RAQAMLI EKSPERTIZALARNI ISO XALQARO STANDARTLARIGA MOSLASHTIRISHNING AYRIM MASALALARI

Shohzod Abdullayev
Toshkent davlat yuridik universiteti
Kiber huquqi yo'nalishi magistranti
shaxzodabdullayev9705@gmail.com

Annotatsiya. Ushbu maqolada raqamli dalillarning huquqiy va texnik xususiyatlari, ularni to'plash, saqlash, tekshirish, transportirovka qilish va baholashga oid masalalari, raqamli dalillar bilan ishlash sohasida amalga oshirilgan ilmiy-amaliy tadqiqotlar, nazariyotchi olimlar hamda amaliyotchi xodimlar fikr-mulohazalari, raqamli dalillarning maqbulligini ta'minlash, ularni identifikatsiya va autentifikatsiya qilish, ekspert xulosalarini tekshirish va baholashga oid masalalar tadqiq etilgan.

Kalit so'zlar: kibermakon, kiberhujum, raqamli dalillar, raqamli ekspertiza, dalillar maqbulligi, ISO standartlari.

Abstract. In this article, the legal and technical features of digital evidence, the issues related to their collection, storage, verification, transportation and evaluation, scientific and practical researches carried out in the field of working with digital evidence, opinions of theoreticians and practitioners, the acceptability of digital evidence are discussed. Issues related to provision, their identification and authentication, verification and assessment of expert opinions are studied.

Key words: cyber space, cyber attack, digital evidence, digital expertise, admissibility of evidence, ISO standards

Аннотация. В статья рассмотрены правовые и технические особенности цифровых доказательств, вопросы, связанные с их сбором, хранением, проверкой, транспортировкой и оценкой, научно-практические исследования, проводимые в области работы с цифровыми доказательствами, мнения теоретиков и практиков, обсуждаются вопросы приемлемости цифровых доказательств, изучаются вопросы, связанные с предоставлением, их идентификацией и аутентификацией, проверкой и оценкой экспертных заключений.

Ключевые слова: киберпространство, кибератака, цифровые доказательства, цифровая экспертиза, допустимость доказательств, стандарты ИСО.

Kirish. Jahon hamjamiyati yangi davr - axborot jamiyati davriga kirib, kompyuterlar va telekommunikatsiya tizimlari inson va davlat hayotining barcha sohalarini qamrab olgan. Ammo insoniyat o'zini telekommunikatsiya va global kompyuter tarmoqlari xizmatiga qo'yib, bu texnologiyalarni suiiste'mol qilish uchun qanday imkoniyatlar yaratilishini oldindan sezmagan. Bugungi kunda virtual makonda faoliyat yuritayotgan jinoyatchilar qurbonlari nafaqat odamlarga, balki butun davlatlarga aylanishi mumkin [1].

Shu bilan birga, axborot xavfsizligiga qarshi jinoyatlarni bir necha jinoyatchilar uyushmasi yoki guruhi sodir qilishi mumkin. Kibermuhitda sodir yetilgan jinoyatlar soni kompyuter tarmoqlaridan foydalanuvchilar soniga mutanosib ravishda o‘sib bormoqda va Xalqaro jinoyat politsiyasi tashkiloti – Interpol hisob-kitoblariga ko‘ra, global internet tarmog‘ida ushbu jinoyatchilikning o‘sish sur’ati sayyoramizda eng tezkor hisoblanadi [2].

Zamonaviy dunyoda axborot texnologiyalari hamda internet orqali sodir etilayotgan jinoyatlarning soni kun sayin ortib bormoqda. Statistik ma’lumotlarga ko‘ra, hozirgi vaqtda dunyo aholisining 4 mlrd.dan ortig‘i internet foydalanuvchisi hisoblanib, kiberxavfsizlik bo‘yicha xalqaro ekspertlar 2019-yilda kiberhujumlar har 14 sekundda sodir bo‘lishini ta’kidladi [3]. Har yili kiberjinoyatchilik oqibatida yetkazilgan moddiy zararning miqdori dunyo YAIMning 1 %ni tashkil etadi [4].

2020-yilning aprel oyidagi ma’lumotga ko‘ra, O‘zbekistonda internet tarmog‘idan foydalanuvchilarning soni 18.4 mln.ga yetgan (bu umumiy aholining 55 foiziga to‘g‘ri keladi), aholining 76 foizi yoki 25 140 000 o‘zbekistonliklar mobil telefonga egalar, shuningdek, O‘zbekistondan xalqaro tarmoqlarga umumiy ulanish tezligi 104,1 Gbit /s. ni tashkil etgan [3]. Ayni paytda “UZ” milliy domenida 66 mingdan ortiq faol domen bor. 2017-yilda O‘zbekistonda 53 mingga yaqin faol domen mavjud bo‘lib, 2018-yilda ularning soni 65 mingga yetgan.

