KIBERJINOYATLAR TUSHUNCHASI, TASNIFI VA ULARNI ANIQLASHDA RAQAMLI DALILLARNING O‘RNI

Karimboyev Jo’shqinbek Ergashbek o’g’li
O’zbekiston Respublikasi IIV Akademiyasi kunduzgi ta’lim 3-o’quv kursi kursanti

Annotatsiya: *Zamonaviy raqamli jamiyatda kiberjinoyatlar eng tez o‘sib borayotgan va eng katta iqtisodiy zarar keltirayotgan jinoyat turiga aylandi. Mazkur maqolada kiberjinoyatlarning huquqiy mohiyati, xalqaro va milliy tajribaga asoslangan tasnifi, shuningdek, ularni aniqlash va isbotlashda raqamli dalillarning hal qiluvchi roli atroflicha tahlil qilinadi. Kiberjinoyatlarning asosiy turlari va O‘zbekistondagi statistik holati keltirilgan holda, raqamli dalillarning o‘ziga xos xususiyatlari, turlari hamda ularni xodimlar tomonidan qonuniy va maqbul holda olinishiga alohida urg‘u beriladi. Maqola oxirida O‘zbekiston huquqni muhofaza qilish tizimida kiberjinoyatlarga qarshi kurashish tizimini yanada takomillashtirish bo‘yicha amaliy takliflar berilgan.*

Kalit so‘zlar: *kiberjinoyat, raqamli dalil, raqamli forensika, kiberxavfsizlik, dalil zanjiri, moliyaviy kiberfiribgarlik, phishing, ISO/IEC 27037, hash-qiymat, tezkor-qidiruv faoliyati, kiberjinoyatlarni aniqlash.*

THE CONCEPT, CLASSIFICATION AND THE ROLE OF DIGITAL EVIDENCE IN DETECTION OF CYBERCRIMES

Abstract: *In modern digital society, cybercrimes have become the fastest-growing criminal phenomenon, causing the largest economic damage. This article comprehensively analyzes the legal essence of cybercrimes, their classification based on international and national experience, as well as the decisive role of digital evidence in their detection and proving. The main types of cybercrimes and the statistical situation in Uzbekistan are presented, with special emphasis on the specific characteristics and types of digital evidence and the necessity of their lawful and proper collection by law enforcement officers. The article concludes with practical recommendations aimed at further improving the system of combating cybercrimes within the law enforcement agencies of the Republic of Uzbekistan.*

Key words: *cybercrime, digital evidence, digital forensics, cybersecurity, chain of custody, financial cyber fraud, phishing, ISO/IEC 27037, hash value, investigative activities, detection of cybercrimes.*

ПОНЯТИЕ, КЛАССИФИКАЦИЯ КИБЕРПРЕСТУПЛЕНИЙ И РОЛЬ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ В ИХ ВЫЯВЛЕНИИ

Аннотация: *В современном цифровом обществе киберпреступления превратились в наиболее быстро растущий и наносящий наибольший*

экономический ущерб вид преступности. В данной статье подробно анализируются правовая сущность киберпреступлений, их классификация на основе международного и национального опыта, а также решающая роль цифровых доказательств в их выявлении и доказывании. Приводятся основные виды киберпреступлений и статистическая ситуация в Узбекистане, при этом особое внимание уделяется специфическим характеристикам и видам цифровых доказательств, а также необходимости их законного и надлежащего изъятия сотрудниками правоохранительных органов. В заключительной части статьи предлагаются практические рекомендации по дальнейшему совершенствованию системы борьбы с киберпреступлениями в правоохранительных органах Республики Узбекистан.

