KIBERXAVFSIZLIKKA QARSHI QARATILGAN JINOYATLARNI TERGOV QILISHDA ZARAR KELTIRUVCHI DASTURLAR TAHLILI

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

Annotatsiya: *Globallashuv sharoitida kiberxavfsizlikka qarshi qaratilgan jinoyatlar tobora kengayib, ularning xavflilik darajasi va ijtimoiy xavfi oshib bormoqda. Ayniqsa, zarar keltiruvchi dasturlardan foydalanish orqali sodir etilayotgan jinoyatlar raqamli makonda huquqbuzarliklarning yangi shakllarini yuzaga keltirmoqda. Mazkur tezis kiberjinoyatlarni tergov qilish samaradorligini oshirishda zarar keltiruvchi dasturlarni kriminalistik tahlil qilishning ilmiy-nazariy asoslarini ishlab chiqish va amaliy mexanizmlarini takomillashtirishga qaratilgan. Tadqiqot doirasida zarar keltiruvchi dasturlarning kriminalistik ahamiyati, ularni identifikatsiya qilish, klassifikatsiya qilish hamda tergov jarayonida raqamli dalil sifatida to‘plash va ekspertiza qilishning o‘ziga xos xususiyatlari chuqur o‘rganilgan. Kriminalistika, axborot texnologiyalari huquqi va raqamli forenzika sohalaridagi ilg‘or xorijiy va milliy tajriba qiyosiy tahlil qilinib, mavjud muammolar va kamchiliklar aniqlangan. Asosiy natija sifatida zarar keltiruvchi dasturlarning kriminalistik klassifikatsiyasi tizimi taklif etilgan bo‘lib, bu ularning turlarini aniqlash, faoliyat mexanizmlarini tushunish va jinoyatning izlarini izlashda amaliy ahamiyatga ega. Shuningdek, tergovga qadar tekshiruv va tergov jarayonida zarar keltiruvchi dasturlarni aniqlash, ularning funksional xususiyatlarini o‘rganish va jinoyat ishi bo‘yicha ahamiyatli ma’lumotlarni ajratib olish bo‘yicha metodik tavsiyalar ishlab chiqilgan.*

Kalit so‘zlar: *Kiberxavfsizlik, kiberjinoyat, malware, zararli dasturlar, raqamli makon, raqamli izlar, raqamli kriminalistika.*

Kirish

Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha jabhalariga chuqur singib, ulkan imkoniyatlar bilan birga misli ko‘rilmagan xavf-xatarlarni ham keltirib chiqarmoqda. Raqamli makonda sodir etilayotgan jinoyatlarning soni va murakkabligi geosiyosiy chegaralarni tan olmagan holda, global miqyosda o‘sib bormoqda. Ayniqsa, kiberxavfsizlikka qarshi qaratilgan jinoyatlarda zarar keltiruvchi dasturlar (malware) asosiy qurol sifatida qo‘llanilishi ularning xavflilik darajasini yanada oshirmoqda. Ushbu dasturlar nafaqat shaxsiy ma’lumotlar xavfsizligiga tahdid soladi, balki davlat miqyosidagi muhim infratuzilmalarning ishlashiga, iqtisodiy barqarorlikka va milliy xavfsizlikka ham jiddiy putur yetkazishi mumkin. Shunday sharoitda, mazkur turdagi jinoyatlarni samarali

tergov qilish va ularning oldini olish mexanizmlarini takomillashtirish dolzarb ahamiyat kasb etmoqda.

