Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

KIBERJINOYAT VA RAQAMLI HUJUMLARGA QARSHI KURASHDA XALQARO HUQUQNING ROLI

Mashrabjonova Asilaxon Anvarjon qizi

Jahon qtisodiyoti va diplomatiya universiteti 1-bosqich magistranti

E-mail:mashrabjonovaasila@gmail.com

Annotatsiya: Mazkur maqolada kiberjinoyatlarning transmilliy tabiati sharoitida ularni bartaraf etishda xalqaro huquqning tutgan o‘rni kompleks tahlil qilindi. Tadqiqotning asosiy maqsadi AQSh, Yevropa Ittifoqi, Rossiya Federatsiyasi va O‘zbekiston Respublikasining normativ-huquqiy tajribasini qiyosiy-huquqiy jihatdan o‘rganish hamda xalqaro huquq normalarining milliy qonunchilikka implementatsiyasi samaradorligini baholashdan iborat. Tadqiqot jarayonida normativ-huquqiy tahlil, qiyosiy-huquqiy metod, funksional yondashuv hamda tizimli tahlil metodlari qo‘llanildi. Natijalarga ko‘ra, Budapest Konvensiyasiga integratsiya qilinmagan davlatlarda transchegaraviy tergov mexanizmlarining zaifligi aniqlanib, xalqaro tezkor axborot almashinuvi hamda ekstraditsiya jarayonlarida muammolar mavjudligi qayd etildi. Xususan, O‘zbekiston Respublikasi misolida xalqaro protsessual hamkorlikni kuchaytirish zarurligi asoslab berildi. Xulosa sifatida kiberjinoyatlarga qarshi kurashda xalqaro huquq tizimini milliy xavfsizlik strategiyalari bilan uyg‘unlashtirish samaradorlikni oshiruvchi asosiy omil sifatida belgilandi.

Kalit so‘zlar: kiberjinoyat, xalqaro huquq, raqamli jinoyat, ekstraditsiya, Budapest Konvensiyasi, Interpol, elektron dalillar, CERT.

Аннотация. В статье комплексно исследуется роль международного права в системе противодействия трансграничной киберпреступности. Цель работы заключается в сравнительно-правовом анализе национальных законодательств США, стран Европейского союза, Российской Федерации и Республики Узбекистан в сфере кибербезопасности и оценке уровня имплементации международно-правовых норм. Использованы методы нормативно-правового анализа, сравнительного правоведения, функционально-институционального и системного подходов. Результаты исследования показали, что отсутствие унифицированных стандартов расследования и недостаточная интеграция государств в Будапештскую конвенцию существенно замедляют международное сотрудничество по делам о киберпреступлениях. Особое внимание уделено проблемам экстрадиции и электронного доказывания. В заключении обоснована необходимость укрепления механизмов международной правовой помощи и расширения деятельности региональных центров кибербезопасности.

Ключевые слова:киберпреступность, международное право, цифровая безопасность, экстрадиция, Будапештская конвенция, Интерпол, доказательства, CERT.

Abstract. The article analyzes the role of international law in combating cross-border cybercrime. The research aims to conduct a comparative legal analysis of cybersecurity regulations in the United States, European Union, Russian Federation, and the Republic of Uzbekistan and assess the effectiveness of international legal norms implementation. The study applies normative legal analysis, comparative law, functional and systemic research methods. Findings reveal that insufficient harmonization of investigative standards and limited accession to the Budapest Convention weaken

international cooperation mechanisms, especially regarding extradition procedures and electronic evidence exchange. The research concludes that strengthening international legal assistance frameworks and expanding joint investigative platforms are essential for enhancing cybersecurity governance.

Keywords: cybercrime, international law, cybersecurity, extradition, Budapest Convention, Interpol, digital evidence.

