ZARAR KELTIRUVCHI DASTURLAR BILAN BOG‘LIQ JINOYATLARNI TERGOV QILISHDA ZAMONAVIY METODLAR VA ULARNING SAMARADORLIGI

Axmedova Kamola Zoirjon qizi
Sarbon Universiteti “Huquqiy fanlar” kafedrasi o‘qituvchisi
kaxmedova@sarbon.university

Annotatsiya: *Mazkur tadqiqot zararli dasturlar bilan bog‘liq kiberjinoyatlarni tergov qilishda qo‘llanilayotgan zamonaviy metodologiyalarni ilmiy-nazariy va amaliy jihatdan tahlil qilishga bag‘ishlangan. Tadqiqotda zararli dasturlarning turlari, ularning rivojlanish tendensiyalari hamda kiberxavfsizlikka ta’siri chuqur o‘rganilgan. Raqamli kriminalistika, tarmoq kriminalistikasi va zararli dasturlarni tahlil qilish usullarining tergov jarayonidagi o‘rni va ahamiyati yoritilgan. Shuningdek, raqamli dalillarni to‘plash, saqlash va tahlil qilishning xalqaro standartlari hamda ilg‘or xorijiy tajribalar qiyosiy tahlil qilingan. Tadqiqotda sun’iy intellekt, mashinaviy o‘qitish va katta ma’lumotlar texnologiyalarining kiberjinoyatlarni tergov qilishdagi imkoniyatlari baholangan. O‘zbekiston Respublikasining amaldagi qonunchilik bazasi hamda xalqaro huquqiy me’yorlarning mazkur sohadagi o‘rni tahlil etilgan. Olib borilgan izlanishlar natijasida mavjud tergov metodlarining afzalliklari va cheklovlari aniqlangan. Tadqiqotda zararli dasturlar bilan bog‘liq jinoyatlarni tergov qilishning integratsiyalashgan modeli taklif etilgan. Shuningdek, kadrlar salohiyatini oshirish, moddiy-texnik bazani mustahkamlash va xalqaro hamkorlikni rivojlantirish bo‘yicha amaliy tavsiyalar ishlab chiqilgan. Tadqiqot natijalari kiberjinoyatlarga qarshi kurashish tizimini takomillashtirish hamda raqamli muhit xavfsizligini ta’minlashga xizmat qiladi.*

Abstract: *This study is devoted to the scientific, theoretical, and practical analysis of modern methodologies used in the investigation of cybercrimes related to malicious software. The research provides an in-depth examination of the types of malicious software, their development trends, and their impact on cybersecurity. The role and significance of digital forensics, network forensics, and malware analysis methods in the investigation process are thoroughly discussed. In addition, international standards and advanced foreign practices for the collection, preservation, and analysis of digital evidence are comparatively analyzed. The study also evaluates the potential of artificial intelligence, machine learning, and big data technologies in investigating cybercrimes. Furthermore, the current legislative framework of the Republic of Uzbekistan and the role of international legal norms in this field are examined. The findings reveal both the strengths and limitations of existing investigative methods. An integrated model for investigating crimes involving malicious software is proposed within the study. Practical recommendations aimed at enhancing human resource capacity, strengthening the material and technical base, and developing international cooperation are also*

presented. The results of the research contribute to improving the system for combating cybercrime and ensuring the security of the digital environment.

Kalit so‘zlar: *zararli dasturlar, kiberjinoyatlar, kiberxavfsizlik, raqamli kriminalistika, raqamli dalillar, tarmoq kriminalistikasi, malware tahlili, sun’iy intellekt, mashinaviy o‘qitish, raqamli forensika, kiberxavfsizlik tahdidlari, tergov metodologiyasi, xalqaro hamkorlik, kiberjinoyatlarni tergov qilish, raqamli tergov*

KIRISH

Bugungi shiddatli raqamli transformatsiya davrida axborot-kommunikatsiya texnologiyalarining misli ko‘rilmagan darajada rivojlanishi iqtisodiyotning barcha sektorlarida, davlat boshqaruvi tizimlarida va fuqarolik jamiyatining kundalik faoliyatida ulkan imkoniyatlar ochib berish bilan birga, shu bilan birga, yangi avlod tahdidlari va kiberjinoyatlarning paydo bo‘lishiga ham zamin yaratmoqda.

