“KIBERJINOYATLARNI TERGOV QILISHDA XALQARO-HUQUQIY HAMKORLIK: MUAMMOLAR VA IMKONIYATLAR”

Shohzod Abdullayev
Toshkent davlat yuridik universiteti Kiber huquqi yo‘nalishi magistranti
E-mail: shaxzodabdullayev9705@gmail.com
Tel: 97 491 77 11

Annotatsiya

Mazkur tezisda hozirgi kunda dolzarb hisoblangan kiberjinoyatchilik hamda ushbu sohadagi mavjud amaliy muammolar va ularning yechimlarini ishlab chiqish yuzasidan takliflar berishga, kiberjinoyatchilikka qarshi kurashda mavjud muammolar, kiberjinoyatlarga qarshi kurashda xalqaro-huquqiy hamkorlik, tergovchi hamda prokurolarning faoliyatidagi mavjud muammolar, kiberjinoyatlarni aniqlash, uning sabablarini o‘rganib bartaraf etish, raqamli dalillarning maqbulligini ta’minlash kabi masalalar tahlil etishga bag‘ishlangan.

Kalit so‘zlar: kibermakon, kiberjinoyat, kiberhujum, ekstraditsiya, raqamli dalil, dalillar maqbulligi, yurisdiksiya muammolari, ransomware, cyberstalking, DDoS hujum, ISO standartlari.

"INTERNATIONAL-LEGAL COOPERATION IN THE INVESTIGATION OF CYBER CRIMES: CHALLENGES AND OPPORTUNITIES"

Abstract

In this thesis, we will make proposals regarding cybercrime, which is currently considered relevant, and the existing practical problems in this field and the development of their solutions, existing problems in the fight against cybercrime, international legal cooperation in the fight against cybercrime, existing problems in the activities of investigators and prosecutors, identifying cybercrime, and studying its causes. It is devoted to the analysis of issues such as elimination of research, ensuring the acceptability of digital evidence.

Keywords: cyberspace, cybercrime, cyberattack, extradition, digital evidence, admissibility of evidence, jurisdictional issues, ransomware, cyberstalking, DDoS attack, ISO standards.

«МЕЖДУНАРОДНО-ПРАВОВОЕ СОТРУДНИЧЕСТВО В РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ: ВЫЗОВЫ И ВОЗМОЖНОСТИ»

Аннотация

В данной дипломной работе внесу предложения относительно киберпреступности, что в настоящее время считается актуальным, и существующих практических проблем в этой сфере и разработки их решений, существующих проблем в борьбе с киберпреступностью, международно-правового сотрудничества в борьбе с киберпреступностью, существующих проблем в деятельности следователей и прокуроров, выявления киберпреступлений и изучения их причин, посвящена анализу таких вопросов, как ликвидация исследований, обеспечение приемлемости цифровых доказательств.

Ключевые слова: киберпространство, киберпреступность, кибератака, экстрадиция, цифровые доказательства, допустимость доказательств, юрисдикционные вопросы, программы-вымогатели, кибersталкинг, DDoS-атака, стандарты ISO.

Kiberjinoyatlarni tergov qilishning asosiy muammolaridan biri shundaki, tergovchilar hatto jinoyatchilarni topishga muvaffaq bo‘lganda ham, ular boshqa davlat hududida, ya’ni boshqa yurisdiksiyada bo‘lganligi sababli qamoqqa olish imkoniyatiga ega bo‘lmaydilar. Yurisdiksiya masalasi kiberjinoyatlarni tergov qilish va unga qarshi kurash yo‘lidagi eng katta muammolardan biridir.

Uzoq vaqt davomida va yuqori darajadagi tekshiruvlar natijasi kiberjinoyatchilarning boshqa bir xorijiy davlatda joylashganligini ko‘rsatsa nima bo‘ladi? Albatta, ularni javobgarlikka tortishning yagona yo‘li bu chet el huquq-tartibot idoralari bilan hamkorlik qilishdir. Ammo bunday vaziyatda xorijiy davlatlar huquqni muhofaza qilish organlari hamkorlik qilishni istamasa yoki tergovchilarga yordam berish uchun texnik imkoniyatlarga ega bo‘lmasa-chi? Afsuski, bunday holat ssenariysi aksariyat hollarda doim takrorlanadi. Bu kabi holatlar kiberjinoyatlarni tergov qilish uchun katta qiyinchilik tug‘diradi va xalqaro hamkorlikdan boshqa yechim yo‘qdek.

Kiberjinoyatlar - transchegaraviy jinoyatlar hisoblanadi va yurisdiksiya masalasini hal qilish, davlatlardan o‘zlarining milliy qonunchiligini uyg‘unlashtirish va butun dunyo bo‘ylab huquqni muhofaza qilish idoralari o‘rtasidagi hamkorlikni rivojlantirish ustida bosh qotirishni talab qiladi. Darhaqiqat, Interpol (Xalqaro Politsiya Kuchlari) jinoyatchilikka, jumladan kiberjinoyatlarga qarshi xalqaro hamkorlik rejasiga ega bo‘lib, unga ko‘pchilik davlatlar qo‘shilgan.

