

KIBERJINOYATLAR VA TRANSMILLIY JINOYATLARGA QARSHI GLOBAL HAMKORLIK.

Qulmurodov Temur O'ktam o'g'li

Buxoro Davlat Universiteti "Tarix va Yuridik" fakulteti "Yurisprudensiya" yo`nalishi 4-bosqich talabasi
Gmail: qulmurodovtemur51@gmail.com TEL: +998992473341

Annotatsiya: Raqamli texnologiyalar va globallashuv jarayonlarining jadallashuvi kiberjinoyatlar hamda transmilliy jinoyatlarning yangi shakllarini yuzaga keltirdi. Mazkur jinoyatlar milliy chegaralardan tashqarida sodir etilishi, murakkab tarmoqlar orqali amalga oshirilishi va yuqori darajadagi texnologik salohiyatni talab etishi bilan ajralib turadi. Ushbu maqolada kiberjinoyatlar va transmilliy jinoyatlarga qarshi kurashda global hamkorlikning zarurati, mavjud xalqaro-huquqiy mexanizmlar, institutlar faoliyati hamda ularning samaradorligi tahlil qilinadi. Shuningdek, xalqaro hamkorlikni kuchaytirish yo'llari va istiqbollari ilmiy asosda yoritiladi.

Kalit so'zlar: Kiberjinoyat, transmilliy jinoyat, global hamkorlik, xalqaro huquq, kiberxavfsizlik, BMT, INTERPOL.

Аннотация: Ускорение процессов цифровых технологий и глобализации привело к появлению новых форм киберпреступности и транснациональной преступности. Данные преступления характеризуются совершением за пределами национальных границ, осуществлением через сложные сети и требованием высокого уровня технологического потенциала. В данной статье анализируется необходимость глобального сотрудничества в борьбе с киберпреступностью и транснациональной преступностью, существующие международно-правовые механизмы, деятельность институтов, а также их эффективность. Кроме того, на научной основе рассматриваются пути и перспективы укрепления международного сотрудничества.

Ключевые слова: Киберпреступность, транснациональная преступность, глобальное сотрудничество, международное право, кибербезопасность, ООН, ИНТЕРПОЛ.

Abstract: The acceleration of digital technologies and globalization processes has led to the emergence of new forms of cybercrime and transnational crime. These crimes are characterized by their commission beyond national borders, their execution through complex networks, and the requirement for a high level of technological capacity. This article analyzes the necessity of global cooperation in combating cybercrime and transnational crime, existing international legal mechanisms, the activities of relevant



institutions, and their effectiveness. In addition, the ways and prospects for strengthening international cooperation are examined on a scientific basis.

Keywords: *Cybercrime, transnational crime, global cooperation, international law, cybersecurity, UN, INTERPOL.*

KIRISH

“Tinchlik har qanday holatda ham hayotimizga kerak, chunki u har bir insonning sharaflari va xavfsiz hayot kechirishining shartidir.”

Kofe Annan

XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi insoniyat hayotining barcha sohalariga chuqur kirib bordi. Shu bilan birga, raqamli makon jinoyatchilik uchun yangi imkoniyatlar yaratdi.

Kiberjinoyatlar va transmilliy jinoyatlar bugungi kunda global xavfsizlikka tahdid soluvchi asosiy omillardan biri sifatida namoyon bo'lmoqda.

Ushbu jinoyatlar bir davlat doirasida emas, balki bir nechta davlat hududini qamrab olgani bois ularga qarshi kurashish milliy choralar bilangina cheklanishi mumkin emas. Shu nuqtayi nazardan, global hamkorlik muhim strategik ahamiyat kasb etadi.

Asosiy qism

Kiberjinoyatlar tushunchasi axborot tizimlari va kompyuter texnologiyalaridan foydalanib sodir etiladigan jinoyatlarni anglatadi. Ular orasida noqonuniy kirish (hacking), elektron firibgarlik, shaxsiy ma'lumotlarni o'g'irlash, zararli dasturlar tarqatish va kiberjosuslik keng tarqalgan.

Transmilliy jinoyatlar esa bir nechta davlat hududini qamrab oladigan yoki oqibatlarini xalqaro miqyosda namoyon bo'ladigan jinoyatlar sifatida e'tirof etiladi. BMT ta'rifiga ko'ra, jinoyat agar u bir nechta davlatda sodir etilsa yoki jinoyat guruhlari xalqaro xarakterga ega bo'lsa, transmilliy jinoyat hisoblanadi.

Bugungi kunda ushbu jinoyatlarning aksariyati kibertexnologiyalar bilan uyg'unlashgan holda amalga oshirilmoqda.