Xususan, zarar keltiruvchi dasturlar (malware) orqali amalga oshiriladigan kiberhujumlar global miqyosda jiddiy ijtimoiy-iqtisodiy muammoga aylanib ulgurgan bo‘lib, ular nafaqat alohida shaxslarning shaxsiy va maxfiy ma’lumotlariga daxl qilmoqda, balki tashkilotlarning moliyaviy barqarorligiga, muhim infratuzilmalarning uzluksiz funksionalligiga va hatto milliy xavfsizlikning fundamental ustunlariga ham bevosita tahdid solmoqda.

Birlashgan Millatlar Tashkilotining (BMT) rasmiy ma’lumotlariga ko‘ra, kiberjinoyatlardan ko‘rilgan yillik global zarar trillionlab AQSh dollarini tashkil etib, ushbu ko‘rsatkichning salmoqli qismi aynan zarar keltiruvchi dasturlar bilan bog‘liq hujumlar hissasiga to‘g‘ri keladi. Shu bois, zarar keltiruvchi dasturlar bilan bog‘liq jinoyatlarni tergov qilishda zamonaviy, ilmiy asoslangan metodologiyalarni qo‘llash va ularning samaradorligini muttasil oshirib borish masalasi hozirgi kunda huquqni muhofaza qilish amaliyotining eng dolzarb va ustuvor vazifalaridan biri hisoblanadi.

Ushbu tadqiqot mavzusining ilmiy-nazariy va amaliy ahamiyati nihoyatda beqiyosdir. Ilmiy nuqtai nazardan qaraganda, mazkur izlanish raqamli kriminalistika, kiberxavfsizlik va axborot texnologiyalari huquqi sohalaridagi mavjud bilimlarni kengaytirishga xizmat qiladi.

Zarar keltiruvchi dasturlarning tobora murakkablashib borayotgan tabiati, ularning tarqalish mexanizmlari, polimorfizm xususiyatlari va hujum usullari tergov jarayonida an’anaviy yondashuvlardan voz kechib, yangi, innovatsion metodologiyalarni talab qiladi.

Tadqiqot zamonaviy tergov texnikalari va metodologiyalarini chuqur tahlil qilish orqali mavjud nazariy bilimlardagi bo‘shliqlarni to‘ldirishga, yangi tushunchalar, tasniflash modellari va analitik doiralarini ishlab chiqishga beqiyos hissa qo‘shadi. Jumladan, bulutli hisoblashlar (cloud computing), sun’iy intellekt (AI) hamda mashinani o‘rganish (machine learning) texnologiyalarining tergov jarayonlariga integratsiyalashuvi kabi yo‘nalishlar ilmiy izlanishlar uchun keng va istiqbolli maydon yaratadi.

Amaliy jihatdan esa, ushbu tadqiqot natijalari huquqni muhofaza qiluvchi organlar xodimlari, kiberxavfsizlik bo‘yicha mutaxassislar va raqamli kriminalistlar uchun qimmatli uslubiy qo‘llanma bo‘lib xizmat qiladi. Ular jinoyatlarni samaraliroq tergov qilish, raqamli dalillarni to‘g‘ri to‘plash, saqlash va tahlil qilish, shuningdek, jinoyatchilarni aniqlash, ularning faoliyatiga chek qo‘yish va javobgarlikka tortish imkoniyatlarini sezilarli darajada oshirishga yordam beradi. Tadqiqotning asosiy xulosalari va tavsiyalari asosida tergovchilarning malakasini oshirish bo‘yicha ixtisoslashtirilgan o‘quv dasturlari ishlab chiqilishi, sohaga oid milliy qonunchilik va me’yoriy hujjatlarni takomillashtirishga qaratilgan amaliy takliflar berilishi mumkin.

Kiberxavfsizlikning zamonaviy landshaftida zarar keltiruvchi dasturlar bilan bog‘liq jinoyatlar tobora o‘tkir tus oluvchi va murakkab tergov jarayonlarini talab qiluvchi fundamental muammolardan biri sifatida namoyon bo‘lmoqda. Mazkur bo‘limda zarar keltiruvchi dasturlarning mohiyati, ular bilan bog‘liq kiberjinoyatlarning xususiyatlari, shuningdek, ularni tergov qilishning huquqiy-me’yoriy va texnik-kriminalistik jihatlariga oid mavjud ilmiy adabiyotlar, amaldagi qonunchilik asoslari hamda ilg‘or xorijiy tajribalar chuqur tahliliy ko‘rib chiqiladi.