Kiberjinoyatchilikda yurisdiksiya muammosining so‘nggi misollaridan biri "Love Bug" virusi bilan bog‘liq. Dunyo bo‘ylab milliardlab zarar keltirgan ushbu virus Filippin fuqarosi tomonidan yaratilgan va ishga tushirilgan. Mazkur shaxsning xatti-harakatlari Filippin

tergovchilari tomonidan aniqlangan, ammo uning qilmishida Filippinning mavjud moddiy qonunchiligini buzish holati yo‘qligi sababli javobgarlikka torta olishmadi. Negaki, Filippinning hakerlik uchun jazo belgilangan “Elektron tijorat to‘g‘risida”gi qonuni "Love Bug" virusi Internetda paydo bo‘lganidan keyin kuchga kirgan. Shunday qilib, ushbu shaxsning xatti-harakati virus zarar etkazgan boshqa mamlakatlarda javobgarlikka sabab bo‘lgan bo‘lsa-da, faqat mazkur shaxs Filippin davlati yurisdiksiyada bo‘lganligi sababli, xorij huquq-tartibot idoralari unga nisbatan qidiruv e’lon qilish va jinoiy javobgarlikka tortish masalasini hal eta olmadilar. Hozirgi vaqtda ko‘pgina mamlakatlar o‘zlarining jinoiy qonunchiligini yangiladilar va raqamli jinoyatlarni jazolanadigan jinoyat sifatida o‘z qonunchiligiga kiritib qo‘ydilar.

Ikki tomonlama jinoyat prinsipiga asosan "Qo‘shaloq jinoyat" - xalqaro yurisdiksiya masalalari bilan chambarchas bog‘liq bo‘lgan xalqaro huquq tushunchasi hisoblanadi. Ekstraditsiya to‘g‘risidagi shartnomalar shaxsni ekstraditsiya qilish uchun “ikki tomonlama jinoiylikni” talab qiladi, ya’ni shaxsning qilmishi jinoyat sodir etilgan yurisdiksiyada hamda jinoyatchini ekstraditsiya qilishni talab qilayotgan yurisdiksiyada jinoyat deb hisoblanishi lozim. Yuqorida aytib o‘tilgan "Love Bug" virusi misolida, 20 mamlakatda millionlab kompyuter foydalanuvchilariga zarar yetkazgan va milliardlab dollar zarar keltirgan, hakerni jazolanishi mumkin bo‘lgan boshqa mamlakatga ekstraditsiya qilish mumkin emas edi, chunki virus ishga tushirilgan vaqtda, bu kabi xatti-harakat Filippin qonunchiligiga muvofiq jinoyat deb hisoblanmagan.

Amaldagi xalqaro normalarga ko‘ra, yurisdiksiyaning huquqiy tushunchasi hududni ma’nosini o‘z ichiga oladi, bunda bir mamlakat yurisdiksiya doirasi uning hududiy chegaralari chegaralari bilan belgilanadi. Yurisdiksiyaning ushbu hududiy tushunchasi kiberjinoyatchilarni jinoiy javobgarlikka tortish uchun samarasiz. Kiberjinoyat qayerda sodir etilganligini aniqlash qiyin bo‘lishi mumkin, chunki jinoyatchi va jabrlanuvchi turli mamlakatlarda joylashgan bo‘lishi hamda jinoyatchi jabrlanuvchiga hujum qilish jarayonida bir necha mamlakatlar kompyuter tizimlaridan foydalanishi mumkin. Mamlakatlar yurisdiksiyasining hududiy tushunchasini iloji boricha kengaytirish orqali kiberjinoyatlarda yurisdiksiya masalalarini qisman hal qilish mumkin. Masalan, kiberjinoyatlarga qarshi kurashda umumiy yurisdiksiyaga ega davlatlar hududida jinoyat sodir etilganda yoki jinoyatning biron bir qismi sodir etilganda jabrlanuvchi yoki kiberjinoyatchi o‘sha mamlakatning o‘zida jinoiy javobgarlikka tortiladi.

Xalqaro yurisdiksiya muammosini hal qilish uchun nima qilish mumkin?

Kiberjinoyatlar transmilliy bo‘lganligi sababli, davlatlar kiberjinoyatlarning paydo bo‘layotgan turlarini jinoyat deb topuvchi qonunlarni qabul qilishlari kerak. Masalan, "Love Bug" virusini oladigan bo‘lsak, agar Filippinda virus tarqalayotgan paytda hakerlik uchun jinoiy javobgarlik to‘g‘risidagi qonun bo‘lganida, uning yaratuvchisi jinoiy javobgarlikka

tortilishi mumkin edi. Jinoiy qonunlarni uyg‘unlashtirish kiberjinoyatchilarning o‘zlarining xatti-harakatlari jazosiz qolishi xayolotidan qochishga yordam beradi.

Kiberjinoyatlarga qarshi kurashning yana bir muhim taktikasi - bu butun dunyo bo‘ylab huquqni muhofaza qilish idoralari muhim dalillarni olish, saqlash va transportirovka qilish, jinoyatchilarni kuzatish hamda ushlash uchun tezkor hamkorlik qilishlarini ta’minlashdir.

Hozirgacha nimalar qilindi?

