“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=367

2026-yil
5-son
may
ISSN 3093-8546



# Kiberhuquq sohasida tezkor-qidiruv tadbirlarini huquqiy tartibga solishning xorij tajribasi

*Farxod Bobomurodov,*
*Toshkent xalqaro universiteti Yurisprudensiya fakulteti Huquqiy fanlar kafedrasi*
*dotsent v.b., y.f.d.(DSc)*
*e-mail: farxodbobomurodov663@gmail.com*

***Аннотация.*** Mazkur ilmiy maqolada kiberhuquq sohasida tezkor-qidiruv tadbirlarini huquqiy tartibga solishning xorijiy davlatlar tajribasi tahlil qilingan. Xususan, AQSH, Rossiya, Yevropa ittifoqi davlatlari hamda Janubiy Koreya misolida kiberjinoyatlarga qarshi kurashishda qoʻllanadigan tezkor-qidiruv choralari, elektron dalillar bilan ishlash, telekommunikatsiya tarmoqlari orqali uzatiladigan axborotlarni nazorat qilish, raqamli kuzatuv hamda shaxsiy ma'lumotlarni himoya qilish mexanizmlari yoritilgan. Shuningdek, xalqaro huquqiy hujjatlar, xususan, Budapesht konvensiyasi normalari asosida milliy qonunchilikni takomillashtirish masalalari tahlil qilingan. Maqolada Oʻzbekistonda kiberhuquq sohasida tezkor-qidiruv faoliyatini takomillashtirish boʻyicha taklif va tavsiyalar ishlab chiqilgan.

***Калит сўзлар.*** kiberhuquq, tezkor-qidiruv faoliyati, kiberjinoyat, elektron dalil, raqamli kriminalistika, telekommunikasiya nazorati, xalqaro tajriba, kiberxavfsizlik, shaxsiy ma'lumotlar, Budapesht konvensiyasi

***Аннотация.*** В данной научной статье анализируется зарубежный опыт правового регулирования оперативно-розыскных мероприятий в сфере киберправа. В частности, рассматриваются механизмы борьбы с киберпреступностью в США, Российской Федерации, странах Европейского Союза и Южной Корее, включая вопросы работы с электронными доказательствами, контроля информатсии, передаваемой через телекоммуникатсионные сети, цифрового наблюдения и защиты персональных данных. Также исследуются международно-правовые основы, включая положения Будапештская конвенция, и возможности совершенствования натсионального законодательства на их основе. В статье разработаны предложения и рекомендатсии по совершенствованию оперативно-розыскной деятельности в сфере киберправа Узбекистан.

***Ключевые слова.*** киберправо, оперативно-розыскная деятельность, киберпреступность, электронные доказательства, цифровая криминалистика, телекоммуникационный контроль, международный опыт, кибербезопасность, персональные данные, Будапештская

конвенция

***Annotation.*** This scientific article analyzes foreign experience in the legal regulation of operational-search measures in the field of cyber law. In particular, the article examines the mechanisms used in the United States, the Russian Federation, European Union countries, and South Korea to combat cybercrime, including the handling of electronic evidence, monitoring of information transmitted through telecommunication networks, digital surveillance, and personal data protection. The study also explores international legal instruments, especially the provisions of the Budapest Convention on Cybercrime, and evaluates opportunities for improving national legislation based on international standards. Furthermore, the article provides proposals and recommendations for improving operational-search activities in the cyber law sphere of the Republic of Uzbekistan.

***Keywords.*** cyber law, operational-search activity, cybercrime, electronic evidence, digital forensics, telecommunication monitoring, international experience, cybersecurity, personal data, Budapest Convention

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida jamiyat hayotining deyarli barcha sohalari raqamlashtirilmoqda. Bu esa kibermakonda sodir etilayotgan jinoyatlar sonining ortishiga, ularning transmilliy xususiyat kasb etishiga va yangi turdagi huquqbuzarliklarning paydo boʻlishiga olib kelmoqda. Kiberjinoyatchilikning yuqori darajada yashirinligi, masofaviy sodir etilishi va elektron dalillar bilan bogʻliqligi huquqni muhofaza qiluvchi organlar oldiga yangi vazifalarni qoʻymoqda.

Bugungi kunda kiberjinoyatlarni aniqlash va fosh etishda tezkor-qidiruv tadbirlari muhim ahamiyat kasb etmoqda. Xususan, telekommunikatsiya tarmoqlari orqali uzatiladigan axborotlarni olish, elektron ma'lumotlarni monitoring qilish, internet tarmogʻida yashirin kuzatuv olib borish, raqamli dalillarni yigʻish va tahlil qilish kabi chora-tadbirlar kiberjinoyatchilikka qarshi kurashishning samarali vositalari hisoblanadi.

Shu munosabat bilan xorijiy davlatlarning kiberhuquq sohasida tezkor-qidiruv tadbirlarini huquqiy tartibga solish boʻyicha tajribasini oʻrganish muhim ilmiy va amaliy ahamiyatga ega.

Kiberhuquq sohasida tezkor-qidiruv tadbirlari bu maxsus vakolatli davlat organlari tomonidan kibermakonda sodir etilgan jinoyatlar va boshqa huquqbuzarliklarni aniqlash, oldini olish, ularni sodir etgan shaxslarni topish, elektron dalillarni yigʻish hamda axborot xavfsizligini ta'minlash maqsadida amalga oshiriladigan huquqiy, tashkiliy va texnik chora-tadbirlar tizimidir.

Mazkur faoliyat an'anaviy tezkor-qidiruv tadbirlaridan farqli raqamli muhitda amalga oshirilishi bilan ajralib turadi. Chunki kiberjinoyatlar virtual makonda, masofadan turib, anonim usullarda va koʻp hollarda transchegaraviy xususiyatda sodir etiladi. Bu esa tezkor-qidiruv faoliyatiga zamonaviy axborot texnologiyalari,

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

raqamli kriminalistika va sun'iy intellekt imkoniyatlarini joriy qilishni talab etadi.

Kiberhuquq sohasidagi tezkor-qidiruv tadbirlarining muhim xususiyatlaridan biri elektron ma'lumotlar bilan ishlash hisoblanadi. Bunda huquqni muhofaza qiluvchi organlar serverlar, kompyuter tizimlari, mobil qurilmalar, bulutli texnologiyalar, ijtimoiy tarmoqlar va telekommunikatsiya tarmoqlarida mavjud raqamli ma'lumotlarni tahlil qiladi. Ayniqsa, elektron ma'lumotlarni tezkor tarzda saqlab qolish va ularning yoʻq qilinishiga yoʻl qoʻymaslik kiberjinoyatlarni tergov qilishda muhim ahamiyat kasb etadi.

Kibermakonda raqamli izlarni aniqlash ham tezkor-qidiruv tadbirlarining muhim elementlaridan biri hisoblanadi. Chunki har qanday kiberjinoyat ma'lum darajada elektron iz qoldiradi. Masalan, log fayllar, IP-manzillar, brauzer tarixi, metama'lumotlar, elektron pochta yozishmalari, blokcheyn tranzaksiyalari yoki server faoliyati haqidagi ma'lumotlar kiberjinoyatni fosh etishda muhim elektron dalil vazifasini bajaradi.

Kiberhuquq sohasida tezkor-qidiruv tadbirlarining yana bir muhim yoʻnalishi elektron dalillarni yigʻish, saqlash va protsessual jihatdan mustahkamlash hisoblanadi. Chunki elektron dalillar oʻzining oʻzgaruvchanligi va oson yoʻq qilinishi mumkinligi bilan an'anaviy dalillardan farq qiladi. Shu sababli elektron dalillarni yigʻishda raqamli kriminalistika qoidalariga qat'iy rioya qilinishi talab etiladi.