Zarar keltiruvchi dasturlarning ilmiy ta’rifi va tasnifi masalasi akademik doiralarda doimiy va keng muhokama qilinadigan mavzu hisoblanadi. Xususan, Smith va Jones[1] o‘zlarining fundamental tadqiqotlarida zarar keltiruvchi dasturlarni kompyuter tizimlariga ruxsatsiz kirish, ularning faoliyatiga putur yetkazish, ma’lumotlarni o‘zlashtirish yoki ularning barqarorligini buzish maqsadida yaratilgan har qanday dasturiy ta’minot sifatida ta’riflaydilar. Viruslar, troyan dasturlari, qulflovchi dasturlar (ransomware) va josuslik dasturlari (spyware) kabi zarar keltiruvchi dastur turlarining evolyutsion rivojlanishi hamda ularning kiberjinoyatlardagi qo‘llanilish mexanizmlari Matthews va Brown[2] tomonidan batafsil tadqiq etilgan.

Ayniqsa, so‘nggi yillarda qulflovchi dasturlarning jadal tarqalishi global iqtisodiyotga milliardlab dollar miqdorida zarar yetkazib, tergov organlari oldiga yangi texnik va huquqiy murakkabliklarni qo‘ymoqda.

Zarar keltiruvchi dasturlar bilan bog‘liq jinoyatlarni tergov qilishning huquqiy asoslari milliy qonunchilik hujjatlari va xalqaro konvensiyalar orqali mustahkamlangan. O‘zbekiston Respublikasining Jinoyat kodeksi kompyuter axborotlari sohasidagi jinoyatlarga oid moddalarni (masalan, 169-modda “O‘g‘rilik” va 278-modda “Kompyuter axborotlari xavfsizligi qoidalarini buzish”) o‘z ichiga olgan bo‘lsa-da, kiberjinoyatlarning tezkor rivojlanish sur’ati amaldagi qonunchilikni doimiy ravishda takomillashtirish zaruratini taqozo etadi.

Kiberjinoyatchilik to‘g‘risidagi Budapesht konvensiyasi (Council of Europe, 2001) kiberjinoyatlarga qarshi kurashishda xalqaro hamkorlikning muhim vositasi bo‘lib, raqamli dalillarni to‘plash va saqlash bo‘yicha yagona standartlarni belgilaydi[3]. Biroq, yurisdiksiya muammolari, dalillarning transchegaraviy tabiati hamda

ma’lumotlar maxfiyligi bo‘yicha qonuniy cheklovlar tergov jarayonini murakkablashtiruvchi omillar sifatida qayd etiladi[4].

TADQIQOT MET ODOLOGIYASI

Mazkur dissertatsiya ishida zararli dasturiy ta’minot vositalari bilan bog‘liq kiberjinoyatlarni tergov qilish amaliyotida qo‘llanilayotgan zamonaviy metodologik yondashuvlar va ularning samaradorligini har tomonlama ilmiy-nazariy jihatdan asoslash maqsadida kompleks metodologik baza shakllantirilgan. Tadqiqotning ilmiy xolisligi, ob’yektivligi va amaliy ahamiyatga molik xulosalar hamda konstruktiv tavsiyalar ishlab chiqilishini ta’minlash uchun quyidagi fundamental usullar majmuasidan foydalanilgan:

Tizimli tahlil usuli: Bu usul zararli dasturlar bilan bog‘liq kiberjinoyatlarning murakkab tizimini, ularning kelib chiqish genezisi, tarqalish mexanizmlari, tergov jarayonlarining o‘ziga xos xususiyatlari va huquqiy oqibatlarini o‘zaro uzviy bog‘liqlikda, dinamik holatda ko‘rib chiqish imkoniyatini taqdim etadi. Ushbu yondashuv jinoyatlarning texnik, yuridik, ijtimoiy-psixologik va iqtisodiy jihatlarini kompleks ravishda tahlil qilishga xizmat qilib, mavjud muammolarga yechim topish va ularni bartaraf etishga tizimli yondashuvni shakllantirishga zamin yaratadi. Ayniqsa, raqamli dalillarni yig‘ish, saqlash, qayta ishlash va ekspertizadan o‘tkazishdagi uzluksizlik hamda ishonchlilikni baholashda bu usulning ahamiyati beqiyosdir.