Kriminalistika fani va amaliyoti uchun zarar keltiruvchi dasturlar tahlili o‘ta muhim yo‘nalish hisoblanadi. An’anaviy tergov usullari raqamli dalillarni yig‘ish, tahlil qilish va ulardan xulosa chiqarishda ko‘pincha ojizlik qiladi. Jinoyat sodir etish mexanizmini to‘liq tushunish, jinoyatchilar shaxsini aniqlash, ularning maqsadlari va harakat usullarini ochib berishda zarar keltiruvchi dasturlarning texnik xususiyatlarini, tarqalish yo‘llarini va zarar yetkazish salohiyatini chuqur o‘rganish zarurati tobora ortib bormoqda. Raqamli izlarni to‘g‘ri sharhlash, ularning haqiqiyligini va yuridik ahamiyatini tasdiqlash tergov jarayonining ajralmas qismiga aylangan bo‘lib, bu sohada yuqori malakali mutaxassislarga va zamonaviy metodologiyalarga bo‘lgan ehtiyojni kuchaytirmoqda.

MATERIALLAR VA USULLAR

Mazkur tadqiqotning metodologik asosi kiberxavfsizlikka qarshi qaratilgan jinoyatlarni tergov qilishda zarar keltiruvchi dasturlarni tahlil qilishning nazariy va amaliy jihatlarini chuqur o‘rganishga qaratilgan bo‘lib, kriminalistika fanining umumiy qonuniyatlari hamda zamonaviy axborot texnologiyalari imkoniyatlarini uyg‘unlashtiradi. Tadqiqot jarayonida ilmiy bilishning dialektik usuli markaziy o‘rinni egalladi, bu esa o‘rganilayotgan hodisalarni ularning rivojlanishi va o‘zaro bog‘liqligida ko‘rib chiqish imkonini berdi.

Nazariy tadqiqot usullari doirasida mavzuga oid mahalliy va xorijiy adabiyotlar, qonunchilik hujjatlari, huquqni qo‘llash amaliyoti materiallari, shuningdek, kiberxavfsizlik va kriminalistika sohasidagi ilmiy-texnik nashrlar tizimli va qiyosiy tahlil qilindi. Bu usul zarar keltiruvchi dasturlarning evolyutsiyasi, ularni tergov qilishning huquqiy va uslubiy asoslari, shuningdek, xalqaro tajriba bilan tanishish imkoniyatini berdi. Induktiv va deduktiv yondashuvlar yordamida umumiy nazariy xulosalardan xususiy amaliy tavsiyalarga o‘tildi va aksincha, konkret holatlardan umumiy qonuniyatlar chiqarildi. Sintez usuli orqali turli manbalardan olingan ma’lumotlar yagona tizimga birlashtirilib, tadqiqotning butunligi ta’minlandi.

Empirik tadqiqot usullari sifatida sud-ekspertiza amaliyotida qo‘llaniladigan zarar keltiruvchi dasturlarni tahlil qilishning kriminalistik usullari va vositalari atroflicha o‘rganildi. Jumladan, amaliy misollar va keys-studiya tahlili yordamida kiberjinoyatlarni tergov qilishda zarar keltiruvchi dasturlar tahlilining o‘ziga xos xususiyatlari, yuzaga keladigan muammolar va ularni bartaraf etish yo‘llari chuqur tahlil qilindi. Modellashtirish usuli orqali zarar keltiruvchi dasturlarning tarqalish mexanizmlari, ularning kompyuter tizimlariga ta’siri va tergov jarayonidagi izlari vizuallashtirildi. Ekspert xulosalari va soha mutaxassislarining fikrlari umumlashtirilib, amaliy tavsiyalar ishlab chiqishda asosiy manba sifatida foydalanildi.

Shuningdek, tizimli-funksional tahlil usuli yordamida zarar keltiruvchi dasturlarni tergov qilish jarayonining har bir bosqichi alohida tizim elementlari

sifatida ko‘rib chiqildi va ularning o‘zaro bog‘liqligi hamda tergov samaradorligiga ta’siri baholandi. Bu usullar majmuasi tadqiqot mavzusini har tomonlama va ob’ektiv o‘rganish, uning nazariy va amaliy ahamiyatini asoslash, shuningdek, ilmiy jihatdan asoslangan xulosalar va amaliy tavsiyalar ishlab chiqish uchun mustahkam zamin yaratdi.