Har bir foydalanuvchida Internet xizmatlari borligi, ularning kiberterrorizm qurboni bo‘lishi mumkinligini anglatadi. UZCERT- Axborot xavfsizligi insidentlariga chora ko‘rish xizmatining ma’lumotlariga ko‘ra, davlat organlarining axborot tizimlarida 2018-yil va 2019-yil birinchi choragida axborot xavfsizligi hodisalari monitoringi o‘tkazilganida 54.953.759 ta axborot xavfsizligi buzilishi aniqlangan. Ulardan 2.502.353 tasining xavfi yuqori daraja bo‘lgan [5].

Bir so‘z bilan aytganda, global axborotlashtirish va kompyuterlashtirish asrida insoniyat hayotiga olamshumul ixtirolar bilan bir qatorda, axborot xavfsizligiga tahdid solayotgan kompyuter jinoyatchiligi kabi ulkan muammolar ham kirib kelmoqda.

Agar statistik ma’lumotlarga e’tibor qaratadigan bo‘lsak, 2016 yil butun dunyoda 600 million jinoyat sodir etilgan bo‘lib, ulardan 40 millioni kiberjinoyatlar hisoblanadi. Bu esa Belgiya, Shvetsariya, Shvetsiya kabi davlatlar aholisidan ko‘pdir. 2018 yil davomida dunyoda yiliga 556 miliion, har bir kunda 1,5 million, xar bir sekundda 18 nafar shaxslar kiberjinoyatchilik qurboni bo‘ladi [6].

Kiberjinoyatchilikning oldini olish tizimini yaratish masalalari davlat siyosati darajasiga ko‘tarilganligi mavzuning naqadar jiddiy ekanligidan dalolatdir.

Jumladan, O‘zbekiston Respublikasi Prezidentining 2022-yilning 28-yanvardagi “2022 — 2026-yillarga mo‘ljallangan yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi 60-sonli farmonida kiberjinoyatlarni fosh etish bo‘yicha tezkor-qidiruv faoliyatini isloh qilish, moliyaviy xizmatlarni ko‘rsatishda kiberxavfsizlikni ta’minlash; moliyaviy xizmatlarni raqamlashtirish orqali ularning ommabopligini oshirishni nazarda tutish, “2023 — 2026-yillarga mo‘ljallangan

O‘zbekiston Respublikasining kiberxavfsizlik strategiyasi”ni ishlab chiqish, kiberjinoyatchilik uchun jinoiy javobgarlikni qayta ko‘rib chiqish, axborot maydonidagi kiberhujum va tahdidlarni monitoring qilish tizimini yanada takomillashtirish [7] masalalari dolzarb vazifalar sifatida belgilangan.

Shuningdek, O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi “Raqamli O‘zbekiston — 2030” Strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi 6079-son Farmoni bilan mamlakatimizda raqamli iqtisodiyotni faol rivojlantirish, barcha tarmoqlar va sohalarda, eng avvalo, davlat boshqaruvi, ta’lim, sog‘liqni saqlash va qishloq xo‘jaligida zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish bo‘yicha kompleks chora-tadbirlar amalga oshirilmoqda [8].

Yuqoridagilardan kelib chiqadiki, davlat boshqaruvi tizimidagi ijtimoiy-iqtisodiy hamda boshqa sohalarning raqamlashtirilishi, ya’ni raqamli texnologiyalardan foydalanilishi keng joriy etilishi o‘z-o‘zidan mazkur sohalarda axborot xavsizligi, ularni huquqiy himoyasi hamda sodir etilgan kiberjinoyatlarni tergov qilish bilan bog‘liq bo‘lgan muammolarni yuzaga keltiradi.

Axborot-texnologiyalar vositasida sodir qilingan jinoyatlar, allaqachon rivojlangan xorijiy mamlakatlarda “kiberjinoyatlar” deb nomlanadi va ushbu ijtimoiy xavfli qilmishlarga qarshi kurashish, oldini olish, uning keyingi faoliyatiga to‘sqinlik qilish kabi chora-tadbirlar qonunchiligida belgilangan. Umuman olganda, kiberjinoyatlarning o‘ziga xos xususiyati quyidagilar:

ushbu toifadagi jinoyatlar makon tanlamay, uni istalgan payt dunyoning turli tomonlaridan kutish mumkin;

muntazam ravishda har kuni yangi va oldingilaridan ancha xavfliroq bo‘lgan virus va boshqa zararli dasturlarning yaratilishi;

kiberjinoyatlarga qarshi kurashadigan organlarda malakali va ushbu sohada mukammal bilimlarga ega mutaxassislar mavjud emasligi va buning natijasida jinoyatning kech aniqlanishi;