Har qanday texnologik taraqqiyotda bo'lgani kabi, axborot texnologiyalarining, jumladan internetning rivojlanishi ham ko'plab yangi huquqiy munosabatlar bilan birga yangi jinoyat turlarini hamda an'anaviy jinoyatlarning turlicha sodir etilish shakllarini yuzaga keltirdi. Shu tariqa, kundalik va kasbiy hayotimizni sezilarli darajada yengillashtirgan texnologiya va internet bir tomondan, yangi muammo sifatida ham namoyon bo'ldi.

Kiberjinoyatlar bilan kurashish naqadar mushkul ekani so'nggi yillarda tajriba orqali isbotlangan va barchaga ayon bo'lgan holatdir. Bu kurashning esa huquq tizimi uchun qiyinligi quyidagi omillar bilan izohlanadi:



1. Kiberjinoyatchilik nisbatan yangi hodisa bo'lgani sababli, jinoyatlarning sodir etilish usullari bo'yicha aniq andozalar ishlab chiqishning imkoni yo'q. Bu esa mazkur hodisaga qarshi kurashda resurslar qanday taqsimlanishi kerakligini ko'rsatib beradigan "jinoyat xaritalari"ni yaratishga to'sqinlik qiladi. Muammoning haqiqiy ko'lami haqida mavjud ma'lumotlarimiz cheklangan bo'lsada, bu jinoyatchilik turi tez sur'atlarda ortib borayotgani shubhasizdir.

2. Yangi jinoyatchilik turi bilan yuzma-yuz kelinayotgani bois, huquqni muhofaza qiluvchi organlar ushbu soha bilan hali yetarlicha tanish emas. Ichki ishlar va prokuratura organlari nisbatan tezroq moslashmoqda, deb aytish mumkin bo'lsada, tergovchi, surishtiruvchi, prokuror va sudyalarning axborot jinoyatlari masalalarida hozircha yetarli texnik bilimga ega ekanini aytish qiyin, bu borada jiddiy ta'limga ehtiyoj mavjud. Qolaversa, yangi jinoyat sodir etish usullari juda tez paydo bo'layotgani sababli, ushbu vakolatli shaxslarning bilimlarini doimiy ravishda yangilab borish ham zarur.

3. Kiberjinoyatchilikning o'ziga xos xususiyatlaridan biri bu jinoyatchi bilan jabrlanuvchi o'rtasida makon jihatidan masofa mavjudligidir. Bundan tashqari, axborot texnologiyalarining ishlash xususiyati sababli jinoyat ko'pincha bir nechta davlatlarni qamrab oladi, darhaqiqat, kiberjinoyatlarning asosiy belgisi ularning chegaralarni tan olmasligidir. Shuningdek, jinoyat qayerda sodir etilgan deb hisoblanishi ham yuzaga keladi. Jinoyatning ko'pincha bir nechta davlat hududini qamrab olishi davlatlarning suveren tengligi tamoyili nuqtayi nazaridan muammolar keltirib chiqaradi. Bu holat xalqaro huquqning asosiy tamoyillaridan biri bo'lgan davlatning huquqni qo'llash vakolati tegishli davlatning aniq roziligisiz uning hududidan tashqarida amalga oshirilmasligi haqidagi qoida bilan chambarchas bog'liq. Natijada, tegishli davlatning roziligisiz boshqa bir davlat uning hududida tergov harakatlarini olib bora olmaydi. Bu esa kiberjinoyatchilikka qarshi kurashdagi asosiy to'siqlardan birini yuzaga keltiradi. Davlat vakolatlari o'z hududidan tashqariga amal qila olmasligi sababli, kiberjinoyatchilikka qarshi kurash tushunchasi yetarli bo'lmay qolmoqda. Chunki kiberjinoyatchilik barcha jinoyatlar ichida transchegaraviy xususiyatga ega bo'lsada, davlatlarning huquqni qo'llash vakolati hududiy bo'lishi shart.

4. Kiberjinoyatlarni aniqlash ehtimoli an'anaviy jinoyatlarga nisbatan ancha past. Darhaqiqat, bu jinoyatlarni sodir etish vositalari hamda tizimlari doimiy ravishda o'zgaruvchandir. Internetdan anonim foydalanish imkoniyati sababli jinoyatchilarni aniqlash imkoniyati ba'zan juda cheklangan bo'ladi. Bundan tashqari, jabrlanuvchilar, ayniqsa obro'-e'tibor yo'qotishdan cho'chiydigan tijorat kompaniyalar bunday jinoyatlar haqida xabar qilishni istamasliklari mumkin. Shuningdek, axborot tizimlari haqida yetarli bilimga ega bo'lmagan shaxslar ko'p hollarda vaziyatning o'zi haqida ham xabardor bo'lmay qolishlari ehtimoli mavjud.



