KIBERJINOYATCHILIK SOHASIDA XALQARO HUQUQIY HAMKORLIK

Sulaymonov Samandar Otabek o'g'li
Mirzo Ulug'bek nomidagi O'zbekiston Milliy universitetining
Ijtimoiy fanlar fakulteti "Yurisprudensiya:
biznes huquqi" yo'nalishi 4-kurs talabasi
streamsrescuer@gmail.com
+998938399959

МЕЖДУНАРОДНОЕ ПРАВОВОЕ СОТРУДНИЧЕСТВО В ОБЛАСТИ КИБЕРПРЕСТУПНОСТИ

INTERNATIONAL LEGAL COOPERATION IN THE FIELD OF CYBERCRIME

Annotatsiya: Ushbu maqolada kiberjinoyatchilik sohasida xalqaro huquqiy hamkorlikning dolzarb masalalari tahlil qilingan. Zamonaviy axborot texnologiyalarining jadal rivojlanishi natijasida yuzaga kelayotgan kiberjinoyatlar va ularning transmilliy xususiyati davlatlar o'rtasida samarali hamkorlikni taqozo etmoqda. Maqolada xalqaro huquq normalari, konvensiyalar va ikki tomonlama bitimlarning o'rni hamda ahamiyati yoritilgan. Shuningdek, kiberjinoyatchilikka qarshi kurashishda xalqaro tashkilotlar faoliyati, huquqni muhofaza qiluvchi organlar o'rtasidagi axborot almashinuvi va hamkorlik mexanizmlari tahlil etilgan. Mazkur yo'nalishda xalqaro huquqiy bazani takomillashtirish va hamkorlik samaradorligini oshirish zarurati asoslab berilgan.

Kalit so'zlar: kiberjinoyatchilik, xalqaro huquq, xalqaro hamkorlik, kiberxavfsizlik, transmilliy jinoyatlar, xalqaro konvensiyalar, huquqni muhofaza qiluvchi organlar, axborot almashinuvi, raqamli xavfsizlik.

Аннотация: В данной статье анализируются актуальные проблемы международного правового сотрудничества в области киберпреступности. Киберпреступления, возникающие в результате стремительного развития современных информационных технологий и их транснационального характера, требуют эффективного сотрудничества между государствами. В статье подчеркивается роль и значение международных правовых норм, конвенций и двусторонних соглашений. Также анализируется деятельность международных организаций по борьбе с киберпреступностью, обмен информацией и механизмы сотрудничества между правоохранительными органами. Обосновывается необходимость совершенствования международно-правовой базы и повышения эффективности сотрудничества в этой области.

Ключевые слова: киберпреступность, международное право, международное сотрудничество, кибербезопасность, транснациональные преступления, международные конвенции, правоохранительные органы, обмен информацией, цифровая безопасность.

Abstract: This article analyzes the current issues of international legal cooperation in the field of cybercrime. Cybercrimes arising as a result of the rapid development of modern information technologies and their transnational nature require effective cooperation between states. The article highlights the role and importance of international legal norms, conventions and bilateral agreements. It also analyzes the activities of international organizations in combating cybercrime, information exchange and cooperation mechanisms between law enforcement agencies. The need to improve the international legal framework and increase the effectiveness of cooperation in this area is substantiated.

Keywords: cybercrime, international law, international cooperation, cybersecurity, transnational crimes, international conventions, law enforcement agencies, information exchange, digital security.

Zamonaviy axborot jamiyatida internet va raqamli texnologiyalarning jadal rivojlanishi hayotning barcha sohalarini tubdan o'zgartirdi. Biroq bu rivojlanish o'z navbatida yangi xavf-xatarlarni ham keltirib chiqardi. Kiberjinoyatchilik – ya'ni kompyuter tizimlari, tarmoqlar va raqamli muhit orqali amalga oshiriladigan jinoiy harakatlar – bugungi kunda dunyo miqyosida eng dolzarb muammolardan biriga aylandi.