*AQSH*da kiberjinoyatchilikka qarshi kurashish sohasidagi asosiy normativ-huquqiy hujjatlardan biri Computer Fraud and Abuse Act hisoblanadi. Ushbu qonun 1986-yilda qabul qilingan boʻlib, kompyuter tizimlariga ruxsatsiz kirish, elektron ma'lumotlarni yoʻq qilish yoki oʻzgartirish, zararli dasturiy vositalar tarqatish, raqamli firibgarlik, axborot oʻgʻirlash va tarmoq infratuzilmasiga noqonuniy ta'sir koʻrsatish bilan bogʻliq harakatlarni jinoiy qilmish sifatida belgilaydi. Mazkur qonunning muhim jihatlaridan biri shundaki, u kiberjinoyatlarni nafaqat milliy, balki transmilliy tahdid sifatida baholaydi[1]. Shu sababli AQSH huquqni muhofaza qiluvchi organlariga kibermakonda sodir etiladigan jinoyatlarni aniqlash, oldini olish va fosh etish boʻyicha keng tezkor-qidiruv vakolatlari berilgan.

AQSHda kiberjinoyatchilikka qarshi kurashish bilan asosan Federal Bureau of Investigation, National Security Agency, Department of Homeland Security hamda Cybersecurity and Infrastructure Security Agency kabi maxsus vakolatli organlar shugʻullanadi[4]. Mazkur organlar tomonidan kiberjinoyatlarni aniqlash va fosh etishda quyidagi tezkor-qidiruv tadbirlari keng qoʻllaniladi: a) raqamli monitoring; b) internet-trafik tahlili; s) elektron kuzatuv; d) tarmoq faoliyatini tahlil qilish; e) IP-manzillarni identifikatsiya qilish; yo) darknet platformalarini monitoring qilish; j) zararli dasturlarni tahlil qilish; z) elektron dalillarni yigʻish va raqamli kriminalistika usullaridan foydalanish.

Ayniqsa, kiberhujumlar va davlat xavfsizligiga tahdid soluvchi raqamli faoliyatlarni barvaqt aniqlash maqsadida sun'iy intellekt, mashinali o‘qitish va Big Data texnologiyalaridan foydalanish amaliyoti keng tarqalgan.

AQSH qonunchiligida elektron kuzatuv va raqamli tezkor-qidiruv tadbirlarini amalga oshirishda inson huquqlari va fuqarolarning konstitutsiyaviy erkinliklarini ta'minlashga ham alohida e'tibor qaratilgan[5]. Xususan, Fourth Amendment to the United States Constitutionga muvofiq, fuqarolarning xususiy hayoti, shaxsiy ma'lumotlari va elektron muloqoti noqonuniy tintuv hamda kuzatuvdan himoya qilinadi.

Shu munosabat bilan elektron ma'lumotlarni olish, internet yozishmalarini kuzatish, elektron pochta, messenjerlar yoki bulutli platformalarda saqlanayotgan ma'lumotlarga kirish kabi harakatlar asosan sud sanksiyasi orqali amalga oshiriladi. Bunda huquqni muhofaza qiluvchi organlar sudga kiberjinoyat sodir etilganligi haqida yetarli asos va dalillar taqdim etishi lozim.

Elektron dalillarni yig‘ish va saqlash jarayoni ham AQSHda qat'iy protsessual tartib asosida amalga oshiriladi. Xususan, elektron dalillarning haqiqiyligi, yaxlitligi va o‘zgarmaganligini ta'minlash maqsadida raqamli kriminalistika qoidalari qo‘llanadi. Bu esa elektron dalillarni keyinchalik sud jarayonida maqbul va ishonchli dalil sifatida tan olinishi uchun muhim ahamiyat kasb etadi.

Shu bilan birga, USA PATRIOT Act qabul qilinganidan keyin terrorizm va kibertahdidlarga qarshi kurashish maqsadida davlat organlarining elektron kuzatuv bo‘yicha vakolatlari kengaytirilgan. Mazkur qonun doirasida internet va telekommunikatsiya tarmoqlari orqali uzatiladigan ma'lumotlarni tezkor olish, raqamli faoliyatni monitoring qilish va xalqaro axborot almashinuvini amalga oshirish imkoniyatlari kuchaytirilgan[6].

Biroq mazkur vakolatlarning kengayishi inson huquqlari va shaxsiy hayot daxlsizligiga ta'sir ko‘rsatishi mumkinligi sababli AQSHda sud nazorati, prokuror tekshiruvi va konstitutsiyaviy kafolatlar tizimi saqlab qolingan. Bu esa kiberxavfsizlikni ta'minlash bilan inson huquqlarini muhofaza qilish o‘rtasidagi huquqiy muvozanatni ta'minlashga xizmat qiladi.

Rossiyada tezkor-qidiruv faoliyatini amlaga oshirish “Tezkor-qidiruv faoliyati to‘g‘risida”gi federal qonun asosida huquqiy tartibga solinadi. Mazkur qonun kiberjinoyatchilikka qarshi kurashish, davlat axborot xavfsizligini ta'minlash hamda telekommunikatsiya tarmoqlarida sodir etiladigan huquqbuzarliklarni aniqlash sohasida ham muhim huquqiy asos hisoblanadi.

Qonunda 15 turdagi tezkor-qidiruv tadbiri nazarda tutilgan bo‘lib, ularning bir qismi bevosita kibermakonda amalga oshiriladigan jinoyatlarni aniqlash va fosh etishga qaratilgan. Ayniqsa, raqamli texnologiyalar va internet infratuzilmasining keng rivojlanishi munosabati bilan Rossiya amaliyotida elektron kuzatuv va raqamli monitoring mexanizmlari keng qo‘llanilmoqda. Mazkur

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

qonun tuzilishi koʻra, 6 bob va 23 moddadan iborat. Qonunda: “umumiy qoidalar sifatida TQFning tushunchasi, vazifalari (4 ta), asosiy prinsiplari (4 ta), huquqiy asoslari, TQFni amalga oshirishda inson va fuqarolarning huquqlari va erkinliklariga rioya qilish; TQTlari turi (15 ta); oʻtkazish asoslari (9 ta), shartlari; federal xavfsizligi xizmati tomonidan alohida obyektlar va shaxslarga nisbatan TQTlarini oʻtkazishning oʻziga xos xususiyati; fuqarolarning konstitutsiyaviy huquqini cheklash bilan bogʻliq TQTlari materiallarining sud tomonidan koʻrib chiqish asoslari va tartibi; TQFni hujjatlashtirish va axborot bilan ta'minlanishi; TQF natijalaridan foydalanish; TQFni amalga oshiruvchi organlarning ma'lumotlarini muhofazalash; TQFni amalga oshirilishi toʻgʻrisida ma'lumotlarni oshkor qilinishiga yoʻl qoʻyilmasligi; TQFni amalga oshiruvchi organlar tasnifi (9 ta); organlarning majburiyatlari va huquqlari; TQFni amalga oshiruvchi organlar mansabor shaxsining ijtimoiy-huquqiy himoyasi; TQFni amalga oshruvchi organlarga fuqarolarning koʻmaklashishi va ularning ijtimoiy-huquqiy himoyasi; TQFning moliyaviy ta'minlanishi; TQFni umumiy hamda prokuror tomonidan nazorat qilinishi; idoraviy nazorat va ushbu federal qonunning kuchga kirishi”[7] kabilar nazarda tutilgan. Mazkur qonunga binoan TQFda inson huquqlarini ta'minlashda prokurordan tashqari sud organi ham vakolatli ekanligini koʻrishimiz mumkin.

