KIBERJINOYATLARGA QARSHI KURASHDA RAQAMLI KRIMINALISTIKA TEXNOLOGIYALARINING AHAMIYATI

Raxmanova Mohidil Egamberdiyevna
O'zbekiston respublikasi ichki ishlar vazirligi
Akademiya Kriminalistik ekspertizalar kafedrasi katta o'qituvchi
mohidil.rahmonova88@gmail.com Tel: 971100203
https://doi.org/10.5281/zenodo.20269898

ARTICLE INFO

Qabul qilindi: 14-may 2026 yil
Ma'qullandi: 16-may 2026 yil
Nashr qilindi: 18-may 2026 yil

KEYWORDS

raqamli kriminalistika, kiberjinoyat, raqamli dalillar, kiberxavfsizlik, kriminalistika laboratoriyasi, axborot xavfsizligi, raqamli ekspertiza, xalqaro standartlar, dasturiy vositalar, tergov jarayoni, elektron dalillar, texnologiyalar.

ABSTRACT

Ushbu maqolada kiberjinoyatlarga qarshi kurashishda raqamli kriminalistika texnologiyalarining o'rni va ahamiyati tahlil qilinadi. Zamonaviy axborot-kommunikatsiya texnologiyalarining rivojlanishi bilan bir qatorda kiberjinoyatlar soni va murakkabligi ortib borayotgani, bu esa raqamli dalillar bilan ishlashning zamonaviy usullarini qo'llash zaruratini yuzaga keltirayotgani yoritiladi. Maqolada raqamli kriminalistika texnologiyalarining kiberjinoyatlarni aniqlash, tergov qilish, raqamli dalillarni yig'ish, saqlash va tahlil qilishdagi imkoniyatlari ko'rib chiqiladi. Shuningdek, kriminalistika laboratoriyalarida qo'llaniladigan zamonaviy dasturiy vositalar, xalqaro standartlar va innovatsion yondashuvlarning amaliy ahamiyati ochib beriladi. Tadqiqot natijasida raqamli kriminalistika texnologiyalarini rivojlantirish kiberxavfsizlikni ta'minlashning muhim omillaridan biri ekanligi asoslab beriladi.

XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalarida raqamlashtirish jarayonlarini keskin tezlashtirdi. Davlat boshqaruvi, moliya-bank tizimi, elektron tijorat, sog'liqni saqlash, ta'lim, transport va telekommunikatsiya kabi strategik yo'nalishlarda raqamli texnologiyalarning keng joriy etilishi inson faoliyatini yanada qulay va samarali tashkil etishga xizmat qilmoqda. Shu bilan birga, raqamli muhitning kengayishi yangi turdagi tahdidlar, xususan kiberjinoyatchilikning rivojlanishiga ham zamin yaratmoqda. Natijada axborot xavfsizligini ta'minlash, raqamli ma'lumotlarni himoya qilish hamda kiberjinoyatlarga qarshi samarali kurashish bugungi kunning dolzarb masalalaridan biriga aylandi.

Hozirgi davrda kiberjinoyatlar global xavfsizlikka tahdid solayotgan asosiy omillardan biri sifatida e'tirof etilmoqda. Jahon miqyosida amalga oshirilayotgan kiberhujumlar nafaqat yirik korporatsiyalar va davlat tashkilotlariga, balki oddiy fuqarolarning shaxsiy ma'lumotlari va moliyaviy resurslariga ham katta zarar yetkazmoqda. Tadqiqotlarga ko'ra, 2024-yilda kiberjinoyatlar natijasida jahon iqtisodiyotiga yetkazilgan zarar hajmi trillionlab AQSH dollariga yetgan bo'lib, kelgusi yillarda ushbu ko'rsatkich yanada ortishi prognoz

qilinmoqda[1]. Ayniqsa, sun'iy intellekt texnologiyalari asosida amalga oshirilayotgan zamonaviy kiberhujumlar, phishing sxemalari, zararli dasturlar, ransomware va deepfake texnologiyalarining rivojlanishi kiberxavfsizlik tizimlariga jiddiy tahdid tug'dirmoqda.[1]

