CZU: 343.98:004

CRIMINALISTICA DIGITALĂ ÎN COMBATEREA FRAUDELOR

Constantin RUSNAC,
doctor în drept, conferențiar universitar

Lucrarea analizează criminalistica digitală ca direcție integrată în criminalistica generală, adaptată noilor realități tehnologice generate de criminalitatea informatică. Sunt evidențiate particularitățile urmelor electronice – natura nemterială, instabilitatea, dependența de mediul tehnologic – și aspecte generale ale metodologiei de lucru cu acestea: descoperirea, fixarea, ridicarea și conservarea. Articolul propune o clasificare riguroasă a fraudelor informatice și cibernetice, evidențiind importanța cooperării internaționale și necesitatea formării specialiștilor în criminalistica digitală, în contextul provocărilor juridice actuale.

Cuvinte-cheie: criminalistică digitală, urme electronice, fraudă informatică, tehnologie, investigare.

DIGITAL FORENSICS IN COMBATING FRAUD

Constantin RUSNAC,
PhD, Associate Professor

The paper analyzes digital forensics as an integrated branch of general forensic science, adapted to the new technological realities generated by cybercrime. It highlights the specific characteristics of electronic traces—such as their immaterial nature, volatility, and dependence on the technological environment—as well as general aspects of the methodology applied in handling them: identification, documentation, collection, and preservation. The article proposes a rigorous classification of computer and cyber frauds, emphasizing the importance of international cooperation and the necessity of training specialists in digital forensics, in the context of current legal challenges.

Key words: digital criminalistics, electronic traces, computer fraud, technology, investigation.

1. INTRODUCERE

Proliferarea tehnologiilor digitale a determinat o transformare profundă a mediului în care se manifestă comportamentele infracționale. În acest context, criminalistica digitală s-a conturat ca o direcție specializată a științelor criminalistice, oferind un cadru metodologic și tehnic indispensabil în descoperirea, analizarea și valorificarea probelor de natură electronică. Investigarea fraudelor comise prin mijloace informatice presupune „aplicarea unor tehnici avansate de descoperire, conservare și examinare a urmelor electronice, în vederea stabilirii mecanismului infracțional și stabilirii persoanelor implicate"[8, p.4].

Formele moderne de fraudă – de la accesul neautorizat la sisteme informatice și manipularea datelor electronice, până la utilizarea ilegală a instrumentelor de plată și a identităților digitale – ridică provocări semnificative organelor de urmărire penală. Aceste fapte, caracterizate prin mobilitate, disimulare și sofisticare tehnologică, necesită o abordare criminalistică adaptată realităților cibernetice. În acest sens,

1. INTRODUCTION.

The proliferation of digital technologies has led to a profound transformation of the environment in which criminal behaviors manifest. In this context, digital forensics has emerged as a specialized branch of forensic sciences, providing an essential methodological and technical framework for discovering, analyzing, and utilizing electronic evidence. The investigation of fraud committed through digital means requires the "application of advanced techniques for identifying, preserving, and examining electronic traces, with the purpose of establishing the criminal mechanism and identifying the persons involved" [8, p.4].

Modern forms of fraud—ranging from unauthorized access to information systems and manipulation of electronic data to the illicit use of payment instruments and digital identities—pose significant challenges to law enforcement authorities. These offenses, characterized by mobility, concealment, and technological sophistication, necessitate a forensic approach tailored to cyber realities. In this regard, digital

criminalistica digitală facilitează obținerea unui material probator relevant, contribuind la reconstituirea procesului infracțional și la fundamentarea acțiunilor procesual-penale.

Mai mult decât atât, evoluția continuă a mediului digital impune actualizarea constantă a metodelor criminalistice, precum și dezvoltarea cooperării interinstituționale între experți în domeniul juridic, tehnologic și investigativ. Eficacitatea reacției penale împotriva fraudelor informatice depinde, astfel, de capacitatea sistemului judiciar de a integra instrumentele criminalisticii digitale într-un cadru procedural riguros și adaptat cerințelor probatorii contemporane.

2. METODE ȘI MATERIALE APLICATE

Articolul științific se bazează preponderent pe o metodologie calitativă, specifică cercetării teoretico-aplicative din domeniul criminalisticii. Autorul utilizează analiza conceptuală și deductivă, integrând elemente de doctrină și interpretare criminalistică, pentru a evidenția particularitățile criminalisticii digitale și aplicabilitatea acesteia în investigarea fraudelor informatice.

3. REZULTATE ȘI DISCUȚII

În contextul contemporan, marcat de o expansiune accelerată a fenomenelor infracționale în mediul virtual, se impune o reconsiderare a modului în care criminalistica se adaptează noilor realități tehnologice. În viziunea noastră, criminalistica digitală trebuie privită nu ca un domeniu izolat, ci ca o direcție specializată, integrată organic în structura criminalisticii generale.

În primul rând, criminalistica digitală reprezintă aplicarea adaptată a metodelor, principiilor și tehnicilor criminalistice în sfera datelor informatice, a urmelor electronice și a dispozitivelor digitale implicate în activități infracționale. Această subramură se axează pe analiza și valorificarea elementelor probatorii în format digital, fără a contraveni paradigmelor deja consacrate ale criminalisticii.

Tot în această ordine de idei, considerăm că delimitarea criminalisticii digitale ca domeniu separat ar putea genera un dezechilibru metodologic și o ruptură artificială între investigarea clasică și cea digitală. În fond, obiectivul criminalisticii rămâne același – identificarea, fixarea, conservarea, examinarea și interpretarea

forensics facilitates the collection of relevant evidence, contributing to the reconstruction of criminal activities and the substantiation of procedural and judicial actions.

Moreover, the continuous evolution of the digital environment requires the constant updating of forensic methods, as well as the development of interinstitutional cooperation between experts in legal, technological, and investigative fields. The effectiveness of the criminal justice response to cyber frauds thus depends on the judiciary's ability to integrate digital forensic tools within a rigorous procedural framework, adapted to contemporary evidentiary requirements.

2. APPLIED METHODS AND MATERIALS

The scientific article is predominantly based on a qualitative methodology, specific to the theoretical and applied research in the field of criminalistics. The author employs conceptual and deductive analysis, integrating elements of doctrine and criminalistic interpretation, in order to highlight the particularities of digital criminalistics and its applicability in the investigation of cyber frauds.