NATIJALAR

Tadqiqotning natijasi kiberxavfsizlikka qarshi qaratilgan jinoyatlarni tergov qilishda zarar keltiruvchi dasturlarning kriminalistik jihatlarini kompleks va tizimli tahlil qilishga qaratilgan yangi konseptual yondashuvni ilgari surish bilan belgilanadi. Jumladan, tadqiqot doirasida quyidagi ilmiy yangiliklar qo‘lga kiritilgan:

Birinchidan, zarar keltiruvchi dasturiy ta’minotning an’anaviy texnik tasniflaridan farqli o‘laroq, uning kriminalistik ahamiyatiga asoslangan mualliflik tasnifi ishlab chiqildi. Ushbu tasnif zarar keltiruvchi dasturlarni nafaqat funksional imkoniyatlari, balki jinoyat izlarini shakllantirish xususiyatlari, tergov jarayonida daliliy axborot manbai sifatidagi roli hamda jinoyat subyektini aniqlashdagi potentsialiga ko‘ra guruhlash imkonini beradi. Bu esa tergov taktikasini rejalashtirish va tergov versiyalarini ilgari surishda metodologik asos bo‘lib xizmat qiladi;

Ikkinchidan, “zarar keltiruvchi dasturning raqamli izlari” tushunchasiga kriminalistik ta’rif berilib, uning tuzilmasi, shakllanish mexanizmlari va jinoyat ishi bo‘yicha isbotlash jarayonidagi o‘rni ilmiy jihatdan asoslandi. Raqamli izlarni aniqlash, olish, tadqiq etish va protsessual mustahkamlash bo‘yicha amaliy tavsiyalarni o‘z ichiga olgan, tergov harakatlari va maxsus bilimlardan foydalanishni integratsiya qiluvchi taktik algoritm takomillashtirildi;

Uchinchidan, zarar keltiruvchi dasturlar tahlili asosida kiberjinoyatlar subyektining kriminalistik tavsifi (profil) elementlari boyitildi. Jinoyatchining motivatsiyasi, malaka darajasi, foydalanilgan vositalar va usullar o‘rtasidagi o‘zaro bog‘liqliklar aniqlanib, bu ma’lumotlar asosida noma’lum jinoyatchini qidirish va uning shaxsini aniqlashga yo‘naltirilgan tezkor-qidiruv faoliyati samaradorligini oshirish bo‘yicha takliflar ilgari surildi;

To‘rtinchidan, milliy qonunchilik va huquqni qo‘llash amaliyoti tahlili asosida kiberjinoyatlarni tergov qilish sohasidagi mavjud huquqiy bo‘shliqlar aniqlandi. Xususan, zarar keltiruvchi dasturlarni yaratish, tarqatish va ulardan foydalanish bilan bog‘liq jinoyatlarni kvalifikatsiya qilish, shuningdek, raqamli dalillarning maqbulligi va ishonchliligini ta’minlashga oid protsessual normalarni takomillashtirish yuzasidan ilmiy asoslangan taklif va tavsiyalar ishlab chiqildi. Bu o‘z navbatida, kiberjinoyatlar uchun javobgarlikning muqarrarligini ta’minlashga xizmat qiladi.

MUHOKAMA

Kiberxavfsizlikka qarshi qaratilgan jinoyatlarning kriminalistik tahlili shuni ko‘rsatadiki, aksariyat holatlarda zarar keltiruvchi dasturlar (keyingi o‘rinlarda ZKD) nafaqat jinoyat quroli, balki jinoyat izlarining asosiy tashuvchisi va o‘ziga xos

“raqamli guvoh” vazifasini ham bajaradi. Shu bois, ZKD tahlili tergov jarayonining markaziy bo‘g‘inlaridan biriga aylanib, uning samaradorligi bevosita ushbu tahlilning chuqurligi, ilmiyligi va metodologik to‘g‘riligiga bog‘liqdir. Ushbu tadqiqot doirasida ZKDning kriminalistik ahamiyati uch asosiy yo‘nalishda tahlil qilindi: ZKDning kriminalistik tasnifi, uning raqamli izlarini aniqlash va fiksatsiya qilish metodikasi hamda tergov amaliyotida yuzaga keladigan muammoli vaziyatlar va ularni bartaraf etish yo‘llari.