Yuqorida qayd etilgan maqsadlarga erishishga ko‘maklashish maqsadida bir qator chora-tadbirlar amalga oshirildi, jumladan, Yevropa Kengashi tomonidan “Kiberjinoyat to‘g‘risida”gi konvensiya qabul qilindi, Ushbu Konvensiya ishtirokchilari kiberjinoyatlarning alohida turlarini ta’qiqlovchi qonunlarni qabul qilishga va ularning huquqni muhofaza qilish organlari xodimlarining kiberjinoyatlarni tergov qilish hamda kiberjinoyatchilarni ta’qib qilishda boshqa mamlakatlar huquqni muhofaza qilish organlari xodimlari bilan hamkorlik qilishlarini ta’minlash uchun zarur bo‘lgan qonunchilik yoki boshqa choralarni ko‘rishga va’da berishadi[1].

Transchegaraviy kiberjinoyatchilikka qarshi kurash huquqni muhofaza qilish organlariga jinoyatlarga qarshi samarali kurashishni qiyinlashtiradigan bir qator aktual muammolarni mavjud. Asosiy muammolardan ba’zilari quyidagilardan iborat:

Xalqaro hamkorlikning yo‘qligi: Kiber jinoyatlar bo‘yicha xalqaro hamkorlikni oshirishga qaratilgan sa’y-harakatlarga qaramasdan, ko‘plab mamlakatlarda onlayn faoliyatni tartibga soluvchi turli xil va bazida bir-biriga qarama-qarshi qonun va qoidalar mavjud. Bu davlatlar huquq-tartibot idoralarining axborot almashishi va harakatlarini muvofiqlashtirishini qiyinlashtirishi mumkin.

Cheklangan resurslar: Kiberjinoyat tez o‘sib borayotgan muammo bo‘lib, ko‘plab huquq-tartibot idoralari texnologik o‘zgarishlar tezligiga moslashish uchun kurashmoqda. Ko‘pgina davlat organlari kiberjinoyatlarni tergov qilish uchun zamonaviy texnologiya va dasturiy ta’minotlarga hamda mutaxassislarning cheklangan resurslarga ega.

Texnik qiyinchiliklar: Kiber jinoyatchilar ko‘pincha o‘z faoliyatini va izlarini yashirish uchun murakkab usullardan foydalanadilar. Bu huquq-tartibot idoralari uchun jinoyatchilarni aniqlash va dalillar to‘plashda qiyinchilik tug‘dirishi mumkin.

Siyosiy sabablar: Ayrim hollarda siyosiy sabablar huquqni muhofaza qilish organlariga kiberjinoyatchilarni tergov qilish yoki jinoiy javobgarlikka tortishni qiyinlashtirishi mumkin. Misol uchun, hukumat diplomatik aloqasi yomonlashishidan qo‘rqsa, chet ellik hakerga qarshi ish qo‘zg‘ashda ikkilanishi mumkin.

Davlatlar qonunchiligidagi farqlar yoki qarama-qarshiliklar: Prokuror va tergovchilar uchun jiddiy muammo tug‘diradigan masalalardan biri bu davlatlar qonunchiligidagi farqlar yoki qarama-qarshiliklardir. Bu degani masalan A davlat qonunlariga ko‘ra jinoyat deb

[1] https://www.i-policy.org/2011/02/how-cyber-jurisdiction-affects-cybercrime-prosecution.html

hisoblanmagan xatti-harakat B davlat qonunlarida jinoyat sifatida belgilangan bo‘lishi mumkin. Bugungi kunda dunyoning narigi burchagida o‘tirgan shaxs o‘z davlatidan, hattoki o‘z uyidan chiqmasdan turib osongina boshqa bir davlat hududida yashaydigan shaxsga (jabrlanuvchiga) qarshi harakatlarni (kiberhujumlarni) amalga oshirmoqda.[1][2]

Bunday vaziyatda prokurorlar mazkur ish bilan shug‘ullanishda jiddiy qiyinchiliklarga duch kelishadi. Masalan, xorijiy davlat tergov idoralaridan deyarli hech qanday yordam olisholmaydi chunki ba’zi davlatlar so‘rov, yordam so‘ralayotgan mamlakatda noqonuniy (sodir etilgan harakat o‘sha davlat qonunchiligiga asosan huquqbuzarlik yoki jinoyat deb topilsagina) bo‘lsagina yordam berishlari mumkin. Shu sababli, prokurorlar boshqa davlat hududidan turib sodir etilgan jinoyatlarni tergov qilish jarayonida ayrim muammo va qiyinchiliklarga duch kelishadi. Bu o‘z navbatida tergov jarayonini to‘liq va sifatli tashkil etilishiga ham to‘siq bo‘lmoqda.

Yurisdiksiyani belgilash: Ko‘p hollarda kiberjinoyatchilar bir nechta davlat yurisdiksiyalarida faoliyat yuritadi, bu esa qaysi davlat yoki mamlakatlar jinoyat sodir etilgan jinoyat ustidan yurisdiksiyaga ega ekanligini aniqlashni qiyinlashtiradi. Bu esa huquqni muhofaza qiluvchi organlar o‘rtasida muvofiqlikning yo‘qligiga olib keladi va huquqbuzarlarni jinoiy javobgarlikka tortishni qiyinlashtiradi.