3. RESULTS AND DISCUSSIONS

In the contemporary context, marked by an accelerated expansion of criminal phenomena in the virtual environment, there is a pressing need to reconsider the way criminalistics adapts to new technological realities. In our view, digital criminalistics should not be seen as an isolated field, but rather as a specialized direction, organically integrated within the structure of general criminalistics.

First and foremost, digital criminalistics represents the adapted application of criminalistic methods, principles, and techniques in the realm of computer data, electronic traces, and digital devices involved in criminal activities. This subfield focuses on the analysis and exploitation of digital evidence, without contravening the already established paradigms of criminalistics.

In this regard, we believe that delimiting digital criminalistics as a separate field could generate a methodological imbalance and an artificial divide between classical and digital investigations. Ultimately, the goal of criminal-

urmelor relevante pentru descoperirea adevărului în procesul penal, indiferent de suportul acestora.

Mai mult, criminalistica digitală nu se constituie într-un sistem științific de sine stătător, ci într-un ansamblu de procedee și metode adaptate specificului tehnologic. Astfel, competențele sale se dezvoltă într-un cadru interdisciplinar, dar se subsumează, în mod firesc, criminalisticii generale. Existența unor instrumente tehnice și metodologii distincte nu poate justifica, în opinia noastră, o autonomizare conceptuală, ci doar recunoașterea unui specific profesional care se exprimă în cadrul aceluiași sistem investigativ.

Totodată, trebuie subliniat că metodele utilizate în criminalistica digitală nu sunt în totalitate noi, ci adesea reprezintă extensii sau adaptări ale celor clasice – precum fixarea urmelor, documentarea probelor ori reconstrucția activităților infracționale – transpuse în registrul digital. Astfel, se menține continuitatea epistemologică a disciplinei, chiar dacă se diversifică instrumentarul tehnic.

Prin urmare, din perspectiva noastră, criminalistica digitală se afirmă ca o ramură aplicativă a criminalisticii, al cărei specific este determinat de suportul probatoriu și mediul de manifestare a infracțiunii, nu de o autonomie științifică absolută. Această abordare unitară este esențială pentru asigurarea coerenței actului de investigare și pentru consolidarea eficienței procesului penal într-o societate tot mai digitalizată.

În evoluția actuală a criminalității, probele digitale au devenit tot mai frecvent utilizate în cadrul investigațiilor penale, în special în cauzele care implică infracțiuni comise prin intermediul tehnologiei informației – precum frauda informatică [11, p.116-117], accesul ilegal la sisteme informatice, compromiterea datelor sau spălarea banilor prin rețele virtuale. În opinia noastră, cunoașterea caracteristicilor specifice ale acestui tip de probe este esențială pentru a le putea utiliza corect în procesul penal, atât din punct de vedere criminalistic, cât și procedural.

În primul rând, una dintre trăsăturile principale ale probelor electronice este forma lor nematerială. Acestea nu sunt probe fizice, cum ar fi obiectele sau urmele vizibile, ci sunt reprezentate prin informații electronice stocate sau transmise prin intermediul unor dispozitive informatice. Astfel, ele nu pot fi percepute istics remains the same—identifying, securing, preserving, examining, and interpreting relevant traces to uncover the truth in criminal proceedings, regardless of their medium.

Moreover, digital criminalistics does not constitute an independent scientific system but rather a set of procedures and methods adapted to the technological specifics. Thus, its competencies develop within an interdisciplinary framework but naturally fall under the broader scope of general criminalistics. The existence of distinct technical tools and methodologies cannot justify, in our opinion, a conceptual autonomy, but rather the recognition of a professional specificity expressed within the same investigative system.

At the same time, it must be emphasized that the methods used in digital criminalistics are not entirely new but often represent extensions or adaptations of classical techniques—such as trace securing, evidence documentation, or crime reconstruction—applied in the digital realm. As such, the epistemological continuity of the discipline is maintained, even as the technical toolkit diversifies.

Therefore, from our perspective, digital criminalistics asserts itself as an applied branch of criminalistics, whose specificity is determined by the evidentiary medium and the environment in which the crime manifests, rather than by absolute scientific autonomy. This unified approach is crucial for ensuring the coherence of the investigative process and enhancing the effectiveness of criminal proceedings in an increasingly digitized society.

In the current evolution of criminality, digital evidence has become increasingly prevalent in criminal investigations, especially in cases involving crimes committed through information technology—such as cyber fraud, illegal access to computer systems, data compromise, or money laundering via virtual networks. In our opinion, understanding the specific characteristics of this type of evidence is essential for its correct use in criminal proceedings, both from a criminalistic and procedural standpoint.

First and foremost, one of the main characteristics of electronic evidence is its immaterial form. These are not physical evidence, like objects or visible traces, but are represented by electronic information stored or transmit-

pute direct cu simțurile, ci trebuie identificate și preluate cu ajutorul unor mijloace tehnice specifice. În acest context, criminalistica digitală furnizează metode concrete pentru identificarea, ridicarea și conservarea acestor urme electronice, astfel încât acestea să poată fi valorificate ca mijloace de probă în procesul penal.

În același context, trebuie evidențiată fragilitatea și instabilitatea probelor digitale. „Acestea pot fi modificate, șterse sau alterate într-un timp foarte scurt, fie intenționat, fie din eroare tehnică. De aceea, este esențial ca organele de urmărire penală să intervină prompt, folosind metode criminalistice de documentare și conservare, cum ar fi realizarea copiilor de siguranță (clonarea suporturilor digitale), capturarea sesiunilor de utilizare sau generarea fișierelor de integritate (hash-uri)”[3]. Fără aceste măsuri, se poate compromite valoarea probatorie a informațiilor digitale.

O altă trăsătură importantă este dependența probelor digitale de mediul tehnologic. Acestea nu pot fi analizate și interpretate în afara contextului tehnic care le-a generat. Prin urmare, ele trebuie extrase și prezentate într-o formă clară și inteligibilă pentru a putea fi folosite în procesul penal. Criminalistica contribuie esențial la această etapă, prin metode care permit transpunerea conținutului digital într-un format probator relevant și verificabil.

În opinia noastră, trebuie acordată o atenție deosebită și riscului de modificare sau contrafacere a probelor electronice. Datorită naturii tehnice a acestor informații, ele pot fi copiate sau alterate cu ușurință. Din acest motiv, este obligatoriu să se respecte principiile criminalistice referitoare la lanțul de custodie – adică documentarea completă a modului în care proba a fost ridicată, păstrată, analizată și prezentată în proces. Doar astfel se poate garanta că proba digitală nu a fost modificată și că reflectă realitatea faptică.

