qilish natijasida bir qator muhim xulosalarga kelindi. Avvalo, kiberjinoyatchilikka qarshi samarali kurashni faqat alohida davlatlarning ichki imkoniyatlari bilan ta’minlab bo‘lmaydi, chunki mazkur jinoyatlar transmilliy va chegarasiz xususiyatga ega. Shu sababli davlatlar o‘rtasida to‘g‘ridan-to‘g‘ri hamkorlikni kuchaytirish, yagona universal huquqiy maydon yaratish hamda xalqaro protsessual yordam mexanizmlarini takomillashtirish zarur hisoblanadi. Ayniqsa, elektron dalillarni tezkor olish, saqlash va almashish masalalari zamonaviy jinoyat-protsessual faoliyatning eng muhim yo‘nalishlaridan biri bo‘lib qolmoqda. Yevropa Kengashining Budapesht Konventsiyasi bugungi kunda kiberjinoyatchilikka qarshi kurash bo‘yicha eng samarali va amaliyotda keng qo‘llanilayotgan xalqaro-huquqiy hujjat hisoblanadi. Yevropa Kengashi ma’lumotlariga ko‘ra, ko‘plab davlatlar ushbu Konventsiyani milliy qonunchilikni takomillashtirishda asosiy model sifatida qo‘llamoqda. 2025 yilda BMT tomonidan yangi Kiberjinoyatchilikka qarshi Konventsiyaning qabul qilinishi esa global miqyosda yagona yondashuvni shakllantirishga bo‘lgan ehtiyojning yanada ortganligini ko‘rsatadi. Bu esa xalqaro hamjamiyat kiberjinoyatchilikni jahon xavfsizligiga tahdid sifatida tan olayotganining amaliy ifodasidir.

Ikkinchidan, tadqiqotlar shuni ko‘rsatdiki, ko‘plab davlatlarda kiberjinoyatlar bo‘yicha jinoyat tarkiblari, javobgarlik mezonlari hamda protsessual normalar bir-biridan sezilarli darajada farq qiladi. Bu esa jinoyatchilarni ekstraditsiya qilish, elektron dalillarni olish va xalqaro tergov harakatlarini amalga oshirishda jiddiy to‘siqlarni yuzaga keltiradi. Shu sababli xalqaro konvensiyalar normalarini milliy qonunchilikka to‘liq va samarali implementatsiya qilish, shuningdek ikki va ko‘p tomonlama bitimlar doirasini kengaytirish muhim ahamiyat kasb etadi.

Uchinchidan, ilmiy-amaliy tavsiya sifatida davlatlar o‘rtasida tezkor axborot almashinuvi tizimini yanada mustahkamlash zarur. Xususan, aloqa markazlari, maxsus vakolatli organlar va huquqiy yordam bo‘limlari o‘rtasida doimiy va ishonchli hamkorlik mexanizmini yaratish lozim. Elektron ma’lumotlarni saqlab qolish bo‘yicha tezkor so‘rovlar, raqamli dalillarni real vaqt rejimida uzatish hamda tergov organlari o‘rtasida bevosita aloqa kanallarini rivojlantirish amaliy samaradorlikni oshiradi. Bundan tashqari, davlatlararo treninglar, qo‘shma seminarlar va J-CAT kabi xalqaro operativ hamkorlik dasturlari mutaxassislar malakasini oshirishda muhim rol o‘ynaydi.

To‘rtinchidan, rivojlanayotgan davlatlarda texnik infratuzilmaning yetarli emasligi va malakali kadrlar tanqisligi xalqaro hamkorlik samaradorligini pasaytiruvchi omillardan biri sifatida namoyon bo‘lmoqda. Shu bois xalqaro tashkilotlar tomonidan texnik yordam ko‘rsatish, kiberxavfsizlik bo‘yicha mutaxassislarni tayyorlash va raqamli tergov salohiyatini oshirish bo‘yicha maxsus dasturlarni kengaytirish zarur.

Xulosa qilib aytganda, kiberjinoyatchilikka qarshi kurashda xalqaro-huquqiy hamkorlik nafaqat zarurat, balki zamonaviy global xavfsizlikni ta’minlashning ajralmas sharti hisoblanadi. Tadqiqot natijalari asosida ishlab chiqilgan tavsiyalar kelgusida xalqaro bitimlar doirasida ko‘proq davlatlarni jalb etish, huquqiy yordam jarayonlarini tezlashtirish, elektron dalillar almashuvini soddalashtirish hamda milliy qonunchilikni xalqaro standartlarga moslashtirishga xizmat qiladi. Mazkur yo‘nalishlarda olib boriladigan izchil ishlar global kiberxavfsizlikni mustahkamlashga, davlatlar o‘rtasida ishonchli hamkorlikni rivojlantirishga va kiberjinoyatchilik darajasini sezilarli kamaytirishga xizmat qiladi.

REFERENCES

1. International Cooperation in the Fight Against Cybercrime: Current State and Development Prospects. Klevtsov, K. 2020
2. Mezhdunarodnoe sotrudnichestvo gosudarstv v bor'be s kiberprestupnost'yu. Mezhdunarodnoe publichnoe i chastnoe pravo, no. 4, pp. Nigmatullin, R.V. 2025
3. Reitano, T.; Oerting, T.; Hunter, M. (2015). Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce (J-CAT). Global Initiative Against Transnational Organized Crime.
4. Council of Europe (2026). The global state of cybercrime legislation 2013–2025: a cursory overview.
5. Council of Europe (2025). Cybercrime Convention Committee: Briefing note (August 2024) – Conventions on Cybercrime: the Budapest Convention and the UN Treaty. [Online] Available at: rm.coe.int
6. Council of Europe (n.d.). Benefits of acceding - Cybercrime. Council of Europe.
7. United Nations Office on Drugs and Crime (2019). Cybercrime: University Module Series (Module 7, International Cooperation).
8. African Union (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).
9. Verdelho, P. (2008). The effectiveness of international cooperation against cybercrime: examples of good practice. Council of Europe Cybercrime Projects, March 2008
10. Spoenle, J. (2010). Cloud computing and cybercrime investigations: territoriality vs the power of disposal? Council of Europe, Aug 2010.
11. Schwerha, J. (2010). Law enforcement challenges in transborder acquisition of electronic evidence from cloud providers. Council of Europe, Jan 2010.
12. Cybercrime and Internet jurisdiction. Council of Europe, March 2009.