Birinchi navbatda, ZKDni kriminalistik nuqtai nazardan tasniflash muhim ahamiyat kasb etadi. An’anaviy texnik tasniflash (viruslar, chuvalchanglar, troyanlar va hokazo) tergovchi uchun jinoyatning faqat texnik jihatlarini ochib beradi, biroq uning huquqiy kvalifikatsiyasi va isbotlash predmetiga oid masalalarni to‘liq qamrab olmaydi. Shu sababli, ZKDni tergov maqsadlaridan kelib chiqqan holda, g‘arazli niyat va jinoyat tarkibiga ko‘ra tasniflash metodologik jihatdan to‘g‘ri yondashuv hisoblanadi. Bu borada quyidagi kriminalistik tasnifni taklif etish mumkin: 1) Ma’lumotlarni o‘g‘irlashga qaratilgan ZKDlar (shpion dasturlar, keyloggerlar, snifferlar) – bu turdagi dasturlar tergov uchun shaxsiy yozishmalar, bank rekvizitlari, tijorat sirlari kabi muhim axborotlarning qachon, qanday va kim tomonidan o‘g‘irlanganligini aniqlash imkonini beruvchi raqamli izlarni o‘zida saqlaydi; 2) Moliyaviy firibgarlik uchun mo‘ljallangan ZKDlar (bank troyanlari, fishing skriptlari) – ular tranzaksiyalarni soxtalashtirish, hisob raqamlariga ruxsatsiz kirish kabi harakatlarning mexanizmini tushunish va moliyaviy zanjirni kuzatish uchun asos bo‘ladi; 3) Tizim faoliyatini izdan chiqarish yoki to‘sishga qaratilgan ZKDlar (tovlamachi-shifrlagichlar (ransomware), DDoS-botlar, wiperlar) – bu toifadagi ZKDlar jinoyatning ob’ektiv tomonini, ya’ni keltirilgan zararning hajmi va xususiyatini, shuningdek, jinoyatchining niyatini (masalan, tovlamachilik yoki raqobat kurashi) aniqlashda muhim daliliy ahamiyatga ega; 4) Boshqa jinoyatlarni sodir etish uchun platforma yaratuvchi ZKDlar (botnetlar, bekorlar (backdoors), proksi-dasturlar) – ular jinoyatning latentligini ta’minlash, izlarni yashirish va jinoyatchi shaxsini anonimlashtirishga xizmat qilgani bois, ularning tahlili operativ-qidiruv faoliyati uchun strategik ma’lumotlar manbai hisoblanadi. Ushbu tasnif tergovchiga jinoyatning motivini, maqsadini va sodir etilish usulini (modus operandi) dastlabki bosqichdayoq to‘g‘ri belgilashga yordam beradi.

Ikkinchi muhim yo‘nalish – ZKD tomonidan qoldirilgan raqamli izlarni aniqlash, olish va protsessual rasmiylashtirishning o‘ziga xos metodikasidir. Raqamli izlar o‘zining mo‘rtligi, o‘zgaruvchanligi va ko‘zga ko‘rinmasligi bilan an’anaviy kriminalistik izlardan tubdan farq qiladi. ZKD tahlili jarayonida quyidagi asosiy raqamli dalil manbalari o‘rganiladi: a) Fayl tizimidagi o‘zgarishlar – ZKDning ijro etiluvchi fayli, uning konfiguratsiya fayllari, yaratgan yoki o‘zgartirgan boshqa fayllar. Ularning metama’lumotlari (yaratilgan, o‘zgartirilgan va oxirgi kirilgan vaqt) jinoyatning xronologiyasini tiklashda muhim rol o‘ynaydi; b) Operatsion tizim reestridagi (Windows uchun) yozuvlar – ZKDning avtomatik ishga tushishini