Ayrim holatlarda, juda ko‘p mamlakatlar jinoyatchini tergov qilish va jinoiy javobgarlikka tortishdan manfaatdor ekanligini ko‘rsatiladi[3]. Bunday muammolarni hal qilish uchun ular boshqa yurisdiksiyalardagi tergovchilar bilan muzokaralar olib borishlari va yurisdiksiyani qanday qilib eng yaxshi tarzda aniqlash mumkinligini belgilashlari kerak.

Biroq, agar jinoyat jabrlanuvchi joylashgan yoki xatti-harakatlarning oqibatlari sodir bo‘lgan mamlakatda ayblanishi kerak bo‘lsa, jinoyatchi o‘sha davlatga ekstraditsiya qilinishi kerak bo‘ladi. Bu ko‘pincha agarda ikki davlat o‘rtasida ekstraditsiya shartnomasi bo‘lmasa tergovchilar va prokurorlar uchun muammo tug‘diradi.

Dalillarni to‘plash: So‘nggi paytlarda kiberjinoyatchilikning kuchayib borishi butun dunyoda xavotir uyg‘otmoqda. Bu o‘z navbatida prokurorlar va tergov organlarida boshqa davlat hududida sodir etilgan jinoiy xatti-harakatlarni tergov qilishda hamda jinoyatchilarni javobgarlikka tortish uchun dalillarni to‘plashda katta muammo va qiyinchiliklarga duch kelishmoqda. Xalqaro kontekstda onlayn xizmat ko‘rsatuvchi provayderlardan dalillarni saqlash va to‘plashni qaysi davlat yurisdiksiyasi tartibga solishini aniqlash ko‘pincha qiyin va ko‘p vaqt talab etadigan jarayondir. Bundan tashqari, tahlillar natijalari shuni ko‘rsatadiki, onlayn sodir etilgan jinoyatlar qurbonlari soni, real hayotda sodir etilgan jinoyatlar soniga

[2] [1] D. Marc Goodman and W. Brenner Susan, ‘The Emerging Consensus on Criminal Conduct in Cyberspace’ (2002) vol. 3, Journal of Law & Technology, pp 4-24.

[3] Dr Russell and G. Smith, Investigating Cybercrime: Barriers and Solutions (Pacific Rim Fraud Conference Sydney, 11 September 2003). Available at: <http://www.aic.gov.au/media_library/conferences/other/smith_russell/2003-09-cybercrime.pdf (http://www.aic.gov.au/media_library/conferences/other/smith_russell/2003-09-cybercrime.pdf)> Last Accessed on 11 July 2017.

qaraganda ko‘proqdir[4]. Bu shuni anglatadiki, prokuror va tergov guruhi ayblanuvchiga nisbatan ish qo‘zg‘atish uchun yetarli dalillarga ega bo‘lmaydi. Jabrlanuvchilardan ko‘rsatmalar olinganda ham, ular ko‘pincha jinoyatchilarni aniqlay olmaydilar. Tergovchilar dalillarni olish uchun ko‘pincha xalqaro hamkorlik qilishga majbur bo‘lishadi.

Buning sababi shundaki, bir davlat tergov organlari sodir etilgan huquqbuzarlikka oid ma’lumot va dalillarni olish uchun boshqa davlatning yurisdiksiyasiga bevosita kira olmaydi. Ular ikki davlat o‘rtasida o‘zaro huquqiy yordam yuzasidan boshqa davlat huquqni muhofaza qiluvchi idoralari bilan muzokaralar olib borishlari kerak.

Ba’zida bu muzokaralar jarayoni butunlay davlatlar o‘rtasidagi siyosiy munosabatlarga bog‘liq bo‘ladi. Bu, shuningdek, turli mamlakatlarda kiberjinoyatlarni tergov qilishning ahamiyati nuqtai nazaridan turli xil ustuvorlik va yo‘nalishlarga ega bo‘lishi mumkin. Aksariyat mamlakatlarda kompyuterlardan foydalangan holda sodir etilgan iqtisodiy jinoyatlar, ko‘pincha zo‘ravonlik jinoyati yoki milliy xavfsizlik manfaatlari xavf ostida bo‘lishi mumkin bo‘lgan jinoyatlar keng tarqalgan mamlakatlarda jinoyatning muhimlik iyerarxiyasining pastki qismida turadi. Natijada, sodir etilgan kiberjinoyat yuzasidan yordam so‘rab murojaat qilgan davlatga agarda bu sohada hamkorlik mavjud bo‘lmasa, bunday murojaatlarga e’tiborsizlik bilan qaralishi mumkin[5].