Totodată, un aspect deosebit de important este dificultatea de a stabili cu certitudine sursa unei probe electronice. Spre deosebire de probele clasice, care pot fi legate relativ direct de o persoană (de exemplu, o amprentă digitală sau un obiect lăsat la locul faptei), în cazul probelor digitale este necesară o analiză detaliată pentru a demonstra legătura dintre un document electronic sau o activitate informatică și autorul presupus al faptei. Această atribuție se realizează prin corelarea urmelor digitale cu

ted through computer devices. Therefore, they cannot be directly perceived by the senses and must be identified and collected using specific technical means. In this context, digital criminalistics provides concrete methods for identifying, retrieving, and preserving these electronic traces so that they can be utilized as evidence in criminal proceedings.

In the same context, the fragility and instability of digital evidence must be highlighted. “These can be modified, deleted, or altered in a very short time, either intentionally or due to technical error. Therefore, it is essential that criminal investigation authorities intervene promptly, using criminalistic documentation and preservation methods, such as creating backup copies (cloning digital media), capturing usage sessions, or generating integrity files (hashes).” Without these measures, the evidentiary value of digital information can be compromised.

Another important characteristic is the dependence of digital evidence on the technological environment. These cannot be analyzed and interpreted outside the technical context that generated them. Therefore, they must be extracted and presented in a clear and intelligible form in order to be used in criminal proceedings. Criminalistics plays a crucial role in this stage by providing methods that allow the conversion of digital content into a relevant and verifiable evidentiary format.

In our opinion, particular attention should be given to the risk of modification or counterfeiting of electronic evidence. Due to the technical nature of this information, it can be easily copied or altered. For this reason, it is mandatory to respect the criminalistic principles regarding the chain of custody—namely, the complete documentation of how the evidence was collected, preserved, analyzed, and presented in court. Only in this way can it be guaranteed that the digital evidence has not been altered and that it reflects the factual reality.

Moreover, an especially important aspect is the difficulty in establishing the source of digital evidence with certainty. Unlike classic evidence, which can be directly linked to a person (for example, a fingerprint or an object left at the crime scene), digital evidence re-

alte mijloace de probă – cum ar fi audierea, rapoartele de expertiză etc.

În această ordine de idei, criminalistica are un rol central în valorificarea judiciară a probelor digitale, deoarece doar prin aplicarea unor metode riguroase se poate asigura că acestea respectă cerințele legale de autenticitate, integritate, proveniență și relevanță pentru cauza penală.

În contextul digitalizării accelerate a societății, fraudele informatice și cibernetice au cunoscut o diversificare semnificativă, devenind una dintre cele mai dinamice forme ale criminalității moderne. În opinia noastră, pentru a asigura o reacție penală eficientă și o investigare criminalistică adecvată, este necesară o clasificare riguroasă a acestor infracțiuni, în funcție de elementele structurale, modul de operare și specificul mijloacelor tehnice utilizate.

În primul rând, considerăm oportună delimitarea terminologică între **frauda informatică** și **frauda cibernetică**, termeni care în practică sunt adesea utilizați interschimbabil, deși reflectă nuanțe distincte. Frauda informatică [5] presupune folosirea unui sistem informatic ca instrument principal în comiterea faptei, în timp ce frauda cibernetică [1, p.85-86] are o arie mai extinsă, incluzând și atacurile asupra infrastructurilor informatice sau asupra fluxurilor de date din spațiul virtual.

În această ordine de idei, o primă clasificare poate fi realizată **în funcție de obiectul vizat**:

• **Fraude orientate asupra datelor** – cum ar fi furtul de identitate digitală, falsificarea datelor informatice, interceptarea neautorizată a comunicațiilor sau manipularea bazelor de date.

• **Fraude orientate asupra resurselor tehnice** – incluzând accesul ilegal la sisteme informatice, utilizarea neautorizată a rețelelor, infectarea cu programe malițioase (malware, spyware, ransomware).

• **Fraude asupra tranzacțiilor financiare** – cele mai frecvente în practica judiciară, precum compromiterea cardurilor bancare, phishing-ul, clonarea datelor de autentificare și deturnarea transferurilor electronice.

Totodată, în același context, frauda cibernetică poate fi clasificată **în funcție de modul de operare (modus operandi** [2, p.74-78]**)**, ceea ce are o relevanță majoră din punct de vedere criminalistic, întrucât permite conturarea profilului făptuitorului și stabilirea tipologiei

quires a detailed analysis to demonstrate the connection between an electronic document or computer activity and the alleged perpetrator. This task is accomplished by correlating digital traces with other forms of evidence—such as testimony, expert reports, etc.

In this regard, criminalistics plays a central role in the judicial use of digital evidence, as only through the application of rigorous methods can it be ensured that this evidence meets the legal requirements of authenticity, integrity, provenance, and relevance to the criminal case.

In the context of the accelerated digitization of society, cyber and computer frauds have seen significant diversification, becoming one of the most dynamic forms of modern criminality. In our opinion, to ensure an effective criminal response and proper criminalistic investigation, a rigorous classification of these offenses is necessary, based on structural elements, modus operandi, and the specific technical means employed.

First and foremost, we find it useful to establish a terminological distinction between computer fraud and cyber fraud, terms that are often used interchangeably in practice, despite reflecting distinct nuances. **Computer fraud** involves the use of a computer system as the primary tool in the commission of the offense, while **cyber fraud** encompasses a broader scope, including attacks on information infrastructures or data flows in the virtual space.

In this context, an initial classification can be made based on the targeted object:

• **Frauds targeting data** – such as digital identity theft, falsification of computer data, unauthorized interception of communications, or manipulation of databases.

• **Frauds targeting technical resources** – including illegal access to computer systems, unauthorized use of networks, infection with malicious software (malware, spyware, ransomware).

• **Frauds involving financial transactions** – the most common in judicial practice, such as compromising bank cards, phishing, cloning authentication data, and diverting electronic transfers.

At the same time, in the same context, **cyber fraud** can be classified based on the modus operandi (modus operandi), which is of major relevance from a criminalistics standpoint,

infracționale:

• **Fraude cu caracter manipulatoriu** – unde făptuitorul obține date confidențiale [9, p.20] prin înșelăciune, cum este cazul tehnicilor de phishing sau inginerie socială.

• **Fraude de tip invaziv** – prin compromiterea directă a sistemelor informatice (hacking, exploatarea vulnerabilităților, accesul fără drept).