Ключевые слова: *киберпреступление, цифровое доказательство, цифровая криминалистика, кибербезопасность, цепочка хранения доказательств, финансовое кибермошенничество, фишинг, ISO/IEC 27037, хеш-значение, оперативно-розыскная деятельность, выявление киберпреступлений*

Zamonaviy axborot jamiyatida kiberjinoyatlar eng jadal rivojlanayotgan va eng katta iqtisodiy zarar yetkazayotgan jinoyat turlaridan biriga aylandi. Tahlillarga koʻra, dunyo boʻylab har yili 500 milliondan ortiq kiber hujumlar uyushtiriladi. Har soniyada 12 nafar insondan biri kibermakonda sodir etilgan hujumlar qurboniga aylanadi. Amerika Qoʻshma Shtatlari, Fransiya, Angliya, Germaniya, Belgiya, Luksemburg kabi rivojlangan davlatlarda jinoyatlarning 60-65 foizi kiber hujumlar orqali sodir etilmoqda. Oʻzbekistonda ham soʻnggi uch yilda bu turdagi jinoyatlar 8,3 baravarga koʻpayib, hozirda umumiy jinoyatchilikning qariyb 5 foiziga yetgan. Xususan, noqonuniy bank-moliya operatsiyalari orqali oʻzgalarning plastik kartadagi mablagʻlarini oʻzlashtirish, zararli viruslar tarqatish, qimor va tavakkalchilikka asoslangan onlayn oʻyinlar, diniy aqidaparastlikka qaratilgan axborot xurujlari, onlayn savdo maydonidagi firibgarlik jinoyatlari koʻpayib bormoqda.[178]Cybersecurity Ventures ma'lumotlariga koʻra, 2025 yilda kiberjinoyatlarning jahon iqtisodiyotiga yetkazgan zarari 9,5 trillion AQSh dollaridan oshadi.[179] Oʻzbekistonda ham 2024 yilda UzCERT markazi tomonidan 15 mingdan ortiq kiberhujum qayd etilgan boʻlib, bu oʻtgan yilga nisbatan 48 % koʻpdir. Shiddat bilan rivojlanib borayotgan zamonda har bir inson o'zining moliyaviy xavfsizligini ta'minlay olishi, kibermakonda turli xil tajovuzlarga qarshi immunitet shakllanishi, ayniqsa muhim ahamiyat kasb etadi. Bunda har birimiz hozirgi kunda kiberjinoyat tushunchasi, shuningdek, sodir etilayotgan kiberjinoyatlarning turlari va tavsifi haqida yetarlicha bilimga ega bo'lishimiz firibgarlarning tuzog'iga tushib qolmasligimiz uchun zamin yaratadi.

Kiberjinoyatlar – kibermakonda kompyuter texnologiyalari va internetdan foydalangan holda sodir etiladigan jinoyatlar hisoblanadi. Bu axborot

[178] Xatamov R. (IIV Akademiyasi boshlig'i, professor). Kiber makonda sodir etilayotgan jinoyatlarga qarshi kurashish: muammolar va yechimlar. IIV Akademiyasi ilmiy anjumani materiallari. 2024 y. (Raqamli dalillarni to'plash va xalqaro hamkorlik masalalari)
[179] https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

texnologiyalarining rivojlanishi natijasida paydo bo'lgan yangi turdagi jinoyatlar bo'lib, moliyadan tortib sog'liqni saqlash, ta'lim va davlat idoralarigacha bo'lgan ko'plab sohalarga ta'sir qiladi. Kiberjinoyatlarning quyidagi asosiy xususiyatlarini tahlil qilamiz:

Axborot tizimiga zarar yetkazish – ma’lumotlarni o‘g‘irlash, yo‘q qilish yoki o‘zgartirish.

Moliyaviy va iqtisodiy zarar – onlayn firibgarlik, bank kartalaridagi mablag’larni o‘g‘irlash.

Shaxsiy hayotga tajovuz – shaxsiy ma’lumotlarni noqonuniy to‘plash, shantaj qilish.

Davlat xavfsizligiga tahdid – kibersabotaj, kiberterrorchilik, terrorizmni moliyalashtirish.