Davlatlar homiylik qiladigan kiberjinoyatlar: Bir qator tadqiqotlar shuni ko‘rsatadiki, ayrim davlatlar homiyligidagi agentlar kiberjinoyat bilan shug‘ullanadilar va buni davlat hukumati tomonidan qo‘llab kelinadi. Masalan, Xitoy hukumati keng tarqalgan iqtisodiy va sanoat josusligi bilan shug‘ullangani, AQSh hukumati esa kiberkuzatuvning yirik dasturlari bilan shug‘ullangani haqida bir qancha da’volar ilgari surilgan[6]. Davlat tomonidan homiylik qilingan ushbu harakatlar ularni sodir etgan davlat qonunlariga ko‘ra jinoiy harakat sifatida belgilanishi mumkin emas, lekin odatda o‘ziga nisbatan bunday harakat sodir etilgan davlat tomonidan jinoyatlar sifatida qaraladi. Shunga qaramay, prokurorlar va tergovchilar davlatga qarshi bunday kiberhujumni qo‘llab-quvvatlashga oid juda kuchli dalillarni keltirsalar ham, bunday hollarda ular deyarli hech narsa qila olishmaydi.

Masalan, 2014-yilda Shimoliy Koreya hakerlari AQShning Sony Pictures Entertainment kompaniyasiga xakerlik hujumini uyushtirishda ayblanib bu hujumni Shimoliy Koreya hukumati tomonidan homiylik qilingani haqida iddaolar ilgari surilgan edi. AQSh razvedkasining xulosasiga ko‘ra, kiberhujum Shimoliy Koreyadadan turib amalga oshirilgan hukumat bunga homiylik qilgan bo‘lishi mumkinligi ta’kidlandi. Shimoliy Koreya hukumati nafaqat bu ayblovni rad etdi, balki jinoyatni ochishda xalqaro hamkorlik qilishdan va bu

[4] Jo Bryce, ‘Online sexual exploitation of children and young people’ in Yvonne Jewkes and Majid Yar (eds), Handbook of Internet Crime (Willan Publishing, 2010) at page. 322.
[5] Dr Russell and G. Smith (n 6).
[6] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab & Steve Chon, ‘Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime’ (2014) Vol. 8:1, International Journal of Cyber Criminology, pp. 1–20.

harakatlarga yordam berishdan ham bosh tortdi[7]. Bundan ko‘rinib turibdiki, boshqa davlatning hamkorligi va yordamisiz chet el hukumatlari tomonidan kiberjinoyatlarni sodir etgan shaxslarga nisbatan samarali qonuniy choralar ko‘rish mexanizmi mavjud emas.

Ekstraditsiyani ta’minlash: "Qo‘shaloq jinoyat". Ekstraditsiyani ta’minlash tergovchi va prokuratura guruhi uchun eng qiyin bosqichlardan biridir. Ekstraditsiya nafaqat tegishli ikki davlat o‘rtasida tegishli shartnoma mavjudligini, balki ko‘rib chiqilayotgan xatti-harakat ham gumonlanuvchini yuborayotgan, ham qabul qilayotgan davlat qonunlarida jinoiy javobgarlikka tortilishi belgilab qo‘yilgan bo‘lishi, ya’ni “ikki tomonlama jinoiylik”ni talab qiladi. Ammo kiberjinoyatlar bilan bog‘liq ishlarda, bu ko‘pincha bunday emas.

Shuningdek, 2013-yilda butun dunyoda katta shov-shuvlarga sabab bo‘lgan Snowden ishi haqida ham shunday deyish mumkin. Edward Joseph Snowden – amerikalik kompyuter mutaxassisi, AQSh Markaziy razvedka boshqarmasi hamda AQSh milliy xavfsizlik agentligining sobiq xodimi bo‘lgan.

Snouden 2013-yilning iyun oyida Amerika maxsus xizmatlarining butun dunyodagi internet foydalanuvchilarini kuzatib borish imkonini beradigan maxsus dasturlari haqida OAVga ma’lumot bergan edi.

Snowden AQShdan qochib, dastlab Gongkonga boradi. 15-iyun kuni AQSh Hon Kongdan amaldagi ikki tomonlama ekstraditsiya to‘g‘risidagi shartnomaga muvofiq, Snowdenni hibsga olishni hamda AQShga topshirishni so‘rab murojaat qildi. 23-iyun kuni Hon Kong ma’muriyati AQShni ekstraditsiya to‘g‘risidagi so‘rovni asossiz deb topganligi hamda Gonkongni tark etishga ruxsat berganligini ma’lum qildi. 2013-yil 7-avgust kuni AQSh va Rossiya prezidentlarining avgust oyida rejalashtirilgan uchrashuvlari bekor qilinishiga sabab, Barak Obama, Rossiyaning Snoudenni AQShga topshirish haqidagi talablarini bajarmagani uchun, Rossiya prezidenti Vladimir Putin bilan uchrashuvini bekor qildi - degan taxminlari e’lon qilindi.

Bundan kelib chiqadiki, ekstraditsiya masalasida samarali hamkorlik qilish uchun ikki davlat o‘rtasidagi siyosiy munosabatlar ham ijobiy bo‘lishi ahamiyatlidir.

Shaxsni aniqlash va topish qiyin: Tergovchilar va prokurorlar kiberolamda sodir etilgan jinoyatni kim tomonidan amalga oshirilgani, jinoyatchining shaxsini aniqlashda jiddiy qiyinchiliklarga duch kelishadi[8].