Kiberjinoyatchilik an'anaviy jinoyatchilikdan tubdan farq qiladi. Birinchidan, u davlat chegaralarini tan olmaydi: jinoyatchi bir mamlakatda turib, jahonning istalgan nuqtasidagi qurboniga zarar yetkazishi mumkin. Ikkinchidan, bu sohadagi jinoyatlar nihoyatda tez sur'atda rivojlanib, yangi shakllarda namoyon bo'lmoqda. Uchinchidan, kiberjinoyatchilikka qarshi kurash faqat bitta davlat kuchlari bilan samarali olib borilishi mumkin emas – bu muammo xalqaro miqyosda hamkorlikni talab qiladi. Shu sababli, kiberjinoyatchilik sohasida xalqaro huquqiy hamkorlik masalasi nafaqat huquqshunoslar, balki siyosatchilar, texnologlar va davlat boshqaruvi mutaxassislari uchun ham muhim ahamiyat kasb etmoqda.

Kiberjinoyatchilik (inglizcha: cybercrime) – raqamli texnologiyalar, kompyuter tizimlari va internet tarmog'i vositasida yoki ularga qarshi yo'naltirilgan jinoiy harakatlar yig'indisi sifatida tavsiflanadi. Bu sohadagi eng keng tarqalgan ta'rif Yevropa Kengashining 2001-yilgi Budapest Konventsiyasida berilgan bo'lib, unga ko'ra kiberjinoyatchilik kompyuter tizimlariga va ularda saqlanadigan ma'lumotlarga qarshi yo'naltirilgan hamda kompyuter tizimlari orqali amalga oshiriladigan jinoyatlarni o'z ichiga oladi.

Xalqaro jinoiy politsiya tashkiloti (Interpol) kiberjinoyatchilikni ikkita asosiy guruhga ajratadi: birinchisi – kompyuter tizimlari va tarmoqlarga to'g'ridan-to'g'ri qaratilgan jinoyatlar (masalan, kompyuter viruslari tarqatish, tarmoqlarga ruxsatsiz kirish); ikkinchisi – kompyuterdan an'anaviy jinoyatlarni amalga oshirishda qurol sifatida foydalanish (masalan, internet-firibgarlik, onlayn-terrorchilik). Kiberjinoyatchilik turlarini quyidagicha tasniflash mumkin:

– kompyuter tizimlariga ruxsatsiz kirish (hacking) – bu turdagi jinoyatlar kompyuter yoki tarmoq tizimlariga egasining roziligisiz kiriıı va ma'lumotlarga ega bo'lishni o'z ichiga oladi. 2022-yilda dunyo bo'yicha bunday hujumlar soni 5,5 milliarddan oshdi.
– zararli dasturlar (malware) tarqatish – viruslar, troyanlar, ransomware kabi dasturlar orqali tizimlarni ishdan chiqarish yoki ma'lumotlarni o'g'irlash. 2023-yilda global iqtisodiyotga etkazilgan zarar 8 trillion AQSh dollaridan oshdi.
– fishing (phishing) va ijtimoiy muhandislik – elektron pochta yoki soxta veb-saytlar orqali foydalanuvchilarni aldab, ularning shaxsiy ma'lumotlari yoki moliyaviy ma'lumotlarini o'g'irlash.
– kiberterrorchilik – davlat infratuzilmalarini (elektr tarmog'i, suv ta'minoti, transport) raqamli hujumlar orqali ishdan chiqarishga urinish.
– onlayn-firibgarlik va kibersud'yo'qotish – elektron tijorat tizimlaridagi firibgarlik, onlayn-bank hisoblarini o'g'irlash, kriptovalyuta sxemalari.
– kiberjasuslik – davlatlarning strategik ma'lumotlariga, harbiy sirlariga yoki korporativ maxfiy axborotiga nisbatan olib boriladigan raqamli razvedka faoliyati.
– bolalarga qarshi kiberzo‘ravonlik – internet orqali bolalarni ekspluatatsiya qilish, bolalar pornografiyasi tarqatish.