5. Kiberjinoyatni aniqlashga xizmat qiladigan dalillarning turi va formati, shuningdek ularni qo'lga kiritish usullari an'anaviy jinoyatlarga nisbatan farq qiladi. Dalillarni qo'lga kiritish qiyin bo'lgani kabi, ularni amaldagi protsessual qoidalarga muvofiq tarzda to'plash ham alohida muammo hisoblanadi. Shu nuqtayi nazardan, ushbu jinoyatlarni tergov qiladigan xodimlar juda yuqori darajadagi mutaxassislikka ega bo'lishi shart. Boshqa tomondan, raqamli dalillarning har qanday vaqtda yo'qolib ketish ehtimoli mavjud.

6. Kiberjinoyatlar juda kam xarajat va sa'y-harakat bilan nihoyatda katta miqdorda zarar yetkazish mumkin. Holbuki, bunday jinoyatlarga qarshi kurashishni amalga oshirish katta mehnat va moliyaviy xarajatlarni talab qilishi mumkin.

Aslida, kompyuter va axborot tizimlari orqali sodir etilgan yoki ularga qarshi yo'naltirilgan jinoyatlar borasida davlatlarning sezgirligida katta farqlar mavjud, bu har bir davlatning iqtisodiyoti va infratuzilmasining qanchalik raqamlashtirilganligi bilan bevosita bog'liq bo'lgan texnik masala hisoblanadi. Shuningdek, jinoyat faoliyatlarining nishonga olinishi jihatidan ham har bir davlat duch keladigan tahdid darajasi turlicha. Shu nuqtayi nazardan, ushbu ikki omil davlatlarning kiberjinoyatchilikka nisbatan ko'rsatadigan javob darajalariga sezilarli ta'sir qiladi.

Kiberjinoyatchilikka qarshi kurash borasida Yevropa Ittifoqi, Yevropa Kengashi, Birlashgan Millatlar Tashkiloti (BMT), Iqtisodiy hamkorlik va taraqqiyot tashkiloti (OECD), Amerika Davlatlari Tashkiloti (OAS) kabi xalqaro tashkilot va tuzilmalar hamda ularning ishtiroki yoki qo'llab-quvvatlashi bilan amalga oshirilayotgan ko'plab tashabbuslar mavjud; shuningdek, hukumatga bog'liq bo'lmagan xalqaro tashkilotlar tomonidan olib borilayotgan turli tashabbuslar ham mavjud.

Iqtisodiy hamkorlik va taraqqiyot tashkiloti OECD doirasida, ilgari ham turli tadqiqotlar mavjud bo'lsada, 2002-yilda OECD Kengashi tomonidan qabul qilingan "Axborot tizimlari va tarmoqlar xavfsizligi uchun OECD Yo'riqnomalari: Xavfsizlik Madaniyatiga Yo'l" hujjati alohida e'tiborga molik.

Dunyo miqyosida sanoatlashgan 8 yirik davlatdan (AQSh, Germaniya, Fransiya, Buyuk Britaniya, Italiya, Yaponiya, Kanada va Rossiya) tashkil topgan

G-8 1997-yilda (o'sha paytda G-7 edi) "Yuqori texnologiyali jinoyatlar bo'yicha kichik qo'mita"ni tuzib, kiberjinoyatchilikka e'tibor qaratdi. Keyinchalik, ushbu davlatlarning Ichki ishlar va Adliya vazirlari yuqori texnologiyali jinoyatlarga qarshi kurashish uchun bir qator tamoyillar va o'n banddan iborat amaliy reja qabul qildilar. Ehtimol, alohida ta'kidlash lozim bo'lgan jihat, G-8 doirasida yaratilgan va xalqaro hamkorlik uchun asosiy manba bo'lib xizmat qiladigan, Budapest Konvensiyasining 35-moddasida ham aks etgan "Contact Points Network" konsepsiyasidir.

Shuningdek, G-8 doirasida olib borilgan turli tadqiqotlarda quyidagi masalalarga e'tibor qaratilgan: raqamli "jinoyat panohlarining" oldini olish



2000-yil, kiberjinoyatchilikka qarshi qo'llaniladigan protsessual vositalar 2001-yil, internetni jinoyat maqsadida ishlatilishini oldini olish uchun global imkoniyat yaratish zaruriyati 2004-yil, samarali qarshi choralarni ishlab chiqish 2006-yil, internetning terror maqsadlarida ishlatilishi 2007-yil.