O'zbekiston Respublikasida ham raqamli texnologiyalarning jadal rivojlanishi bilan bir qatorda kiberjinoyatlar soni keskin ortib bormoqda. Kiberjinoyatlarning asosiy qismi bank kartalari orqali sodir etilayotgan firibgarlik, noqonuniy pul yechib olish, zararli dasturlar yordamida foydalanuvchi ma'lumotlarini qo'lga kiritish, ijtimoiy muhandislik usullari orqali fuqarolarni aldash hamda noqonuniy elektron operatsiyalar bilan bog'liqdir. Mazkur holatlar kiberjinoyatlarni aniqlash va fosh etishda zamonaviy texnologik vositalardan foydalanishni taqozo etadi. Shu nuqtai nazardan raqamli kriminalistika texnologiyalari kiberjinoyatlarga qarshi kurashishda muhim ilmiy-amaliy vosita sifatida namoyon bo'lmoqda.

Raqamli kriminalistika — bu kompyuterlar, mobil qurilmalar, serverlar, tarmoq infratuzilmalari va boshqa elektron vositalarda mavjud bo'lgan raqamli dalillarni aniqlash, yig'ish, saqlash, tiklash, tahlil qilish va sud-tergov jarayonlarida foydalanishga qaratilgan kriminalistikaning zamonaviy yo'nalishidir. Ushbu texnologiyalar yordamida o'chirilgan fayllarni tiklash, zararli dasturlar faoliyatini aniqlash, foydalanuvchi harakatlarini rekonstruksiya qilish, tarmoq hujumlari manbalarini aniqlash hamda elektron dalillarning haqiqiyligini tekshirish imkoniyati yaratiladi. Bugungi kunda raqamli kriminalistika texnologiyalari kriminalistika laboratoriyalarida keng qo'llanilmoqda. Zamonaviy laboratoriyalarda EnCase, FTK, Autopsy, Cellebrite UFED, Magnet AXIOM kabi maxsus dasturiy vositalardan foydalanilib, raqamli qurilmalardan dalillar olish va ularni kompleks tahlil qilish amalga oshiriladi. Shu bilan birga, xalqaro standartlar asosida ishlab chiqilgan metodik yondashuvlar ekspertiza jarayonining ishonchliligi va dalillarning protsessual maqbulligini ta'minlashda muhim ahamiyat kasb etadi. Xususan, National Institute of Standards and Technology (NIST), National Institute of Justice (NIJ), INTERPOL, Europol hamda International Organization for Standardization / International Electrotechnical Commission tomonidan ishlab chiqilgan standart va metodikalar raqamli dalillar bilan ishlashning yagona xalqaro tizimini shakllantirishga xizmat qilmoqda. Mazkur standartlar raqamli dalillarning yaxlitligi, autentikligi va sud jarayonida qabul qilinishini ta'minlashda muhim omil hisoblanadi. Mazkur maqolaning maqsadi kiberjinoyatlarga qarshi kurashishda raqamli kriminalistika texnologiyalarining o'rni va ahamiyatini ilmiy jihatdan tahlil qilish, zamonaviy kriminalistika laboratoriyalarida qo'llanilayotgan texnologik vositalar hamda xalqaro standartlarning amaliy ahamiyatini yoritishdan iboratdir.

Tadqiqot metodologiyasi. Mazkur tadqiqotda kiberjinoyatlarga qarshi kurashishda raqamli kriminalistika texnologiyalarining ahamiyatini ilmiy jihatdan tahlil qilishga qaratilgan kompleks metodologik yondashuv qo'llanildi. Tadqiqot jarayonida nazariy, tahliliy va qiyosiy metodlardan foydalanildi hamda xalqaro tashkilotlar tomonidan ishlab chiqilgan standartlar va metodik tavsiyalar asosiy ilmiy manba sifatida o'rganildi.

Tadqiqotning metodologik asosini raqamli kriminalistika, axborot xavfsizligi va kiberxavfsizlik sohalaridagi zamonaviy ilmiy yondashuvlar tashkil etadi. Xususan, raqamli

[1] https://www.techradar.com/

dalillar bilan ishlash jarayonlarini o‘rganishda National Institute of Standards and Technology (NIST), National Institute of Justice (NIJ), International Organization for Standardization / International Electrotechnical Commission tomonidan ishlab chiqilgan xalqaro standartlar va metodik tavsiyalar tahlil qilindi.

