UNIVERSITATEA DE STAT DIN MOLDOVA

Cu titlu de manuscris
C.Z.U.: 343.98:004(043.3)

PURICI SVETLANA

METODICA CERCETĂRII INFRACȚIUNILOR DIN DOMENIUL INFORMATICII

SPECIALITATEA: 554.04 – CRIMINALISTICĂ, EXPERTIZĂ JUDICIARĂ, INVESTIGAȚII OPERATIVE

Teză de doctor în drept

Conducător științific: GOLUBENCO Gheorghe,
dr. în drept, profesor universitar

Autor: PURICI Svetlana

CHIȘINĂU, 2018

Cuprins

ADNOTARE

Purici Svetlana, „Metodica cercetării infracțiunilor din domeniul informaticii”, teză de doctor în drept. Specialitatea: 554.04 – Criminalistică, expertiză judiciară, investigații operative, Chișinău, 2018.

Structura tezei: 140 pagini text de bază, adnotare în limbile română, engleză și rusă, lista abrevierilor, introducere, trei capitole, concluzii generale și recomandări, bibliografia din 360 titluri, 25 anexe, declarația privind asumarea răspunderii, CV-ul. Rezultatele obținute sunt publicate în 12 lucrări științifice.

Cuvinte-cheie: criminalitate informatică, internet, sistem informatic, probe electronice, versiuni criminalistice, metodică, cercetarea infracțiunilor, măsuri speciale de investigații.

Domeniul de studiu derivă din cele mai importante și mai noi aspecte ale cercetării infracțiunilor din domeniul informaticii, coroborând perspectiva doctrinar-normativă cu cea practico-aplicativă.

Scopul și obiectivele lucrării: ***Scopul*** tezei rezidă în elaborarea metodicii de cercetare a infracțiunilor din domeniul informaticii în vederea descoperirii, cercetării eficiente, prevenirii și combaterii acestor infracțiuni. Dintre ***obiectivele*** lucrării menționăm: analiza studiilor din literatura de specialitate referitoare la metodica de cercetare a infracțiunilor din domeniul informaticii; prezentarea modelului criminalistic al acestei categorii de infracțiuni; descrierea situațiilor tipice și a versiunilor criminalistice; expunerea particularităților tactice de efectuare a unor acțiuni de urmărire penală și măsuri speciale de investigații în domeniul dat.

Noutatea și originalitatea științifică a rezultatelor obținute derivă din faptul că studiul nostru reprezintă o primă încercare de cercetare științifică multiaspectuală a infracțiunilor informatice la nivel național. Este o abordare complexă, însoțită de analiza și evaluarea viziunilor doctrinare în materie, constituind astfel un veritabil suport științifico-practic în soluționarea multor probleme în procesul de investigare a infracțiunilor informatice.

Problema științifică importantă soluționată rezidă în elaborarea metodicii de cercetare criminalistică a infracțiunilor din domeniul informaticii, ceea ce a contribuit la identificarea procedeelor tactice, metodice și tehnice adecvate, în vederea aplicării lor la investigarea acestor infracțiuni.

Semnificația teoretică și valoarea aplicativă a lucrării. Valențele teoretice ale lucrării sunt relevate de caracterul interdisciplinar al cercetării, or criminalitatea informatică are loc în spațiul virtual, ceea ce revendică abordarea ei nu doar din punct de vedere juridic, dar și informatic. Metodele aplicate și constatările efectuate în urma cercetării pot servi drept ghid pentru studenții, practicienii și alți specialiști din domeniul dreptului.

Implementarea rezultatelor științifice vizează, în primul rând, activitatea practică în sfera respectivă, iar concluziile studiului pot fi aplicate unor noi cercetări teoretice în domeniu.

ANNOTATION

Purici Svetlana, "Methodological research of cybercrime", PhD thesis in law. Specialty: 554.04 - forensics, judicial expertise, operative investigations, Chișinău 2018.

The structure of the thesis: 140 pages of main text, annotation, abbreviations list, introduction, three chapters, conclusions and recommendations, a bibliography consisting of 360 titles, 25 annexes, liability statement, CV. The obtained results are published in 12 scientific works.

Keywords: cybercrime, internet, information system, electronic samples, Forensic versions, methods, crime investigation, special investigative measures.

The field of the scientific work derives from the new most important aspects of the criminal investigation in the field of informatics, corroborating the doctrinal-normative and practical-applicative perspective.