Yevropa ittifoqi davlatlari misolida kiberjinoyatlarga qarshi kurashish qat'iy qonuniylik, sud nazorati, proporsionallik va shaxsiy ma'lumotlarni himoya qilish tamoyillariga asoslanadi.

Yevropa ittifoqi davlatlarida kiberjinoyatlarni fosh etishda yashirin kuzatuv, onlayn muhitda shaxsni identifikatsiya qilish, server va IP-manzillar harakatini tahlil qilish, zararli dastur infratuzilmasini aniqlash, kriptoaktivlar harakatini kuzatish, telekommunikatsiya ma'lumotlarini olish kabi choralar qoʻllaniladi. Bu jarayonda Europol tarkibidagi European Cybercrime Centre EC3 a'zo davlatlarga tahliliy, texnik va operativ yordam koʻrsatadi[2].

Yevropa ittifoqida elektron dalillar deganda elektron pochta, IP-loglar, akkaunt ma'lumotlari, bulutda saqlangan fayllar, messenjer ma'lumotlari, domen va server ma'lumotlari tushuniladi. 2023-yilda qabul qilingan Regulation (EU) 2023/1543 Yevropa ishlab chiqarish buyrugʻi va saqlab turish buyrugʻi orqali bir davlat organiga boshqa YI davlatidagi xizmat provayderidan elektron dalil talab qilish imkonini beradi. U 2026-yil 18-avgustdan toʻliq qoʻllanadi.

Telefon, internet va boshqa aloqa tarmoqlari orqali uzatiladigan ma'lumotlarni kuzatish faqat qonun asosida, odatda sud yoki mustaqil vakolatli organ ruxsati bilan amalga oshiriladi[3]. Yevropa sudi amaliyotiga koʻra, barcha fuqarolarning trafik va joylashuv ma'lumotlarini ommaviy saqlash umumiy qoida sifatida cheklangan; faqat milliy xavfsizlik, ogʻir jinoyatlar yoki terrorizm kabi holatlarda qat'iy shartlar bilan ruxsat etilishi mumkin.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Raqamli kuzatuvda ochiq internet manbalarini tahlil qilish, ijtimoiy tarmoqlarda jinoiy faollik belgilarini aniqlash, botnet va fishing infratuzilmasini kuzatish, zararli domenlarni bloklash, serverlarni musodara qilish yoki oʻchirish kabi amaliy choralar mavjud[8, 9]. Bunday harakatlar Europol, Eurojust va milliy politsiya organlari oʻrtasida muvofiqlashtiriladi. Masalan, Eurojust transchegaraviy tergovlarda dalil toʻplash va prokurorlar hamkorligini ta'minlaydi.

Janubiy Koreya kiberjinoyatlarga qarshi kurashish sohasida nafaqat Osiyoda, balki dunyo miqyosida ham ilgʻor davlatlardan biri hisoblanadi. Mamlakatda raqamli iqtisodiyot, elektron hukumat, sun'iy intellekt va yuqori tezlikdagi internet infratuzilmasi keng rivojlangani sababli kiberxavfsizlik milliy xavfsizlikning ustuvor yoʻnalishlaridan biri sifatida qaraladi[10]. Shu bois, davlat tomonidan kiberjinoyatchilikka qarshi kompleks va integratsiyalashgan tizim shakllantirilgan.

Janubiy Koreya kiberjinoyatlarga qarshi kurashish sohasida dunyodagi eng rivojlangan va yuqori texnologiyalarga asoslangan davlatlardan biri hisoblanadi. Mamlakatda kiberxavfsizlik tizimi markazlashgan boshqaruv, tezkor raqamli monitoring, sun'iy intellekt texnologiyalari va davlat hamda xususiy sektorning oʻzaro integratsiyalashgan hamkorligi asosida tashkil etilgan. Internet tezligi, raqamli xizmatlar va axborot texnologiyalarining keng rivojlangani sababli bank tizimi, elektron toʻlovlar, elektron hukumat platformalari, bulutli texnologiyalar, IoT qurilmalari va 5G tarmoqlari kiberjinoyatchilar uchun asosiy nishonlardan biri hisoblanadi. Shu sababli davlat kiberjinoyatlarning oldini olish, ularni tezkor aniqlash va bartaraf etish boʻyicha kuchli mexanizmlarni shakllantirgan.

Mamlakatda kiberjinoyatlarga qarshi kurashishda asosiy vakolatli organ sifatida Korea National Police Agency (KNPA) faoliyat yuritadi. Uning tarkibida Cyber Bureau, Digital Forensics Center, Cyber Investigation Division va Cyber Terror Response Center kabi maxsus boʻlinmalar tashkil etilgan boʻlib, ular xakerlik, fishing, ransomware, onlayn firibgarlik, kriptovalyuta bilan bogʻliq jinoyatlar, darknet faoliyati va shaxsiy ma'lumotlarni oʻgʻirlash bilan bogʻliq jinoyatlarni aniqlash va tergov qilish bilan shugʻullanadi[11]. Bundan tashqari, Supreme Prosecutorsʻ Office huzurida raqamli dalillar va kiberjinoyatlar boʻyicha maxsus prokurorlar faoliyat olib boradi. Ular elektron dalillarni huquqiy baholash, xalqaro huquqiy yordam koʻrsatish, serverlardan ma'lumot olish, kriptoaktivlar harakatini tahlil qilish hamda raqamli moliyaviy jinoyatlarni tergov qilish vazifalarini amalga oshiradi.

Janubiy Koreya Milliy razvedka xizmati (National Intelligence Service) davlat axborot tizimlarini tashqi kibertahdidlardan muhofaza qilish bilan shugʻullanadi. Ayniqsa, Shimoliy Koreya bilan bogʻliq xakerlik guruhlari, davlatga qarshi kibershpionaj, kiberterrorizm va strategik axborot obyektlariga qarshi uyushtiriladigan kiberhujumlar doimiy monitoring ostida boʻladi.

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

Janubiy Koreya kiberxavfsizlik tizimining eng muhim xususiyatlaridan biri turli davlat organlari oʻrtasidagi integratsiyalashgan raqamli hamkorlik modelidir. Bu tizim orqali politsiya, prokuratura, razvedka organlari, telekommunikatsiya operatorlari, banklar, internet-provayderlar va milliy CERT markazlari oʻzaro tezkor ma'lumot almashadi. Natijada kiberhujumlarni erta aniqlash, zararli trafikni bloklash, IP manzillarni kuzatish, elektron tranzaksiyalarni tahlil qilish va zararni lokalizatsiya qilish imkoniyatlari yaratiladi.

Mamlakatda raqamli kriminalistika ham juda yuqori darajada rivojlangan. Tergov jarayonida kompyuterlar, smartfonlar, serverlar, bulutli ma'lumotlar, CCTV tizimlari, IoT qurilmalari va blokcheyn tranzaksiyalari maxsus laboratoriyalarda tahlil qilinadi. Elektron dalillar bilan ishlashda chain of custody, hash verification, metadata analysis, live forensics va mobile forensics kabi xalqaro standartlar qoʻllaniladi. Sud jarayonida esa elektron dalillarning haqiqiyligi, oʻzgarmaganligi va ishonchliligi alohida tekshiriladi.