Tadqiqot davomida quyidagi metodlardan foydalanildi:

1. Tahliliy metod. Mazkur metod asosida kiberjinoyatlar dinamikasi, ularning zamonaviy shakllari hamda raqamli kriminalistika texnologiyalarining amaliy imkoniyatlari o‘rganildi. Turli ilmiy maqolalar, statistik ma’lumotlar, xalqaro hisobotlar va rasmiy manbalar tahlil qilinib, kiberjinoyatlarning jamiyat va iqtisodiyotga salbiy ta’siri yoritildi.

2. Qiyosiy-huquqiy metod. Ushbu metod yordamida turli davlatlarda raqamli kriminalistika faoliyatini tashkil etish tajribasi, xalqaro standartlar va kriminalistika laboratoriyalari faoliyati o‘zaro taqqoslandi. Xususan, AQSH, Buyuk Britaniya va Yevropa Ittifoqida qo‘llanilayotgan metodik yondashuvlar O‘zbekiston amaliyoti bilan qiyosiy ravishda o‘rganildi.

3. Tizimli yondashuv metodi. Raqamli kriminalistika jarayoni yagona tizim sifatida ko‘rib chiqildi. Tadqiqot davomida raqamli dalillarni yig‘ish, saqlash, nusxalash, tahlil qilish va sudga taqdim etish bosqichlari o‘zaro bog‘liq tizim sifatida tahlil qilindi. Shu asosda kriminalistika laboratoriyalarining kiberjinoyatlarga qarshi kurashdagi o‘rni baholandi.

4. Statistik tahlil metodi. Kiberjinoyatlar soni, iqtisodiy Metod miqdori hamda kiberhujumlar dinamikasi bo‘yicha rasmiy Metodi73ic ma’lumotlar o‘rganildi. Xususan, xalqaro kiberxavfsizlik tashkilotlari va O‘zbekiston Respublikasi huquqni muhofaza qiluvchi organlari tomonidan e’lon qilingan Metodi73ic ma’lumotlardan foydalanildi.

5. Empirik kuzatuv metodi. Kriminalistika laboratoriyalarida qo‘llanilayotgan zamonaviy dasturiy vositalar va texnologiyalar o‘rganildi. Xususan, mobil qurilmalar, kompyuter tizimlari va tarmoq infratuzilmalaridan raqamli dalillar olish jarayonlari amaliy nuqtai nazardan tahlil qilindi.

Mazkur metodologik yondashuv tadqiqot mavzusini kompleks ravishda o‘rganish, raqamli kriminalistika texnologiyalarining amaliy ahamiyatini ochib berish hamda kiberjinoyatlarga qarshi kurashishda xalqaro tajribaning o‘rnini aniqlash imkonini berdi.

Adabiyotlar tahlili. Raqamli kriminalistika va kiberjinoyatlarga qarshi kurash masalalari so‘nggi yillarda xalqaro miqyosda keng tadqiq etilayotgan ilmiy yo‘nalishlardan biriga aylandi. Mazkur sohada olib borilgan ilmiy tadqiqotlar asosan raqamli dalillar bilan ishlash metodologiyasi, kriminalistika laboratoriyalari faoliyati, xalqaro standartlar hamda zamonaviy texnologiyalarni amaliyotga joriy etish masalalariga qaratilgan.

Raqamli kriminalistika sohasidagi dastlabki ilmiy-metodik yondashuvlar National Institute of Standards and Technology (NIST) tomonidan ishlab chiqilgan qo‘llanmalarda o‘z aksini topgan. Xususan, NISTning “Guide to Integrating Forensic Techniques into Incident Response” nomli metodik qo‘llanmasida raqamli dalillar bilan ishlashning asosiy bosqichlari: ma’lumotlarni yig‘ish, tadqiq qilish, tahlil qilish va hisobot tayyorlash jarayonlari ilmiy asoslangan holda yoritilgan. Mazkur metodika bugungi kunda ko‘plab kriminalistika laboratoriyalarida asosiy amaliy standart sifatida qo‘llaniladi.

Shuningdek, National Institute of Justice (NIJ) tomonidan ishlab chiqilgan “Electronic Crime Scene Investigation: A Guide for First Responders” qo‘llanmasida elektron jinoyat sodir etilgan hodisa joyida raqamli dalillar bilan ishlashning protsessual va texnik jihatlari batafsil

bayon etilgan. Mazkur tadqiqotlar raqamli dalillarni yig‘ish jarayonida dalillarning yaxlitligini saqlash muhimligini asoslab beradi.