Misol uchun, Bangladeshdan tashqarida X ning facebook akkauntini buzib, uning hisobidan jinoyat sodir etish uchun foydalanishi mumkin. Shunday qilib, dastlabki bosqichda, facebook akkaunti egasi boshqa birov tomonidan sodir etilgan jinoyat uchun javob beradi.

Bundan tashqari, jinoyatchilar o‘zlarining shaxsini va joylashuvini yashirish uchun murakkab usullardan foydalanishlari mumkin. Shu munosabat bilan, Yevropolning so‘nggi hisobotida

[7] David E. Sanger and Nicole Perlrothdec, U.S. Said to Find North Korea Ordered Cyberattack on Sony, (2014). Available at: <https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html> Last Accessed on 2nd of July 2017.

[8] R. Broadhurst & P. Grabosky, ‘Computer-Related Crime in Asia: Emergent Issues’ in R. Broadhurst & P. Grabosky (Eds.), Cyber-crime: The Challenge in Asia (Hong Kong: Hong Kong University Press) at pp. 347–360.

aytilishicha, "shifrlash", "anonimlashtirish" vositalari, "virtual valyutalar" va "Darknet" dan jinoyatchilarning foydalanishi kuchayishi huquqni muhofaza qilish organlariga endilikda jinoyatchining jismoniy joylashuvini, jinoiy infratuzilmasini yoki elektron dalillarni aniqlash imkoniyatini qiyinlashtiradigan vaziyatga olib kelishini ta'kidlagan[9]. Bunday vaziyatlarda dalillarni to'plash yoki maxsus tergov vakolatlaridan foydalanish qaysi davlat yurisdiksiyaga tegishli ekanligi, shuningdek, jinoiy faoliyatni nazorat qilish va turli xil maxfiy tadbirlarni amalga oshirish qaysi davlat qonunlari va huquqi asosida tartibga solishi noma'lumligicha qolmoqda.

Transchegaraviy kiberjinoyat eng katta muammolari jinoyatchilarni aniqlash va izlashning qiyinligidir. Jinoyatchilar o'zlarining shaxsiy ma'lumotlarini va joylashuvlarini yashirish uchun turli usullardan foydalanishlari mumkin, shu jumladan, virtual xususiy tarmoqlar (VPN) va boshqa anonimlashtiruvchi vositalardan ham. Bu, tergov organlarining kiberjinoyatchilarni aniqlash va ularni qo'lga olishni qiyinlashtiradi, ayniqsa, jinoyatchilar kiberjinoyatlar uchun jinoyat qonunchiligi zaif yoki umuman mavjud bo'lmagan davlatlarda faoliyat yuritayotgan bo'lsalar.

Transchegaraviy kiberjinoyatchilikka qarshi kurash murakkab va qiyin vazifadir, ammo unga qarshi kurash samarali bo'lishi uchun bir nechta yechimlar mavjud. Asosiy yechimlardan ba'zilari quyidagilardan iborat:

Xalqaro-huquqiy hamkorlikning yaxshilash: Transchegaraviy kiberjinoyatchilikka qarshi kurashda turli mamlakatlar huquq-tartibot idoralari o'rtasidagi hamkorlik muhim ahamiyatga ega. Bu axborot va razvedka ma'lumotlarini almashish, tergovlarni muvofiqlashtirish va muammoga qarshi kurashish uchun qo'shma strategiyalarni ishlab chiqishni o'z ichiga olishi mumkin.

Resurslarni oshirish: Huquqni muhofaza qilish idoralari kiberjinoyatchilarni samarali tergov qilish va jinoiy javobgarlikka tortish uchun yetarli resurslarga muhtoj. Bu ixtisoslashtirilgan o'quv mashg'ulotlari va texnologiyalarni moliyalashtirish, shuningdek, kiber jinoyatlarni tergovqilishni qo'llab-quvvatlash uchun qo'shimcha tajribali xodimlarni jalb etishni o'z ichiga olishi mumkin.

Qonunlar va boshqa huquqiy asoslarni kuchaytirish: Ko'pgina mamlakatlar kiberjinoyatchilikka qarshi samarali kurashish uchun o'z qonunlari va qoidalarini yangilash ustida ishlamoqda. Bu kiberjinoyatlarning yangidan-yangi turlari paydo bo'layotganligi va qonunchilikni ham tez-tez yangilash zarurati mavjudligi sabab mumkin.

Davlat-xususiy sheriklikni kengaytirish: Davlat va xususiy sektor tashkilotlari axborot almashish va kiberjinoyat xavfini kamaytirish strategiyalarini ishlab chiqish uchun birgalikda ishlashi mumkin. Bu huquqni muhofaza qilish idoralari, xususiy kompaniyalar va kiberxavfsizlik bo'yicha ekspertlar o'rtasidagi hamkorlikni o'z ichiga oladi.

[9] Eurojust and Europol, Common challenges in combating cybercrime (Brussels, 13 March 2017, 7021/17).

Texnologiya va vositalarni yaxshilash: Yangi texnologiyalar va vositalarni ishlab chiqish huquqni muhofaza qilish organlariga kiberjinoyatlarni yanada samaraliroq tergov qilish va jinoiy javobgarlikka tortishda yordam beradi. Bu huquqbuzarlarni aniqlash va kuzatish vositalarini, shuningdek raqamli dalillarni tahlil qilish va talqin qilish usullarini o‘z ichiga oladi.