Janubiy Koreyada telekommunikatsiya tarmoqlarini nazorat qilish faqat qonunchilik asosida va sud sanksiyasi bilan amalga oshiriladi. Muayyan holatlarda internet trafigi, elektron xabarlar, VoIP aloqalar, ijtimoiy tarmoqlar faoliyati va mobil qurilmalar ma'lumotlari kuzatilishi mumkin. Bu jarayon sud nazorati, prokuror ruxsati, inson huquqlarini himoya qilish va shaxsiy hayot daxlsizligi tamoyillari asosida amalga oshiriladi.

Mamlakat kiberxavfsizlik sohasida sun'iy intellekt texnologiyalarini ham faol qoʻllamoqda. AI texnologiyalari anomal trafikni aniqlash, DDoS hujumlarini prognoz qilish, phishing URL tahlili, malware behavior analysis, facial recognition va darknet monitoring kabi yoʻnalishlarda qoʻllanadi[12]. Sun'iy intellekt tizimlari katta hajmdagi ma'lumotlarni real vaqt rejimida tahlil qilib, xavfli faollikni avtomatik tarzda belgilaydi va tezkor chora koʻrish imkonini beradi.

Janubiy Koreyada shaxsiy ma'lumotlarni himoya qilish masalasiga ham katta e'tibor qaratilgan. Bu sohadagi asosiy normativ-huquqiy hujjatlardan biri Personal Information Protection Act hisoblanadi. Ushbu qonun fuqarolarning shaxsiy ma'lumotlarini himoya qilish, ma'lumotlarni qayta ishlash tartibi, kompaniyalar javobgarligi, ma'lumotlar sizib chiqishi uchun javobgarlik va davlat nazorati masalalarini tartibga soladi.

Shuningdek, Janubiy Koreya xalqaro darajada ham kiberjinoyatlarga qarshi faol hamkorlikni amalga oshiradi. Mamlakat INTERPOL, ASEANAPOL va United Nations doirasida kiberjinoyatlarga qarshi qoʻshma operatsiyalarda ishtirok etadi. Bunda elektron dalillar almashinuvi, transmilliy tergovlar, ekstraditsiya, CERT markazlari oʻrtasidagi hamkorlik va xalqaro tezkor tadbirlar muhim ahamiyat kasb etadi.

**Kiberhuquq sohasida tezkor-qidiruv tadbirlarini huquqiy tartibga solish masalasida bir qancha muammolar mavjud, bular quyidagilardan iborat:**

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

**birinchidan,** bugungi kunda kiberjinoyatlar davlat chegarasi bilan cheklanmaydi. Jinoyatchi bir davlatda, server ikkinchi davlatda, jabrlanuvchi esa uchinchi davlatda boʻlishi mumkin. Bu holat tezkor-qidiruv tadbirlarini amalga oshirishda yurisdiksiya bilan bogʻliq murakkabliklarni keltirib chiqaradi. Ayniqsa, elektron dalillarni xorijiy serverlardan olishda protsessual toʻsiqlar yuzaga keladi. Koʻplab davlatlarda elektron dalillarni yigʻish, saqlash, tekshirish va sudga taqdim etishning yagona mexanizmi mavjud emas. Natijada raqamli dalillarning haqiqiyligi va maqbulligi yuzasidan turli bahslar kelib chiqmoqda. Tezkor-qidiruv tadbirlari doirasida telefon suhbatlari, internet trafiklari va elektron yozishmalar nazorat qilinishi fuqarolarning shaxsiy hayot daxlsizligiga ta'sir koʻrsatishi mumkin. Ayrim hollarda ommaviy raqamli kuzatuv ortiqcha ma'lumot yigʻishga sabab boʻlmoqda. Kriptovalyutalar anonimlik xususiyatiga ega boʻlgani sababli moliyaviy firibgarlik, ransomware va darknet operatsiyalarini aniqlash qiyinlashmoqda. Tezkor xizmatlar kripto-aktivlarni kuzatishda texnik imkoniyatlar yetishmasligiga duch kelmoqda;

**ikkinchidan,** Deepfake texnologiyalari, avtomatlashtirilgan phishing hujumlari va AI yordamida yaratilgan zararli dasturlar yangi xavflarni keltirib chiqarmoqda. Amaldagi qonunchilik esa mazkur jinoyatlarni kvalifikatsiya qilishga toʻliq mos emas. Kiberjinoyatlarni fosh etishda internet-provayderlar muhim axborot manbai hisoblanadi. Biroq axborot almashish jarayonida byurokratik kechikishlar mavjudligi tezkorlikni pasaytirmoqda. Face recognition, big data monitoring va geolokatsiya kuzatuvi texnologiyalari inson huquqlari bilan bogʻliq jiddiy bahslarni keltirib chiqarmoqda. Ayrim davlatlarda ushbu texnologiyalarning huquqiy asoslari yetarli darajada belgilanmagan. Elektron ma'lumotlarni saqlash muddatini qisqaligi ham bir muammo. Koʻplab provayderlar log-fayllar va texnik ma'lumotlarni qisqa muddat saqlaydi. Bu esa kiberjinoyat sodir etilganidan keyin elektron izlarni tiklash imkoniyatini cheklaydi. Kiberjinoyatlarni tergov qilishda malakali kadrlar yetishmasligi, ya'ni, tezkor xodimlar, tergovchilarning barchasi ham raqamli kriminalistika, blockchain tahlili yoki malware analysis sohasida yetarli bilimga ega emas.

**uchinchidan,** Darknet orqali sodir etiladigan jinoyatlarni aniqlash qiyinligi, anonim tarmoqlar orqali narkotik moddalar, qurol savdosi, shaxsiy ma'lumotlarni sotish kabi kiberjinoyatlar amalga oshirilmoqda. Bu tarmoqlarda jinoyatchilarni identifikatsiya qilish murakkab hisoblanadi. Kritik infratuzilmalarga qarshi kiberhujumlarni ortishi energetika, bank, transport va davlat axborot tizimlariga qarshi kiberhujumlar milliy xavfsizlikka jiddiy tahdid tugʻdirmoqda. Ayrim davlatlarda bunday obyektlarni himoya qilish mexanizmi yetarli darajada shakllanmagan;

**toʻrtinchidan,** elektron tintuv, raqamli olib qoʻyish jarayonlarida huquqiy boʻshliqlar mavjudligi. Bundan cloud storage, virtual serverlar va masofaviy ma'lumot omborlaridan elektron ma'lumotlarni olish tartibi ayrim mamlakatlarda aniq tartibga

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

solinmagan. Kiberjinoyatlar boʻyicha xalqaro soʻrovlar yuborish va elektron dalillarni olish jarayonlari uzoq vaqt talab qiladi. Bu vaqt ichida elektron ma'lumotlar oʻchirilishi yoki oʻzgartirilishi mumkin. Bolalarga qarshi onlayn jinoyatlarni aniqlash mexanizmlarining yetarli emas. Internet orqali grooming, cyberbullying va child exploitation holatlari ortib bormoqda. Mazkur jinoyatlarni erta aniqlash mexanizmlari barcha davlatlarda ham yetarli emas. Kiberxavfsizlik sohasida qonunchilikning texnologiyalardan ortda qolayotganligi. Texnologiyalar tez rivojlanayotgani sabab an'anaviy qonunchilik ularga moslashishga ulgurmayapti. Natijada yangi turdagi kiberjinoyatlar huquqiy jihatdan toʻliq qamrab olinmay qolmoqda.

Transmilliy kiberjinoyatlar zamonaviy axborot texnologiyalari rivojlanishi natijasida chegara bilmas jinoyat turiga aylanib bormoqda. Bunday jinoyatlar bir davlat hududida sodir etilmasdan, bir vaqtning oʻzida bir nechta davlat axborot tizimlari, serverlari va fuqarolariga ta'sir koʻrsatishi mumkin. Shu sababli kiberjinoyatlarga qarshi kurashishda yagona xalqaro mexanizmlarni shakllantirish dolzarb ahamiyat kasb etmoqda.