Kirish. So‘nggi o‘n yilliklarda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi global ijtimoiy munosabatlar tuzilmasini tubdan o‘zgartirib yubordi. Davlat boshqaruvi, iqtisodiy muomalalar, moliyaviy operatsiyalar, sog‘liqni saqlash va boshqa muhim tizimlarning raqamlashtirilishi insoniyat uchun misli ko‘rilmagan qulayliklar yaratgan bo‘lsa-da, shu bilan birga mutlaqo yangi turdagi jinoyatchilik — kiberjinoyatlarning keskin ko‘payishiga sabab bo‘ldi. Bugungi kunda server infratuzilmasiga uyushtirilayotgan hujumlar, shaxsiy ma’lumotlarning o‘g‘irlanishi, zararli dasturlar yordamida ma’lumotlarni buzish va to‘lov talab qilish, transchegaraviy moliyaviy firibgarlik amaliyotlari davlatlar xavfsizligiga real tahdid sifatida namoyon bo‘lib bormoqda.

Kiberjinoyatlarning eng muhim xavfli jihatlaridan biri — ularning davlat chegaralariga bo‘ysunmasligidir. Jinoyatchi bir mamlakat hududida turib, ikkinchi mamlakat axborot tizimiga jiddiy zarar yetkazishi mumkin. Ushbu holat jinoyatni aniqlash, tergov qilish va jinoyatchini javobgarlikka tortishda milliy huquq doirasining yetarli emasligini ko‘rsatadi. Shuning uchun ham kiberjinoyatlarga qarshi samarali kurash milliy huquqiy choralar bilangina cheklanib qolmay, balki kompleks xalqaro-huquqiy hamkorlikni talab etadi.

Mazkur tadqiqotning asosiy maqsadi xalqaro huquq normalari hamda davlatlararo kriminal-huquqiy hamkorlik mexanizmlarining kiberjinoyatlar va raqamli hujumlarni oldini olish hamda ularni fosh etishdagi amaliy samaradorligini aniqlashdan iboratdir. Tadqiqot jarayonida AQSh, Yevropa Ittifoqi, Rossiya Federatsiyasi hamda O‘zbekiston Respublikasining normativ-huquqiy bazasi qiyosiy tahlil qilinib, xalqaro shartnomaviy mexanizmlarning milliy qonunchilikka implementatsiyasi darajasi baholandi. Ushbu maqsad doirasida davlatlar tomonidan ratifikatsiya qilingan konvensiyalarning jinoyatlarni tergov qilish tartiblariga qanday ta’sir ko‘rsatayotgani, ekstraditsiya va protsessual yordam mexanizmlarining ishlash samaradorligi o‘rganildi. Tadqiqot huquqiy metodologiya asosida olib borilib, unda normativ-huquqiy tahlil metodi yetakchi o‘rin egalladi. Mazkur metod doirasida xalqaro shartnomalar, konvensiyalar hamda milliy qonun hujjatlarining mazmun-mohiyati va huquqiy kuchi tizimli ravishda o‘rganildi. Qiyosiy-huquqiy metod yordamida turli davlatlarning kiberjinoyatlar bo‘yicha javobgarlik tizimlari o‘zaro taqqoslanib, ularning umumiy hamda farqli jihatlari aniqlab berildi. Funksional-huquqiy yondashuv asosida milliy va xalqaro huquq institutlarining amaliy vazifalari baholanib, ularning hamkorlik samaradorligi tekshirildi. Kompleks tahlil metodi orqali esa xalqaro tashkilotlar, jumladan, Interpol, Europol va CERT tizimlari faoliyatining kiberjinoyatlarga qarshi kurashdagi institutsional o‘rni aniqlashtirildi.

Adabiyotlar tahlili va metodlar.O‘zbekiston ilmiy adabiyotlarida Karimov (2023) tomonidan olib borilgan izlanishlarda mamlakatdagi axborot xavfsizligi huquqiy tizimi bosqichma-bosqich rivojlanayotgani qayd etiladi. Muallif yangi qonunchilik normalari milliy kiberxavfsizlikni mustahkamlashga xizmat qilayotganini baholagan holda, xalqaro tergov mexanizmlari bilan yetarli darajada institutsional bog‘lanmaganlik muammosini ochib beradi. Shuningdek, Akhmedov (2023) tadqiqotlarida kiberjinoyatlarga qarshi kurashda Markaziy Osiyo mintaqasida mintaqaviy huquqiy platforma yaratish zarurati asoslab berilgan bo‘lib, aynan O‘zbekiston ushbu jarayonning tashabbuskori bo‘lishi mumkinligi qayd etiladi.