ta’minlovchi kalitlar, tizim sozlamalariga kiritilgan o‘zgartirishlar uning tizimdagi faoliyat doirasini va “yashash” mexanizmini ko‘rsatadi; c) Tarmoq faoliyati loglari – ZKDning boshqaruv markazi (Command and Control, C&C) serverlari bilan aloqasi, o‘g‘irlangan ma’lumotlarni yuborish uchun foydalanilgan IP-manzillar va portlar jinoyatchining infratuzilmasini aniqlash va uning geografik joylashuvini taxmin qilish uchun asosiy manbadir; d) Operativ xotira (RAM) tahlili – zamonaviy ZKDlarning aksariyati faylsiz (fileless) texnologiyalardan foydalanib, faqat operativ xotirada faoliyat yuritadi. Shu bois, tizimning RAM-dampi tahlili (memory forensics) orqali yashirin jarayonlarni, shifrlangan ma’lumotlarni va tarmoq ulanishlarini aniqlash imkoniyati tug‘iladi. Bu jarayon “jonli tahlil” (live analysis) deb atalib, dalillarning yo‘qolishini oldini olish uchun voqea joyini ko‘zdan kechirishning birinchi daqiqalaridanoq amalga oshirilishi shart.

ZKD tahlilida ikki asosiy metodologik yondashuv qo‘llaniladi: statik va dinamik tahlil. Statik tahlil – bu ZKD kodini ishga tushirmasdan, uning tarkibiy qismlarini (kod qismlari, matnli satrlar, import qilinadigan funksiyalar) o‘rganishdir. Bu usul dasturning potentsial imkoniyatlarini tezkor baholashga imkon beradi. Biroq, zamonaviy ZKDlar o‘z kodini obfuskatsiya (chalkashtirish) va shifrlash orqali tahlildan himoyalaydi. Dinamik tahlil esa ZKDni maxsus izolyatsiya qilingan virtual muhitda (“qum qutisi” – sandbox) ishga tushirib, uning real harakatlarini (qaysi fayllarni yaratishi, reestrga nima yozishi, tarmoqqa qanday so‘rovlar yuborishi) kuzatishni o‘z ichiga oladi. Kriminalistik nuqtai nazardan, dinamik tahlil natijalari jinoyatning ob’ektiv tomonini, ya’ni ijtimoi-xavfli qilmishning bevosita sodir etilish jarayonini isbotlash uchun eng qimmatli dalillarni taqdim etadi. Ushbu tahlillar natijasida olingan ma’lumotlar (hesh-summalar, IP-manzillar, domen nomlari, fayl nomlari) “kompрometatsiya indikatorlari” (Indicators of Compromise, IoC) deb atalib, ular nafaqat bitta jinoyatni ochishda, balki bir-biriga bog‘liq bo‘lgan yoki bir jinoiy guruh tomonidan sodir etilgan jinoyatlar seriyasini aniqlashda ham muhim vosita bo‘lib xizmat qiladi.

Uchinchi tahlil yo‘nalishi – ZKD bilan bog‘liq jinoyatlarni tergov qilishda yuzaga keladigan amaliy va huquqiy muammolardir. Eng asosiy muammolardan biri – bu attributsiya, ya’ni jinoyatni sodir etgan shaxs yoki guruhni aniqlashning murakkabligidir. Jinoyatchilar o‘z shaxslarini yashirish uchun proksi-serverlar, VPN, Tor anonim tarmog‘i kabi vositalardan keng foydalanadilar. Bunday sharoitda, texnik tahlilning o‘zi yetarli bo‘lmaydi. Kriminalistikaning an’anaviy usullari, jumladan, operativ-qidiruv tadbirlari, viktimologik tahlil (jabrlanuvchining faoliyati, uning raqobatchilari yoki dushmanlarini o‘rganish), shuningdek, ZKD kodidagi o‘ziga xos uslub (“dasturchi dastxati”) yoki ishlatilgan til xususiyatlarini lingvistik ekspertizadan o‘tkazish kabi kompleks yondashuv talab etiladi.