kiberjinoyat natijasida muayyan mulk emas, balki axborotlarga nisbatan mulkchilik huquqi yo‘qotiladi;

axborotlarni qayta ishlash jarayonida yo‘l qo‘yilgan xatolik o‘z vaqtida kuzatilmaydi va tuzatilmaydi, natijada kelgusida sodir bo‘ladigan xatolarning oldini olib bo‘lmaydi;

sodir etiladigan kompyuter jinoyatlari o‘z vaqtida e’lon qilinmaydi (hisoblash tarmoqlarida kamchiliklar mavjudligini boshqalardan yashirish, muassasa ishchanlik obro‘yini saqlab qolish va boshqa maqsadlarda);

kiberjinoyatni tergov qilish hamda ochishning o‘ziga xos qiyinligi, juda katta zararga olib kelishi, jinoyatchilarga qarshi kurashish va uning profilaktikasi uchun yagona huquqiy asosning mavjud emasligi kabilar[9].

Mavzuga oid adabiyotlar tahlili. Raqamli dalillar ishni sudga qadar yuritish va sudda ko‘rish bosqichlarida protsessual jarayonlarga ta’sir qilishi, raqamli dalillarning o‘ziga xos xususiyatlari, murakkab tarkibi hamda mexanizmini tushunmasdan ular bilan bog‘liq amaliyotni to‘g‘ri hal etish mumkin emas.

Raqamli tergov jarayonida raqamli dalillarni baholash moddiy dalillarga nisbatan murakkab jarayondir. Sababi, raqamli dalillarni baholashdan avval ham, rioya qilinishi kerak bo‘lgan bir qator talablar mavjud. Rivojlangan mamlakatlarda, jumladan AQShda raqamli dalillarni baholashda tekshirilishi lozim bo‘lgan dastlabki talablar belgilangan.

Xususan, V. Roussev Daubert standartiga asosan raqamli dalillarni sudga taqdim etish yoki ko‘rsatuvlarni baholashning quyidagi asosiy mezonlarini taklif etgan.

Tergov va ekspertiza davomida qo‘llanilgan metodlar nazariy jihatdan asoslangan bo‘lishi.

Sababi, amaldagi qonunchilikka ko‘ra shaxsni davlat nomidan aybdor deb topish uchun tergov organlari yoki sud har qanday vosita va metodlardan foydalanishga haqli emas. Mazkur vosita va metodlar muayyan tadqiqotlar natijasida sinovdan o‘tkazilgan bo‘lishi lozim. Aks holda qaror gumon qilinuvchining foydasiga chiqarilishi lozim.

Kriminalistik amaliyotda qo‘llanilgan uslublar huquqni muhofaza qiluvchi organlarning jurnallari, ro‘znoma yoki internet saytlarida chop etilishi kerakligi. Bunda tergov va sud jarayonida qo‘llanilgan uslubiyotlardan protsessning boshqa ishtirokchilari, jumladan sudyalar va advokatlar ham xabardor bo‘lishi zarur. Aks holda suddaqonuniylik va adolatni ta’minlash mumkin emas.

Tadqiqot usulining xato qilish darajasini aniqlash – bunda tadqiqot o‘tkazishda qo‘llanilayotgan metod va vositalarni ishonchlilik darajasi tekshiriladi.

Amaliyotda qo‘llaniladigan metodlar biror ilmiy jamiyatda qabul qilinishi kerakligi.

Mazkur talab ham juda muhim bo‘lib, ishni sudga qadar yuritish va sud muhokamasi bosqichlarida qo‘llanilayotgan usullarni unifikatsiya qilish imkoniyatini beradi. Ushbu standartlar raqamli dalillarining to‘g‘riligi va ekspert ko‘rsatuvlarini haqqoniyligini tekshirishda keng imkoniyat beradi.

2017-yilda Antvi-Boasiako (Antwi-Boasiako) va Venterlar (Venter) tomonidan raqamli dalillarni maqbulligining texnik va huquqiy talablari bo‘yicha “Raqamli dalillar maqbulligini baholashning yagona modeli” (Harmonized Model for Digital Evidence Admissibility Assessment (HM –DEAA)) ishlab chiqilgan. Mazkur modelda raqamli dalillarni baholashning quyidagi uch bosqichi ko‘rsatilgan.

a) Raqamli dalillarning maqbulligini baholash. Mazkur bosqichda raqamli dalillarni olishda protsessual qonunchilik va xalqaro standlarga rioya etilganligi hamda ularning ahamiyati kriminalistik jihatdan baholanadi.

b) Raqamli dalillar ko‘rib chiqish. Ushbu bosqichda raqamli dalillarning yaxlitligi, ya’ni ularni olish, saqlash va tahlil qilishda ekspertiza protseduralari va vositalariga rioya qilinganligi baholanadi.