The aim and objectives of the research: *the aim* of the thesis lies in the elaboration of the methodology for the investigation of cybercrimes, in order to discover, to effectively investigate, to prevent and fight these crimes. Among *the objectives* of the paper are: analysis of the specialized literature referring to the methodology of investigation of the cybercrimes; presenting the forensic model of this category of crimes; description of typical situations and forensic versions; the exposure of the tactical peculiarities of carrying out criminal investigation actions and special investigative measures in the given field.

The novelty and the originality of the results of the research derives from the fact that it is the first scientific incursion at national level. It is a multidisciplinary approach accompanied by the analysis and evaluation of the doctrinal visions in the field, thus notifying a real scientific-practical support for solving many problems in the investigation of cybercrime.

The important scientific problem solved in the respective field through the research carried out consists in the elaboration of the forensic research methodology of the cybercrimes, the characterization of the tactical, methodical and technical peculiarities applied in the investigation of these crimes.

The theoretical significance and the applicative value of the scientific work. the theoretical valences of the work are highlighted by the interdisciplinary character of research, or cybercrime taking place in the virtual space, requiring an intense approach not only from a legal point of view, but also from informatics point of view. This thesis has the value of a guide for students, practitioners and other specialists in the field.

The implementation of scientific results is primarily a matter of practical activity, but the conclusions of the research can be equally applicable to new theoretical examinations of the field.

АННОТАЦИЯ

Пурич Светлана. „Методика расследования преступлений в области информатики". Дисс. докт. юрид. наук, Кишинэу, 2018. Специальность: 554.04 – Криминалистика, судебная экспертиза, оперативные расследования.

Структура работы: Введение, 3 главы, общие выводы и рекомендации, библиография из 360 источников, 25 приложений, 140 страниц основного текста. Результаты опубликованы в 12 научных работах.

Ключевые слова: информационная преступность, интернет, электронные доказательства, криминалистические версии, специальные меры по расследованию преступлений.

Область исследования: Работа относится к разделу криминалистической методики.

Цель и основные задачи диссертации. *Цель:* Разработка рекомендаций по предупреждению, раскрытию и расследованию преступлений в сфере информатики. *Задачи*: анализировать публикации по методике расследования преступлений в сфере информатики; представить развернутую криминалистическую модель преступлений в области информатики; описать типичные следственные ситуации и криминалистические версии; показать особенности проведения следственных действий и специальных мероприятий по выявлению и раскрытию такого рода преступлений на первоначальном и последующем этапах их расследования.

Новизна и научная оригинальность диссертации определена тем, что данная работа является одним из первых исследований в нашей стране по методике расследования преступлений в области информатики. *Оригинальность* состоит в многооаспектном подходе к данной проблеме, исходя из научного обоснования и практических рекомендаций по улучшению расследования данного вида преступлений, включая алгоритм действий по осмотру места происшествия, обыска и выемки электронных документов, аргументации соблюдения специфических правил при проведении оперативно-следственных мероприятий в рамках их расследования.

Решенная важная научная проблема состоит в разработке методики криминалистического расследования преступлений в области информатики, что способствовало выявлению тактических, методических и технических приемов с целью их применения при расследовании данных преступлений.

Теоретическая важность и прикладное значение работы состоит в развитии доктрины методики расследования преступлений в области информатики с учетом обобщенного опыта нашей страны и последних научно-технических достижений и информационных технологий в борьбе с современной преступностью, а также в характеристике тактических, методических и технических особенностей, применяемых в расследовании этих преступлений.

Внедрение научных результатов направлена прежде всего на практическую деятельность в соответствующей сфере, а выводы исследования могут быть применены к новым теоретическим исследованиям при расследования преступлений в области информатики.

LISTA ABREVIERILOR

alin. - alineat
ARP - Address Resolution Protocol
art. - articol
BD - Blu-Ray Disc
BIOS - Basic Input/Output System
cache - memorie de tip static RAM
CCo - Cod contravențional
CD - Compact Disc
CDR - Call Data Records Database (descifrările convorbirilor telefonice)
CE - Consiliul Europei
CtEDO - Curtea Europeană pentru Drepturile Omului
CNA - Centrul Național Anticorupție
CP - Cod penal
CPP - Codul de procedură penală
CRC - Cyclic redundancy checker
CRM - Constituția Republicii Moldova
CSI - Comunitatea Statelor Independente
CSJ - Curtea Supremă de Justiție
CVV - Card Verification Value
DDoS - Distributed Denial of Service
DNS - Domain Name System – sistem de nume de domeniu
DVD - Digital Video Disk
EIR - Equipment Identity Register
Etc. - Etcetera
GSM - Global System for Mobile Communications
GPS - Global Positioning System
GPRS - General Packet Radio Service
HDD - Hard disk drive (disc dur)
HTML - Hiper Text Markup Language
ICCID - Integrated Circuit Card Identification
INI - Inspectoratul Național de Investigații
IGP - Inspectoratul General al Poliției
IMAP - Protocol de Acces la Mesaje Internet
IMEI - International Mobile Equipment Identity
IMSI - Identitatea Internațională a Telefonului Mobil
IP - Internet Protocol
ISP - Internet Service Provider (furnizor de servicii internet)
IT - tehnologia informațională
LAN - rețea locală
lit. - litera
MAC - Media Acces Control
MAI - Ministerul Afacerilor Interne
MDL - leu moldovenesc
MD5 - Message Digest 5
M.Of. - Monitorul Oficial
MSISDN - Numărul Internațional ISDN al Stației Mobile
p. - Pagina
pct. - punct
PG - Procuratura Generală

