KIBERJINOYATLARNING OLDINI OLISHDA TEZKOR-QIDIRUV TADBIRLARINING MOHIYATI, TURLARI VA O‘TKAZISH TARTIBI: XORIJIY DAVLATLAR TAJRIBASINING QIYOSIY-HUQUQIY TAHLILI

Bobomurodov Farxod Boymurotovich

Toshkent xalqaro universiteti Yurisprudensiya fakulteti Huquqiy fanlar kafedrasi dotsent v.b., yuridik fanlar doktori (DSc)

Ташкентский международный университет, факультет юриспруденции, и.о. доцента кафедры юридических наук, доктор юридических наук (DSc)

Tashkent International University, Faculty of Jurisprudence, acting Associate Professor of the Department of Legal Sciences, Doctor of Legal Sciences (Dsc)

Annotatsiya. *Mazkur maqolada kiberjinoyatlarning oldini olishda tezkor-qidiruv tadbirlarining nazariy-huquqiy mohiyati, turlari va ularni o‘tkazish tartibi kriminologik hamda qiyosiy-huquqiy jihatdan tahlil qilingan. Kiberjinoyatchilikning transmilliy xususiyati, Internet monitoringi, raqamli kuzatuv, elektron dalillar bilan ishlash, raqamli profayling, “predictive policing” va sun’iy intellekt texnologiyalarining tezkor-qidiruv faoliyatidagi ahamiyati yoritilgan. Shuningdek, Amerika Qo‘shma Shtatlari, Rossiya Federatsiyasi, Janubiy Koreya, Xitoy, Yaponiya, Buyuk Britaniya hamda Singapur tajribasi asosida kiberjinoyatchilik profilaktikasida qo‘llaniladigan tezkor-qidiruv mexanizmlari qiyosiy tahlil qilingan.*

Kalit so‘zlar: *kiberjinoyatchilik, tezkor-qidiruv faoliyati, Internet monitoringi, raqamli kuzatuv, elektron dalillar, kiberprofayling, “predictive policing”, kiberxavfsizlik, kriminologik profilaktika, sun’iy intellekt, “darknet”, “Big Data”, “cyber monitoring”, “digital forensics”, transmilliy jinoyatchilik.*

THE ESSENCE, TYPES, AND PROCEDURES OF OPERATIONAL-SEARCH MEASURES IN THE PREVENTION OF CYBERCRIMES: A COMPARATIVE LEGAL ANALYSIS OF FOREIGN COUNTRIES' EXPERIENCE

Abstract. *This scientific article analyzes the theoretical and legal essence, types, and procedures of operational-search measures aimed at preventing cybercrime from criminological and comparative legal perspectives. The study examines the transnational nature of cybercrime, as well as the significance of internet monitoring, digital surveillance, handling of electronic evidence, cyber profiling, predictive policing, and artificial intelligence technologies within operational-search activities. In addition, based on the experience of the United States, European, the Russian Federation, South Korea, China, Japan, the United Kingdom, and Singapore, a comparative analysis of operational-search mechanisms used in cybercrime prevention is conducted.*

Keywords: *cybercrime, operational-search activity, internet monitoring, digital surveillance, electronic evidence, cyber profiling, predictive policing, cybersecurity, criminological prevention, artificial intelligence, darknet, Big Data, cyber monitoring, digital forensics, transnational crime.*

Hozirgi global raqamlashuv sharoitida axborot-kommunikasiya texnologiyalari jamiyat hayotining deyarli barcha sohalariga chuqur kirib bordi. Elektron hukumat, raqamli iqtisodiyot, onlayn bank xizmatlari, cloud texnologiyalari, kriptovalyutalar, sun’iy intellekt, “Internet of Things” (IoT) hamda “Big Data” tizimlarining jadal rivojlanishi insoniyat taraqqiyoti uchun yangi imkoniyatlar yaratmoqda. Biroq, mazkur jarayonlar bilan bir qatorda, kiberjinoyatchilikning yangi, murakkab va yuqori intellektual shakllari paydo bo‘lmoqda.

Bugungi kunda kiberjinoyatchilik jahon miqyosidagi eng xavfli transmilliy tahdidlardan biri sifatida baholanmoqda. Federal Bureau of Investigationning Internet Crime Complaint Center (IC3) 2024-yillik hisobotiga ko‘ra, 2024-yil davomida AQSHda 859 532 ta kiberjinoyat bo‘yicha murojaat qayd etilgan bo‘lib, ular natijasida yetkazilgan umumiy zarar 16,6 milliard AQSH dollarini tashkil etgan. Bu 2023-yilga nisbatan 33 foizga o‘sganini ko‘rsatadi. Hisobotda fishing, extortion, shaxsiy ma’lumotlarni buzish va kriptovalyuta bilan bog‘liq investitsiya firibgarliklari eng xavfli jinoyat turlari sifatida qayd etilgan.

2025-yil yakunlari bo‘yicha e’lon qilingan dastlabki xalqaro tahlillarda esa kiberjinoyatchilikdan kelgan moliyaviy zarar yanada ortgani qayd etilmoqda. Jumladan, FBI Internet Crime Report ma’lumotlariga ko‘ra, 2025-yilda kiberjinoyatlar natijasidagi zarar qariyb 20,9–21 milliard dollarga yetgan. Shuningdek, 2025-yilda IC3 markaziga 1 milliondan ortiq murojaat kelib tushgan bo‘lib, eng ko‘p uchragan jinoyatlar sifatida fishing, kriptovalyuta firibgarligi, “business email compromise” va “ransomware” hujumlari qayd etilgan [4].

2026-yilning 4 oyi bo‘yicha xalqaro tahlillar kiberjinoyatchilik global xavfsizlikka tahdid soluvchi eng xavfli transmilliy jinoyat turlaridan biri bo‘lib qolayotganini ko‘rsatmoqda. Jahon miqyosida raqamli iqtisodiyotning jadal rivojlanishi, sun’iy intellekt texnologiyalarining ommalashuvi, cloud infratuzilmalardan foydalanishning kengayishi hamda kriptovalyuta aylanmalarining o‘sishi kiberjinoyatchilikning yangi va murakkab shakllarini keltirib chiqarmoqda. Xalqaro tahlil markazlari, axborot xavfsizligi kompaniyalari va huquqni muhofaza qiluvchi organlar ma’lumotlariga ko‘ra, 2026-yilning aprel oyiga qadar bo‘lgan davrda “deepfake” texnologiyalari orqali firibgarlik, “cryptocurrency scam”, “cloud infrastructure attacks” hamda “supply chain cyber attacks” holatlari sezilarli darajada oshgan [16].

Ayniqsa, sun’iy intellekt texnologiyalarining jinoiy maqsadlarda qo‘llanilishi kiberjinoyatchilikning xavfliligini yangi bosqichga olib chiqmoqda [28]. Ilgari fishing xabarlari texnik va til jihatdan sodda shaklda tarqatilgan bo‘lsa, hozirgi vaqtda “generative AI” texnologiyalari yordamida inson psixologiyasiga moslashtirilgan, yuqori ishonch uyg‘otuvchi va real tashkilotlar uslubini taqlid qiluvchi xabarlar avtomatik tarzda yaratilmoqda. Bu esa ommaviy fishing kampaniyalarining “sanoat darajasi”ga chiqishiga sabab bo‘lmoqda. Kiberjinoyatchilar AI yordamida millionlab elektron pochta manzillari va ijtimoiy tarmoq akkauntlarini tahlil qilib, muayyan shaxsga yo‘naltirilgan “spear-phishing” hujumlarini amalga oshirmoqdalar.

Shu bilan birga, “deepfake” texnologiyalaridan foydalanib amalga oshirilayotgan firibgarlik holatlari ham keskin ko‘paymoqda. Xususan, ovoz va video tasvirlarni sun’iy tarzda yaratish orqali bank operatsiyalarini tasdiqlash, tashkilot rahbarlari nomidan soxta topshiriqlar yuborish yoki moliyaviy mablag‘larni noqonuniy o‘tkazish kabi holatlar xalqaro amaliyotda tobora ko‘proq kuzatilmoqda. Bu esa raqamli identifikatsiya va elektron ishonch tizimlariga nisbatan xavflarni kuchaytirmoqda[26; 27].