Yana bir jiddiy muammo – bu anti-forensik texnologiyalarning qo‘llanilishidir. ZKD yaratuvchilari o‘z dasturlariga tahlilni qiyinlashtiruvchi maxsus modullarni qo‘shadilar: virtual muhitni aniqlash (agar dastur “qum qutisi”da ishlayotganini

sezsa, o‘z faoliyatini to‘xtatadi), kodning polimorfizmi va metamorfizmi (har bir yangi zararlanganda kod o‘zgarib turadi), ma’lumotlarni o‘chirish (wiper funksiyasi) va shifrlash. Bunga qarshi kurashish uchun tergov organlari xodimlari va ekspertlar nafaqat zamonaviy dasturiy-apparat vositalariga, balki revers-injiniring (teskari muhandislik) sohasida chuqur bilimga ega bo‘lishlari lozim.

Transchegaraviy jinoyatlar masalasi ham alohida e’tiborni talab qiladi. ZKDning boshqaruv serverlari bir davlatda, jinoyatchilar ikkinchi davlatda, jabrlanuvchilar esa uchinchi davlatda joylashgan bo‘lishi odatiy holdir. Bu esa tergov jarayonida turli yurisdiksiyalardagi huquqiy to‘siqlarga va dalillarni olishdagi qiyinchiliklarga olib keladi. Ushbu muammoning yechimi xalqaro huquqiy yordam ko‘rsatish to‘g‘risidagi shartnomalar mexanizmini takomillashtirish, xalqaro tezkor-tergov guruhlarini tuzish va kiberpolitsiya tuzilmalari o‘rtasida real vaqt rejimida axborot almashinuvini yo‘lga qo‘yish bilan bog‘liqdir.

Xulosa

Olib borilgan tadqiqot natijalari shuni ko‘rsatadiki, kiberxavfsizlikka qarshi qaratilgan jinoyatlarni tergov qilish jarayonida zarar keltiruvchi dasturiy ta’minotlar (ZKD) tahlili bugungi kunda kriminalistik faoliyatning eng murakkab va dinamik rivojlanayotgan yo‘nalishlaridan biridir. Tadqiqot ZKDlarning zamonaviy ko‘rinishlari – polimorf va metamorf viruslar, shifrlangan zararli kodlar hamda tergovga qarshi (antiforensik) texnologiyalardan foydalanuvchi dasturlar mavjud kriminalistik metodika va vositalar uchun jiddiy muammo tug‘dirayotganini tasdiqladi. Amaldagi tergov amaliyoti ko‘p hollarda reaktiv xarakterga ega bo‘lib, jinoyat sodir etilganidan so‘ng raqamli izlarni tahlil qilishga asoslanadi, bu esa ZKDlarning o‘zini-o‘zi yo‘q qilish yoki modifikatsiyalash xususiyatlari oldida samarasiz bo‘lib qolmoqda. Shuningdek, tergovchi va ekspert-kriminalistlarning zararli kodlarni chuqur tahlil qilish bo‘yicha maxsus bilim va texnik imkoniyatlari o‘rtasida nomutanosiblik mavjudligi, normativ-huquqiy bazaning esa kiberjinoyatlar transformatsiyasi tezligiga hamohang takomillashmayotgani aniqlandi.