Kiberjinoyatlarni quyidagi mezonlar bo’yicha bo‘yicha tasniflashimiz mumkin:

1. Tuzilishi bo‘yicha

- Oddiy foydalanuvchiga qaratilgan jinoyatlar (shaxsiy ma’lumotlarni o‘g‘irlash, phishing).
- Korporativ va davlat tizimlariga qaratilgan hujumlar (DDoS hujumlari, ma’lumotlar bazasiga kirish).

2. Ma’lumotlarga qaratilgan jinoyatlar

- Ma’lumotlarni o‘g‘irlash (hacking, ransomware).
- Ma’lumotlarni buzish yoki yo‘q qilish.
- Shaxsga doir ma’lumotlarni ruxsatsiz yig’ish, tarqatish.

3. Moliyaviy jinoyatlar

- Onlayn firibgarlik, kartadan pul yechish, noqonuniy kredit rasmiylashtirish;
- Noqonuniy kriptovalyutalar aylanmasi va elektron to‘lov tizimlariga hujumlar.

4. Axborot va kommunikatsiya jinoyatlari

- Spam, zararli dasturlar tarqatish.
- Internet orqali tajovuz, tahdid yoki firibgarlik.

Ushbu tasnif BMT va Yevropa Kengashi konvensiyalariga asoslangan bo‘lib, kiberjinoyatlarni “kiberbog‘langan” (texnologiyaga asoslangan) va “kiber qo‘llab-quvvatlangan” (an’anaviy jinoyatlarni raqamlashtirgan) turlarga ajratishga imkon beradi. O‘zbekistonda kiberjinoyatlarning 98 foizi bank kartalari bilan bog‘liq bo‘lib, bu moliyaviy tarmoqning zaifligini ko‘rsatadi.

Kiberjinoyatlarni aniqlash jarayonida raqamli dalillar (digital evidence) asosiy rol o‘ynaydi. Raqamli dalillar – bu kompyuterlar, mobil qurilmalar, tarmoqlar va bulutli saqlashdan olingan ma’lumotlar bo‘lib, log fayllar, elektron pochta, metadata, internet tarixi va zararli dastur izlarini o‘z ichiga oladi.

Ular kiberjinoyatlarni tergov qilishning “asosiy umurtqasi” hisoblanadi, chunki an’anaviy dalillardan farqli o‘laroq, ularni saqlash, tahlil qilish va sudda isbotlash uchun maxsus raqamli forensika (digital forensics) usullaridan foydalaniladi.

Yuqoridagi ta’rif Raqamli materiallar (Elektron ma’lumotlar) nima? degan savolni o‘rtaga tashlaydi. Shunday ekan, endi raqamli dalillarning xususiyatlari va turlariga to‘xtalib o‘tamiz. Raqamli dalillarni moddiy (an’anaviy) dalillardan farq qiluvchi ayrim jihatlari mavjud. Ya’ni,

1) Raqamli dalillarning keng qamrovliligi;

2) U moddiy va o‘ziga xos sezgir axborot bilan bog‘liq;

3) Dalillarni to‘plashda huquqni muhofaza qiluvchi organlarning odatiy rolidan tashqariga chiqadigan jinoyat-sud ishlariga bog‘liq masalalarga tegishlidir.

An’anaviy kriminalistikada moddiy dalillarning o‘ziga xos xususiyatlari bo‘lgani kabi raqamli dalillarning ham o‘ziga xos xususiyatlari mavjud.

Biroq ushbu xususiyatlar an’anaviy dalillarning xususiyatlaridan keskin farq qiladi.

Raqamli dalillarning xususiyatlari:

- Ko‘rinmaslik;
- Murakkab tarkibli;
- Izohlashning mushkulligi.

Ushbu xususiyatlar bilan birga raqamli dalillar raqamli ma’lumotlar sifatida quyidagi ko‘rinishlarda uchraydi.