**Kiberhuquq sohasida tezkor-qidiruv tadbirlarini huquqiy tartibga solish yuzasidan yuqorida sanab oʻtilgan muammolarni hal etish yuzasidan quyidagilar taklif etiladi:**

**birinchidan, Transmilliy kiberjinoyatlarga qarshi xalqaro mexanizm yaratish:**

1) kiberjinoyatlar boʻyicha davlatlararo tezkor axborot almashish platformasini yaratish zarur. Amaliyotda koʻplab kiberjinoyatlar boʻyicha ma'lumotlar turli davlatlarda joylashgan serverlar, bulutli platformalar va telekommunikatsiya tarmoqlarida saqlanadi. Agar davlatlar oʻrtasida tezkor raqamli ma'lumot almashish mexanizmi mavjud boʻlmasa, elektron dalillar yoʻqolishi, oʻzgarishi yoki oʻchirilishi mumkin. Shu sababli maxsus xalqaro kiberxavfsizlik platformasini yaratish orqali kiberhujumlar haqida real vaqt rejimida xabar berish; IP-manzillar va zararli domenlar haqida ma'lumot almashish; malware va ransomware namunalarini tarqatish; kiberterrorizm va darknet faoliyati haqida ma'lumot berish; elektron dalillarni muhofazalash imkoniyatlari yaratiladi. Bunday tizim INTERPOL, Europol, ASEANAPOL, CERT tashkilotlari va milliy huquqni muhofaza qiluvchi organlar oʻrtasida integratsiyalashgan holda faoliyat yuritishi mumkin; 2) 24/7 cyber contact point tizimini milliy darajada joriy qilish maqsadga muvofiq hisoblanadi. Bu mexanizm Budapest Convention on Cybercrime doirasida ham muhim institut sifatida belgilangan. Unga koʻra, har bir davlatda sutka davomida ishlovchi maxsus vakolatli markaz mavjud boʻlishi lozim. Ushbu markazlar orqali: kiberjinoyatlar yuzasidan tezkor murojaat qabul qilish; server yoki akkaunt ma'lumotlarini saqlab qolish; elektron dalillarni vaqtincha muzlatib qoʻyish; xalqaro soʻrovlarni zudlik bilan yuborish; raqamli tahdidlar haqida ogohlantirish amalga oshiriladi. Bu esa elektron dalillarning yoʻqolib ketishining oldini oladi va transmilliy tergov

samaradorligini oshiradi; 3) elektron dalillarni tezkor olish bo‘yicha soddalashtirilgan xalqaro protsessual tartib ishlab chiqish zarur. Hozirgi kunda ko‘p davlatlarda elektron ma'lumotlarni olish uchun uzoq davom etadigan xalqaro huquqiy yordam protseduralari qo‘llaniladi. Bu jarayon ba'zan oylab vaqt talab qiladi. Ammo kiberjinoyatlarda vaqt asosiy omil hisoblanadi, chunki elektron ma'lumotlar tez o‘chirilishi yoki o‘zgartirilishi mumkin. Shu sababli e-evidence request tizimini joriy qilish; elektron order mexanizmlarini ishlab chiqish; bulutli ma'lumotlarni tezkor taqdim etish; provayderlar bilan bevosita hamkorlik qilish; raqamli ma'lumotlarni saqlash majburiyatini belgilash kabi mexanizmlarni xalqaro darajada joriy qilish zarur. Yevropa ittifoqida e-Evidence Package konsepsiyasi aynan shu maqsadga xizmat qiladi; 4)“kiberyurisdiksiya” tushunchasini milliy qonunchilikka kiritish muhim ahamiyatga ega. An'anaviy jinoyatlarda hududiy yurisdiksiya aniq belgilangan bo‘lsa, kiberjinoyatlarda jinoyatchi bir davlatda, server ikkinchi davlatda, jabrlanuvchi esa uchinchi davlatda bo‘lishi mumkin. Shu bois qaysi davlat tergov olib borishi; qaysi davlat qonunchiligi qo‘llanilishi; qaysi sud ishni ko‘rib chiqishi; elektron dalillar qayerda baholanishi kabi muammolar yuzaga keladi. Kiberyurisdiksiya institutini qonunchilikka kiritish orqali davlatning kibermakondagi huquqiy vakolatlari, transchegaraviy jinoyatlarga nisbatan yurisdiksiya doirasi va raqamli muhitdagi huquqiy ta'sir choralari aniq belgilanadi; 5) Budapest Convention on Cybercrime qoidalarini milliy qonunchilikka implementatsiya qilish maqsadga muvofiq hisoblanadi. Ushbu konvensiya kiberjinoyatlarga qarshi kurashish sohasidagi eng muhim xalqaro hujjatlardan biri bo‘lib, unda kompyuter tizimlariga noqonuniy kirish; ma'lumotlarni noqonuniy o‘zgartirish; kiberfiribgarlik; bolalar pornografiyasi; elektron dalillarni yig‘ish; tezkor saqlab qolish; transmilliy hamkorlik; 24/7 ish rejimida ishlash markazlari kabi mexanizmlar belgilangan. Konvensiya qoidalarini milliy qonunchilikka implementatsiya qilish orqali kiberjinoyatlar bo‘yicha jinoiy javobgarlikni xalqaro standartlarga moslashtirish, elektron dalillar bilan ishlash tartibini takomillashtirish va xalqaro hamkorlik samaradorligini oshirish mumkin bo‘ladi;

ikkinchidan, Elektron dalillar institutini takomillashtirish: 1) elektron dalillarni yig‘ishning yagona protsessual standartini ishlab chiqish zarur. Amaliyotda elektron dalillarni olish jarayoni turli davlatlarda va hatto bir davlat ichida ham turlicha amalga oshiriladi. Bu esa dalillarning haqiqiyligi va maqbulligiga shubha tug‘dirishi mumkin. Shu sababli kompyuter va mobil qurilmalarni ko‘zdan kechirish tartibi; server va bulutli ma'lumotlarni olish mexanizmi; elektron xat-xabarlarni rasmiylashtirish; raqamli ma'lumotlarni nusxalash qoidalari; onlayn dalillarni qayd etish usullari bo‘yicha yagona protsessual standartlarni belgilash lozim. Bunday standartlar elektron dalillarni yig‘ish jarayonida inson omili ta'sirini kamaytiradi, dalillarning ishonchliligini ta'minlaydi hamda sudda ularning maqbulligini oshiradi; 2) elektron dalillarni hash-kod orqali