2026-yilda “cloud infrastructure attacks”, ya’ni bulutli infratuzilmalarga qilingan hujumlar ham kiberjinoyatchilikning eng xavfli yo‘nalishlaridan biri sifatida baholanmoqda. Chunki davlat organlari, bank tizimlari, elektron hukumat platformalari va yirik korporatsiyalar ma’lumotlarni “cloud” muhitda saqlashga o‘tmoqda. Kiberjinoyatchilar esa mazkur infratuzilmalardagi zaifliklardan foydalanib, katta hajmdagi ma’lumotlarni o‘g‘irlash, “ransomware” hujumlarini amalga oshirish yoki xizmat ko‘rsatish tizimlarini izdan chiqarishga harakat qilmoqda. Ayniqsa, “supply chain cyber attacks”, ya’ni dasturiy ta’minot va ta’minot zanjiri orqali amalga oshiriladigan hujumlar global kiberxavfsizlikning eng dolzarb muammolaridan biriga aylandi. Bunda jinoyatchilar yirik tashkilotga to‘g‘ridan-to‘g‘ri hujum qilish o‘rniga, uning dasturiy ta’minot yetkazib beruvchilari yoki texnik hamkorlari orqali tizimga kirib bormoqda.

Xalqaro miqyosda kiberjinoyatchilikning xavfliligini namoyon qilgan muhim voqealardan biri 2026-yil boshida Interpol tomonidan amalga oshirilgan “Operation Ramz” xalqaro operatsiyasi hisoblanadi. Ushbu operatsiya davomida 13 ta davlatda transmilliy kiberjinoiy tarmoqlarga qarshi tezkor tadbirlar o‘tkazilib, 201 nafar shaxs qo‘lga olingan, 53 ta server musodara qilingan hamda minglab kiberjinoyat qurbonlari aniqlangan. Mazkur holat kiberjinoyatchilikning milliy chegaralar bilan cheklanmasligini, uyushgan raqamli jinoiy guruhlar xalqaro darajada faoliyat yuritayotganini va bu jinoyat turi global xavfsizlikka jiddiy tahdid solayotganini ko‘rsatadi [16].

Zamonaviy kiberjinoyatchilikning xavfliligi, avvalo, uning transmilliy xususiyatga egaligi bilan izohlanadi. Jinoyatchilar bir davlat hududida turib boshqa davlatdagi bank tizimlariga, davlat axborot resurslariga yoki xususiy kompaniyalarga hujum uyushtirishi mumkin [21]. Bu esa yurisdiksiya, ekstraditsiya va xalqaro huquqiy hamkorlik masalalarini murakkablashtiradi. Shu sababli kiberjinoyatchilikka qarshi kurashishda xalqaro hamkorlik va tezkor axborot almashinuvi muhim ahamiyat kasb etmoqda.

Kiberjinoyatchilikning yana bir o‘ziga xos xususiyati uning yuqori latentlikka egaligidir [20]. Ko‘plab holatlarda tashkilotlar va jismoniy shaxslar kiberhujum haqida huquqni muhofaza qiluvchi organlarga murojaat qilmaydilar. Bu esa jinoyatlarning real ko‘lamini aniqlashni qiyinlashtiradi. Ayniqsa, elektron dalillarning tez o‘zgaruvchanligi va oson yo‘q qilinishi kiberjinoyatlarni tergov qilish jarayonini murakkablashtirmoqda.

Shu bilan birga, “VPN”, “proxy”, “darknet”, kriptovalyuta va anonim messenjerlardan foydalanish jinoyatchilarning shaxsini aniqlashni qiyinlashtirmoqda. Anonimlik darajasining yuqoriligi kiberjinoyatchilarda jazodan qochib qolish mumkinligi haqida tasavvurni kuchaytirmoqda. Bu esa uyushgan raqamli jinoiy guruhlarning shakllanishiga olib kelmoqda.

Shu sababli zamonaviy sharoitda kiberjinoyatchilikka qarshi kurashish faqat an’anaviy jazo choralari bilan cheklanib qolmasligi lozim. Kiberjinoyatchilik profilaktikasini kuchaytirish, Internet monitoringi, raqamli profayling, “predictive policing”, elektron dalillar bilan ishlash va sun’iy intellekt asosida tahlil tizimlarini rivojlantirish orqali kibertahdidlarni erta bosqichda aniqlash muhim ahamiyat kasb etadi.

Raqamlashuv sharoitida kiberjinoyatchilik jamiyat va davlat xavfsizligiga jiddiy tahdid soluvchi transmilliy jinoyat turiga aylanmoqda. Internet texnologiyalari, elektron to‘lov tizimlari, “cloud” infratuzilmalar, sun’iy intellekt va kriptovalyuta texnologiyalarining keng rivojlanishi kiberjinoyatlarning sodir etilish usullarini murakkablashtirmoqda. Shu sababli kiberjinoyatchilikka qarshi kurashishda an’anaviy tergov usullari bilan bir qatorda, tezkor-qidiruv tadbirlari ham muhim ahamiyat kasb etmoqda.

Tezkor-qidiruv tadbirlari – bu jinoyatlarni aniqlash, oldini olish, ularni fosh etish va jinoyat sodir etgan shaxslarni aniqlashga qaratilgan maxsus huquqiy, tashkiliy va texnik chora-tadbirlar tizimi [22; 23]. Kiberjinoyatchilik sohasida mazkur tadbirlar Internet muhitidagi jinoiy faollikni kuzatish, elektron dalillarni aniqlash, raqamli ma’lumotlarni tahlil qilish va kibertahdidlarni erta bosqichda aniqlash vazifalarini bajaradi [25].

Tezkor-qidiruv tadbirlarining asosiy mohiyati jinoyatni sodir etilgandan keyin emas, balki uning kelib chiqishiga sabab bo‘luvchi omillarni barvaqt aniqlash va profilaktika qilishdan iborat. Chunki kiberjinoyatchilik yuqori latentlikka ega bo‘lib, ko‘p holatlarda jinoyatchilar virtual muhitda anonim ravishda harakat qiladi. Bu esa kiberjinoyatlarni an’anaviy usullar orqali aniqlashni qiyinlashtiradi. Shu sababli tezkor-qidiruv faoliyati Internet monitoringi, raqamli kuzatuv, onlayn tahlil va elektron razvedka orqali kiberjinoyatchilikni erta bosqichda aniqlash imkonini beradi.

Kiberjinoyatlarning oldini olishda tezkor-qidiruv tadbirlarining o‘ziga xos xususiyatlaridan biri ularning profilaktik xarakterga egaligidir. Masalan, Internet tarmoqlaridagi shubhali faollikni monitoring qilish, “darknet” platformalarini kuzatish, zararli dastur tarqatuvchi manbalarni aniqlash va fishing saytlarni bloklash orqali jinoyat sodir bo‘lishining oldi olinadi. Bu esa jinoyat oqibatlarini bartaraf etishdan ko‘ra samaraliroq hisoblanadi.

Tezkor-qidiruv tadbirlari kibermakondagi kriminogen vaziyatni tahlil qilish imkonini ham beradi. Internet tarmoqlarida qaysi turdagi kiberhujumlar ko‘payib borayotgani, qaysi ijtimoiy guruhlar viktimlashuv xavfi yuqori ekanligi, qaysi dasturiy zaifliklar jinoyatchilar tomonidan ko‘proq qo‘llanilayotgani haqidagi ma’lumotlar profilaktika choralarini samarali tashkil etishga xizmat qiladi. Shu jihatdan tezkor-qidiruv tadbirlari kriminologik prognozlashning muhim vositasi hisoblanadi.