• **Fraude automate** – realizate prin utilizarea de software specializat, cum ar fi roboții de tranzacționare frauduloasă sau programele de extragere automată a datelor.

• În opinia noastră, o altă clasificare relevantă este cea **după nivelul de organizare al activității infracționale**:

• **Fraude individuale sau oportuniste**, comise de persoane izolate, cu un nivel relativ redus de pregătire tehnică.

• **Fraude comise în cadrul grupărilor infracționale organizate**, caracterizate prin distribuția clară a rolurilor (programatori, operatori, spălători de bani digitali etc.), utilizarea unor instrumente criptate și desfășurarea acțiunilor în mai multe jurisdicții.

Această diferențiere are implicații directe asupra **complexității investigației criminalistice**, întrucât fraudele comise în mod organizat presupun o metodologie investigativă mai avansată, implicând cooperarea internațională, analiza sistematică a urmelor digitale și utilizarea expertizelor tehnico-informatice.

De asemenea, considerăm utilă și o clasificare **în funcție de gradul de disimulare și detectabilitate a faptei**:

• **Fraude evidente**, ușor de observat de către victime sau operatorii sistemelor informatice.

• **Fraude ascunse**, disimulate prin tehnologii avansate, care necesită o descoperire criminalistică atentă și utilizarea unor metode specializate de detecție.

În esență, clasificarea fraudelor informatice și cibernetice nu este doar un demers teoretic, ci are o valoare practică directă în plan investigativ. Prin delimitarea categoriilor de fapte, criminalistica poate contribui la construirea unor strategii adecvate de cercetare penală, la identificarea rapidă a făptuitorilor și la asigurarea unui probatoriu complet și legal. Totodată, această clasificare permite organelor judiciare să stabilească proporționalitatea mijloacelor de investigație, gradul de periculozi-

as it allows for the profiling of the perpetrator and the establishment of an offense typology:

• **Manipulative frauds** – where the perpetrator obtains confidential data through deception, as is the case with phishing techniques or social engineering.

• **Invasive frauds** – through the direct compromise of computer systems (hacking, exploiting vulnerabilities, unauthorized access).

• **Automated frauds** – carried out through specialized software, such as fraudulent trading robots or automated data extraction programs.

In our opinion, another relevant classification is based on the level of organization of the criminal activity:

• **Individual or opportunistic frauds**, committed by isolated persons with a relatively low level of technical expertise.

• **Frauds committed within organized criminal groups**, characterized by a clear distribution of roles (programmers, operators, digital money launderers, etc.), the use of encrypted tools, and actions carried out across multiple jurisdictions.

This differentiation has direct implications on the complexity of the criminalistic investigation, as frauds committed in an organized manner require a more advanced investigative methodology, involving international cooperation, systematic analysis of digital traces, and the use of technical-informatic expertise.

Furthermore, we find it useful to classify based on the degree of concealment and detectability of the act:

• **Obvious frauds**, easily observed by victims or system operators.

• **Concealed frauds**, disguised through advanced technologies, requiring careful criminalistic discovery and the use of specialized detection methods.

In essence, the classification of cyber and computer frauds is not merely a theoretical exercise but has direct practical value in the investigative process. By delineating categories of offenses, criminalistics can contribute to the construction of appropriate criminal investigation strategies, the rapid identification of perpetrators, and the provision of complete and legally valid evidence. Moreover, this classification enables judicial authorities to determine the proportionality of investigative means, the

tate socială și particularitățile de intervenție în funcție de natura și complexitatea infracțiunii.

Clasificarea fraudelor informatice și cibernetice trebuie să devină un reper metodologic obligatoriu în cadrul procesului de investigare criminalistică, constituind o bază solidă pentru reacția penală eficientă într-o epocă dominată de transformările digitale.

Investigarea criminalistică a infracțiunilor informatice presupune aplicarea unui proces metodologic riguros, structurat pe etape clar delimitate, în vederea valorificării eficiente a urmelor digitale. În opinia noastră, fiecare etapă a acestui proces are o importanță esențială, întrucât orice neglijență sau eroare procedurală poate compromite integritatea probelor.

În același context, este necesar ca reprezentații organului de urmărire penală să trateze urmele electronice cu aceeași rigoare ca pe cele clasice, adaptând însă metodele criminalistice la specificul mediului digital.

Descoperirea urmelor electronice

În primul rând, etapa descoperirii presupune stabilirea existenței și localizării urmelor digitale, care pot reprezenta date, fișiere, loguri, coduri de acces, metadate sau activități înregistrate în sisteme informatice.

Spre deosebire de urmele clasice, cele digitale sunt intangibile, disimulate sau distribuite pe mai multe suporturi (hard disk, rețele cloud, telefoane inteligente etc.). De aceea, descoperirea acestora presupune utilizarea unor metode și tehnici specifice, cum ar fi:

- scanarea sistemelor informatice;
- analiza jurnalelor de sistem;
- verificarea istoricului comunicațiilor sau a conturilor utilizate.

În opinia noastră, această etapă implică atât cunoștințe criminalistice, cât și expertiză tehnică, fiind deseori realizată în colaborare cu specialiști IT.

Fixarea urmelor electronice

Odată descoperite, urmele digitale trebuie fixate cu acuratețe, pentru a fi introduse în circuitul probator. Fixarea constă în documentarea exactă a modului în care a fost identificată urma, a locației sale, a contextului în care a fost găsită și a structurii tehnice a suportului.

În acest sens, criminalistica utilizează procedee precum:

- fotografierea ecranului (screenshot-uri),
- redactarea procesului-verbal de constatare,

social danger level, and intervention specifics based on the nature and complexity of the offense.

The classification of cyber and computer frauds must become a mandatory methodological benchmark within the criminalistic investigation process, providing a solid foundation for an effective criminal response in an era dominated by digital transformations.

The criminalistic investigation of computer crimes requires the application of a rigorous methodological process, structured into clearly defined stages, in order to efficiently capitalize on digital traces. In our opinion, each stage of this process is of essential importance, as any negligence or procedural error may compromise the integrity of the evidence.

In the same context, it is necessary for representatives of the prosecuting authority to handle electronic traces with the same rigor as traditional evidence, while adapting criminalistic methods to the specificities of the digital environment.

Discovery of Electronic Traces

Firstly, the discovery stage involves establishing the existence and location of digital traces, which can represent data, files, logs, access codes, metadata, or recorded activities in computer systems.