1) Uchuvchi ma’lumotlar

2) Zaxira (Kesh) ma’lumotlari

3) Qoldiq ma’lumotlar

4) Jurnal ma’lumotlari

5) Ulanish ma’lumotlari

Raqamli dalillarning afzalliklari:

Tezlik va global qamrov: ular hujumni real vaqtda kuzatishga imkon beradi va jinoyatchilarni butun dunyo bo‘ylab izlashda yordam beradi. Masalan, ransomware hujumida zararli kodning IP-manzillari va loglari orqali manbani aniqlash mumkin.

Obyektivlik: Metadata va log fayllar firibgarlikni isbotlashda nochor dalillar beradi, masalan, phishing elektron pochtasining sarlavhasi va havola izlari.

Qayta tiklash imkoniyati: O‘chirilgan ma’lumotlarni tiklash orqali zarar miqdorini baholash va oldini olish choralari ko‘rish mumkin.

Raqamli forensika jarayoni quyidagi bosqichlarni o‘z ichiga oladi:Identifikatsiya: Potentsial dalil manbalarini aniqlash (qurilmalar, tarmoqlar).

Saqlash: Dalillarni o‘zgartirishsiz saqlash (hash qiymatlari orqali).

Tahlil: Dasturlar (masalan, EnCase yoki Autopsy) yordamida izlarni ochish.Dalillarni sudda taqdim etish: Dalillarning qonuniyligini isbotlash.

Kiberjinoyatlarni oldini olish borasida olib borilayotgan keng qamrovli islohotlar mobaynida 21.11.2024-yilda “O’zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o’zgartirish va qo’shimchalar kiritish to’g’risida”gi O’RQ-1003 sonli O’zbekiston Respublikasining qonuni qabul qilindi. Mazkur qonun bilan O‘zbekiston Respublikasining ayrim kodeks