Bundan ko‘zlangan maqsad dalillarni topish, saqlash va tahlil qilishda ilmiy asoslangan prinsiplarga rioya etilganligini tekshirish, ish sifatini ta’minlash va natijalarga ishonchni mustahakamlashdir. Shu bilan birga, raqamli dalillar bilan

ishlash va ularni tadqiq qilishda standartlarga amal qilingani (masalan, raqamli kriminalistika vositalarini attestatsiyadan o‘tgani, ishonchliligi va to‘g‘ri ishlashi tasdiqlangani, foydalanishdan avval sinovdan o‘tkazilgani) ham hisobga olinadi.

Bundan tashqari, laboratoriya tadqiqotida amal qilingan standartlar va protokollar ham o‘rganilishi lozim. Bundan maqsad laboratoriyada raqamli dalil-larni tahlil etish va natijalarni ishonchliligini ta’minlash uchun ishonchli metodlar, raqamli qurilmalar va dasturiy vositalar, kompetentli hodimlar hamda asoslangan xulosalar berish imkoniyati mavjudligini aniqlashdir.

c) Raqamli dalillarning maqbulligi bo‘yicha qaror qabul qilish. Ushbu bosqichda raqamli dalillarning haqiqiyligi, yaxlitligi va ishonchliligi ikkinchi bosqich natijalariga asosan baholanadi. Masalan, raqamli dalillarni olish metodlari va vositalari ishonchliligi nuqtai nazaridan baholanadi hamda ekspertlarning ko‘rsatuvlari solishtiriladi. Natijalar haqiqiy deb topilishi uchun ular xolis tarzda talqin qilinishi, xatolar, noaniqliklar va cheklovlar haqidagi ma’lumotlar oshkor qilinishi kerak. V.Roussev, Antvi-Boasiakova Venterlar tomonidan taklif etilgan mezonlar qanchalik mukammal bo‘lmasin, ularda raqamli dalillarning baholashning ahloqiy talablari ko‘rsatilmagan. Ta’kidlash joizki, ahloqiy talablar ham mazkur dalil turini baholashda printsial ahamiyatga ega. Zero, amaldagi qonunchilikka ko‘ra shaxsiy ma’lumotlar mahfiy ma’lumotlar sirrasiga kiradi [10].

Xulosa va takliflar. Xulosa qilib aytganda, ilg‘or xorijiy amaliyotlar va standartlarda raqamli dalillarni baholashning xalqaro darajada tan olingan qoidalari belgilangan. Ularni milliy qonunchilikka moslashtirilishi quyidagi masalalarni ijobiy hal etilishiga yordam beradi:

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

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

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

to‘rtinchidan, sohada davlatlar o‘rtasida yuzaga kelgan nizolarda O‘zbekiston Respublikasi manfaatlari ishonchli himoyasini ta’minlash imkoniyatini beradi [10].

Shuningdek, raqamli ekspertizani amalga oshiruvchi alohida boshqarma tashkil etilishi hamda kiberjinoyatlarni har bir turlari tergov qilish bo‘yicha mutaxassis-kadrlar ish olib borishlari lozim.

Foydalanilgan adabiyotlar ro‘yxati

1. Olimov Azizjon Anvar o‘g‘li - Kiberjinoyatchilikka qarshi kurashishning tashkiliy-huquqiy asoslari va ularni takomillashtirish masalalari: milliy va xorijiy tajriba
2. https://www.interpol.int/Crimes/Cybercrime
3. S.Morgan. Official Annual Cybercrime Report 2019 // Cybersecurity Ventures.

4. http://www.statista.com/ (The Statistics Portal)
5. https://wearesocial.com/digital-2020
6. https://uzcert.uz/blog/saidakbar/kiberbezopasnost-uzbekistana-v-tsifrakh-itogi-2018-goda/
7. O‘zbekiston Respublikasi Prezidentining 2022-yilning 28-yanvardagi “2022 — 2026-yillarga mo‘ljallangan yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida”gi 60-sonli farmoni
8. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi “Raqamli O‘zbekiston — 2030” Strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi 6079-son Farmoni, https://lex.uz/ru/docs/-5030957#-5031756
9. Ro‘ziev R.N., Salaev N.S. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya. – Toshkent: TDYUU, 2018, 6-bet.
10. Istam ASTANOV, Bakhtiyor KHAMIDOV – “Elektron yohud raqamli dalillarga oid umumnazariy masalalar: muammo va yechim” - Jamiyat va innovatsiyalar - Journal home page: https://inscience.uz/index.php/socinov/index