Unlike physical traces, digital ones are intangible, concealed, or distributed across multiple media (hard disks, cloud networks, smartphones, etc.). Therefore, their discovery requires the use of specific methods and techniques, such as:

- Scanning computer systems.
- Analyzing system logs.
- Verifying communication history or accounts used.

In our opinion, this stage requires both criminalistic knowledge and technical expertise, often carried out in collaboration with IT specialists.

Fixation of Electronic Traces

Once discovered, digital traces must be accurately fixed to be introduced into the evidentiary process. Fixation consists of the exact documentation of how the trace was identified, its location, the context in which it was found, and the technical structure of the medium.

In this regard, criminalistics employs methods such as:

• înregistrarea parametrilor tehnici relevanți.

Fixarea este un garant al transparenței și reproductibilității procesului de investigare, constituind o etapă indispensabilă pentru demonstrarea autenticității probei în instanță.

Ridicarea urmelor electronice

Etapa ridicării presupune extragerea fizică sau logică a datelor informatice stabilite anterior. Aceasta se realizează prin metode tehnice specializate, menite să evite alterarea conținutului informațional. În acest context, se utilizează:

• clonarea integrală a suporturilor digitale (copii forensice);

• exportarea fișierelor într-un format sigur;

• documentarea operațiunilor în procesul-verbal de ridicare etc.

În opinia noastră, ridicarea trebuie să respecte principiul non-alterării probei, astfel încât orice modificare produsă asupra conținutului original să poată fi exclusă cu certitudine. Totodată, trebuie respectate prevederile legale privind autorizarea percheziților informatice și a extragerii de date.

Conservarea urmelor electronice

Un element esențial al procesului criminalistic este păstrarea probelor într-un mod sigur și controlat. Urmele digitale sunt extrem de vulnerabile la modificări, ștergeri sau atacuri cibernetice, motiv pentru care se impune aplicarea unor măsuri riguroase de conservare:

• criptarea datelor extrase;

• utilizarea dispozitivelor de stocare securizate;

• păstrarea în laboratoare certificate;

• respectarea lanțului de custodie.

În această ordine de idei, criminalistica digitală se bazează pe trasabilitatea completă a fiecărei operațiuni efectuate asupra probei, pentru a garanta integritatea acesteia până la prezentarea în fața instanței.

În procesul de investigare a infracțiunilor informatice, utilizarea metodelor și tehnicilor criminalistice adecvate este esențială pentru obținerea unor dovezi digitale solide. Aceste metode trebuie să fie alese cu atenție, în funcție de specificul probelor și de obiectivele investigației. În opinia noastră, tehnicile moderne, cum ar fi imaging, carving, analiza metadatelor și timeline analysis, joacă un rol crucial în descoperirea și conservarea probelor elec-

• Screenshotting (taking screenshots).

• Drafting the minutes of observation.

• Recording relevant technical parameters.

Fixation guarantees the transparency and reproducibility of the investigative process, being an indispensable stage for demonstrating the authenticity of the evidence in court.

Seizure of Electronic Traces

The seizure stage involves the physical or logical extraction of the previously identified computer data. This is done using specialized technical methods that avoid altering the informational content. In this context, the following techniques are used:

• Complete cloning of digital media (forensic copies).

• Exporting files to a secure format.

• Documenting operations in the seizure minutes.

In our opinion, the seizure must adhere to the principle of non-alteration of evidence, so that any modification of the original content can be definitively excluded. Moreover, the legal provisions concerning the authorization of digital searches and data extraction must be respected.

Conservation of Electronic Traces

A crucial element of the criminalistic process is the safe and controlled preservation of evidence. Digital traces are extremely vulnerable to modifications, deletions, or cyberattacks, which is why rigorous conservation measures must be implemented:

• Data encryption.

• Using secure storage devices.

• Keeping evidence in certified laboratories.

• Ensuring chain of custody integrity.

In this regard, digital criminalistics relies on the complete traceability of every operation performed on the evidence to ensure its integrity until it is presented in court.

The Use of Criminalistic Methods in the Investigation of Computer Crimes

In the investigation of computer crimes, the use of appropriate criminalistic methods and techniques is essential for obtaining solid digital evidence. These methods must be carefully selected based on the nature of the evidence and the objectives of the investigation. In our opinion, modern techniques such as imaging, carving, metadata analysis, and timeline

tronice.

Imagingul, cunoscut și sub denumirea de clonare forensică, reprezintă o tehnică fundamentală în investigarea probelor digitale, fiind esențială pentru salvarea și protejarea datelor originale de pe dispozitivele informatice. Prin această metodă, se realizează o copie exactă a unui dispozitiv de stocare, cum ar fi un hard disk sau un server, care include atât datele vizibile, cât și informațiile ascunse (fișiere șterse, date fragmentate etc.).

În opinia noastră, imagingul este absolut necesar, având în vedere că integritatea probelor trebuie păstrată intactă pe întreaga durată a procesului judiciar. De asemenea, se asigură faptul că analiza ulterioară a datelor se poate face fără riscul de a modifica sau corupe probele originale.

Imagingul poate fi realizat prin software specializat, care creează o copie bit cu bit a întregului sistem de fișiere. În acest fel, investigatorul poate examina datele fără a interveni direct asupra dispozitivului original, ceea ce asigură protecția și respectarea principiului integrității probelor.

Carving (Recuperarea fișierelor șterse) reprezintă o tehnică utilizată pentru recuperarea fișierelor șterse sau corupte de pe dispozitivele de stocare. Spre deosebire de alte metode de recuperare, carvingul nu depinde de structura sistemului de fișiere, ceea ce înseamnă că poate extrage fișiere chiar și atunci când acestea nu mai sunt indexate sau când informațiile despre locația acestora au fost pierdute.

Carvingul presupune analizarea sector cu sector a unui dispozitiv de stocare pentru a localiza și extrage fișierele pe baza semnăturilor acestora (headere, structuri de fișiere etc.). Acest proces poate fi esențial în investigarea unor infracțiuni informatice, unde datele au fost șterse intenționat de făptuitori pentru a ascunde urmele activității lor ilegale.

În opinia noastră, carvingul este o tehnică care trebuie utilizată cu mare atenție, deoarece există riscul de a extrage fișiere irelevante sau corupte. Totuși, pentru procurori și anchetatori, aceasta reprezintă o metodă de recuperare completă a informațiilor, esențială în procesul de probatoriu digital.

Analiza metadatelor.