Kiberjinoyatchilikka qarshi tezkor-qidiruv tadbirlarining mohiyati elektron dalil bilan ishlashda ham namoyon bo‘ladi. Kiberjinoyatlarda dalillar raqamli shaklda bo‘lgani sababli ular tez o‘zgarishi, yo‘q qilinishi yoki boshqa davlat serverlarida saqlanishi mumkin. Shu sababli tezkor ravishda ma’lumotlarni saqlab qolish, trafik ma’lumotlarini aniqlash, IP-manzillarni kuzatish va server faoliyatini tahlil qilish muhim ahamiyat kasb etadi. Bu esa raqamli kriminalistika va tezkor-qidiruv faoliyatining o‘zaro integratsiyasini talab qiladi [17; 18; 19.]

Zamonaviy sharoitda sun’iy intellekt va «Big Data» texnologiyalarining rivojlanishi tezkor-qidiruv tadbirlarining samaradorligini yanada oshirmoqda. «Predictive policing» tizimlari orqali kibertahdidlarni oldindan prognoz qilish, zararli faollikni avtomatik aniqlash va xavfli Internet segmentlarini real vaqt rejimida monitoring qilish imkoniyati paydo bo‘lmoqda. Bu esa kiberjinoyatchilik profilaktikasini yangi bosqichga olib chiqmoqda.

Xorijiy davlatlar tajribasi ham tezkor-qidiruv tadbirlarining kiberjinoyatchilik profilaktikasida muhim o‘rin tutishini ko‘rsatmoqda. Xususan, Federal Bureau of Investigation, Europol European Cybercrime Centre (Ec3), Interpol hamda Korea Internet & Security Agency kabi tuzilmalar Internet monitoringi, raqamli razvedka, «AI-based analytics» va «undercover cyber operations» orqali kiberjinoyatlarni erta bosqichda aniqlash va profilaktika qilish mexanizmlarini keng qo‘llamoqda.

Shu bilan birga, tezkor-qidiruv tadbirlarini amalga oshirishda inson huquqlari va shaxsiy hayot daxlsizligi kafolatlarini ta’minlash muhim ahamiyat kasb etadi [24]. Internet monitoringi, raqamli kuzatuv va ma’lumotlarni yig‘ish jarayonlari qonuniylik, proporsionallik va sud nazorati prinsiplari asosida amalga oshirilishi lozim. Aks holda raqamli nazorat inson huquqlariga tajovuz qilish xavfini keltirib chiqarishi mumkin.

Amerika Qo‘shma Shtatlari kiberjinoyatchilikka qarshi kurashishda dunyodagi rivojlangan va texnologik jihatdan kuchli davlatlardan biridir. Mamlakatda kiberxavfsizlikni ta’minlash va kiberjinoyatchilikka qarshi kurashish federal darajada muvofiqlashtirilgan kompleks tizim asosida amalga oshiriladi [13]. Xususan, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, National Security Agency hamda National Cyber Investigative Joint Task Force kabi maxsus tuzilmalar kibertahdidlarni aniqlash, Internet muhitidagi jinoiy faollikni monitoring qilish, raqamli razvedka olib borish va kiberjinoyatlarni profilaktika qilish bilan shug‘ullanadi [14]. AQSH amaliyotining asosiy xususiyati shundaki, kiberjinoyatchilikka qarshi kurashish faqat jinoyat sodir etilgandan keyin reaksiya bildirishga emas, balki jinoyatni tayyorgarlik bosqichida aniqlash va uning oldini olishga qaratilgan. Shu bois, AQSH modeli kriminologiyada profilaktikaga yo‘naltirilgan kiberxavfsizlik modeli sifatida baholanadi. Mazkur yondashuv doirasida Internet monitoringi, raqamli profayling, «undercover cyber operations» va sun’iy intellekt asosida tahlil texnologiyalari keng qo‘llaniladi [1].

Internet monitoringi kiberjinoyatchilikka qarshi kurashning muhim tezkor-qidiruv mexanizmlaridan biri hisoblanadi. Davlat organlari Internet tarmoqlari, ijtimoiy platformalar, messenjerlar,

«cloud» muhitlar va «darknet» segmentlarini muntazam kuzatib boradi. Ayniqsa, «darknet» muhitida narkotik vositalar savdosi, zararli dasturlar tarqatilishi, shaxsiy ma’lumotlar savdosi va kriptovalyuta orqali noqonuniy operatsiyalar monitoring qilinadi [5]. Bu orqali jinoiy guruhlarning virtual aloqalari, moliyaviy sxemalari va kiberhujumlarga tayyorgarlik jarayonlari haqida tezkor ma’lumotlar to‘planadi.

Virtual muhitda yashirin tezkor faoliyat olib borish AQSH amaliyotida keng qo‘llaniladigan usullardan biri hisoblanadi. Mutaxassislar «darknet» forumlari, kriptovalyuta platformalari va yopiq onlayn hamjamiyatlarga kirib, jinoiy guruhlar haqida ma’lumot to‘playdi [15]. Bunday operatsiyalar orqali zararli dasturlar sotuvchilari, kiberfiribgarlik guruhlari va transmilliy raqamli jinoiy uyushmalar faoliyati aniqlanadi.

Raqamli profayling tizimi orqali shaxslarning IP-manzili, Internet faolligi, ijtimoiy tarmoqlardagi harakatlari va raqamli izlari tahlil qilinadi. Ayniqsa, «Big Data» texnologiyalari bilan integratsiya qilingan raqamli profayling tizimlari jinoyatchilik tendensiyalarini prognoz qilishda muhim ahamiyat kasb etmoqda.

Rossiya Federatsiyasida kiberjinoyatchilikka qarshi kurashish va tezkor-qidiruv faoliyati markazlashgan davlat nazorati asosida tashkil etilgan bo‘lib, mazkur sohada huquqiy hamda texnik mexanizmlar shakllantirilgan. Kiberjinoyatchilikka qarshi tezkor-qidiruv tadbirlari, avvalo, Rossiya Federatsiyasining “Tezkor-qidiruv faoliyati to‘g‘risida”gi Federal qonuni asosida amalga oshiriladi [29]. Mazkur qonun huquqni muhofaza qiluvchi organlarga jinoyatlarni aniqlash, oldini olish, fosh etish va jinoyat sodir etgan shaxslarni aniqlash maqsadida raqamli kuzatuv, telekommunikatsiya monitoringi va elektron ma’lumotlar bilan ishlash imkoniyatini beradi. Rossiya amaliyotining muhim xususiyatlaridan biri “Система оперативно-розыскных мероприятий” (SORM) tizimining joriy etilganidir. SORM telekommunikatsiya tarmoqlari va Internet muhitini davlat darajasida monitoring qilish imkonini beruvchi markazlashgan raqamli kuzatuv mexanizmi hisoblanadi. Ushbu tizim orqali Internet trafigi, telefon aloqalari, elektron xatlar, messenjerlardagi ma’lumot almashinuvi va boshqa raqamli kommunikatsiyalar monitoring qilinishi mumkin. Kriminologik nuqtai nazardan, SORM tizimi kibertahdidlarni erta bosqichda aniqlash, raqamli jinoiy guruhlar harakatini kuzatish va transmilliy kiberjinoyatchilikka qarshi tezkor choralar ko‘rish imkonini beradi.

Telekommunikatsiya monitoringi davlat kiberxavfsizlik siyosatida muhim o‘ringa ega. Internet-provayderlar telekommunikatsiya operatorlari tezkor xizmatlar bilan integratsiya qilingan bo‘lib, huquqni muhofaza qiluvchi organlarga muayyan ma’lumotlarni tezkor tarzda taqdim etish majburiyati yuklatilgan. Bu esa Internet muhitidagi shubhali faollikni doimiy nazorat qilish, zararli kontentlarni aniqlash va kiberhujumlarga qarshi tezkor javob qaytarish imkonini yaratadi. Ayniqsa, ekstremistik materiallar, terrorchilikka oid axborotlar, fishing tarmoqlari va onlayn firibgarlik sxemalarini aniqlashda mazkur tizim keng qo‘llanilmoqda.