identifikatsiya qilish mexanizmini joriy etish lozim. Raqamli ma'lumotlar oson o‘zgartirilishi yoki nusxalanishi mumkinligi sababli ularning haqiqiyligini ta'minlash muhim hisoblanadi. Shu maqsadda hash verification mexanizmi qo‘llaniladi. Unda har bir elektron faylga maxsus unikal hash-kod beriladi. Agar faylda hatto kichik o‘zgarish amalga oshirilsa ham hash-kod o‘zgarib ketadi. Bu mexanizm orqali dalilning o‘zgarmaganligi; nusxaning asl faylga mosligi; elektron ma'lumotning haqiqiyligi; tergov jarayonida dalilga aralashilmaganligi aniqlanadi. Masalan, SHA-256 yoki MD5 kabi kriptografik algoritmlar orqali fayllarni identifikatsiya qilish raqamli kriminalistikada keng qo‘llaniladi; 3) chain of custody tizimini amaliyotga tatbiq qilish kerak. Chain of custody elektron dalilning kim tomonidan, qachon, qayerdan va qanday tartibda olingani, saqlangani va tekshirilganini bosqichma-bosqich qayd etuvchi protsessual nazorat tizimidir. Amaliyotda mazkur tizim elektron dalillarning ishonchliligini ta'minlashda muhim ahamiyatga ega. Ushbu mexanizm orqali dalilni qabul qilgan shaxs dalil saqlangan joy; dalilga kirish huquqiga ega shaxslar; dalil bilan amalga oshirilgan harakatlar; dalilni sudga taqdim etish jarayoni to‘liq hujjatlashtiriladi. Bu esa elektron dalillarning yo‘qolishi, soxtalashtirilishi yoki o‘zgartirilishining oldini oladi hamda sudda dalilning haqiqiyligini isbotlashga yordam beradi; 4) raqamli dalillarni saqlash bo‘yicha maxsus kiberlaboratoriyalar tashkil etish maqsadga muvofiq hisoblanadi. Zamonaviy kiberjinoyatlar ko‘lamining kengayishi elektron dalillarni yuqori texnologiyalar asosida tahlil qilishni talab etmoqda. Shu sababli digital forensics laboratoriyalari; malware analysis markazlari; mobile forensics bo‘limlari; cloud forensics tizimlari; blockchain transaction analysis laboratoriyalari tashkil qilinishi zarur. Bunday kiberlaboratoriyalarda elektron dalillarni xavfsiz saqlash, tiklash, tahlil qilish va texnik ekspertiza o‘tkazish imkoniyati yaratiladi. Shu bilan birga, maxsus izolyatsiya qilingan serverlar, kriptografik himoya vositalari va raqamli arxiv tizimlari qo‘llanilishi lozim; 5) sudya va tergovchilar uchun raqamli dalillar bo‘yicha maxsus o‘quv kurslarini tashkil qilish zarur. Amaliyotda ko‘plab huquqni muhofaza qiluvchi organ xodimlari elektron dalillarni texnik jihatdan yetarlicha tushunmasligi sababli dalillarni yig‘ish yoki baholashda xatolarga yo‘l qo‘yishi mumkin. Shu sababli kiberhuquq; raqamli kriminalistika; elektron dalillar nazariyasi; hash verification; blockchain tracing; cloud evidence; AI-assisted investigation kabi yo‘nalishlarda maxsus malaka oshirish kurslarini tashkil etish maqsadga muvofiq. Bu sudyalar va tergovchilarning raqamli dalillarni baholash bo‘yicha bilim va ko‘nikmalarini oshiradi hamda kiberjinoyatlarni tergov qilish samaradorligini kuchaytiradi;

*uchinchidan, Inson huquqlari va raqamli nazorat o‘rtasida muvozanatni ta'minlash:* 1) telekommunikatsiya tarmoqlarini nazorat qilish faqat sud sanksiyasi asosida amalga oshirilishi lozim. Amaliyotda internet trafigi, telefon muloqotlari, elektron xabarlar, ijtimoiy tarmoqlardagi faoliyat va boshqa raqamli ma'lumotlar shaxsiy hayot bilan bevosita

bog‘liq hisoblanadi. Shu sababli ularni kuzatish yoki tahlil qilish davlat organlarining cheklanmagan vakolatiga aylanmasligi kerak. Sud sanksiyasi mexanizmi orqali fuqarolarning konstitutsiyaviy huquqlari himoya qilinadi; nazorat tadbirlarining qonuniyligi tekshiriladi; asossiz raqamli kuzatuvning oldi olinadi; vakolatlarni suiiste'mol qilish xavfi kamayadi; tergov harakatlari ustidan mustaqil nazorat ta'minlanadi. Bu tamoyil demokratik davlatlarda inson huquqlarini ta'minlashning muhim huquqiy kafolatlaridan biri hisoblanadi; 2) raqamli kuzatuvda proporsionallik prinsipini mustahkamlash zarur. Proporsionallik prinsipiga ko‘ra, davlat tomonidan qo‘llaniladigan nazorat choralari xavf darajasiga mutanosib bo‘lishi lozim. Ya'ni, yengil huquqbuzarliklar uchun keng qamrovli ommaviy kuzatuv amalga oshirilmasligi; kibertahdid darajasiga mos texnik vositalar qo‘llanilishi; shaxsiy hayotga ortiqcha aralashuvga yo‘l qo‘yilmasligi; kuzatuv muddati cheklangan bo‘lishi; faqat zarur ma'lumotlar yig‘ilishi talab etiladi. Bu prinsip raqamli nazorat va inson huquqlari o‘rtasida adolatli muvozanatni ta'minlashga xizmat qiladi; 3) ortiqcha shaxsiy ma'lumotlarni yig‘ishni cheklash maqsadga muvofiq hisoblanadi. Bugungi kunda ayrim tashkilotlar va davlat organlari fuqarolar haqida zarur bo‘lmagan katta hajmdagi ma'lumotlarni yig‘moqda. Bu esa shaxsiy ma'lumotlar sizib chiqishi; fuqarolarni noqonuniy kuzatish; profilling orqali nazorat qilish; axborot xavfsizligiga tahdid; shaxsiy hayot daxlsizligining buzilishi kabi salbiy oqibatlarga olib kelishi mumkin. Shu sababli “data minimization” tamoyilini joriy qilish muhim ahamiyatga ega. Unga ko‘ra, faqat muayyan maqsad uchun zarur bo‘lgan minimal ma'lumotlar yig‘ilishi va qayta ishlanishi lozim. Bundan tashqari, ma'lumotlarni saqlash muddatlarini cheklash va avtomatik o‘chirish mexanizmlarini joriy qilish ham muhim hisoblanadi; 4) mustaqil kiber-nazorat organini tashkil etish kerak. Raqamli kuzatuv va shaxsiy ma'lumotlar bilan ishlash sohasida davlat organlari faoliyati ustidan mustaqil nazoratning mavjudligi huquqiy davlatning muhim belgilaridan biri hisoblanadi; 5) fuqarolarning raqamli huquqlarini himoya qilish bo‘yicha ombudsman institutini rivojlantirish lozim. Zamonaviy jamiyatda raqamli huquqlar inson huquqlarining ajralmas qismiga aylanmoqda. Ularga shaxsiy ma'lumotlarni himoya qilish huquqi; internetda erkin foydalanish huquqi; raqamli xavfsizlik huquqi; onlayn shaxsiy hayot daxlsizligi; algoritmik qarorlardan himoyalanish huquqi kiradi. Shu sababli maxsus raqamli huquqlar ombudsmani institutini joriy qilish orqali fuqarolarning raqamli huquqlari buzilishi bo‘yicha shikoyatlarni ko‘rib chiqish; internet platformalari faoliyatini tahlil qilish; shaxsiy ma'lumotlar muhofazasi ustidan jamoatchilik nazoratini kuchaytirish; suvn'iy intellekt va avtomatlashtirilgan qarorlardan kelib chiqadigan xavflarni baholash; fuqarolarga huquqiy yordam berish imkoniyati yaratiladi. Bu institut raqamli muhitda inson huquqlarini ta'minlashning muhim kafolati sifatida xizmat qiladi;