Buyuk Britaniyada Association of Chief Police Officers (ACPO) tomonidan ishlab chiqilgan “Good Practice Guide for Digital Evidence” qo‘llanmasi raqamli kriminalistika sohasidagi eng muhim metodik manbalardan biri hisoblanadi. Ushbu qo‘llanmada raqamli dalillar bilan ishlashning fundamental tamoyillari ishlab chiqilgan bo‘lib, ular dalillarni o‘zgartirmaslik, barcha harakatlarni hujjatlashtirish va ekspertiza natijalarining qayta tekshirilishini ta’minlashga qaratilgan.

Bundan tashqari, International Organization for Standardization va International Electrotechnical Commission tomonidan ishlab chiqilgan ISO/IEC 27037 hamda ISO/IEC 27043 standartlari raqamli dalillarni identifikatsiya qilish, yig‘ish, saqlash va tahlil qilish bo‘yicha xalqaro mezonlarni belgilaydi. Ushbu standartlar kriminalistika laboratoriyalarida ekspertiza jarayonining ishonchliligini ta’minlashda muhim o‘rin tutadi.

Kiberjinoyatlarga qarshi kurashishda xalqaro tashkilotlarning ilmiy-amaliy faoliyati ham alohida ahamiyatga ega. Jumladan, INTERPOL hamda Europol tomonidan transmilliy kiberjinoyatlar bo‘yicha olib borilgan tadqiqotlar raqamli kriminalistika texnologiyalarining zamonaviy jinoyatchilikka qarshi kurashdagi ahamiyatini ochib beradi. Ushbu tashkilotlar tomonidan ishlab chiqilgan tavsiyalar xalqaro hamkorlikni rivojlantirish va raqamli dalillar almashinuvini takomillashtirishga xizmat qiladi. So‘nggi yillarda ilmiy adabiyotlarda sun’iy intellekt, bulutli texnologiyalar va IoT qurilmalarining raqamli kriminalistikaga ta’siri ham keng tadqiq etilmoqda. Zamonaviy tadqiqotlar katta hajmdagi ma’lumotlarni avtomatik tahlil qilish, zararli dasturlarni aniqlash hamda deepfake texnologiyalarini ekspertiza qilish masalalariga alohida e’tibor qaratmoqda. Tahlil qilingan ilmiy manbalar shuni ko‘rsatadiki, raqamli kriminalistika texnologiyalarini rivojlantirish kiberjinoyatlarga qarshi kurashish samaradorligini oshirishning muhim omillaridan biri hisoblanadi. Shu bilan birga, xalqaro standartlarni milliy amaliyotga joriy etish, kriminalistika laboratoriyalarini modernizatsiya qilish va malakali mutaxassislar tayyorlash dolzarb vazifalardan biri bo‘lib qolmoqda.

Natijalar. Mazkur tadqiqot davomida kiberjinoyatlarga qarshi kurashishda raqamli kriminalistika texnologiyalarining ahamiyati, xalqaro standartlarning o‘rni hamda kriminalistika laboratoriyalarining amaliy faoliyati kompleks ravishda tahlil qilindi. Tadqiqot natijalari shuni ko‘rsatdiki, zamonaviy axborot texnologiyalarining rivojlanishi bilan bir qatorda kiberjinoyatlar soni va murakkabligi ham ortib bormoqda. Shu sababli raqamli dalillar bilan ishlashning ilmiy asoslangan metodologiyasini shakllantirish va xalqaro standartlarga mos laboratoriya tizimini rivojlantirish muhim ahamiyat kasb etmoqda. Tahlillar natijasida aniqlanishicha, raqamli kriminalistika texnologiyalari kiberjinoyatlarni fosh etishda eng muhim vositalardan biri hisoblanadi. Xususan, kompyuter tizimlari, mobil qurilmalar, serverlar, bulutli saqlash tizimlari va tarmoq infratuzilmalaridan olinadigan raqamli dalillar jinoyat mexanizmini aniqlash, jinoyatchining harakatlarini rekonstruksiya qilish hamda sud-tergov jarayonida ishonchli dalillar bazasini shakllantirish imkonini beradi. Tadqiqot davomida xalqaro tashkilotlar tomonidan ishlab chiqilgan metodik tavsiyalar va standartlarning amaliy ahamiyati ham o‘rganildi. Jumladan, National Institute of Standards and Technology (NIST), National Institute of Justice (NIJ), Association of Chief Police Officers (ACPO), INTERPOL hamda International Organization for Standardization / International Electrotechnical Commission standartlari raqamli dalillar bilan ishlashda yagona protsessual yondashuvni shakllantirishga