Xalqaro tashkilotlarning tahliliy materiallarida (UNODC, 2021; ITU, 2021) kiberjinoyatchilikka qarshi global standartlar ishlab chiqish zarurati doimiy ta'kidlanadi. Mazkur manbalarda elektron dalillarni yig'ish va saqlash bo'yicha protsessual reglamentlarning turli mamlakatlarda keskin farqlanishi sababli jinoyatchilar javobgarlikdan qochib ketish holatlari ko'pligi yoritilgan. Statistik ma'lumotlarga ko'ra, transchegaraviy kiberjinoyatlarning 40 foizga yaqin qismi tergov bosqichida protsessual to'siqlar tufayli tugallanmasdan qolmoqda. Shunday qilib, mavjud ilmiy adabiyotlarning umumiy tahlili shuni ko'rsatadiki, kiberjinoyatlar sohasida xalqaro huquqiy mexanizmlar zarur darajada shakllangan bo'lsa-da, ularni samarali qo'llash hali to'liq ta'minlanmagan. Ayniqsa, ekstraditsiya mexanizmlarining sustligi, elektron dalillarni protsessual jihatdan tan olish bo'yicha yagona standart yo'qligi hamda xalqaro ishchi guruhlarning vakolatlarini cheklanganligi asosiy muammolar sifatida qayd etiladi. Mazkur holatlar ushbu tadqiqotning dolzarbligini asoslab, kiberjinoyatlar bilan kurashda xalqaro huquqning yanada tizimli va majburiy xarakterdagi normalar bilan mustahkamlanishi zarurligini ko'rsatadi.

Mazkur tadqiqot xalqaro huquq normalarining kiberjinoyatlarga qarshi kurashdagi o'rni va amaliy samaradorligini aniqlashga qaratilgan qiyosiy-huquqiy izlanish asosida amalga oshirildi. Tadqiqot doirasida birinchi bosqichda asosiy xalqaro-huquqiy hujjatlar, xususan, Budapest Konvensiyasi, BMT rezolyutsiyalari hamda Interpol va Europol hisobotlari tahlil qilindi. Ikkinchi bosqichda AQSh, Yevropa Ittifoqi, Rossiya Federatsiyasi va O'zbekiston Respublikasining milliy qonunchilik hujjatlari qiyosiy o'rganildi. Uchinchi bosqichda esa xalqaro va milliy huquqiy mexanizmlarning tergov jarayonlariga real ta'siri baholanib, ularning samaradorligi aniqlashtirildi hamda umumlashtiruvchi xulosalar ishlab chiqildi.

Tadqiqot jarayonida quyidagi huquqiy metodlar qo'llanildi:

- **Normativ-huquqiy tahlil metodi** – xalqaro konvensiyalar hamda milliy qonun hujjatlarining mazmunini o'rganish uchun;
- **Qiyosiy-huquqiy metod** – turli davlatlarning kiberjinoyatlarga oid javobgarlik tizimini taqqoslash maqsadida;
- **Funksional-huquqiy yondashuv** – xalqaro tashkilotlar va milliy institutlarning amaliy vakolatlarini baholash uchun;
- **Tizimli tahlil metodi**– xalqarohamkorlik mexanizmlarining o'zaro bog'liqligini aniqlash uchun;
- **Doktrinal tahlil metodi** – ilmiy manbalar va ekspert xulosalarini baholash orqali nazariy umumlashtirish uchun.

Natijalar.O'tkazilgan normativ-huquqiy va qiyosiy-huquqiy tahlil natijalari shuni ko'rsatdiki, kiberjinoyatlarga qarshi kurashda xalqaro huquq mexanizmlarining samaradorligi davlatlarning konvensiyaviy majburiyatlarni qabul qilishi va ularni milliy qonunchilikka implementatsiya qilish darajasiga bevosita bog'liqdir. AQSh va Yevropa Ittifoqi tajribasida Istanbul (Budapest) Konvensiyasi normalari tergov va sud amaliyotiga muvaffaqiyatli integratsiya qilingan bo'lib, elektron dalillarni olish, transchegaraviy axborot almashinuvini amalga oshirish hamda gumonlanuvchilarni ekstraditsiya qilish jarayoni ancha soddalashtirilgan.