Raqamli kuzatuv (digital surveillance) ham kiberjinoyatchilikka qarshi kurashishning muhim mexanizmi hisoblanadi. Huquqni muhofaza qiluvchi organlar muayyan shaxsning geolokatsiyasi, Internet faolligi, elektron qurilmalari va raqamli harakatlarini tahlil qilish imkoniyatiga ega. Mobil qurilmalar, IP-manzillar, SIM-kartalar va internet-trafik ma’lumotlarini tahlil qilish orqali jinoyatchilarning virtual aloqalari va harakat yo‘nalishlari aniqlanadi. Bu esa uyushgan kiberjinoiy guruhlarning tuzilishi, moliyaviy sxemalari va raqamli infratuzilmasini o‘rganish imkonini beradi.

So‘nggi yillarda Rossiya Federasiyasida «*darknet» muhitini monitoring qilishga* ham alohida e’tibor qaratilmoqda [30]. «Darknet» platformalari orqali giyohvandlik vositalari, shaxsiy ma’lumotlar savdosi, zararli dasturlar tarqatish va boshqa raqamli jinoyatlar amalga oshirilishi sababli mazkur muhit davlat organlari tomonidan doimiy kuzatib boriladi. Ayniqsa, kriptovalyuta operatsiyalarini tahlil qilish orqali noqonuniy moliyaviy aylanmalar va transmilliy jinoiy tarmoqlar aniqlanmoqda. Bu maqsadda «blockchain analytics» va raqamli profayling usullari ham qo‘llaniladi.

Janubiy Koreya kiberxavfsizlik sohasida Osiyo mintaqasidagi eng rivojlangan va texnologik jihatdan ilg‘or davlatlardan biri hisoblanadi. Mamlakatda raqamli iqtisodiyot, elektron hukumat, onlayn bank tizimlari va yuqori tezlikdagi Internet infratuzilmasining keng rivojlangani kiberxavfsizlikni milliy xavfsizlikning ustuvor yo‘nalishlaridan biriga aylantirgan [7]. Shu sababli Janubiy Koreyada kiberjinoyatchilikka qarshi kurashish va uning profilaktikasi davlat siyosati darajasida tashkil etilgan bo‘lib, mazkur sohada Korea Internet & Security Agency, milliy kiberpolitsiya, raqamli tahlil markazi va maxsus kiberxavfsizlik bo‘linmalari faoliyat yuritadi.

Janubiy Koreya tajribasining asosiy xususiyati shundaki, mamlakatda kiberjinoyatchilikka qarshi kurashish faqat jinoyatlarni fosh etishga emas, balki uning barvaqt oldini olish va xavflarni erta bosqichda aniqlashga qaratilgan [10]. Mamlakatda “real-time cyber monitoring”, “predictive policing”, “ISP cooperation” va “AI-based analytics” tizimlari yuqori darajada joriy etilgan.

Internet tarmoqlari, davlat axborot tizimlarini real vaqt rejimida kuzatish tizimi yagona kiberxavfsizlik infratuzilmasi orqali o‘zaro integratsiya qilingan. Bu esa Internet muhitidagi shubhali faollikni, zararli dasturlar tarqalishini, kiberhujumlarga tayyorgarlik harakati va ma’lumotlar o‘g‘irlanishi holatlarini tezkor aniqlash imkonini beradi. Ayniqsa, davlat axborot tizimlari, strategik infratuzilmalarga qilingan kiberhujumlarni barvaqt aniqlash milliy xavfsizlik nuqtai nazaridan muhim ahamiyatga ega.

Jinoyatni oldindan prognoz qilish texnologiyalari sun’iy intellekt va mashinali o‘qitish algoritmlari orqali kiberjinoyatlarni sodir etish ehtimoli yuqori bo‘lgan holatlar bashorat qilinadi. Masalan, muayyan IP-manzil, Internet trafigi, fishing shablonlari yoki botnet harakatlaridagi anomal o‘zgarishlar avtomatik tahlil qilinib, ehtimoliy kibertahdidlar haqida oldindan ogohlantirish tizimi ishlaydi. Bu esa huquqni muhofaza qiluvchi organlarga jinoyat sodir bo‘lishidan avval profilaktik choralarni amalga oshirish imkonini beradi.

Internet-provayderlar bilan hamkorlikni yo‘lga qo‘yish orqali huquqni muhofaza qiluvchi organlar bilan muntazam ravishda axborot almashinuvi amalga oshiriladi. Bu orqali zararli trafik manbalari, fishing saytlar, botnet tarmoqlari va noqonuniy onlayn faollik tezkor aniqlanadi. Internet-provayderlar kiberhujumlar haqidagi ma’lumotlarni maxsus kiberxavfsizlik markazlariga uzatib, milliy raqamli xavfsizlik tizimining muhim subyekti sifatida ishtirok etadi.

Sun’iy intellekt va Big Data asosida tahlil qilish kiberxavfsizlik modelini muhim elementlaridan biri hisoblanadi. Mazkur texnologiyalar orqali shubhali faollik, fishing hujumlari, botnet tarmoqlari, “malware” tarqalishi va ransomware operatsiyalari avtomatik tarzda tahlil qilinadi. AI tizimlari internet muhitidagi millionlab harakatlarni real vaqt rejimida qayta ishlab, xavfli tendensiyalarni belgilaydi va ehtimoliy kiberhujumlar haqida avtomatik signal yuboradi. Bu kiberjinoyatchilikka qarshi kurashishda inson omili bilan bog‘liq xatolarni kamaytirish va tahlil tezligini oshirish imkonini beradi.

Darknet va kriptovalyuta monitoringi kiberxavfsizlik tizimining muhim yo‘nalishlaridan biri hisoblanadi. Darknet orqali amalga oshiriladigan giyohvandlik va shaxsga doir ma’lumotlar savdosi kabi jinoyatlarga qarshi maxsus kiberbo‘linmalar tashkil etilgan. Ushbu bo‘linmalar blokcheyn tahlili, kriptovalyuta tranzaksiyalarini kuzatish, yashirin forumlarni monitoring qilish va virtual aktivlar harakatini tahlil qilish orqali tezkor-qidiruv tadbirlarini amalga oshiradi.

Xitoyda kiberjinoyatlarga qarshi kurashish sohasida asosiy vakolatli subyektlar sifatida Jamoat xavfsizligi vazirligi, Davlat xavfsizligi vazirligi, maxsus kiberpolitsiya bo‘linmalari, milliy axborot xavfsizligi markazlari hamda raqamli monitoring platformalari faoliyat yuritadi. Ularning faoliyati

markazlashgan raqamli boshqaruv tizimi asosida amalga oshiriladi [2]. Bu esa mamlakat miqyosida kiberxavflarni yagona platforma orqali kuzatish va tezkor choralar ko‘rish imkonini beradi.

Kiberjinoyatlarning oldini olishda qo‘llaniladigan muhim tezkor-qidiruv tadbirlaridan biri *real vaqtda kiberkuzatuv* hisoblanadi. Mamlakatda internet tarmoqlari, davlat serverlari, bank tizimlari, ijtimoiy tarmoqlar va telekommunikatsiya infratuzilmalari doimiy monitoring qilinadi. Bu jarayonda: tarmoqqa noqonuniy kirish, xakerlik harakatlari, DDoS hujumlari, fishing platformalari zararli dasturlar tarqalishi, shubhali internet-trafik avtomatik ravishda aniqlanadi. Mazkur tizim sun’iy intellekt, “Big Data” va “cloud monitoring” texnologiyalari bilan integratsiya qilingan bo‘lib, xavfli faoliyatlarni barvaqt prognoz qilish imkonini yaratadi [9].