Shu munosabat bilan, tadqiqot natijalariga asoslanib, quyidagi ilmiy-nazariy va amaliy tavsiyalarni ilgari surish maqsadga muvofiq:

1. Ilmiy-nazariy jihatdan: ZKDlarni kriminalistik tadqiq etishning an’anaviy yondashuvlaridan voz kechib, ularning xulq-atvorini (behavioral analysis) va tarmoqdagi faolligini real vaqt rejimida tahlil qilishga asoslangan proaktiv metodologiyani ishlab chiqish lozim. Ushbu metodologiya sun’iy intellekt va mashinali o‘qitish (machine learning) algoritmlarini integratsiya qilish orqali potentsial tahdidlarni oldindan bashorat qilish (prognostik funksiya) va noma’lum ZKDlarni avtomatik tarzda klassifikatsiya qilish imkonini berishi kerak.

2. Amaliy jihatdan:

- Huquqni muhofaza qiluvchi organlar uchun ZKDlar xulq-atvori patternlari, kod fragmentlari va raqamli signaturalarining yagona milliy ma’lumotlar bazasini yaratish va uni xalqaro antitahdid markazlari bilan muntazam sinxronizatsiya qilib borish.

- Tergovchilar va ekspert-kriminalistlar uchun zararli kodlarni revers-injiniring qilish, dinamik tahlil (“sandbox” muhitida) va tarmoq trafigini monitoring qilish bo‘yicha chuqurlashtirilgan malaka oshirish kurslarini tizimli yo‘lga qo‘yish.

- ZKDlar bilan bog‘liq raqamli ashyoviy dalillarni olish, qadoqlash, saqlash va tadqiqotga yuborish bo‘yicha yagona, zamonaviy texnik talablarga javob beradigan standartlashtirilgan kriminalistik protokollarni amaliyotga joriy etish.

3. Normativ-huquqiy jihatdan: Jinoyat-protsessual qonunchiligiga “virtual tintuv”, “masofaviy ko‘zdan kechirish” kabi yangi tergov harakatlarini kiritish, shuningdek, raqamli dalillarni, xususan, zararli dasturiy kodlarni olish va legallashtirish tartibini soddalashtiruvchi va aniqlashtiruvchi o‘zgartirishlar kiritish taklif etiladi. Xalqaro hamkorlik doirasida kiberxavf intellekti (Cyber Threat Intelligence) almashinuvi bo‘yicha transchegaraviy protokollarni takomillashtirish va tezkor-tergov guruhlari faoliyatini muvofiqlashtirish mexanizmlarini mustahkamlash zarur. Ushbu kompleks chora-tadbirlarning implementatsiyasi kiberjinoyatlarni tergov qilish samaradorligini oshirishga xizmat qiladi.

Foydalanilgan adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasi Jinoyat kodeksi.
2. Mirziyoyev, Sh. M. (2017). Tanqidiy tahlil, qat’iy tartib-intizom va shaxsiy javobgarlik – har bir rahbar faoliyatining asosiy mezoni bo‘lishi kerak. O‘zbekiston Respublikasi Prezidentining Oliy Majlisga Murojaatnomasi.
3. Shukurov,U. (2019). Kiberjinoyatlarni tergov qilishning o‘ziga xos xususiyatlari. Huquq va burch, (3), 45-48.
4. Jo‘rayev, H. (2020). Axborot xavfsizligi va kiberhimoya asoslari. Toshkent: Fan va texnologiyalar.
5. Kim, D. (2018). Cybercrime Investigation and Digital Forensics. Springer.
6. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.
7. National Institute of Standards and Technology (NIST). (2013). Guide to Computer Security Log Management. NIST Special Publication 800-92.
8. SANS Institute. (2021). Malware Analysis Fundamentals. SANS Technical Papers.
9. Northcutt, S., & Novak, J. (2012). Network Intrusion Detection: An Analyst's Handbook. New Riders.
10. Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.
11. Prosise, J., & Mandia, K. (2003). Incident Response & Computer Forensics. McGraw-Hill Education.