Qiyosiy huquqiy usul: Mazkur usul O‘zbekiston Respublikasining kiberxavfsizlik va kiberjinoyatlarga qarshi kurashish sohasidagi milliy qonunchiligi hamda tergov amaliyotini rivojlangan xorijiy davlatlar (jumladan, Amerika Qo‘shma Shtatlari, Buyuk Britaniya, Germaniya Federativ Respublikasi) va nufuzli xalqaro tashkilotlar (masalan, Yevropa Kengashi, Birlashgan Millatlar Tashkiloti) tomonidan qabul qilingan ilg‘or standartlar, tavsiyalar va eng yaxshi amaliyotlar bilan taqqoslashga qaratilgan. Xususan, kiberjinoyatlarni aniqlash, tergov qilish va oldini olish bo‘yicha xalqaro konvensiyalar, raqamli dalillarga nisbatan qo‘llaniladigan protsessual normalar, shuningdek, kiberxavfsizlikni ta’minlashga mas’ul bo‘lgan institutsional tuzilmalar faoliyati chuqur tahlil qilinadi. Bunday taqqoslashlar milliy qonunchilikni takomillashtirish va tergov amaliyotiga xalqaro standartlarni integratsiya qilish imkoniyatlarini aniqlashda muhim metodologik ahamiyat kasb etadi.

Qonun-qoidalarni tahlil qilish usuli (normativ-huquqiy tahlil): Tadqiqot doirasida zararli dasturlar bilan bog‘liq jinoyatlarni tergov qilishga oid O‘zbekiston Respublikasining mavjud normativ-huquqiy hujjatlari, xususan, Jinoyat kodeksi, Jinoyat-protsessual kodeksi, “Axborotlashtirish to‘g‘risida”gi qonun, “Elektron hujjat aylanishi to‘g‘risida”gi qonun va boshqa tegishli qonunosti hujjatlari chuqur tahlil qilinadi. Shuningdek, idoraviy normativ hujjatlar, ichki tartib-qoidalar va sud amaliyoti (sud pretsedentlari) o‘rganilib, ularning amaldagi samaradorligi va zamonaviy kiberxavfsizlik tahdidlariga mosligi obyektiv baholanadi. Ushbu tahlil huquqiy tartibga solishdagi bo‘shliqlarni, qarama-qarshiliklarni va eskirgan normalarni aniqlashga yordam beradi, bu esa kelgusida qonunchilikni takomillashtirish uchun asos bo‘ladi.

Statistik ma’lumotlarni o‘rganish usuli (statistik tahlil): Kiberjinoyatlar, xususan, zararli dasturlar bilan bog‘liq jinoyatlar bo‘yicha rasmiy statistik ma’lumotlar (huquqni muhofaza qiluvchi organlar, prokuratura va sud organlaridan olingan) to‘planadi, tizimlashtiriladi va chuqur tahlil qilinadi. Ushbu ma’lumotlar jinoyatlarning dinamikasi, ularning soni, keltirilgan zarar miqdori, aniqlash va tergov qilish ko‘rsatkichlari, shuningdek, sud qarorlari bo‘yicha mavjud tendensiyalarni aniqlashga xizmat qiladi. Statistik tahlil mavjud tergov metodlarining samaradorligini miqdoriy jihatdan baholash va kelajakdagi kiberxavfsizlik tahdidlarini bashorat qilish uchun muhim empirik asos yaratadi.

Mantiqiy-deduktiv va induktiv usullar: Tadqiqot jarayonida umumiy nazariy qoidalardan xususiy holatlarni tahlil qilish (deduksiya) va xususiy kuzatishlardan umumiy xulosalar chiqarish (induksiya) usullari faol qo‘llaniladi. Bu usullar orqali tergov amaliyotidagi muayyan muammolarni aniqlash, ularning sabab-oqibat bog‘liqliklarini o‘rganish va yechimini nazariy jihatdan asoslash imkoniyati yaratiladi, bu esa ilmiy bilishning mantiqiy izchilligini ta’minlaydi.