Prognozli profilaktik tahlili sun’iy intellekt va algoritmlar yordamida shubhali IP-manzillar; kiberjinoyat sodir etish ehtimoli yuqori bo‘lgan akkauntlar, onlayn firibgarlik sxemalari; kriptovalyuta orqali amalga oshirilayotgan noqonuniy operatsiyalar; darknet faoliyati tahlil qilinadi. Bu orqali huquqni muhofaza qiluvchi organlar jinoyat sodir etilmasidan avvalroq profilaktik choralar ko‘rish imkoniyatiga ega bo‘ladi. Bu tadbirni amalga oshirilishi, ayniqsa, onlayn moliyaviy firibgarlik va telekommunikatsiya orqali sodir etiladigan jinoyatlarga qarshi samarali qo‘llaniladi.

Internet-provayderlar va raqamli platformalar bilan hamkorlik qilish orqali huquqni muhofaza qiluvchi organlar o‘z vakolati doirasida IP-manzillarni aniqlash, foydalanuvchilarni identifikatsiya qilish, elektron ma’lumotlarni saqlash, shubhali akkauntlarni bloklash, zararli kontentni o‘chirish, tarmoq trafigini tahlil qilish kabi tezkor tadbirlarni amalga oshiradi.

Internetdan foydalanish jarayonida shaxsni identifikatsiya qilish tadbiri kiberjinoyatchilarni aniqlash imkoniyatini oshiradi.

Sun’iy intellekt texnologiyalari asosida tahlil qilish orqali botnet tarmoqlari, zararli dasturlarni tarqatish, firibgarlik yo‘li bilan ma’lumotlari qo‘lga kiritish, onlayn ekstremistik mazmundagi kontent, moliyaviy firibgarlik, kriptovalyuta operatsiyalari avtomatik monitoringi o‘tkazilishi eng samarali choradir. SI tizimlari millionlab elektron ma’lumotlarni qisqa vaqt ichida qayta ishlab, xavfli faoliyatlarni avtomatik belgilaydi va tegishli organlarga xabar yuboradi. Bu esa kiberjinoyatlarni erta bosqichda aniqlash imkonini beradi.

Raqamli kriminalistika tadbirini o‘tkazish orqali kompyuterlar, mobil qurilmalar, serverlar, bulutli ma’lumotlar va elektron yozishmalar kriminalistik usullar orqali tekshiriladi. Raqamli kriminalistika laboratoriyalarida o‘chirilgan fayllarni tiklash, elektron izlarni aniqlash log-fayllarni tahlil qilish, mobil qurilmalardan ma’lumot olish, kriptovalyuta operatsiyalarini kuzatish kabi ishlar amalga oshiriladi. Bu harakatlar elektron dalillardan sud jarayonida samarali foydalanish imkonini beradi.

Yaponiya kiberjinoyatlarga qarshi kurashish va ularning oldini olish sohasida texnologiya, raqamli xavfsizlik va huquqiy tartibga solishni uyg‘unlashtirgan davlatlardan biri hisoblanadi. Mamlakatda axborot-kommunikasiya texnologiyalari, elektron tijorat, raqamli bank tizimi va intellektual infratuzilmaning yuqori darajada rivojlanganligi sababli kiberxavfsizlik milliy xavfsizlikning muhim qismi sifatida qaraladi. Shu bois kiberjinoyatlarni barvaqt aniqlash, profilaktika qilish va fosh etish maqsadida zamonaviy tezkor-qidiruv tadbirlari keng qo‘llaniladi [6]. Kiberjinoyatlarga qarshi kurashish sohasida asosiy vakolatli subyektlar sifatida Milliy politsiya agentligi, maxsus kibertergov bo‘linmalari, axborot xavfsizligi markazlari, raqamli kriminalistika laboratoriyalari hamda milliy kiberxavfsizlik strategiyasi bo‘yicha davlat organlari faoliyat yuritadi. Ularning faoliyati davlat va xususiy sektor o‘rtasidagi hamkorlik asosida amalga oshiriladi. Bu esa kiberxavflarni tezkor aniqlash va ularga qarshi samarali choralar ko‘rish imkonini yaratadi [8].

Davlat organlari tomonidan kiberjinoyatlarni aniqlash, profilaktika qilish va fosh etishda quyidagi: 1) real vaqt rejimida kiberkuzatuv; 2) tarmoq trafigini tahlil qilish; 3) prognozli profilaktik tahlil; 4) sun’iy intellekt asosida tahlil; 5) raqamli kriminalistika; 6) zararli dasturlarni tahlil qilish; 7) fishingni aniqlash tizimlari; 8) darknet monitoringi; 9) kriptovalyuta operatsiyalarini kuzatish, ya’ni blokcheyn tahlili orqali noqonuniy operatsiyalarni aniqlash; 10) elektron aloqalarni nazorat qilish; 11) ijtimoiy tarmoqlarni monitoring qilish; 12) IP-manzillarni aniqlash; 13) internet-provayderlar bilan hamkorlik; 14) bulutli ma’lumotlarni tekshirish; 15) log-fayllarni tahlil qilish; 16) botnet tarmoqlarini aniqlash; 17) kiberrazvedka; 18) yashirin kiberoperasiyalar; 19) elektron dalillarni saqlash; 20) xalqaro kiberhamkorlik operatsiyalar; 21) muhim infratuzilmalarni monitoring qilish; 22) anomal faoliyatni avtomatik aniqlash; 23) mobil qurilmalar kriminalistikasi; 24) kompyuter yoki telefondagi fayllarni shifrlash hujumlariga qarshi tezkor choralar; 25) kiberhodisalarga tezkor javob berish; 26) biometrik identifikatsiya tizimlari asosida yuzni tanish va biometrik ma’lumotlar orqali shubhali shaxslarni aniqlash; 27) IoT qurilmalar xavfsizligini monitoring qilish(“aqlli qurilmalar” orqali amalga oshiriladigan kiberhujumlarni kuzatish); 28) kibersavodxonlik profilaktika dasturi asosida aholi va tashkilotlar uchun kiberxavfsizlik bo‘yicha profilaktik o‘quv tadbirlarini o‘tkazish 29) moliyaviy kiberfiribgarlikni aniqlash. Bu tadbir orqali onlayn bank va to‘lov tizimlaridagi shubhali operatsiyalarni tahlil qilinadi; 30) kiberhodisa simulyatsiya mashqlarini amalga oshirish (*davlat organlari va kompaniyalar ishtirokida kiberhujumlarga qarshi maxsus mashqlar o‘tkazish*) kabi zamonaviy tezkor-qidiruv tadbirlari qo‘llaniladi.

Buyuk Britaniya kiberjinoyatlarga qarshi kurashish va ularning oldini olish sohasida huquqiy mexanizmlar, raqamli texnologiyalar va xalqaro hamkorlikni samarali uyg‘unlashtirgan davlatlardan biri hisoblanadi. Mamlakatda raqamli iqtisodiyot, elektron tijorat, bank tizimi va davlat xizmatlarining keng raqamlashtirilganligi sababli kiberxavfsizlik milliy xavfsizlikning strategik yo‘nalishlaridan biri sifatida qaraladi. Kiberjinoyatlarni barvaqt aniqlash, profilaktika qilish va fosh etish maqsadida zamonaviy tezkor-qidiruv tadbirlari keng qo‘llaniladi.

Kiberjinoyatlarga qarshi kurashishida asosiy vakolatli subyektlar sifatida National Crime Agency, National Cyber Security Centre, maxsus kiberpolitsiya bo‘linmalari, razvedka xizmatlari hamda raqamli kriminalistika markazlari faoliyat yuritadi [12]. Ushbu organlar davlat va xususiy sektor bilan hamkorlik asosida yagona kiberxavfsizlik tizimini shakllantirgan. Ushbu davlat organlarining maxsus bo‘linmalari tomonidan kiberjinoyatlarni barvaqt aniqlash, profilaktika qilish va fosh etishda quyidagi: 1) real vaqt rejimida kiberkuzatuv; 2) tarmoq trafigini tahlil qilish; 3) prognozli profilaktik tahlil; 4) sun’iy intellekt asosida tahlil; 5) raqamli kriminalistika; 6) zararli dasturlarni tahlil qilish; 7) fishingni aniqlash tizimlari; 8) darknet monitoringi; 9) kriptovalyuta operatsiyalarini kuzatish; 10) elektron aloqalarni nazorat qilish; 11) ijtimoiy tarmoqlarni monitoring qilish; 12) IP-manzillarni aniqlash; 13) internet-provayderlar bilan hamkorlik; 14) bulutli ma’lumotlarni tekshirish; 15) log-fayllarni tahlil qilish; 16) botnet tarmoqlarini aniqlash; 17) kiberrazvedka; 18) yashirin kiberoperatsiyalar; 19) elektron dalillarni saqlash; 20) xalqaro kiberhamkorlik operatsiyalari; 21) muhim infratuzilmalarni monitoring qilish; 22) anomal faoliyatni avtomatik aniqlash; 23) mobil qurilmalar kriminalistikasi; 24) kompyuter va telefondagi fayllarni shifrlash hujumlariga qarshi tezkor choralar; 25) kiberhodisalarga tezkor javob berish kabi zamonaviy tezkor-qidiruv tadbirlari amalga oshiriladi.