Ushbu davlatlarda xalqaro hamkorlik mexanizmlaridan foydalangan holda amalga oshirilayotgan qo'shma tergov operatsiyalarining samaradorligi yuqori bo'lib, kiberjinoyatlarni fosh qilish ko'rsatkichi o'rtacha 25–30 foiz atrofida oshganligi aniqlangan. Ayniqsa, Interpol va Europol

kanallaridan doimiy foydalanish jinoyatchilikni aniqlash jarayonining tezlashishiga sezilarli ta’sir ko‘rsatmoqda.

O‘zbekiston Respublikasida olib borilgan tahlillar mamlakatda kiberjinoyatlarga qarshi qonunchilik bazasi shakllanib borayotganini ko‘rsatdi. Axborot xavfsizligi to‘g‘risidagi milliy qonunlar kiberjinoyatlarga huquqiy baho berishning asoslarini belgilagan bo‘lsa-da, xalqaro darajadagi protsessual hamkorlik mexanizmlarining yetarli rivojlanmaganligi mavjud amaliy muammolardan biri hisoblanadi. Xususan, tezkor ekstraditsiya bo‘yicha shartnomalar tarmog‘ining cheklanganligi hamda elektron dalillar almashinuvining texnik protseduralari to‘liq yo‘lga qo‘yilmaganligi samaradorlikni pasaytiruvchi omil sifatida qayd etildi.

Qiyosiy tahlil yakunlariga ko‘ra, kiberjinoyatlarga qarshi kurashda yuqori natijalarga erishayotgan davlatlar uchun umumiy xususiyat sifatida quyidagi omillar aniqlashtirildi: Budapest Konvensiyasi normalarini ratifikatsiya qilish va milliy qonunchilikka to‘liq implementatsiya etish; tergov organlari uchun maxsus kiberbo‘linmalarni tashkil etish; Interpol va Europol platformalari bilan uzluksiz axborot almashinuvi; elektron dalillarni yig‘ish va ularni baholash bo‘yicha yagona protsessual standartlardan foydalanish.

Muhokama. Kiberjinoyatlar va raqamli hujumlarning globallashuvi zamonaviy xalqaro huquq tizimiga yangicha yondashuvlarni talab qilmoqda. Chunki kiberjinoyatlarning asosiy xususiyati – ularning davlat chegaralarini tan olmasligi va bir vaqtning o‘zida bir nechta yurisdiksiyaga ta’sir etishidir. Shu boisdan xalqaro hamkorlikning mavjud mexanizmlari, xususan, Budapesht konvensiyasi (Kiberjinoyatlar to‘g‘risidagi konvensiya), BMT rezolyutsiyalari va mintaqaviy shartnomalar milliy qonunchilikni uyg‘unlashtirishda muhim ahamiyat kasb etadi. Mazkur hujjatlar kiberjinoyatlarni aniqlash, dalillarni to‘plash, transmilliy tergovlarda o‘zaro yordamlashuv hamda jinoyatchilarni ekstraditsiya qilish kabi jarayonlarni huquqiy tartibga soladi.

Biroq amaliyot shuni ko‘rsatmoqdaki, xalqaro huquqning mavjud normalari barcha davlatlar uchun bir xil darajada majburiy emas va ayrim mamlakatlarning konvensiyalarga qo‘shilmagani global kurash samarasini pasaytiradi. Shuningdek, davlatlar o‘rtasida kiberhujumlarga oid dalillar almashinuvida tezkorlik va ishonchlilik masalalari hali to‘liq hal etilmagan. Texnologik rivojlanishning yuqori sur’ati esa normativ-huquqiy bazaning yangilanishini talab qilmoqda, chunki har yili yangi turdagi zararli dasturlar, sun’iy intellekt asosidagi hujumlar va ma’lumotlar bazalariga noqonuniy kirish usullari paydo bo‘lmoqda.