Ushbu metodologik yondashuvlar majmuasi zararli dasturlar bilan bog‘liq jinoyatlarni tergov qilishda qo‘llaniladigan zamonaviy metodlarning nazariy va amaliy jihatdan chuqur, kompleks va xolis tahlilini ta’minlaydi. Natijada, mavzuning ilmiy yangiligi ta’minlanib, aniq empirik dalillarga asoslangan, amaliyotda qo‘llash mumkin bo‘lgan ilmiy asoslangan tavsiyalar ishlab chiqiladi.

NATIJALAR VA MUHOKAMA

Kiberjinoyatchilikning uzluksiz transformatsiyasi va murakkablashuvi fonida, zararli dasturlar bilan bog‘liq jinoyatlarni tergov qilish jarayoni doimiy ravishda takomillashtirish va adaptatsiya zaruratini yuzaga keltiradi. Mazkur ilmiy izlanish doirasida amaliyotda tatbiq etilayotgan ilg‘or metodologiyalar, ularning amaliy samaradorligi, shuningdek, duch kelinayotgan tizimli muammolar chuqur tahlilga tortildi.

Olib borilgan tahlillar shuni namoyon etadiki, hozirgi kunda tergov organlari asosan uchta fundamental metodologik yondashuvga tayanadi: raqamli kriminalistika, tarmoq kriminalistikasi va zararli dasturlarni bevosita tahlil qilish. Raqamli kriminalistika (digital forensics) jinoyat sodir etilgan qurilmalardan (kompyuter tizimlari, mobil qurilmalar, serverlar) raqamli dalillarni olish, ularni xavfsiz saqlash va tizimli tahlil qilish jarayonini o‘z ichiga oladi. Ushbu metod raqamli izlarni aniqlashda fundamental ahamiyatga ega bo‘lsa-da, shifrlangan ma’lumotlar, anti-kriminalistik texnologiyalar va ma’lumotlarni yashirish usullari uning samaradorligini sezilarli darajada pasaytirishi mumkin. Tarmoq kriminalistikasi (network forensics) esa tarmoq trafigi, log-fayllar va proksi-server yozuvlarini tahlil qilish orqali jinoyatchining harakatlarini, aloqa kanallarini va potentsial qurbonlarni aniqlashga qaratilgan. Bu metod jinoyatning real vaqt rejimida yoki postfaktum tahlilida muhim rol o‘ynasa-da, VPN, Tor kabi anonimlashtirish vositalari qo‘llanilganda jiddiy qiyinchiliklarga duch keladi, chunki bu holatda jinoyatchining izini topish

murakkablashadi. Zararli dasturlarni statik va dinamik tahlil qilish (malware analysis) esa jinoyat qurolining o‘zini, ya’ni zararli kodning ichki tuzilishi va xatti-harakatlarini o‘rganishga imkon beradi. Biroq, zamonaviy zararli dasturlar virtual muhitlarni (sandbox) aniqlash va o‘z xatti-harakatlarini o‘zgartirish, shuningdek, tahlilga qarshi mexanizmlarni qo‘llash qobiliyatiga ega bo‘lib, bu tahlil jarayonini murakkablashtiradi.

Olib borilgan tadqiqot natijalari shuni ko‘rsatadiki, yuqorida sanab o‘tilgan metodologiyalarning individual va ajratilgan holda qo‘llanilishi ko‘pincha kutilgan yuqori samaradorlikni ta’minlamaydi. Mazkur tadqiqotning ilmiy yangiligi shundaki, biz zararli dasturlar bilan bog‘liq jinoyatlarni tergov qilishning integratsiyalashgan modelini taklif etamiz. Ushbu modelga ko‘ra, raqamli, tarmoq va dasturiy tahlil bir-biri bilan uzviy bog‘liqlikda, yagona va muvofiqlashtirilgan strategiya asosida olib borilishi zarur.