Metadatele sunt informațiile ascunse care descriu caracteristicile unui fișier digital, fără a face parte din conținutul acestuia. Aces-

analysis play a crucial role in the discovery and preservation of electronic evidence.

Imaging (Forensic Cloning)

Imaging, also referred to as forensic cloning, is a fundamental technique in the investigation of digital evidence, essential for preserving and protecting the original data from computing devices. Through this method, an exact copy of a storage device, such as a hard drive or server, is made, encompassing both visible data and hidden information (deleted files, fragmented data, etc.).

In our opinion, imaging is absolutely necessary, as it ensures the integrity of the evidence remains intact throughout the entire judicial process. It also ensures that subsequent analysis of the data can be conducted without the risk of modifying or corrupting the original evidence.

Imaging is performed using specialized software, which creates a bit-by-bit copy of the entire file system. In this manner, investigators can examine the data without directly intervening with the original device, thus ensuring the protection of the evidence and upholding the principle of integrity.

Carving (File Recovery)

Carving is a technique used to recover deleted or corrupted files from storage devices. Unlike other recovery methods, carving does not depend on the file system structure, meaning it can extract files even when they are no longer indexed or when location information has been lost.

Carving involves analyzing a storage device sector by sector to locate and extract files based on their signatures (headers, file structures, etc.). This process can be essential in investigating cybercrimes, where data may have been intentionally deleted by perpetrators to conceal traces of their illegal activities.

In our opinion, carving must be employed with great caution, as there is a risk of recovering irrelevant or corrupted files. Nonetheless, for prosecutors and investigators, it represents a method of complete information recovery, essential in the process of digital evidence gathering.

Metadata Analysis

Metadata refers to the hidden information that describes the characteristics of a digi-

tea pot include date precum data și ora creării, autorul fișierului, locația unde a fost salvat, istoricul modificărilor și multe altele. În multe cazuri, metadatele sunt extrem de utile pentru reconstruirea activităților informatice ale unei persoane, precum și pentru stabilirea legăturilor temporale între diferite evenimente.

Analiza metadatelor poate ajuta în identificarea sursei și autenticității unui fișier, fiind o tehnică esențială în procesul de investigare criminalistică. De exemplu, în cazul unei fraude financiare informatice, analiza metadatelor poate dezvălui dacă documentele au fost create sau modificate înainte de a fi prezentate ca probă în fața instanței. În opinia noastră, analiza metadatelor oferă un punct de plecare pentru aprofundarea cercetării, permițând investigarea unui fișier în contextul său mai larg.

Totuși, trebuie subliniat faptul că metadatele pot fi modificate sau eliminate de utilizatorii avansați sau de programele de ștergere, iar o corelare a acestora cu alte dovezi este esențială pentru validarea lor.

Timeline analysis (Analiza cronologică a activităților) sau analiza cronologică, reprezintă procesul de reconstruire a unei linii temporale a activităților informatice pe baza datelor și a fișierelor stocate pe un dispozitiv. Această tehnică permite investigarea evenimentelor dintr-o perioadă dată și este utilă pentru a identifica relațiile de cauzalitate, succesiunea activităților și pentru a stabili momentul în care au avut loc infracțiunile.

Prin **analiza cronologică**, investigatorii pot înțelege tiparul de comportament al infractorilor, cum ar fi orele la care au fost realizate accesările neautorizate, modificările aduse fișierelor sau transferurile de date suspecte. Această tehnică este deosebit de utilă în cazurile în care faptele infracționale sunt legate de activități desfășurate pe o perioadă mai lungă de timp.

Analiza cronologică este o metodă foarte eficientă pentru a corobora dovezile digitale cu alte probe fizice, precum mărturiile martorilor sau documentele tradiționale. De asemenea, această tehnică ajută la evidențierea măsurilor de precauție sau ascundere aplicate de făptuitori.

Provocările actuale [4, p.99-104], cu referire la subiectul vizat sunt, în opinia noastră, multiple și complexe. În acest context, investigațiile digitale sunt esențiale pentru a aduna dovezi solide, iar evoluțiile tehnologice, dar și schimbări-

tal file without being part of its content. This can include data such as the file's creation date and time, author, location where it was saved, modification history, and much more. In many cases, metadata is extremely useful in reconstructing an individual's computing activities, as well as in establishing temporal connections between various events.

Metadata analysis can help identify the source and authenticity of a file, making it an essential technique in criminal investigations. For example, in cases of cyber financial fraud, metadata analysis can reveal whether documents were created or modified prior to being presented as evidence in court.

In our opinion, metadata analysis offers a starting point for further research, enabling investigation of a file within its broader context. However, it is crucial to note that metadata can be modified or deleted by advanced users or deletion programs, and therefore, correlating this data with other evidence is essential for validating its accuracy.

Timeline Analysis

Timeline analysis involves the process of reconstructing a chronological sequence of computing activities based on data and files stored on a device. This technique allows for the investigation of events over a specific period, and is useful for identifying causal relationships, the sequence of activities, and for establishing when the criminal activities occurred.

This technique is valuable in uncovering the sequence of events related to cybercrimes, as it helps track actions taken by perpetrators and reveals the key moments when illegal activities took place.

Chronological Analysis

Through chronological analysis, investigators can gain insight into the criminal behavior patterns, such as the times when unauthorized access occurred, modifications made to files, or suspicious data transfers. This technique is particularly useful in cases where criminal activities span over an extended period.

Chronological analysis is a highly effective method for corroborating digital evidence with other physical evidence, such as witness testimonies or traditional documents. Additionally, this technique helps to highlight the precautions or concealment measures em-

le din cadrul legislației internaționale, impun o adaptare constantă a metodelor și tehnicilor criminalistice. Este imperios necesar să abordăm, în mod detaliat, problemele juridice și probatorii, dar și necesitatea formării specialiștilor în criminalistica digitală, ca direcții de dezvoltare ale acestui domeniu.

Probleme juridice și probatorii în investigarea digitală

În opinia noastră, una dintre principalele dificultăți în combaterea criminalității informatice o reprezintă problemele juridice și probatorii care pot apărea în cursul investigațiilor digitale. Aceste provocări sunt direct legate de natura particulară a dovezilor digitale și de reglementările juridice care trebuie să le guverneze.

Un prim aspect juridic important se referă la legalitatea obținerii probelor digitale. Deși tehnologia avansează rapid, multe dintre reglementările legale sunt încă insuficient de clare în ceea ce privește manipularea probelor digitale, protejarea drepturilor fundamentale ale persoanelor și respectarea normelor internaționale privind confidențialitatea datelor. De exemplu, într-o investigație de hacking, poate apărea întrebarea dacă este legal să se acceseze un server al unei persoane sau al unei companii fără consimțământul acesteia, chiar și în condițiile unui mandat de percheziție.