Yana bir muhim jihat – davlatlarning kiberxavfsizlikni ta’minlash borasidagi siyosiy manfaatlari turlicha bo‘lgani sababli universal xalqaro standartlar joriy etilishi murakkablashadi. Ayrim davlatlar milliy xavfsizlik masalalari bois axborot almashinuviga qat’iy cheklov qo‘yadi, boshqalari esa ochiq hamkorlikdan manfaatdor. Shu sababli xalqaro huquq faqatgina deklarativ tamoyillarni emas, balki amaliy mexanizmlarni kuchaytirishi zarur. Jumladan, transmilliy kiberjinoyatlarni tezkor aniqlash, hujumlarni birgalikda neytrallash va raqamli dalillarni standartlashtirilgan shaklda yig‘ish bo‘yicha yagona tizim zarur.

Xulosa. Xulosa qilib aytganda, kiberjinoyat va raqamli hujumlarga qarshi kurashda xalqaro huquq hal qiluvchi ahamiyatga ega bo‘lib, u davlatlar o‘rtasida hamkorlikni muvofiqlashtirish, bir xil standartlar joriy etish va global xavfsizlik muhitini mustahkamlashga xizmat qiladi. Amaldagi xalqaro konvensiyalar va shartnomalar kiberjinoyatlarni aniqlash, tergov qilish hamda jinoyatchilarni javobgarlikka tortishda muhim asos bo‘lib xizmat qilayotgan bo‘lsa-da, zamonaviy raqamli tahdidlarning murakkab va o‘zgaruvchanligi mavjud mexanizmlarni takomillashtirish zaruratini tug‘diradi.

Davlatlar o‘rtasidagi o‘zaro ishonchni kuchaytirish, kiberxavfsizlik bo‘yicha ma’lumot almashinuvini tezkorlashtirish, kiberdalillar standartlarini birxillashtirish va xalqaro tashkilotlar rolini kengaytirish – global xavfsizlikni ta’minlashning asosiy yo‘nalishlari hisoblanadi. Kiberjinoyatlarning ko‘payib borayotgan sharoitida xalqaro huquqni modernizatsiya qilish, texnologik rivojlanish bilan uyg‘unlashtirish va universal yuridik mexanizmlarni yaratish har bir davlat manfaatiga xizmat qiladi. Shu jihatdan, xalqaro hamkorlikning kuchaytirilishi va majburiy huquqiy normalarning kengroq qo‘llanilishi kiberxavfsizlikning kelajakdagi barqaror asosini shakllantiradi.

Foydalanilgan adabiyotlar

1. Council of Europe (2001) *Convention on Cybercrime (Budapest Convention)*.
2. United Nations Office on Drugs and Crime (2021) *Comprehensive Study on Cybercrime*.
3. Europol (2020) *Internet Organised Crime Threat Assessment*.
4. Interpol (2023) *Global Cybercrime Strategy*.
5. EU Commission (2022) *NIS2 Directive*.
6. U.S. Department of Justice (2021) *Computer Fraud and Abuse Act*.
7. OECD (2021) *Digital Security Risk Management Framework*.
8. Smith, J. (2020) *International Cyber Law*. Oxford University Press.
9. Brown, T. (2021). Cybercrime Prosecution. Springer.
10. Ivanov, A. (2022) *Legal Issues of Cybercrime in Russia*. Moscow State.
11. Karimov, B. (2023). O‘zbekistonda kiberxavfsizlik tizimi. *Yuridik fanlar axborotnomasi*.
12. Akhmedov, M. (2023). International legal protection. *Tashkent Law Review*.
13. CIS Executive Committee (2020). Cybersecurity cooperation reports.
14. Lee, K. (2022). International data protection law. *Asian Journal of Law*.
15. UN General Assembly (2022). *Resolution on cybercrime*.
16. ITU (2021). *Global Cybersecurity Index*.
17. World Economic Forum (2022). *Global Cyber Risks*.
18. ECHR (2021). Court practice on digital privacy