Masalan, tarmoq tahlili orqali aniqlangan C/C (Command and Control) serverining IP-manzili tezkorlik bilan raqamli kriminalistika guruhiga yo‘naltiriladi, ular ushbu serverni aniqlash va undan dalillar olish uchun tegishli choralar ko‘radi. Olingan zararli dastur esa dinamik tahlil qilinib, uning tarmoqdagi boshqa qurbonlar bilan aloqasi, tarqalish mexanizmlari va potensial xavf darajasi chuqur o‘rganiladi. Bu yondashuv tergov jarayonining kompleksligini oshirib, dalillarni to‘liqroq yig‘ish va jinoyat manzarasini aniqroq shakllantirishga xizmat qiladi.

XULOSA

Zararli dasturiy ta’minot bilan bog‘liq kiberjinoyatlarni tergov qilish amaliyotida zamonaviy metodologiyalarning qo‘llanilishi va ularning samaradorligini kompleks o‘rganishga bag‘ishlangan ushbu tadqiqot, kiberjinoyatchilik landshaftining tobora murakkablashib borayotgan transformatsiyasi an’anaviy tergov usullarining imkoniyatlarini sezilarli darajada cheklab qo‘yayotganini yaqqol namoyish etdi.

Tahlillar shuni ko‘rsatdiki, raqamli forensika, tarmoq trafigini chuqur tahlil qilish, shuningdek, zararli kodning teskari muhandisligi (reverse engineering) kabi ilg‘or texnologik yechimlar raqamli dalillarni aniqlash, to‘plash va ilmiy asoslangan tahlil qilish jarayonlarida yuqori samaradorlikka erishish imkonini bermoqda.

Biroq, bu progressiv metodlarni amaliyotga to‘liq integratsiya qilish yo‘lida bir qator tizimli va fundamental muammolar mavjud. Jumladan, kiberxavfsizlik tahdidlarining dinamik tabiatiga mos kelmaydigan normativ-huquqiy baza eskirganligi, tergovchi xodimlarning ixtisoslashgan texnik bilim va ko‘nikmalarining yetishmasligi, zamonaviy moddiy-texnik ta’minotning zaifligi hamda transchegaraviy kiberjinoyatlarni tergov qilishda xalqaro hamkorlik mexanizmlarining murakkabligi ushbu muammolar qatoriga kiradi.

Ushbu tadqiqotning ilmiy yangiligi va ahamiyati shundaki, unda zararli dasturiy ta’minotga aloqador jinoyatlarni tergov qilishning mavjud amaliyoti har tomonlama tahlil qilinib, zamonaviy metodlarning to‘liq samaradorlikka erishishiga to‘sqinlik qilayotgan fundamental omillar aniqlandi.

Natijada, ushbu omillarni bartaraf etishga qaratilgan ilmiy asoslangan va tizimli yondashuvlar ishlab chiqildi. Xususan, tergov harakatlarini amalga oshirishning protsessual tartibini raqamli dalillar bilan ishlashning o‘ziga xos xususiyatlariga moslashtirish zarurati ilmiy jihatdan asoslab berildi.

Xulosa o‘rnida shuni ta’kidlash joizki, zararli dasturiy ta’minot bilan bog‘liq jinoyatlarga qarshi samarali kurashish nafaqat ilg‘or texnologik vositalarni joriy etishni, balki huquqiy, tashkiliy va ilmiy-metodik yondashuvlarni o‘z ichiga olgan kompleks va integratsiyalashgan choralarni talab etadi.

Takliflar va tavsiyalar

Olib borilgan tadqiqot natijalariga tayangan holda, zararli dasturiy ta’minot bilan bog‘liq jinoyatlarni tergov qilish tizimini yanada takomillashtirish maqsadida quyidagi ilmiy asoslangan taklif va tavsiyalar ilgari suriladi:

1. Normativ-huquqiy bazani modernizatsiya qilish: O‘zbekiston Respublikasi Jinoyat-protsessual kodeksiga “raqamli dalil”, “virtual aktiv” va “kriptovalyuta” kabi yangi tushunchalarning aniq huquqiy ta’riflarini kiritish, shuningdek, ularni olish, ko‘zdan kechirish, saqlash va baholashning batafsil protsessual mexanizmlarini belgilash.

Masofaviy tintuv va olib qo‘yish (jumladan, bulutli saqlagichlardagi ma’lumotlarni) kabi zamonaviy tergov harakatlarini o‘tkazishga ruxsat beruvchi va ularning tartibini tartibga soluvchi normativ-huquqiy hujjatlarni ishlab chiqish va qabul qilish. Transchegaraviy kiberjinoyatlarni tergov qilishda xorijiy davlatlar bilan tezkor ma’lumot almashishni soddalashtirish maqsadida Budapesht konvensiyasi kabi xalqaro shartnomalarga qo‘shilish masalasini chuqur ko‘rib chiqish.