PIN	- Personal Indentification Number
PUK	- Personal Unblocking Code
P2P	- Peer to peer (de la utilizator la utilizator)
RAM	- memorie cu acces aleatoriu
RM	- Republica Moldova
SHA-1	- Secure Hash Algorithm
SIM	- Subscriber Identity Module
SMS	- Short Message Service
SUA	- Statele Unite ale Americii
SV	- Serviciul Vamal
TCP	- Transmission Control Protocol
UE	- Uniunea Europeană
USB	- Universal Serial Bus (Magistrală Serială Universală)
USD	- dolar american
URL	- Uniform Resource Locator
VPN	- Virtual Private Network
WAN	- rețea de bandă largă
3G	- generația a treia de tehnologie telefonică mobilă
4G	- generația a patra de tehnologie telefonică mobilă

INTRODUCERE

Actualitatea și importanța problemei abordate. Dezvoltarea IT și continua globalizare a rețelelor informatice au condus la un progres incontestabil al societății și la asigurarea transparenței în viața publică, dar au determinat și apariția unei noi forme de criminalitate – *criminalitatea informatică*.

Internetul, în forma în care îl cunoaștem la etapa actuală, a trecut printr-un proces complex de evoluție, devenind, în prezent, un instrument indispensabil omului în viața cotidiană și oferind un mediu ce permite desfășurarea diferitor acțiuni, chiar și a celor nepermise de lege. Treptat, lumea virtuală a internetului a evoluat și din perspectiva oportunităților pe care le oferă oamenilor, fiind, fără îndoială, un izvor nesecat de resurse informaționale valoroase, dar și un spațiu imens pentru victime și infractori. Astfel, răspândirea internetului a facilitat migrarea infracțiunilor tradiționale în spațiul virtual, ceea ce a condus la apariția infracțiunilor informatice.

Progresul semnificativ în dezvoltarea IT și a mijloacelor care formează spațiul cibernetic a adus nu doar beneficii, el a avut și un șir întreg de consecințe negative, în special legate de posibilitatea utilizării acestor tehnologii și mijloace în scopuri incompatibile cu sarcinile de asigurare a securității personale, naționale și internaționale.

Criminalitatea informatică constituie un pericol sporit atât pentru subiecții individuali, cât și pentru statele lumii, precum și pentru întreaga comunitate internațională, având un caracter transfrontalier. Lupta cu această categorie de infracțiuni trebuie să devină una dintre prioritățile comunității internaționale, impunându-se elaborarea unor reglementări similare pentru combaterea lor.

În ultimii ani, creșterea numărului de ISP, accesul liber la abonamente gratuite și lejeritatea cu care poți cădea în cursa unui infractor informatic au sporit complexitatea investigațiilor criminalistice în domeniu. Din perspectiva unei asemenea problematici, infracțiunile din mediul respectiv prezintă dificultăți în identificarea subiectului activ sau, dincolo de orice îndoială rezonabilă, a autorului real al infracțiunii în cauză.

Astfel, lipsa unui cadru normativ juridic internațional uniformizat, a diferitor strategii globale, insuficiența instrumentelor internaționale de cooperare, reglementările confuze la nivel național, complexitatea procedurii de cercetare a infracțiunilor informatice și necesitatea unei pregătiri adecvate a organelor de urmărire penală și a specialiștilor în domeniu, resursele financiare limitate în vederea cercetării acestor tipuri de infracțiuni, disperarea victimelor și ezitarea lor de a apela la organele de drept, precum și vulnerabilitatea internetului ca platformă

complexă, creează impedimente serioase în activitatea de urmărire penală și în atragerea infractorilor informatici la răspundere penală.

În prezent, organele de urmărire penală se confruntă cu o adevărată provocare în asigurarea unui spațiu sigur într-o eră digitală, pentru că infractorii opun rezistență și sunt mereu în pas cu ultimele tehnologii. Performanțele calculatoarelor, ale telefoanelor mobile și internetului, ale tabletelor și altor gadget-uri sunt însușite foarte rapid de către infractori, pentru a le folosi drept instrumente în realizarea unor scopuri infracționale.