va qonunlariga raqamli dalillar tushunchasini, raqamli dalillarni to‘plash, taqdim etish, mustahkamlash, ko‘zdan kechirish, tekshirish va baholash, ularni saqlash, qaytarish hamda yo‘q qilish tartibini belgilovchi o‘zgartirish va qo‘shimchalar kiritildi. Kiberjinoyatlarni aniqlashda raqamli dalillarning ahamiyati va ularni tezkor xodimlar tomonidan qonuniy ravishda olish zarurati beqiyos darajada katta. Zamonaviy kiberjinoyatlarda ko‘pincha jismoniy iz qolmaydi: jinoyatchi minglab kilometr uzoqlikda bo‘lishi, qurol o‘rniga kod ishlatishi, “jinoyat joyi” esa serverlarda, smartfonlarda yoki bulutli xizmatlarda joylashgan bo‘ladi. Shu sababli, log-fayllar, IP-manzillar, metadata, elektron pochta sarlavhalari, messenjerlardagi yozishmalar, blockchain tranzaksiyalari, GPS-ma’lumotlari, o‘chirilgan fayllarning qoldiqlari kabi raqamli dalillar deyarli yagona ob’ektiv isbot vositasiga aylanadi. Aynan ular jinoyatchining harakatlarini aniq vaqt, joy va usul bilan bog‘lab, kimligini aniqlashga, yetkazilgan zararni hisoblashga hamda sudda rad etib bo‘lmaydigan dalil sifatida taqdim etishga imkon beradi.Raqamli dalilning eng katta zaif tomoni shundaki, u juda oson o‘zgartirilishi yoki yo‘q qilinishi mumkin. Gumonlanuvchining o’z telefonini qo‘lga kiritib, oddiygina yoqib ko‘rish, parol so‘rash, internetga ulash yoki hatto tezkor xodimning barmoq izi qoldirishi butun dalil zanjirini buzib, sudda foydalanish imkoniyatidan mahrum qilishi mumkin. Shu sababli, O‘zbekiston Respublikasi Jinoyat-protsessual kodeksining “Tezkor-qidiruv faoliyati to‘g‘risida”gi qonun hamda xalqaro standartlarda (ISO/IEC 27037, NIST SP 800-86, ACPO Good Practice Guide) raqamli dalillarni olish, saqlash va tahlil qilishda qat’iy tartib-qoidalari belgilab qo‘yilgan.Tezkor xodim birinchi bo‘lib voqea joyiga yetib kelganda yoki dalilni qo’lga kiritganda dalilning butun taqdiri uning harakatlariga bog‘liq bo‘ladi. U qurilmani o‘chirmasligi kerak (chunki operativ xotiradagi muhim ma’lumotlar yo‘qoladi), agar qurilma o‘chirilgan bo‘lsa, uni yoqmasligi, Wi-Fi va mobil internetni uzishi (masalan, Faraday sumkasi yoki “airplane mode” orqali), qurilmaga hech qanday dastur o‘rnatmasligi va barmoq izi qoldirmasligi lozim. Dalilni olishda albatta write-blocker (yozishni bloklovchi) uskunalaridan foydalaniladi, qurilmaning to‘liq forensik nusxasi (bit-by-bit image) olinadi va har bir nusxaning hash-qiymati (SHA-256) hisoblanib, maxsus protokolda qayd etiladi. “Dalil zanjiri” (chain of custody) hujjati sekundlik aniqlikda to‘ldiriladi: kim olgan, qachon olgan, qayerdan olgan, kimdan kimaga o‘tkazgan – har bir harakat imzo va vaqt bilan tasdiqlanadi. Agar zanjirning bir bo‘g‘inida uzilish bo‘lsa, eng muhim raqamli dalil ham sudda qabul qilinmaydi. Shunday qilib, raqamli dalilning isbot kuchini saqlab qolishi xodimning qonunga to‘liq rioya qilgan holda harakat qilishiga bog‘liq. Tezkor xodimning birinchi harakatlari noto‘g‘ri bo‘lsa, eng zamonaviy forensik laboratoriya va eng tajribali ekspert ham dalilni tiklay olmaydi. Shu bois, Ichki ishlar vazirligi tizimida raqamli forensika bo‘yicha doimiy o‘quv kurslari tashkil etilishi, tezkor xodimlar maxsus tayyorgarliklardan o‘tishi va har bir hududiy bo‘linmada raqamli dalillarni tezkor olish uchun zarur jihozlar (write-blocker, forensik planshetlar, Faraday sumkalari va h.k) bilan ta’minlanishi bugungi kunda eng dolzarb vazifalardan biridir. Faqat shunday

yondashuv orqaligina kiberjinoyatchilarni qonun oldida javobgarlikka tortish va fuqarolarimizning raqamli xavfsizligini ta’minlash mumkin bo‘ladi.

Kiberjinoyatlar bugungi kunda nafaqat eng tez o‘sib borayotgan, balki iqtisodiy zarar ko‘lami va jamiyatga tahdid darajasi bo‘yicha an’anaviy jinoyatlardan keskin ustun kelayotgan transmilliy xavf-xatardir. O‘zbekiston Respublikasida 2024-yilda kiberjinoyatlar soni 2023-yilga nisbatan 9,1 baravar oshib, umumiy jinoyatlarning 44,4 % ini tashkil etgani, ularning 98 % dan ortig‘i moliyaviy yo‘nalishda sodir etilgani mamlakatimiz raqamli iqtisodiyoti va fuqarolar moliyaviy xavfsizligi uchun jiddiy signaldir. Ushbu jinoyatlarning o‘ziga xosligi – ularning deyarli butunlay raqamli izlarga asoslanishidadir. Shuning uchun raqamli dalillar (log-fayllar, metadata, tranzaksiya izlari, forensik obrazlar) kiberjinoyatni aniqlash, isbotlash va jinoyatchini javobgarlikka tortishning yagona ishonchli va obyektiv vositasiga aylandi. Biroq, raqamli dalilning sudda qabul qilinishi uning qonuniy, o‘zgarmas va uzluksiz zanjirda olinganligiga to‘liq bog‘liq bo‘lib, bu esa tezkor xodimlardan tortib ekspert-kriminalistgacha bo‘lgan barcha ishtirokchilarning yuqori malaka va qat’iy intizomni talab qiladi. Bu borada yanada samarali natijalarga erishish hamda kiberjinoyatlarni aniqlash va fosh etish, shuningdek aybdorlarga nisbatan qonuniy va adolatli chora ko’rilishida quyidagi bir qator takliflarni ilgari surib o’taman:

- O‘zbekiston Respublikasi Jinoyat-protsessual kodeksiga “Raqamli dalillarni olish, saqlash va ekspertizadan o‘tkazish tartibi” to‘g‘risida alohida bob kiritish, shuningdek ISO/IEC 27037 va ACPO standartlariga to‘liq moslashtirilgan milliy yo‘riqnoma qabul qilish.
- Barcha tezkor vakil, ekspert va tergovchilarni “Digital Evidence First Responder”(CDEFR) xalqaro sertifikatidan majburiy o‘tkazish va har yili qayta attestatsiyadan o‘tish tizimini joriy qilish.
- Ichki ishlar vazirligi tizimida har bir viloyatda kamida bitta to‘liq jihozlangan raqamli forensika laboratoriyasini tashkil etish hamda markaziy apparatda “Kiberjinoyatlarga qarshi tezkor-ekspert guruhi” (24/7)ni shakllantirish.

F O Y D A L A N I L G A N A D A B I Y O T L A R :

1. O‘zbekiston Respublikasining Qonuni – “O’zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o’zgartirish va qo’shimchalar kiritish to’g’risida”, O‘RQ – 1003-sonli 21.11.2024-yil
2. O‘zbekiston Respublikasining Qonuni – “Kiberxavfsizlik to’g’risida”, O‘RQ – 764, 15.04.2022-yil
3. O‘zbekiston Respublikasining Qonuni – “Normativ-huquqiy hujjatlar to‘g‘risida”, O‘RQ – 681, 20.04.2021-yil
4. Xatamov R. (IIV Akademiyasi boshlig'i, professor). Kiber makonda sodir etilayotgan jinoyatlarga qarshi kurashish: muammolar va yechimlar. IIV Akademiyasi

ilmiy anjumani materiallari. 2024 y. (Raqamli dalillarni to'plash va xalqaro hamkorlik masalalari)

5. Abduraximov B.F. (professor). Kiberxavfsizlik va kriminalistika: Raqamli dalillarni tahlil qilish usullari. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti nashriyoti. 2023 y. (Kiberjinoyatlarda raqamli dalillarning o'ziga xosligi va forensika usullari).

6. Kun.uz. Uzbekistan sees 68-fold surge in cybercrime: Nearly 2 trillion UZS stolen in five years. 29.05.2025 y. (Kiberjinoyatlar o'sishi va 44.4% ulushi haqida)

7. Gazeta.uz. Cybercrimes in Uzbekistan increase 68-fold in five years. 31.05.2025 y. (98% bank kartalari bilan bog'liq kiberjinoyatlar va statistika).

8. UzCERT. Uzbekistan strengthened its position in the Global Cyber Security Index. 10.10.2024 y. (Kiberxavfsizlik hodisalari statistikasi)

9. Council of Europe. Budapest Convention on Cybercrime (ETS No. 185). 2001 y.

10. ISO. ISO/IEC 27037:2012 – Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. 2012 y.

11. NIST. SP 800-86: Guide to Integrating Forensic Techniques into Incident Response. 2006 y.

12. ACPO. Good Practice Guide for Digital Evidence. 2012 y.