xizmat qilishi aniqlandi. Ushbu standartlar dalillarning yaxlitligini saqlash, ularning autentikligini tasdiqlash hamda sudda maqbulligini ta’minlashda muhim omil hisoblanadi. Kriminalistika laboratoriyalari faoliyatini o‘rganish natijasida zamonaviy laboratoriyalarda maxsus dasturiy va apparat vositalaridan keng foydalanilishi ma’lum bo‘ldi. Xususan, mobil qurilmalardan ma’lumot olish, o‘chirilgan fayllarni tiklash, tarmoq trafikini tahlil qilish, zararli dasturlarni aniqlash va bulutli muhitdagi ma’lumotlarni ekspertiza qilish imkonini beruvchi texnologiyalar tergov samaradorligini sezilarli darajada oshirishi aniqlandi. Shu bilan birga, laboratoriya faoliyatida avtomatlashtirilgan tahlil tizimlari va sun’iy intellekt texnologiyalaridan foydalanish raqamli dalillarni tezkor qayta ishlash imkonini bermoqda. Tadqiqot davomida bir qator muammolar ham aniqlandi. Jumladan:

- raqamli texnologiyalarning tez o‘zgarishi;
- yangi turdagi zararli dasturlar va kiberhujumlarning paydo bo‘lishi;
- malakali mutaxassislar yetishmasligi;
- ayrim laboratoriyalarda texnik vositalarning eskirganligi;
- xalqaro standartlarning milliy amaliyotga to‘liq integratsiya qilinmaganligi.

Mazkur muammolarni bartaraf etish maqsadida kriminalistika laboratoriyalarini modernizatsiya qilish, xalqaro standartlarni milliy ekspertiza tizimiga joriy etish, ekspertlarning malakasini muntazam oshirib borish hamda sun’iy intellekt asosidagi kriminalistik texnologiyalarni rivojlantirish zarurligi asoslandi. Tadqiqot natijalari shuni ko‘rsatdiki, raqamli kriminalistika texnologiyalarini rivojlantirish va xalqaro standartlarga asoslangan laboratoriya amaliyotini joriy etish kiberjinoyatlarga qarshi kurash samaradorligini oshirish, raqamli dalillarning ishonchliligini ta’minlash hamda sud-tergov faoliyatining sifatini yaxshilashda muhim omil hisoblanadi.

Xulosa. Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kiberjinoyatlar soni, ko‘lami va murakkabligi sezilarli darajada ortib bormoqda. Mazkur holat huquqni muhofaza qiluvchi organlar oldiga raqamli muhitda sodir etilayotgan jinoyatlarni tezkor aniqlash, ishonchli dalillarni to‘plash va ularni sud-tergov jarayonida samarali qo‘llash vazifasini qo‘ymoqda. Shu nuqtai nazardan, raqamli kriminalistika texnologiyalari zamonaviy jinoyatchilikka qarshi kurashning muhim tarkibiy qismi sifatida namoyon bo‘lmoqda.

Tadqiqot natijalari shuni ko‘rsatdiki, raqamli dalillar kompyuter tizimlari, mobil qurilmalar, serverlar, bulutli platformalar va tarmoq infratuzilmalarida saqlanadigan muhim axborot manbasi hisoblanadi. Ushbu dalillarni to‘g‘ri yig‘ish, saqlash, tahlil qilish va sudga taqdim etish jarayonlari esa xalqaro standartlar asosida amalga oshirilgandagina ularning ishonchliligi va protsessual maqbulligi ta’minlanadi.