Un alt aspect este integritatea probelor digitale, care trebuie păstrată în timpul întregului proces de investigație, inclusiv în fazele de colectare, analiză și prezentare a acestora în instanță. Într-un sistem digital, există riscul ca dovezile să fie modificate, șterse sau corupte în timpul procesului de investigare. Prin urmare, respectarea unor norme stricte de chain of custody (lanțul de custodie) este esențială, iar investigatorii trebuie să aibă grijă ca niciun detaliu să nu fie compromis.

De asemenea, în ceea ce privește admisibilitatea [10, p.122] probelor digitale în instanță, provocările sunt multiple. Spre exemplu, probele digitale pot fi contestate pe motive de autenticitate sau integritate, iar evaluarea acestora poate depinde de expertiza tehnică a specialiștilor, ceea ce ridică provocări în privința înțelegerii probelor de către instanțele juridice. De asemenea, extragerea probelor din cloud sau de pe servere internaționale ridică întrebări referitoare la jurisdicția aplicabilă, precum și la drepturile de acces și protecția datelor personale.

ployed by perpetrators.

Current Challenges

In our opinion, the challenges related to the subject at hand are numerous and complex. In this context, digital investigations are essential for collecting solid evidence. Technological advancements, as well as changes in international legislation, necessitate constant adaptation of forensic methods and techniques. It is crucial to address, in detail, the legal and evidentiary issues, as well as the need for the training of specialists in digital forensics, as key directions for the development of this field.

Legal and Evidentiary Issues in Digital Investigations

In our opinion, one of the main difficulties in combating cybercrime lies in the legal and evidentiary challenges that may arise during digital investigations. These challenges are directly related to the particular nature of digital evidence and the legal frameworks that must govern them.

A key legal aspect concerns the legality of obtaining digital evidence. While technology advances rapidly, many legal regulations remain unclear regarding the handling of digital evidence, the protection of individuals' fundamental rights, and adherence to international data privacy standards. For instance, in a hacking investigation, the question may arise as to whether it is legal to access an individual's or company's server without their consent, even with a search warrant.

Another issue pertains to the integrity of digital evidence, which must be preserved throughout the entire investigative process, including during the collection, analysis, and presentation phases in court. In the digital environment, there is a risk that evidence may be altered, deleted, or corrupted during the investigative process. Therefore, strict adherence to the chain of custody is essential, and investigators must ensure that no detail is compromised.

Moreover, with regard to the admissibility of digital evidence in court, challenges abound. For example, digital evidence may be contested on grounds of authenticity or integrity, and its evaluation may depend on the technical expertise of specialists, which presents challenges in terms of how courts understand the evidence. Additionally, extracting evidence

Pentru a răspunde provocărilor actuale în domeniul criminalisticii digitale, în opinia noastră, o formare continuă și specializată a profesioniștilor din domeniu este absolut necesară. Fraudele informatice și alte tipuri de infracțiuni cibernetice sunt extrem de sofisticate și implică tehnologii avansate, de aceea investigatorii, procurorii și judecătorii trebuie să posede cunoștințe tehnice specifice pentru a înțelege și a analiza corect dovezile digitale.

În acest context, formarea specialiștilor în criminalistica digitală trebuie să includă, în mod obligatoriu, atât competențe tehnice, cât și cunoștințe juridice. Investigatorii trebuie să fie instruiți nu doar în utilizarea tehnologiilor de investigare digitală, cum ar fi analiza metadatelor, carvingul sau analiza cronologică, ci și în aplicarea normelor legale și a procedurilor judiciare specifice, astfel încât să poată asigura validitatea și admisibilitatea probelor în instanță.

Totodată, este necesară o cooperare interinstituțională între autoritățile de aplicare a legii, instituțiile educaționale și organizațiile internaționale care lucrează în domeniul criminalisticii digitale. În acest sens, formarea profesională trebuie să fie continuă și să includă schimburi de bune practici și standardizare la nivel internațional.

O altă provocare importantă în combaterea fraudelor informatice este cooperarea [12, p.62-67] internațională și interoperabilitatea tehnologică. Criminalitatea informatică nu se limitează la granițele naționale, iar infractorii cibernetici își desfășoară activitatea pe o scară globală. În acest context, în opinia noastră, colaborarea între instituțiile de aplicare a legii la nivel internațional este esențială pentru combaterea eficientă a infracțiunilor informatice.

„Aceasta presupune schimbul rapid de informații, resurse și expertiză între autoritățile din diferite state, având în vedere că infracțiunile informatice transnaționale pot implica persoane sau organizații care operează pe mai multe jurisdicții" [7]. Organizațiile internaționale precum Interpol, Europol sau FBI joacă un rol important, oferind suport tehnic și logistic, precum și acces la baze de date comune.

În plus, interoperabilitatea tehnologică este crucială pentru ca autoritățile să poată colabora eficient. Diferitele sisteme informatice și instrumentele de investigare digitală trebuie să fie compatibile și să permită schimbul rapid

from the cloud or international servers raises questions regarding the applicable jurisdiction, as well as access rights and personal data protection.

To address the current challenges in digital forensics, we believe that continuous and specialized training for professionals in the field is absolutely necessary. Cyberfrauds and other types of cybercrimes are highly sophisticated and involve advanced technologies. Therefore, investigators, prosecutors, and judges must possess specific technical knowledge to correctly understand and analyze digital evidence.

In this context, training specialists in digital forensics must include both technical skills and legal knowledge. Investigators need to be trained not only in the use of digital investigative technologies such as metadata analysis, carving, or chronological analysis, but also in the application of legal standards and judicial procedures, so they can ensure the validity and admissibility of evidence in court.

Furthermore, interinstitutional cooperation between law enforcement authorities, educational institutions, and international organizations working in digital forensics is required. In this regard, professional training must be continuous and include exchanges of best practices and international standardization.

Another important challenge in combating cyber fraud is international cooperation and technological interoperability. Cybercrime does not respect national borders, and cybercriminals operate on a global scale. In our opinion, collaboration between law enforcement agencies at the international level is essential for the effective combating of cybercrime.