Cybersecurity Ventures kompaniyasining ma'lumotlariga ko'ra, 2025-yilga kelib kiberjinoyatchilikdan global iqtisodiy zarar yiliga 10,5 trillion AQSh dollariga yetishi kutilmoqda. Bu raqam dunyo yirik iqtisodiyotlaridan birining yalpi ichki mahsulotidan ham oshib ketadi.

Kiberjinoyatchilik sohasida xalqaro huquqiy hamkorlik – bu davlatlarning kiber tahdidlarga qarshi birgalikda kurashishi, jinoyatchilarni ta'qib qilish va javobgarlikka tortish maqsadida huquqiy vositalar orqali amalga oshiriladigan hamkorligi tizimi. Bu hamkorlik turli shakllarda namoyon bo'lishi mumkin: ikki tomonlama yoki ko'p tomonlama shartnomalar, xalqaro konventsiyalarga qo'shilish, huquqni muhofaza qilish organlari o'rtasida ma'lumot almashish va boshqalar.

Qonunchilikdagi farqlar. Dunyo davlatlari o'rtasida kiberjinoyatchilikni jinoiy qilish darajasida sezilarli farqlar mavjud. Bir mamlakatda jinoyat deb hisoblanadigan harakat boshqasida qonuniy bo'lishi mumkin (masalan, ma'lum kriptovalyuta operatsiyalari yoki ma'lumotlarga kirish usullari). Bu ikki tomonlama jinoiylashtirish

(double criminality) talabini bajarishni qiyinlashtiradi va extraditsiya so'rovlarini bloklashi mumkin.

Kiberjinoyatchilikka qarshi xalqaro kurashda bir qator tashkilotlar va huquqiy hujjatlar muhim rol o'ynamoqda. Ularni to'g'ri baholash hamkorlikning imkoniyatlari va cheklovlarini tushunishga yordam beradi. 2019-yildan boshlab BMT Bosh Assambleyasi tashabbus bilan kiberjinoyatchilik to'g'risida yangi universal konventsiya ishlab chiqish jarayonini boshladi. Ushbu jarayonning asosiy afzalligi shundaki, u barcha davlatlarni, shu jumladan rivojlanayotgan mamlakatlarni ham qamrab oladigan universal hujjat yaratishga qaratilgan.

Interpol (Xalqaro Jinoiy Politsiya Tashkiloti) kiberjinoyatchilikka qarshi kurashda operativ hamkorlikni ta'minlashda muhim rol o'ynaydi. Tashkilot 194 ta a'zo mamlakat politsiyasi o'rtasida real vaqtda ma'lumot almashish imkonini beruvchi I-24/7 axborot tizimini boshqaradi. Interpol 2014-yildan boshlab maxsus Kiberjinoyatchilik bo'linmasini tuzdi. Europol esa Yevropa Ittifoqi ichidagi kiberxavfsizlik hamkorligini muvofiqlashtiradi. Europol'ning Kiberjinoyatchilik Evropa markazi (EC3) 2013-yildan faoliyat ko'rsatadi va kiberjinoyatlar bilan bog'liq amaliyotlarni bajarishda YeI davlatlariga yordam beradi. Shanxay Hamkorlik Tashkiloti (ShHT) ham axborot xavfsizligi sohasidagi hamkorlikni rivojlantirish yo'nalishida faoliyat olib bormoqda. 2009-yilda ShHT a'zolari tomonidan axborot xavfsizligi sohasida hamkorlik to'g'risidagi bitim imzolangan.

Xulosa qiladigan bo‘lsak, kiberjinoyatchilik sohasida xalqaro huquqiy hamkorlik masalasini o'rganish shuni ko'rsatdiki, bu soha zamonaviy xalqaro huquqning eng dolzarb va murakkab yo'nalishlaridan birini ifodalaydi. Ushbu tadqiqot ishi davomida bir qator muhim xulosalar shakllandi.

Birinchidan, kiberjinoyatchilik o'zining hududsizligi, tezkor rivojlanishi va yuqori texnik murakkabligi bilan an'anaviy jinoyatchilikdan tubdan farqlanadi. Aynan shu xususiyatlar uni milliy miqyosdagi kurash bilan to'liq bartaraf etishni imkonsiz qiladi va xalqaro hamkorlikni mutlaq zarurat sifatida belgilaydi.