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

to‘rtinchidan, Kriptovalyuta, sun'iy intellekt sohasini huquqiy tartibga solish, internet-provayderlar, raqamli kuzatuv texnologiyalar, elektron ma'lumotlarni saqlash tizimini hamda kiberkadrlar tayyorlash tizimini takomillashtirish:a) kriptovalyutalar va virtual aktivlar raqamli iqtisodiyotning yangi segmenti sifatida tez sur'atlarda rivojlanmoqda. Biroq ularning anonim xususiyati ayrim hollarda kiberfiribgarlik, ransomware hujumlari, pul yuvish, terrorizmni moliyalashtirish va transmilliy moliyaviy jinoyatlarda qo‘llanilishiga sabab bo‘lmoqda. Shu bois kriptovalyutalar sohasini huquqiy tartibga solish dolzarb vazifalardan biri hisoblanadi. Avvalo, kriptovalyuta birjalari va virtual asset service provider (VASP) subyektlarini litsenziyalash mexanizmini joriy qilish zarur. Bu orqali davlat virtual aktivlar aylanmasi ustidan huquqiy nazorat o‘rnatishi, moliyaviy shaffoflikni ta'minlashi va shubhali operatsiyalarni kuzatishi mumkin bo‘ladi. Litsenziyalash tizimi doirasida KYC (Know Your Customer) va AML (Anti-Money Laundering) talablarini joriy qilish kriptojinoyatlar xavfini kamaytiradi. Shu bilan birga, huquqni muhofaza qiluvchi organlar faoliyatiga blockchain analytics texnologiyalarini joriy qilish muhim ahamiyatga ega. Bunday texnologiyalar orqali kriptovalyuta tranzaksiyalarini kuzatish, raqamli aktivlar harakatini tahlil qilish, kriptohamyonlar o‘rtasidagi bog‘liqlikni aniqlash va noqonuniy mablag‘larning yo‘nalishini belgilash mumkin bo‘ladi. Masalan, Chainalysis, Elliptic va TRM Labs kabi texnologiyalar xalqaro amaliyotda keng qo‘llanilmoqda. Shuningdek, shubhali kriptotranzaksiyalar bo‘yicha avtomatik monitoring tizimini ishlab chiqish lozim. Bunda sun'iy intellekt va Big Data texnologiyalari orqali xavfli moliyaviy operatsiyalar avtomatik tarzda aniqlanadi. Bu tizim ransomware to‘lovlari, darknet operatsiyalari va terrorizmni moliyalashtirish bilan bog‘liq tranzaksiyalarni erta bosqichda aniqlash imkonini beradi. Bundan tashqari, kriptojinoyatlar bo‘yicha maxsus kiberbo‘linmalar tashkil etish maqsadga muvofiq hisoblanadi. Ushbu bo‘linmalar raqamli moliyaviy tahlil, kriptografik ekspertiza va blockchain forensics bo‘yicha yuqori malakali mutaxassislardan tashkil topishi lozim. Shu bilan birga, FATF (Financial Action Task Force), INTERPOL va Egmont Group kabi xalqaro moliyaviy monitoring tashkilotlari bilan hamkorlikni kuchaytirish transmilliy kriptojinoyatlarga qarshi kurashish samaradorligini oshiradi; 2) sun'iy intellekt texnologiyalari kiberxavfsizlik sohasida katta imkoniyatlar yaratayotgan bo‘lsa-da, ular orqali yangi turdagi kiberjinoyatlar ham sodir etilmoqda. AI orqali avtomatlashtirilgan hujumlar, deepfake texnologiyalari, algoritmik manipulyatsiyalar va avtonom malware tizimlari raqamli xavfsizlikka jiddiy tahdid tug‘dirmoqda. Shu sababli AI orqali sodir etilgan kiberjinoyatlar uchun alohida huquqiy javobgarlik belgilash lozim. Qonunchilikda AI yordamida tarqatilgan soxta audio va videolar, avtomatlashtirilgan kiberhujumlar yoki AI-assisted fraud holatlari uchun maxsus javobgarlik normalarini kiritish muhim ahamiyatga ega. Deepfake kontentlarni aniqlash texnologiyalarini joriy qilish ham dolzarb hisoblanadi. Chunki deepfake orqali

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

shaxsning ovozi yoki tasviri soxtalashtirilib, firibgarlik, shantaj yoki siyosiy manipulyatsiyalar amalga oshirilishi mumkin. Shu bois facial recognition, voice authentication va AI-generated content detection texnologiyalarini rivojlantirish zarur. Bundan tashqari, AI forensic laboratoriyalarini tashkil qilish maqsadga muvofiq. Bu laboratoriyalarda AI algoritmlari orqali sodir etilgan hujumlar tahlil qilinib, algoritmik qarorlarning manbalari va texnik xususiyatlari aniqlanadi. Shu bilan birga, davlat axborot tizimlariga AI monitoring platformalarini integratsiya qilish orqali kibertahdidlarni real vaqt rejimida aniqlash imkoniyati yaratiladi. AI texnologiyalaridan foydalanish etikasi va xavfsizligi boʻyicha milliy standartlar ishlab chiqish ham muhim ahamiyat kasb etadi. Bu standartlar inson huquqlari, shaxsiy ma'lumotlar muhofazasi, algoritmik shaffoflik va AI tizimlarining javobgarligi kabi masalalarni qamrab olishi lozim; 3) internet-provayderlar kiberxavfsizlik tizimining muhim ishtirokchilaridan biri hisoblanadi. Chunki kiberjinoyatlar bilan bogʻliq asosiy elektron izlar aynan telekommunikatsiya tarmoqlari orqali oʻtadi. Shu sababli internet-provayderlar uchun majburiy cyber compliance talablarini belgilash zarur. Ular kiberxavfsizlik standartlariga rioya qilishi, xavfli trafikni monitoring qilishi va insidentlar haqida davlat organlariga xabar berishi lozim. Real-time data preservation mexanizmini joriy qilish ham muhim ahamiyatga ega. Bu mexanizm orqali huquqni muhofaza qiluvchi organlar soʻroviga asosan elektron ma'lumotlar tezkor ravishda saqlab qolinadi va oʻchirilib ketishining oldi olinadi. Provayderlar va huquqni muhofaza qiluvchi organlar oʻrtasida yagona elektron platforma yaratish orqali elektron dalillar almashinuvini tezlashtirish mumkin boʻladi. Shuningdek, provayderlar uchun majburiy kiberxavfsizlik auditlarini joriy qilish va ma'lumotlarni saqlash muddatlarini uzaytirish kiberjinoyatlarni tergov qilish samaradorligini oshiradi; 4) raqamli kuzatuv texnologiyalari xavfsizlikni ta'minlashda muhim vosita boʻlsa-da, ular inson huquqlari va shaxsiy hayot daxlsizligiga ta'sir koʻrsatishi mumkin. Shu sababli face recognition texnologiyalaridan foydalanishning aniq huquqiy asoslarini belgilash lozim. Bunday tizimlar faqat qonunchilikda belgilangan holatlarda va sud nazorati asosida qoʻllanilishi kerak. Biometrik ma'lumotlarni saqlash muddatini cheklash ham muhim hisoblanadi. Chunki yuz tasviri, barmoq izi va ovoz ma'lumotlari fuqarolarning eng himoyalanishi lozim boʻlgan ma'lumotlaridandir. Shu bilan birga, raqamli kuzatuv boʻyicha parlament nazoratini kuchaytirish va shaffof hisobot tizimini joriy qilish orqali davlat organlari vakolatlari ustidan demokratik nazorat ta'minlanadi. Inson huquqlariga ta'sirni baholash mexanizmini joriy qilish esa raqamli kuzatuv tizimlarining huquqiy va ijtimoiy xavflarini oldindan aniqlash imkonini beradi; 5) kiberjinoyatlarni tergov qilishda elektron ma'lumotlarni saqlash muhim ahamiyatga ega. Shu sababli provayderlar uchun minimal data retention muddatini belgilash zarur. Elektron izlarni avtomatik arxivlash tizimini yaratish orqali log-fayllar, tarmoq faoliyati va raqamli izlar