Singapur Respublikasi kiberxavfsizlik va raqamli texnologiyalar sohasida “Smart Nation” konsepsiyasiga binoan davlat boshqaruvi, bank tizimi, transport, elektron xizmatlar va telekommunikatsiya sohalarini to‘liq raqamlashtirgan. Shu sababli kiberxavfsizlikni ta’minlash milliy xavfsizlikning muhim yo‘nalishlaridan biri sifatida qaraladi [3]. Singapurda kiberjinoyatlarni barvaqt aniqlash, oldini olish va fosh etish maqsadida zamonaviy tezkor-qidiruv tadbirlari o‘tkaziladi.

Singapurda kiberjinoyatlarga qarshi kurashish sohasida asosiy vakolatli subyektlar sifatida Singapore Police Force, Cyber Security Agency of Singapore hamda Infocomm Media Development

Authority faoliyat yuritadi. Shuningdek, maxsus kibertergov bo‘linmalari va raqamli kriminalistika markazlari ham mamlakat kiberxavfsizligini ta’minlashda muhim o‘rin tutadi [11]. Ularning faoliyati yagona raqamli xavfsizlik tizimi asosida muvofiqlashtiriladi. Ushbu 3 ta davlat organlarining maxsus bo‘linmalari kiberjinoyatlarni barvaqt aniqlash, profilaktika qilish va fosh etishda quyidagi: 1) real vaqt rejimida kiberkuzatuv; 2) tarmoq trafigini tahlil qilish; 3) prognozli profilaktik tahlil; 4) sun’iy intellekt asosida tahlil; 5) raqamli kriminalistika; 6) zararli dasturlarni tahlil qilish; 7) fishingni aniqlash tizimlari; 8) darknet monitoringi; 9) kriptovalyuta operatsiyalarini kuzatish; 10) elektron aloqalarni nazorat qilish; 11) ijtimoiy tarmoqlarni monitoring qilish; 12) IP-manzillarni aniqlash; 13) internet-provayderlar bilan hamkorlik; 14) bulutli ma’lumotlarni tekshirish; 15) log-fayllarni tahlil qilish; 16) botnet tarmoqlarini aniqlash; 17) kiberrazvedka; 18) yashirin kiberoperatsiyalar; 19) elektron dalillarni saqlash; 20) xalqaro kiberhamkorlik operatsiyalari; 21) muhim infratuzilmalarni monitoring qilish; 22) anomal faoliyatni avtomatik aniqlash; 23) mobil qurilmalar kriminalistikasi (smartfon va planshetlardagi raqamli izlarni tahlil qilish); 24) kompyuter yoki telefondagi fayllarni shifrlash hujumlariga qarshi tezkor choralar; 25) kiberhodisalarga tezkor javob berish; 26) biometrik identifikatsiya tizimlari asosida yuzni tanish va biometrik ma’lumotlar orqali shubhali shaxslarni aniqlash; 27) IoT qurilmalar xavfsizligini monitoring qilish(“aqlli qurilmalar” orqali amalga oshiriladigan kiberhujumlarni kuzatish); 28) kibersavodxonlik profilaktika dasturi asosida aholi va tashkilotlar uchun kiberxavfsizlik bo‘yicha profilaktik o‘quv tadbirlarini o‘tkazish; 29) moliyaviy kiberfiribgarlikni aniqlash; 30) Singapurning raqamli shahar infratuzilmalarini avtomatlashtirilgan monitoring qilish; 31) deepfake aniqlash tizimi asosida sun’iy intellekt orqali soxta audio va videolarni aniqlash; 32) ma’lumotlar sizib chiqishini monitoring qilish ya’ni, maxfiy ma’lumotlarning internetga tarqalishini kuzatish; 33) davlat organlari va kompaniyalar ishtirokida kiberhujumlarga qarshi maxsus simulyatsiya mashqlari o‘tkazish; 34) yangi va hali aniqlanmagan kiberxavflarni barvaqt kuzatish; 35) barcha kiberxavflar haqidagi ma’lumotlarni yagona markaz orqali muvofiqlashtirish kabi o‘ttizdan ortiq zamonaviy tezkor-qidiruv tadbirlari doimiy ravishda o‘tkaziladi.

Yuqorida tahlil qilingan 7 ta davlatda kiberjinoyatlar yuzasidan tezkor-qidiruv tadbirlarini o‘tkazish tartibi va huquqiy asoslari o‘zaro farq qiladi.

Mazkur davlatlarda kiberjinoyatlarni barvaqt aniqlash, profilaktika qilish va fosh etish maqsadida “real-time cyber monitoring”, “digital forensics”, “AI-based analytics”, “predictive policing”, “darknet monitoring” va “cryptocurrency tracking” kabi zamonaviy tezkor-qidiruv tadbirlari qo‘llaniladi. Ushbu tadbirlar Internet trafigini kuzatish, shubhali IP-manzillarni aniqlash, elektron dalillarni yig‘ish, fishing va “malware” hujumlarini tahlil qilish, kriptovalyuta operatsiyalarini monitoring qilish hamda raqamli platformalardagi xavfli faoliyatni aniqlash orqali amalga oshiriladi. AQSH, Yaponiya va Buyuk Britaniyada mazkur tadbirlar asosan sud sanksiyasi va inson huquqlarini himoya qilish prinsipi asosida o‘tkazilsa, Rossiya va Xitoyda davlat xavfsizligi ustuvor hisoblanib, markazlashgan raqamli nazorat mexanizmi keng qo‘llaniladi. Janubiy Koreya va Singapurda esa sun’iy intellekt va Big Data texnologiyalari asosida profilaktik kiberkuzatuv tizimi keng shakllangan.

Ushbu davlatlar qonunchiligi o‘rtasidagi asosiy farq raqamli kuzatuv darajasi, davlat nazorati va shaxsiy hayot daxlsizligiga e’tibor berilishi bilan ahamiyatlidir. AQSH, Yaponiya va Buyuk Britaniyada inson huquqlari va sud nazorati kuchli bo‘lib, elektron kuzatuv qonunchilik bilan cheklangan. Rossiya va Xitoyda esa davlat organlarining Internet va telekommunikatsiya tarmoqlari ustidan nazorati kengroq hisoblanadi. Janubiy Koreya va Singapurning ijobiy tomoni AI va avtomatlashtirilgan tahlil orqali kiberjinoyatlarni barvaqt prognoz qilish imkoniyati yuqori ekanligida namoyon bo‘ladi. Biroq, salbiy tomoni sifatida, raqamli monitoringning yuqori darajasi shaxsiy ma’lumotlar maxfiyligi bilan bog‘liq xavflarni keltirib chiqarishi mumkin. Shu jihatdan mazkur davlatlar tajribasi kiberxavfsizlikni ta’minlashda texnologiya, davlat nazorati va inson huquqlari o‘rtasida muvozanatni saqlash muhim ahamiyat kasb etadi.