Maqolada National Institute of Standards and Technology (NIST), National Institute of Justice (NIJ), Association of Chief Police Officers (ACPO), INTERPOL hamda International Organization for Standardization / International Electrotechnical Commission kabi xalqaro tashkilotlarning raqamli kriminalistika sohasidagi faoliyati tahlil qilinib, ular tomonidan ishlab chiqilgan metodik tavsiyalar va standartlarning amaliy ahamiyati yoritildi. Mazkur standartlar raqamli dalillar yaxlitligini saqlash, ekspertiza jarayonining shaffofligini ta’minlash va sudda dalillarning qabul qilinish darajasini oshirishga xizmat qilishi aniqlandi.

Shuningdek, kriminalistika laboratoriyalarining zamonaviy texnik va dasturiy vositalar bilan jihozlanishi kiberjinoyatlarni tergov qilish samaradorligini oshirishda muhim omil

ekanligi asoslandi. Mobil qurilmalar ekspertizasi, tarmoq trafikini tahlil qilish, zararli dasturlarni aniqlash va sun'iy intellekt asosidagi avtomatlashtirilgan tizimlardan foydalanish tergov jarayonini tezlashtirish hamda katta hajmdagi ma'lumotlarni samarali qayta ishlash imkonini bermoqda.

Tadqiqot davomida raqamli kriminalistika sohasida mavjud ayrim muammolar ham aniqlandi. Jumladan, zamonaviy kiberxavflarning murakkablashuvi, malakali mutaxassislar yetishmasligi, texnik bazaning barcha hududlarda bir xil darajada rivojlanmaganligi hamda xalqaro standartlarning milliy amaliyotga to'liq joriy etilmaganligi ushbu yo'nalishdagi dolzarb masalalar sifatida baholandi.

Xulosa sifatida aytish mumkinki, kiberjinoyatlarga qarshi kurashishda raqamli kriminalistika texnologiyalarini rivojlantirish, xalqaro standartlarni milliy ekspertiza tizimiga integratsiya qilish, zamonaviy kriminalistika laboratoriyalarini tashkil etish hamda yuqori malakali mutaxassislarni tayyorlash bugungi kunning eng muhim vazifalaridan biridir. Mazkur chora-tadbirlar raqamli dalillar bilan ishlash samaradorligini oshirish, kiberjinoyatlarni tezkor fosh etish va axborot xavfsizligini mustahkamlashga xizmat qiladi.

Foydalanilgan adabiyotlar:

1. National Institute of Standards and Technology. Guide to Integrating Forensic Techniques into Incident Response (SP 800-86). Gaithersburg, MD: NIST, 2006. NIST SP 800-86
2. National Institute of Standards and Technology. Guidelines on Mobile Device Forensics (SP 800-101 Rev.1). Gaithersburg, MD: NIST, 2014.
3. NIST SP 800-101 Rev.1
4. National Institute of Justice. Electronic Crime Scene Investigation: A Guide for First Responders. Washington, DC: NIJ, 2001.
5. NIJ Electronic Crime Scene Investigation Guide
6. Association of Chief Police Officers. ACPO Good Practice Guide for Digital Evidence. London, 2012. ACPO Good Practice Guide for Digital Evidence
7. International Organization for Standardization / International Electrotechnical Commission. ISO/IEC 27037:2012 — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva: ISO, 2012. ISO/IEC 27037 Standard
8. International Organization for Standardization / International Electrotechnical Commission. ISO/IEC 27043:2015 — Incident Investigation Principles and Processes. Geneva: ISO, 2015. ISO/IEC 27043 Standard
9. INTERPOL. Global Cybercrime Strategy. Lyon, 2022.
10. INTERPOL Cybercrime Strategy
11. Europol. Internet Organised Crime Threat Assessment (IOCTA). Hague: Europol, 2024. Europol IOCTA Reports
12. United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime. Vienna: UNODC, 2013. UNODC Cybercrime Study
13. International Association of Computer Investigative Specialists. Certified Forensic Computer Examiner (CFCE) Program Materials.
14. IACIS Official Website
15. Digital Forensic Research Workshop. Digital Forensic Research Conference Proceedings. DFRWS Official Website

16. Casey, E. Digital Evidence and Computer Crime. 3rd edition. Academic Press, 2011.
17. Carrier, B. File System Forensic Analysis. Addison-Wesley Professional, 2005.
18. Nelson, B., Phillips, A., Enfinger, F., Steuart, C. Guide to Computer Forensics and Investigations. Cengage Learning, 2018.
19. Sammons, J. The Basics of Digital Forensics. 3rd edition. Syngress, 2021.