Ikkinchidan, hozirgi kunga qadar shakllangan xalqaro huquqiy baza, jumladan Budapest Konventsiyasi, Interpol va Europol tizimi hamda BMT doirasidagi tashabbuslar muhim asos yaratdi. Biroq bu baza hali to'liq va universal emas: yirik davlatlarning konventsiyadan chetda qolishi, qonunchilikdagi farqlar va huquqiy yordam jarayonlarining sekinligi jiddiy muammolarligicha qolmoqda.

Uchinchidan, O'zbekistonning milliy tajribasi so'nggi yillarda jiddiy rivojlanish ko'rsatdi. Milliy qonunchilik kuchaytirildi, instituttsional tizim shakllantirildi va xalqaro hamkorlik aloqalari kengaytirildi. Biroq texnik salohiyat, malakali kadrlar va xalqaro integratsiya darajasini oshirish bo'yicha islohotlar davom ettirilishi zarur.

Yakuniy xulosa sifatida ta'kidlash mumkinki, kibermakon inson sivilizatsiyasining yangi umumiy hududi bo'lib, uning xavfsizligini ta'minlash barcha

davlatlarning umumiy mas'uliyatidir. Xalqaro huquqiy hamkorliksiz bu xavfsizlikni ta'minlash mumkin emas.

Foydalanilgan adabiyotlar:

1. Council of Europe. Convention on Cybercrime (Budapest Convention), ETS No. 185. – Budapest, 23.XI.2001. – URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
2. United Nations General Assembly Resolution 74/247. Countering the use of information and communications technologies for criminal purposes. – New York: UN, 2019.
3. United Nations General Assembly Resolution 75/282. Open-ended ad hoc intergovernmental committee of experts on cybercrime. – New York: UN, 2021.
4. Shanghai Cooperation Organisation Agreement on cooperation in the field of information security. – Yekaterinburg, 2009.
5. O'zbekiston Respublikasining Jinoyat kodeksi. 22.09.1994-y. – Toshkent: Adolat, 2023.
6. O'zbekiston Respublikasining "Axborot xavfsizligi to'g'risida"gi Qonuni. – Toshkent, 2021.
7. Broadhurst R., Grabosky P., Alazab M. (eds). Cybercrime: The Challenge in Asia. – Hong Kong University Press, 2021. – 312 p.
8. Clough J. Principles of Cybercrime. 3rd ed. – Cambridge University Press, 2022. – 548 p.
9. Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. – Polity Press, 2007. – 280 p.
10. Brenner S.W. Cyberthreats: The Emerging Fault Lines of the Nation State. – Oxford University Press, 2008. – 352 p.
11. Saminov M., Xoliqov A. Axborot xavfsizligi asoslari. – Toshkent: TDIU, 2022. – 246 b.
12. Mirzaev B. Xalqaro kiber huquq: O'zbekiston tajribasi. – Toshkent: Akademiya, 2023. – 198 b.
13. Tropina T. Self-Regulation and Cybercrime: The Expanding Role of Internet Industry in Fighting Cybercrime // Journal of Internet Law. – 2019. – Vol. 22, No. 9. – P. 3–12.
14. Maurer T. Cyber Mercenaries: The State, Hackers, and Power // Cambridge Studies in International Relations. – Cambridge University Press, 2018. – 266 p.
15. Schmitt M.N. (ed). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. – Cambridge University Press, 2017. – 642 p.
16. Qodirov A. Kiberjinoyatchilikka qarshi kurashda O'zbekistonning xalqaro hamkorlik tajribasi // O'zbekiston huquqi. – 2023. – № 4. – B. 45–52.
17. Umarov Sh. Raqamli iqtisodiyot sharoitida kiberxavfsizlik va huquqiy tartibga solish masalalari // Iqtisodiyot va innovatsion texnologiyalar. – 2022. – № 2. – B. 88–97.