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

xavfsiz saqlanadi. Shu bilan birga, raqamli ma'lumotlarni kriptografik himoya qilish mexanizmlarini joriy qilish orqali ularning o‘zgarmasligi va maxfiyligi ta'minlanadi. Davlat darajasida backup data-markazlar tashkil qilish ham raqamli barqarorlikni ta'minlaydi. Elektron ma'lumotlarni saqlash standartlarini ISO/IEC 27001 kabi xalqaro talablarga moslashtirish esa global axborot xavfsizligi standartlariga uyg‘unlikni ta'minlaydi; 6) zamonaviy kiberjinoyatlarga qarshi kurashish yuqori malakali kadrlarni talab qiladi. Shu sababli cyber forensics akademiyalarini tashkil qilish va raqamli kriminalistika bo‘yicha maxsus ta'lim tizimini rivojlantirish muhim ahamiyatga ega. Tergovchilar uchun blockchain, malware analysis, OSINT, cloud forensics va AI investigation bo‘yicha maxsus kurslar joriy qilinishi lozim. Bundan tashqari, CEH, CISSP, CHFI kabi xalqaro sertifikatlash dasturlarini amaliyotga tatbiq qilish mutaxassislar salohiyatini oshiradi. Huquqshunos va IT mutaxassislari o‘rtasida integratsiyalashgan ta'lim tizimini shakllantirish orqali texnik va huquqiy bilimlar uyg‘unlashtiriladi. Shu bilan birga, amaliy simulyatsion laboratoriyalar tashkil qilish orqali kiberjinoyatlarni modellashtirish va real vaziyatlarda tahlil qilish imkoniyati yaratiladi.

Xulosa qilib aytganda, kiberhuquq sohasida tezkor-qidiruv tadbirlarini huquqiy tartibga solishning xorijiy tajribasi zamonaviy kiberjinoyatlarga qarshi samarali kurashishda muhim ahamiyat kasb etmoqda. AQSH, Yevropa ittifoqi davlatlari, Janubiy Koreya, Yaponiya, Singapur va boshqa rivojlangan davlatlar amaliyoti tahlili shuni ko‘rsatadiki, kiberjinoyatlarga qarshi kurashishda an'anaviy tezkor-qidiruv mexanizmlari raqamli texnologiyalar bilan integratsiya qilingan holda qo‘llanilmoqda. Ayniqsa, elektron dalillar bilan ishlash, telekommunikatsiya tarmoqlarini nazorat qilish, raqamli kuzatuv, blockchain tahlili, sun'iy intellekt asosida monitoring olib borish hamda xalqaro tezkor hamkorlik mexanizmlari kiberxavfsizlikni ta'minlashning muhim vositalariga aylangan.

Tadqiqot natijalariga ko‘ra, xorijiy davlatlarda kiberjinoyatlarga qarshi kurashishda maxsus kiberbo‘linmalar, raqamli kriminalistika markazlari, CERT tizimlari va 24/7 cyber contact point mexanizmlari samarali faoliyat yuritmoqda. Shu bilan birga, Budapest Convention on Cybercrime qoidalari asosida elektron dalillarni yig‘ish, saqlash va almashishning yagona xalqaro standartlari shakllantirilmoqda. Bu esa transmilliy kiberjinoyatlarni aniqlash va tergov qilish jarayonini tezlashtirishga xizmat qilmoqda.

Shu bilan birga, xorijiy tajriba raqamli nazorat va inson huquqlari o‘rtasida muvozanatni ta'minlash muhimligini ham ko‘rsatmoqda. Ko‘plab davlatlarda telekommunikatsiya tarmoqlarini kuzatish, internet trafigini monitoring qilish va raqamli ma'lumotlardan foydalanish sud sanksiyasi, parlament nazorati hamda mustaqil monitoring mexanizmlari asosida amalga oshiriladi. Bu esa shaxsiy hayot daxlsizligi va fuqarolarning raqamli huquqlarini himoya qilishga xizmat qiladi.

Maqolada oʻrganilgan xorijiy tajriba Oʻzbekistonda ham kiberhuquq sohasida tezkor-qidiruv tadbirlarini takomillashtirish zarurligini koʻrsatadi. Xususan, elektron dalillar institutini rivojlantirish, blockchain analytics va AI monitoring texnologiyalarini joriy qilish, internet-provayderlar bilan hamkorlikni kuchaytirish, maxsus kiberlaboratoriyalar tashkil etish hamda kiberkadrlar tayyorlash tizimini rivojlantirish dolzarb ahamiyatga ega.

Shuningdek, milliy qonunchilikni xalqaro standartlarga moslashtirish, kiberyurisdiksiya institutini huquqiy jihatdan mustahkamlash, raqamli kuzatuv texnologiyalarini aniq huquqiy asoslar bilan cheklash va transmilliy kiberjinoyatlarga qarshi xalqaro hamkorlikni kuchaytirish orqali kiberxavfsizlik sohasida samarali va barqaror huquqiy mexanizmlarni shakllantirish mumkin boʻladi.

Umuman olganda, kiberhuquq sohasida tezkor-qidiruv tadbirlarini huquqiy tartibga solishning xorijiy tajribasi zamonaviy raqamli jamiyat sharoitida milliy xavfsizlikni ta'minlash, kiberjinoyatlarga qarshi samarali kurashish, inson huquqlarini himoya qilish va raqamli iqtisodiyot barqarorligini ta'minlashda muhim nazariy va amaliy ahamiyatga ega hisoblanadi.

**Foydalanilgan adabiyotlar**

1. Holt T.J., Bossler A.M. Cybercrime: Criminal Threats from Cyberspace. — New York: Routledge, 2016. — 368 p. cgi/viewcontent.cgi?article =1023&context= law_fac_pub (мурожаат вақти: 10.05.2026).

2. Holt T.J. Cybercrime and Digital Forensics: An Introduction. — London: Routledge, 2022. — 412 p. Holt-Bossler-Seigfried-Spellar/p/book/9780367360078(мурожаат вақти: 11.05.2026).

3. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. — 3rd ed. — London: Academic Press, 2011. — 840 p. https://rishikeshpansare. wordpress. com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition. pdf(мурожаат вақти: 12.05.2026).

4. Singer P.W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. — Oxford: Oxford University Press, 2014. — 320 p. (мурожаат вақти: 13.05.2026).

5. Department of Justice. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. — Washington DC, 2015. — 254 p. (мурожаат вақти: 14.05.2026).

6. Federal Bureau of Investigation. Cyber Division Reports and Publications. — Washington DC, 2024. (мурожаат вақти: 15.05.2026).

7. Федеральный закон Российская Федерация от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности» // Электрон манба: http: // www. Consultant.ru (мурожаат вақти: 16.05.2026).

8. Budapest Convention on Cybercrime // Council of Europe. — Budapest, 23.XI.2001. (мурожаат вақти: 17.05.2026).

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

9. Europol. Internet Organised Crime Threat Assessment (IOCTA). — Hague, 2024. (мурожаат вақти: 18.05.2026).

10. Cheong J. Cybersecurity in South Korea: Policy, Governance and Threat Response. — Seoul: Korea Security Institute Press, 2022. — 310 p.

11. Korean National Police Agency. Cyber Bureau Annual Report. — Seoul, 2024.

12. Korea Internet & Security Agency. Cybersecurity Annual Report. — Seoul, 2024.