Kiberjinoyatlarning yana bir muammosi raqamli dalillarni to‘plash va saqlashning qiyinligidir. Raqamli dalillar oson o‘zgartirilishi yoki yo‘q qilinishi mumkin. Dalillarni boshqa davlatlarda joylashgan serverlardan va boshqa raqamli qurilmalardan olish jarayonida ularning maqbulligini saqlash qiyin bo‘lishi mumkin. Bu, kiberjinoyatchilarga qarshi kurashda jarayonini qiyinlashtiradi va jinoyatlarning ochilishini sekinlashtiriradi.

Bugungi kunda amaliyotda O‘zbekiston Respublikasida axborot texnologiyalari vositalari orqali sodir etilgan jinoyatlar (kiberjinoyatlar) ni tergov qilish (jinoyat joyini ko‘zdan kechirish, jinoyat vositalarini texnik talablar asosida ko‘zdan kechirish, raqamli dalillarni standartlar asosida olish va uni labaratoriyada ekspertizadan o‘tkazish) jarayonlari Xalqaro standartlar (ISO-27037 standarti)ga javob bermasligi kabi muammolar mavjud.

Yechim: Kiberjinoyatlarni tergov qilish jarayonini ilg‘or xorijiy amaliyotlar va standartlarga moslashtirish. Ushbu standartlarda raqamli dalillarni baholashning xalqaro darajada tan olingan qoidalari belgilangan. Ularni milliy qonunchilikka moslashtirilishi quyidagi masalalarni ijobiy hal etilishiga yordam beradi:

birinchidan, huquqni qo‘llash faoliyati shaffofligini ta’minlanadi;

ikkinchidan, ishni sudga qadar yuritish va sud bosqichlarida raqamli dalillarni to‘plash, saqlash, tekshirish va baholashning ilmiy asoslangan, obyektiv, qonuniy va adolatli mexanizmi joriy etiladi;

uchinchidan, raqamli dalillar bilan ishlash sohasida nafaqat jinoyat sudlari uchun balki ma’muriy, fuqarolik, iqtisodiy hamda hakamlik sudlari uchun ham yagona uslubiy qoidalarni belgilanadi;

to‘rtinchidan, sohada davlatlar o‘rtasida yuzaga kelgan nizolarda O‘zbekiston Respublikasi manfaatlari ishonchli himoyasini ta’minlash imkoniyatini beradi.

TAKLIFLAR: Kiberjinoyatlarni tegov qilish jarayonida raqamli dalillar bilan ishlash jarayoniga ISO standartlarini, jumladan ISO-27037 standarti talablari asosida raqamli dalillarni to‘g‘ri aniqlash, to‘plash, olish va saqlashni ta’minlash tartibini qonunchilikka implimentatsiya qilish lozim.

Qonun hujjatlarini ishlab chiqish: ISO 27037 standarti talablariga javob beradigan tartib-qoidalarni ishlab chiqish va qonunda nazarda tutish. Ushbu tartib-qoidalar raqamli dalillar bilan ishlashning barcha jihatlarini qamrab olishi kerak: **identifikatsiya qilish va to‘plashdan tortib saqlash va saqlashgacha.**

Malakali mutaxassislar tayyorlash: Raqamli dalillar bilan ishlashda ishtirok etuvchi barcha xodimlar tegishli tarzda rivojlangan xorijiy davlatlarda o‘qitilishi va malaka oshirishga yuborilishi.

Moddiy texnik bazani yangilash: Bu yangi vositalar yoki texnologiyalarni sotib olishni, mavjud resurslarni almashtirishni yoki yangilarini sotib olishni o‘z ichiga olishi mumkin **(bizda raqamli tergovlar hozirda BELKOSOFT yordamida amalga oshiriladi)**.

Xulosa sifatida shuni aytish mumkinki, so‘nggi paytlarda jinoyatchilar jinoyat sodir etishda yangi texnologiyalardan foydalanmoqda. Shu bois, prokuror va tergovchilar uchun jinoyatchini topish, jinoyatni tushunish va haqiqiy aybdorlarga nisbatan jinoyat ishini qo‘zg‘atish juda qiyin bo‘lib bormoqda. Tergovchilar to‘g‘ridan-to‘g‘ri tergov olib bora olmasalar va boshqa xorijiy davlat organlari taqdim etgan ma’lumotlarga tayanmasalar, bu ahvolni yanada qiyinlashadi. Shu sababli, ushbu soha yanada chuqurroq o‘rganilishi kerak va davlatlar birgalikda kelishib, kiberjinoyatlar bilan bog‘liq mavjud qonunlarni uyg‘unlashtirish uchun chuqur tadqiqot ishlarini olib borishda tashabbus ko‘rsatishlari lozim. Davlatlar ushbu muammolarni hal qilish uchun kiberjinoyatchilikka qarshi kurash bilan bog‘liq hamma narsani qamrab oluvchi xalqaro shartnomani ishlab chiqish va tasdiqlash haqida o‘ylashlari shart.raqamli tergovlarni olib borishda xalqaro standartlarni joriy etmas ekanmiz, kun sari rivojlanib borayotgan texnologiyalar zamonida axborot texnologiyalari orqali sodir etilgan jinoyatlarni ochish hamda ularning zararlarini qoplash masalasi bizda oqsayveradi. Shuning uchun rivojlangan davlatlarning kiberjinoyatlarni tergov qilish metodlari hamda ISO ning raqamli tergovga oid xalaqaro standartlarini milliy qonunchiligimizga implementatsiya qilish lozim.