Kiberjinoyatchilikka qarshi kurashda INTERPOL, EUROPOL va EUROJUSTning ishlari muhimdir. Shu boradagi muhim tashabbuslardan biri EUROPOL tomonidan "High Tech Crime Centre" (Yuqori Texnologiyali Jinoyatlar Markazi)ning tashkil etilishi bo'lib, uning maqsadi Yevropa bo'ylab chegara oshuvchi kiberjinoyatlar bo'yicha tergovni muvofiqlashtirishdir. Shuningdek,

2010-yilda EUROPOL doirasida, Yevropa Komissiyasi, EUROJUST va Yevropa Ittifoqi davlatlarining kiberjinoyatchilikka qarshi kurash bo'limlari rahbarlaridan iborat "European Cybercrime Task Force (EUCTF)" (Yevropa Kiberjinoyat Timi) platformasi tashkil etilgan. Shuningdek, BMTning Transmilliy uyushgan jinoyatchilikka qarshi konvensiyasi davlatlar o'rtasida jinoyatchilikka qarshi kurashda huquqiy asos bo'lib xizmat qiladi. INTERPOL, EUROPOL va boshqa mintaqaviy tashkilotlar jinoyatchilarni aniqlash, qidiruv e'lon qilish va tezkor ma'lumot almashinuvida muhim rol o'ynaydi.

Xulosa

Xulosa qilib aytganda, kiberjinoyatlar va transmilliy jinoyatlar zamonaviy global xavfsizlik tizimi oldida turgan eng murakkab va dolzarb muammolardan biri hisoblanadi. Raqamli texnologiyalarning jadal rivojlanishi, axborot makonining chegarasizligi hamda jinoyatchilikning tobora uyushgan va transchegaraviy tus olishi ushbu tahdidlarning ko'lamini yanada kengaytirmoqda. Mazkur jinoyatlar an'anaviy huquqni qo'llash mexanizmlarining imkoniyatlarini cheklab, davlatlardan yangicha yondashuv va hamkorlikni talab etmoqda.

Tahlillar shuni ko'rsatadiki, kiberjinoyatlarga qarshi kurash faqat milliy darajadagi huquqiy va institutsional choralar bilan samarali amalga oshirilishi mumkin emas. Chunki kiberjinoyatlarning asosiy xususiyati ularning hududiy chegaralarni tan olmasligi, jinoyat subyektlari va oqibatlarining bir vaqtning o'zida bir nechta davlatlarga taalluqli bo'lishidir. Shu sababli, xalqaro-huquqiy mexanizmlar, davlatlararo hamkorlik va tezkor axborot almashinuvi ushbu sohadagi muhim omillardan biri bo'lib qolmoqda.

BMT, INTERPOL, EUROPOL, EUROJUST, OECD va Yevropa Kengashi kabi xalqaro va mintaqaviy tashkilotlar tomonidan ishlab chiqilgan konvensiyalar, strategiyalar va amaliy mexanizmlar kiberjinoyatlar hamda transmilliy jinoyatlarga qarshi kurashda muhim huquqiy va tashkiliy asos bo'lib xizmat qilmoqda. Xususan, Budapesht Konvensiyasi, BMTning Transmilliy uyushgan jinoyatchilikka qarshi konvensiyasi va G-8 doirasidagi tashabbuslar xalqaro hamkorlikni mustahkamlashga sezilarli hissa qo'shgan.





Shu bilan birga, kiberjinoyatchilikka qarshi kurashda mutaxassislarining texnik va huquqiy bilimlarini oshirish, raqamli dalillar bilan ishlash bo'yicha protsessual mexanizmlarni takomillashtirish, shuningdek, davlatlar o'rtasida ishonch va hamkorlik muhitini mustahkamlash dolzarb vazifa bo'lib qolmoqda.

Xulosa o'rnida ta'kidlash joizki, kiberjinoyatlar va transmilliy jinoyatlarga qarshi samarali kurash faqat kompleks, tizimli va global yondashuv asosida, xalqaro hamjamiyatning birgalikdagi sa'y-harakatlari orqali ta'minlanishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Birlashgan Millatlar Tashkiloti. Transmilliy uyushgan jinoyatchilikka qarshi konvensiya. Nyu-York, 2000.
2. Yevropa Kengashi. Kiberjinoyatchilik to'g'risidagi Budapesht Konvensiyasi. Budapesht, 2001.
3. INTERPOL. Cybercrime and International Police Cooperation. Lyon, 2019.
4. United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime. New York, 2013.
5. Wall, D. S. Cybercrime: The Transformation of Crime in the Information Age. Polity Press, Cambridge, 2007.
6. Brenner, S. W. Cybercrime and the Law: Challenges, Issues, and Outcomes. Northeastern University Press, Boston, 2010.
7. Clough, J. Principles of Cybercrime. Cambridge University Press, Cambridge, 2015.
8. Europol. Internet Organised Crime Threat Assessment (IOCTA). The Hague, 2020.