Yuqorida sanab o‘tilgan davlatlarning vakolatli organlari tomonidan kiberjinoyatlarning oldini olish bilan bog‘liq tezkor-qidiruv tadbirlarini o‘tkazishda amaliyotda qo‘yidagi *huquqiy, tashkiliy* va *taktik* muammolar mavjudligi ma’lum bo‘ldi:

birinchidan, ko‘plab davlatlarda an’anaviy tezkor-qidiruv tadbirlari bo‘yicha normalar mavjud bo‘lsa-da, kibermakonda amalga oshiriladigan raqamli kuzatuv, onlayn monitoring, elektron ma’lumotlarni yashirin olish, “cloud-ma’lumotlar” bilan ishlash kabi harakatlarning huquqiy tartibi to‘liq shakllanmagan. Natijada huquqni muhofaza qiluvchi organlar amaliyotida protsessual noaniqliklar kelib chiqmoqda. Masalan, AQSHda elektron kuzatuv bo‘yicha keng vakolatlar mavjud bo‘lsa, Yevropa davlatlarida shaxsiy hayot daxlsizligiga oid cheklovlar kuchli hisoblanadi. Bu esa transmilliy kiberjinoyatlarni tergov qilishda huquqiy ziddiyatlarni keltirib chiqaradi;

ikkinchidan, kiberjinoyatlar bo‘yicha elektron dalillar juda tez o‘zgaruvchan xususiyatga ega. Log-fayllar, IP-manzillar, server ma’lumotlari yoki bulutli platformalarda saqlangan ma’lumotlar qisqa vaqt ichida o‘chirilishi yoki o‘zgartirilishi mumkin. Bu tezkor-qidiruv tadbirlarining samaradorligiga salbiy ta’sir ko‘rsatadi. Amaliyotda ayrim hollarda elektron dalilni olish jarayoni qonuniy tartibda rasmiylashtirilmagani sababli sud tomonidan ular nomaqbul dalil sifatida baholanmoqda. Ayniqsa kriptovalyuta operatsiyalari va “darknet” bilan bog‘liq jinoyatlarda bu muammo yaqqol namoyon bo‘ladi;

uchinchidan, kiberjinoyatlarni aniqlashda internet-provayderlar, ijtimoiy tarmoqlar, messenjerlar va xosting kompaniyalari muhim axborot manbai hisoblanadi. Biroq ayrim davlatlarda mazkur subyektlarning huquqni muhofaza qiluvchi organlar bilan hamkorlik qilish tartibi aniq belgilanmagan. Masalan, ayrim xalqaro platformalar foydalanuvchi ma’lumotlarini milliy huquqni muhofaza qiluvchi organlarga taqdim etishdan bosh tortadi yoki juda kech taqdim qiladi. Natijada tezkor-qidiruv tadbirlarini o‘tkazish jarayonida ortiqcha vaqt sarflanadi;

to‘rtinchidan, hozirgi kunda “predictive policing”, “facial recognition”, “AI-based surveillance” kabi sun’iy intellekt texnologiyalar kiberjinoyatlarni oldini olishda keng qo‘llanilmoqda. Biroq bunday texnologiyalar fuqarolarning shaxsiy hayoti daxlsizligi, axborot erkinligi va shaxsiy ma’lumotlar muhofazasiga xavf tug‘dirishi mumkin. Masalan, Xitoyda real-name registration, ommaviy raqamli monitoring tizimi kiberxavfsizlikni ta’minlashda samarali hisoblansa-da, inson huquqlari nuqtai nazaridan bahsli masala sifatida ko‘rilmoqda;

beshinchidan, kibermakondagi jinoyatlarning oldini olish uchun raqamli kriminalistika, “blockchain analysis”, “malware analysis”, “network forensics” va AI texnologiyalari bo‘yicha yuqori malakali mutaxassislar talab etiladi. Biroq ko‘plab davlatlarda huquqni muhofaza qiluvchi organlar xodimlarining texnik bilimlari yetarli emas. Hozirda rivojlanayotgan ayrim davlatlarda raqamli kriminalistika laboratoriyalari, zamonaviy server monitoringi tizimlari va “AI-based monitoring” texnologiyalari yetarli darajada rivojlanmagan.

Kibermakondagi jinoyatlarning oldini olish bo‘yicha tezkor-qidiruv tadbirlarini o‘tkazish amaliyotida kuzatilgan *huquqiy, tashkiliy, taktik* muammolarni hal etish borasida quyidagilar taklif etiladi:

Birinchidan, kibermakonda tezkor-qidiruv tadbirlarini o‘tkazishning alohida huquqiy mexanizmlarini joriy etish. Kiberjinoyatlarga qarshi kurashish maqsadida raqamli kuzatuv, Internet monitoringi, elektron ma’lumotlarni olish, cloud-ma’lumotlar bilan ishlash, kriptovalyuta operatsiyalarini kuzatish kabi harakatlarning aniq protsessual tartibini belgilash maqsadga muvofiq. Buning uchun milliy qonunchilikka “*kiber tezkor-qidiruv tadbirlari*” tushunchasini kiritish va ularni amalga oshirish asoslari, muddatlari, sud sanksiyasi hamda nazorat tartibini belgilash zarur. Masalan, Janubiy

Koreyada elektron monitoring va “AI-based cyber investigation” bo‘yicha maxsus raqamli mexanizmlar joriy etilgan.

Ikkinchidan, elektron dalillar bilan ishlashning yagona raqamli standartini ishlab chiqish. Elektron dalillarni yig‘ish, saqlash, identifikatsiya qilish, ekspertiza qilish, sudga taqdim etish bo‘yicha yagona raqamli standart joriy etish lozim. Xususan, «hash verification», «blockchain timestamp» va «chain of custody» tizimlarini qo‘llash elektron dalillarning haqiqiyligini ta’minlashga xizmat qiladi. Masalan, Singapur va Yaponiyada raqamli kriminalistika laboratoriyalari elektron dalillarni avtomatik himoya qilish tizimlari bilan jihozlangan.

Uchinchidan, internet-provayderlar va raqamli platformalar bilan majburiy kiberxavfsizlik hamkorligini kuchaytirish. Kiberjinoyatlarni tezkor aniqlash maqsadida internet-provayderlar, bank platformalari, ijtimoiy tarmoqlar va xosting kompaniyalarining huquqni muhofaza qiluvchi organlar bilan hamkorlik qilish tartibini kuchaytirish zarur. Eng avvalo, elektron ma’lumotlarni saqlash muddatini belgilash, shubhali trafik haqida avtomatik xabar berish, fishing platformalarini tezkor bloklash, kiberjinoyatlar bo‘yicha yagona axborot bazasini yaratish maqsadga muvofiq deb hisoblaymiz. Masalan, Singapur va Janubiy Koreyada «ISP cooperation» mexanizmi yuqori darajada shakllangan.

To‘rtinchidan, “AI-based monitoring” va “predictive policing” kabi sun’iy intellekt texnologiyalarini inson huquqlari kafolatlari asosida joriy etish. Sun’iy intellekt asosida kiberkuzatuv tizimlarini joriy etishda sud sanksiyasini belgilash, mustaqil nazorat organlarining vakolatlarini, shaxsiy ma’lumotlar muhofazasi va algoritmlar shaffofligi kabi huquqiy kafolatlarni mustahkamlash zarur. Bu bir tomondan kiberjinoyatlarni barvaqt aniqlash imkonini bersa, ikkinchi tomondan inson huquqlari buzilishining oldini oladi. Masalan, bugun Yevropa davlatlarida sun’iy tizimlar ustidan qat’iy huquqiy nazorat amalga oshirilmoqda.

Beshinchidan, kibertergov va raqamli kriminalistika sohasida maxsus kadrlar tayyorlash tizimini rivojlantirish. Kiberjinoyatlarni fosh etish samaradorligini oshirish maqsadida: kibertergov, raqamli kriminalistika, blokcheyn kriminalistikasi, zararli dasturlarni tahlil qilish, tarmoq razvedkasi, sun’iy intellekt asosida kibertahlil yo‘nalishlari bo‘yicha maxsus ta’lim va amaliy trening tizimlarini joriy qilish lozim. Shuningdek, huquqni muhofaza qiluvchi organlar huzurida raqamli simulyatsion markazlar va kiberpoligonlar tashkil etish maqsadga muvofiq. Masalan, Janubiy Koreya va Singapurda kiberpolitsiya xodimlari uchun doimiy AI asosidagi o‘quv-trening tizim (AI-based training) markazlari tashkil etilgan bo‘lib, bu kiberjinoyatlarni tezkor fosh etish samaradorligini oshirmoqda.