"This requires the rapid exchange of information, resources, and expertise between authorities from different countries, given that transnational cybercrimes can involve individuals or organizations operating across multiple jurisdictions" [7]. International organizations such as Interpol, Europol, or the FBI play a key role by providing technical and logistical support, as well as access to shared databases.

Additionally, technological interoperability is crucial for authorities to collaborate effectively. Different computer systems and digital investigation tools must be compatible and enable the rapid exchange of data between

de date între țări, pentru ca traseele digitale ale infracțiunilor să poată fi urmărite și analizate în timp real.

În opinia noastră, această cooperare internațională și interoperabilitatea tehnologică trebuie să fie însoțite de progrese legislative, pentru a asigura un cadru uniform și clar în privința procesului de investigare, protecției datelor și respectării drepturilor fundamentale.

4. CONCLUZII

Criminalistica digitală reprezintă o ramură indispensabilă a investigării moderne, adaptată complexității și dinamicii infracționalității informatice. Din analiza efectuată rezultă că urmele digitale, prin caracteristicile lor specifice – imaterialitate, fragilitate, dependență tehnologică – impun metode criminalistice riguroase și specializate pentru a garanta integritatea și relevanța probatorie. Investigarea infracțiunilor informatice necesită un cadru metodologic clar structurat, completat de instrumente tehnice avansate. Totodată, eficiența reacției penale depinde de formarea continuă a specialiștilor și de cooperarea interinstituțională și internațională. Criminalistica digitală nu trebuie privită ca un domeniu autonom, ci ca o extensie funcțională a criminalisticii generale, integrată coerent în sistemul investigativ penal contemporan.

countries, so that the digital traces of crimes can be tracked and analyzed in real time.

In our opinion, this international cooperation and technological interoperability must be accompanied by legislative progress to ensure a uniform and clear framework regarding the investigation process, data protection, and the respect for fundamental rights.

4. CONCLUSIONS

Digital forensics is an indispensable branch of modern investigations, adapted to the complexity and dynamics of cybercrime. From the analysis conducted, it results that digital traces, due to their specific characteristics—intangible, fragile, and technologically dependent—require rigorous and specialized forensic methods to ensure the integrity and evidentiary relevance. Investigating cybercrimes requires a clearly structured methodological framework, complemented by advanced technical tools. Furthermore, the effectiveness of criminal justice responses depends on the continuous training of specialists and interinstitutional and international cooperation. Digital forensics should not be viewed as an autonomous field, but rather as a functional extension of general forensics, coherently integrated into the contemporary criminal investigative system.

REFERINȚE BIBLIOGRAFICE

BIBLIOGRAPHICAL REFERENCES

1. BURUC Al., NISTOR D. Securitatea cibernetică și securitatea națională. Cazul Republicii Moldova. In: Securitatea informațională, Ed. 10, 19 aprilie 2013, Chișinău. Chisinau, Moldova: Departamentul Editorial-Poligrafic al ASEM, 2013, Ediția 10.
2. CAPRIAN, Iurie. Mecanisme ale atacurilor cibernetice în domeniul bancar. In: Univers strategic, 2024, nr. 1(57).
3. CIOREA P. Considerații asupra percheziției informatice. În: Penalmenete/Relevante, nr. I, 2017. Paula-CIOREA-Consideratii-asupra-perchezitiei-informatice.pdf (accesat: 17.03.2025)
4. COJOCARU R., LISNIC S. Noi provocări în legislația cibernetică: evoluția infracțiunilor de prodecere, import, comercializare și punere ilegală la dispoziție a mijloacelor tehnice și produselor program. In: Perspectivele și Problemele Integrării în Spațiul European al Cercetării și Educației, Ed. Volumul XI, 6 iunie 2024, Cahul. Cahul: Tipografia „CentroGrafic" SRL, Cahul, 2024, Vol.11, Partea I.
5. Convenția Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001. ratificată prin Legea RM Nr. 6 din 02-02-2009. În: Monitorul Oficial al Republicii Moldova Nr. 37-40 art. 104 din 20-02-2009
6. Decizia (UE) 2023/436 de autorizare a statelor membre să ratifice, în interesul Uniunii Europene, cel de Al doilea protocol adițional la Convenția privind criminalitatea informatică. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32023D0436

(accesat: 03.03.2025)
7. ODAGIU Iu. Unele probleme și dificultăți în dezvoltarea cri minalisticii digitale. În: Protecția drepturilor și libertăților fundamentale ale omului în procesul asigurării ordinii și securității publice. Materialele Conferinței științifice naționale cu participare internațională, 05 decembrie 2024, ediția a IV-a. Chișinău, 2024.
8. POPA L. Metodica cercetării abuzului sexual în privința copiilor prin utilizarea tehnologiilor informaționale Rezumatul tezei de doctor în drept. Chișinău, 2024.
9. PURICI, Dumitru. Evoluția Criminalității Cibernetice. In: Information Technologies and Security: 2012, 15-16 octombrie 2012, Chișinău. Chișinău, Republica Moldova: Consiliul Național pentru Acreditare și Atestare, 2012.
10. PURICI, Svetlana. Specificul activității speciale de investigație și acțiunii de urmărire penală întreprinse pentru administrarea probelor la cercetarea crimelor cibernetice. In: Studia Universitatis Moldaviae (Seria Științe Sociale), 2015, nr. 11.
11. SPÎNU (DUMNEANU), Ludmila. Evaluările naționale și internaționale în domeniul infracțiunilor informatice. In: Realități și perspective ale învățământului juridic național:: Culegerea comunicărilor, 1-2 octombrie 2019, Chișinău. Chișinău: Centrul Editorial-Poligrafic al Universității de Stat din Moldova, 2019, Vol.2.
12. SURU, Tatiana. Cooperarea internațională în domeniul contracarării criminalității cibernetice. In: Revista Moldovenească de Drept Internațional și Relații Internaționale, 2008, nr. 2.

Despre autor:

Constantin RUSNAC,
doctor în drept, conferențiar universitar,
șef al Catedrei Procedură penală, criminalistică și securitate informațională,
Academia „Ștefan cel Mare" a MAI,
ROR: *https://ror.org/036kvxa54,*
e-mail: navrucnd1@gmail.com,
ORCID: 0000-0002-8122-7711

About the author:

Constantin RUSNAC,
PhD, Associate Professor,
Head of the Department of Criminal Procedure, Criminalistics and Information Security,
„Ștefan cel Mare" Academy of the MIA,
ROR: *https://ror.org/036kvxa54,*
e-mail: navrucnd1@gmail.com,
ORCID ID: 0000-0002-8122-7711