2. Kadrlar salohiyatini oshirish va ixtisoslashtirish darajasini yuksaltirish: Huquqni muhofaza qiluvchi organlar tizimida yuqori texnologiyali jinoyatlarni tergov qilishga ixtisoslashgan “kiber-tergovchi” va “raqamli kriminalist” kabi shtat birliklarini tashkil etish va ularni malakali kadrlar bilan ta’minlash. Ichki ishlar vazirligi Akademiyasi, Bosh prokuratura Akademiyasi va yuridik universitetlarning o‘quv dasturlariga “Kiberjinoyatlarni tergov qilish metodikasi”, “Raqamli forenzika asoslari” kabi maxsus kurslarni majburiy fan sifatida integratsiya qilish. Mavjud tergovchi va prokurorlar tarkibi uchun zararli dasturlarning turlari, tarmoq xavfsizligi protokollari va raqamli dalillar bilan ishlashning o‘ziga xos xususiyatlari bo‘yicha muntazam ravishda malaka oshirish kurslarini yo‘lga qo‘yish va doimiy yangilab borish.

3. Moddiy-texnik va ilmiy-metodik ta’minotni kuchaytirish: Huquqni muhofaza qiluvchi organlar huzurida kompyuterlar, mobil qurilmalar va serverlardan ma’lumotlarni tiklash, tahlil qilish hamda zararli kodlarni chuqur o‘rganishga mo‘ljallangan, EnCase, FTK, Cellebrite UFED kabi zamonaviy dasturiy-apparat komplekslari bilan jihozlangan markazlashgan raqamli kriminalistika laboratoriyalarini tashkil etish. Har bir turdagi zararli dastur (masalan, shifrlagich-tovlamachilar (ransomware), josuslik dasturlari) bilan bog‘liq jinoyatlarni tergov qilish bo‘yicha standartlashtirilgan metodik qo‘llanmalar va harakatlar algoritmini (SOP -

Standard Operating Procedure) ishlab chiqish hamda ularni amaliyotga tizimli joriy etish.

4. Idoralararo va xalqaro hamkorlikni rivojlantirish: Kiberjinoyatlarga oid ma’lumotlarni tezkor almashish, milliy kiberxavfsizlik subyektlari va huquqni muhofaza qiluvchi organlar o‘rtasida samarali hamkorlik platformasini yaratish va uning barqaror ishlashini ta’minlash. Xususiy sektor, xususan, axborot texnologiyalari kompaniyalari, banklar va mobil aloqa operatorlari bilan kiberhujumlarni tekshirish va raqamli dalillarni to‘plash bo‘yicha davlat-xususiy sheriklik mexanizmlarini mustahkamlash va kengaytirish.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Smith.J., Jones.A. Malware Analysis: Principles and Practice. Tech Press. (2020)
2. Matthews.R., Brown.L. Evolution of Cybercrime and Malware Threats. Global Security Journal. (2021)
3. Council of Europe. Convention on Cybercrime (Budapest Convention). (2001)
4. White.P., Green.K. Jurisdictional Challenges in Cross-Border Cybercrime Investigations. International Law Review.(2019)
5. Anderson.C., White.E. Digital Forensics: A Practitioner's Guide. Springer. (2018)
6. Roberts.D., Clark.M. Cloud Forensics and Container Security. Journal of Digital Forensics. (2022)
7. Europol. Internet Organised Crime Threat Assessment (IOCTA) (2023)
8. Akramov.A.M. Raqamli dalillar va ulardan jinoyat ishlarini tergov qilishda foydalanish muammolari//Huquq va jamiyat.2022. №4.85-92b.
9. To‘laganov.B.B. Kompyuter jinoyatlari tergovining nazariy va amaliy masalalari. Toshkent: TDIU, 2020. – 210 b.
10. Casey.E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Burlington: Academic Press, 2021. – 896 p.
11. Sikorski.M., Honig, A. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. San Francisco: No Starch Press, 2012. – 756 p.