Xulosa qilib aytganda, AQSH, Rossiya Fyederatsiyasi, Janubiy Koreya, Xitoy, Yaponiya, Buyuk Britaniya hamda Singapur kabi davlatlarda kiberjinoyatlarga qarshi kurashish sohasida zamonaviy tezkor-qidiruv mexanizmlari rivojlangan. Xususan, mazkur davlatlarda kiberjinoyatlarni tezkor aniqlashda 10–35 tagacha tezkor-qidiruv tadbirlari o‘tkazilishi muhim ahamiyatga ega.

Qiyosiy-huquqiy tahlil natijalari ayrim davlatlarda raqamli kuzatuv va telekommunikatsiya ma’lumotlarini nazorat qilish bo‘yicha keng vakolatlar mavjudligini, boshqa davlatlarda esa inson huquqlari va shaxsiy ma’lumotlar daxlsizligini ta’minlashga ustuvor ahamiyat berilishini ko‘rsatdi. Bu esa kiberxavfsizlikni ta’minlash hamda fuqarolarning konstitutsiyaviy huquq va erkinliklari o‘rtasida muvozanat saqlash zarurligini anglatadi.

Umuman olganda, kiberjinoyatlarning oldini olishda tezkor-qidiruv tadbirlarini huquqiy tartibga solishni takomillashtirish, zamonaviy axborot texnologiyalari va sun’iy intellekt imkoniyatlarini huquqni muhofaza qiluvchi organlar faoliyatiga joriy etish, shuningdek, xorijiy davlatlarning ilg‘or tajribasidan samarali foydalanish O‘zbekistonda kiberxavfsizlikni ta’minlash va kiberjinoyatchilikka qarshi kurashish samaradorligini yanada oshirishga xizmat qiladi.

Foydalanilgan manbalar / References

1. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace. – Santa Barbara: Praeger Publishers, 2010. – 294 p.
2. Creemers R. China's Cybersecurity Law: An Analysis. – Beijing: New America Foundation, 2018. – 74 p.
3. Cyber Security Agency of Singapore. Singapore Cyber Landscape 2025. –Singapore, 2025. –132 p. https://www.csa.gov.sg (Elektron manbaga murojaat qilingan vaqt: 06.05.2026).
4. Federal Bureau of Investigation (FBI). Internet Crime Report 2025. –Washington D.C., 2025. –87 p. https://www.ic3.gov (Elektron manbaga murojaat qilingan vaqt: 07.05.2026).
5. Holt T.J., Bossler A.M., Seigfried-Spellar K.C. Cybercrime and Digital Forensics: An Introduction. – New York: Routledge, 2022. – 540 p.
6. Japan. Basic Act on Cybersecurity. – Tokyo, 2014. https://www.japaneselawtranslation. go.jp (Elektron manbaga murojaat qilingan vaqt: 05.05.2026).
7. Korea Internet & Security Agency (KISA). Cyber Security Report 2025. – Seoul, 2025. – 156 p. https://www.kisa.or.kr (Elektron manbaga murojaat qilingan vaqt: 08.05.2026).
8. National Police Agency of Japan. Cybercrime Situation Report 2025. – Tokyo, 2025. – 98 p. https://www.npa.go.jp (Elektron manbaga murojaat qilingan vaqt: 09.05.2026).
9. People's Republic of China. Cybersecurity Law of the People's Republic of China. – Beijing, 2017. http://www.npc.gov.cn (Elektron manbaga murojaat qilingan vaqt: 10.05.2026).
10. Republic of Korea. Act on Promotion of Information and Communications Network Utilization and Information Protection. – Seoul, 2001. https://elaw.klri.re.kr (Elektron manbaga murojaat qilingan vaqt: 11.05.2026).
11. Singapore. Cybersecurity Act 2018. – Singapore, 2018. https://sso.agc.gov.sg (Elektron manbaga murojaat qilingan vaqt: 12.05.2026).
12. United Kingdom. Investigatory Powers Act 2016. – London, 2016. https://www.legislation.gov.uk/ukpga/2016/25/contents (Elektron manbaga murojaat qilingan vaqt: 13.05.2026).
13. United States Congress. Computer Fraud and Abuse Act (CFAA), 18 U.S.C. §1030. – Washington D.C., 1986. https://www.law.cornell. edu/ uscode/ text/18/1030 (Elektron manbaga murojaat qilingan vaqt: 14.05.2026).
14. USA Patriot Act. Public Law 107–56. – Washington D.C., 2001. https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (Elektron manbaga murojaat qilingan vaqt: 15.05.2026).
15. Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. – Cambridge: Polity Press, 2024. – 312 p.
16. World Economic Forum. Global Cybersecurity Outlook 2026. – Geneva, 2026. Электрон манзил: https://www.weforum.org/reports/global-cybersecurity-outlook-2026/ (murojaat qilingan sana: 16.05.2026).
17. Батурин Ю.М. Проблемы компьютерной преступности. – Москва: Юридическая литература, 1991. – 248 с.
18. Крылов В.В. Информационные компьютерные преступления. – Москва: Норма, 1997. – 286 с.
19. Матчанов А.А., Закиров Б.Э. Роль Интерпола в координации международного сотрудничества в борьбе с киберпреступностью // JMBM. – 2022. – №4. URL: https://cyberleninka.ru/article/n/rol-interpola-v-koordinatsii-mezhdunarodnogo-sotrudnichestva-v-borbe-s-kiberprestupnostyu (дата обращения: 17.05.2026).
20. Tursunov A.S. Kiberjinoyatchilikka qarshi kurashishning huquqiy va tashkiliy asoslari. – Toshkent: TDYU nashriyoti, 2022. – 268 b.
21. O‘zbekiston Respublikasining 2003-yil 11-dekabrdagi 560-II-son “Axborotlashtirish to‘g‘risida”gi qonuni // Elektron manba: URL: http://www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 18.05.2026).
22. O‘zbekiston Respublikasining 2012-yil 25-dekabrdagi O‘RQ-344-son “Tezkor-qidiruv faoliyati to‘g‘risida”gi qonuni // Elektron manba: URL: http://www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 19.05.2026).
23. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi qonuni // Elektron manba: URL: http://www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 20.05.2026).
24. O‘zbekiston Respublikasining 2023-yil 30-aprelda qabul qilingan yangi tahrirdagi Konstitutsiyasi // URL: http://www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 21.05.2026).
25. O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi // URL: http://www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 22.05.2026).
26. O‘zbekiston Respublikasi Oliy sudi Plenumining 2018-yil 24-avgustdagi “Dalillar maqbulligiga oid jinoyat-protsessual qonuni normalarini qo‘llashning ayrim masalalari to‘g‘risida”gi 24-son qarori // Elektron manba: URL: http://www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 22.05.2026).
27. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktyabrdagi PF-6079-son “Raqamli O‘zbekiston – 2030 strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi farmoni // URL: http://www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 22.05.2026).
28. O‘zbekiston Respublikasi Prezidentining 2021-yil 17-fevraldagi PQ-4996-son “Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to‘g‘risida”gi qarori // URL: http://www.lex.uz (Elektron manbaga murojaat qilingan vaqt: 22.05.2026).
29. Российская Федерация. Федеральный закон “Об информации, информационных технологиях и о защите информации”. – Москва, 2006. Электрон манзил: http://www.consultant.ru/document/cons_doc_LAW 61798
30. Российская Федерация. Федеральный закон “Об оперативно-розыскной деятельности”. – Москва, 1995. Электрон манзил: http://www.consultant.ru/ document/ cons doc LAW 7519