Bundan tashqari, kiberjinoyatchilikka qarshi kurashning eng muhim yo‘llarida biri bu huquqni muhofaza qilivchi organlar o‘rtasida xalqaro hamkorlikni oshirishdir. Bu, ma’lumotlarni almashish, tekshiruvlarni koordinatsiyalashtirish va kiber jinoyatlarini tergov qilish va jazolash uchun umumiy standart va protokollarni ishlab chiqish kabi harakatlarni amalga oshirish orqali ta’minlanishi mumkin.

Foydalanilgan adabiyotlar ro‘yxati:

1. D. Marc Goodman and W. Brenner Susan, ‘The Emerging Consensus on Criminal Conduct in Cyberspace’ (2002) vol. 3, Journal of Law & Technology, pp 4-24.
2. Susan W. Brenner and Bert-Jaap Koops, ‘Approaches to Cybercrime Jurisdiction’ (2004) vol. 4 J. High Tech. L. 1 at page 3.
3. See also: Jurisdiction, Legal Guidance: Crown Prosecution Service. Available at: <http://www.cps.gov.uk/legal/h_to_k/jurisdiction/> Last Accessed on 11th July 2017.
4. R v Sheppard and Whittle (2010) EWCA Crim 65.
5. Dr Russell and G. Smith, Investigating Cybercrime: Barriers and Solutions (Pacific Rim Fraud Conference Sydney, 11 September 2003). Available at:

<http://www.aic.gov.au/media_ library /conferences/ other/smith _russell / 2003-09-cybercrime.pdf> Last Accessed on 11th July 2017.

6. Jo Bryce, 'Online sexual exploitation of children and young people' in Yvonne Jewkes and Majid Yar (eds), Handbook of Internet Crime (Willan Publishing, 2010) at page. 322.
7. Dr Russell and G. Smith (n 6).
8. T. Marcus Funk, Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges (Federal Judicial Center, 2014) at page 2-3.
9. Roderic Broadhurst, Peter Grabosky, Mamoun Alazab & Steve Chon, 'Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime' (2014) Vol. 8:1, International Journal of Cyber Criminology, pp. 1–20
10. David E. Sanger and Nicole Perlrothdec, U.S. Said to Find North Korea Ordered Cyberattack on Sony, (2014). Available at: <https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html> Last Accessed on 2nd of July 2017.
11. R. E. Bell, 'The Prosecution of Computer Crime' (2002) vol. 9:4, Journal of Financial Crime, pp. 308-25.
12. R. Broadhurst & P. Grabosky, 'Computer-Related Crime in Asia: Emergent Issues' in R. Broadhurst & P. Grabosky (Eds.), Cyber-crime: The Challenge in Asia (Hong Kong: Hong Kong University Press) at pp. 347–360.
13. BBC News, Pensioner freed after FBI bungle (26 February, 2003). Available at: <http://news.bbc.co.uk/1/hi/england/2799791.stm> Last Accessed on 22nd June 2017. See also: BBC News, How the mix-up happened (26 February, 2003). Available at: <http://news.bbc.co.uk/1/hi/england/2799929.stm> Last Accessed on 22nd June 2017.
14. Eurojust and Europol, Common challenges in combating cybercrime (Brussels, 13 March 2017, 7021/17).
15. Olimov Azizjon Anvar o'g'li - Kiberjinoyatchilikka qarshi kurashishning tashkiliy-huquqiy asoslari va ularni takomillashtirish masalalari: milliy va xorijiy tajriba
16. https://www.interpol.int/Crimes/Cybercrime
17. S.Morgan. Official Annual Cybercrime Report 2019 // Cybersecurity Ventures.
18. http://www.statista.com/ (The Statistics Portal)
19. https://wearesocial.com/digital-2020
20. https://uzcert.uz/blog/saidakbar/kiberbezopasnost-uzbekistana-v-tsifrakh-itogi-2018-goda/
21. O'zbekiston Respublikasi Prezidentining 2022-yilning 28-yanvardagi "2022 — 2026-yillarga mo'ljallangan yangi O'zbekistonning taraqqiyot strategiyasi to'g'risida"gi 60-sonli farmoni

22. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi “Raqamli O‘zbekiston — 2030” Strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi 6079-son Farmoni, https://lex.uz/ru/docs/-5030957#-5031756
23. Ro'ziev R.N., Salaev N.S. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya. – Toshkent: TDYUU, 2018, 6-bet.
24. Istam ASTANOV, Bakhtiyor KHAMIDOV – “Elektron yohud raqamli dalillarga oid umumnazariy masalalar: muammo va yechim” - Jamiyat va innovatsiyalar - Journal home page: https://inscience.uz/index.php/socinov/index