Actualitatea și importanța prezentei teze rezidă și în identificarea soluțiilor pentru o serie de probleme tactico-organizatorice privind cercetarea infracțiunilor informatice, având în vedere absența unor studii teoretice sau practice în cercetările autohtone, precum și faptul că, până în prezent, nu a fost elaborat un algoritm al aplicării tacticii și metodicii de cercetare a infracțiunilor informatice și nu și-a găsit încă soluționare, în practica autohtonă a organelor competente, nici problema audierii, cercetării la fața locului, a percheziției, ridicării și conservării datelor informatice, a expertizei și constatării tehnico-științifice. Totodată, o atenție aparte, în această lucrare, se acordă aplicării măsurilor speciale de investigații în cazul acestor infracțiuni, întrucât, dată fiind lipsa unor recomandări de cercetare a infracțiunilor informatice, a apărut necesitatea de a generaliza și a interpreta din punct de vedere teoretic și practic rezultatele acestor noi experiențe.

Deși există un șir de lucrări dedicate cercetării diferitor caracteristci ale infracțiunilor informatice, aspectele privind tactica și metodica criminalistică, metodologia învingerii și neutralizării activităților de împiedicare a bunei desfășurări a procesului penal la cercetarea acestor categorii de infracțiuni nu au fost studiate anterior în literatura științifică autohtonă.

Toate acestea au determinat actualitatea temei prezentului studiu, o asemenea cercetare în domeniul vizat reprezentând una din sarcinile prioritare ale criminalisticii contemporane.

Scopul și obiectivele tezei. Scopul prezentei lucrări rezidă în elaborarea metodicii de cercetare a infracțiunilor din domeniul informaticii în vederea descoperirii, cercetării eficiente, a prevenirii și combaterii acestor infracțiuni. Atingerea scopului propus este condiționată de realizarea următoarelor ***obiective***:

- analiza studiilor din literatura de specialitate referitoare la metodica de cercetare a infracțiunilor din domeniul informaticii;
- descrierea experienței naționale și internaționale privind descoperirea și cercetarea infracțiunilor vizate;
- identificarea modelului și a caracteristicilor criminalistice ale infracțiunilor informatice;
- relevarea situațiilor tipice și a versiunilor criminalistice;

- descrierea particularităților tactice de efectuare a unor acțiuni de urmărire penală și a măsurilor speciale de investigații în vederea descoperirii acestui gen de infracțiuni;
- elaborarea propunerilor de ameliorare a situației în domeniul vizat, menite să asigure o cercetare eficientă a infracțiunilor informatice;
- elaborarea unor metode eficiente de descoperire, prevenire și de cercetare a infracțiunilor în cauză.

Noutatea și originalitatea științifică a rezultatelor obținute derivă din faptul că studiul nostru reprezintă o primă încercare de cercetare științifică multiaspectuală a infracțiunilor informatice la nivel național. Este o abordare complexă, însoțită de analiza și evaluarea viziunilor doctrinare în materie, constituind astfel un veritabil suport științifico-practic în soluționarea multor probleme în procesul de investigare a infracțiunilor informatice.

Problema științifică importantă soluționată rezidă în elaborarea metodicii de cercetare criminalistică a infracțiunilor din domeniul informaticii, ceea ce a contribuit la identificarea procedeelor tactice, metodice și tehnice adecvate, în vederea aplicării lor la investigarea acestor infracțiuni.

Importanța teoretică. Problema metodelor de investigații a criminalității informatice constituie un subiect de cercetare criminalistică extrem de important. În acest sens, lucrarea noastră reprezintă o sinteză a realizărilor în tehnica, tactica și metodica criminalistică, în diverse aspecte de procedură penală, de activitate specială de investigații, în informatică, în jurisprudența națională, străină și internațională, perspectivele enunțate permițând a expune poziții, a deduce și formula rigori și reguli privind identificarea unor tactici și metode concrete, admisibile în soluționarea eficientă a problemelor apărute în cadrul cercetării infracțiunilor din domeniul informaticii, precum și a propune soluții pentru situațiile create de inconsecvența sau ambiguitatea prevederilor normative.

Valoarea aplicativă a lucrării. În baza rezultatelor cercetării efectuate în lucrare, sunt relevate situațiile tipice și particularitățile specifice ale elaborării versiunilor preliminare în cauzele legate de infracțiunile informatice.

Demersul nostru științific se bazează pe un volum vast de materiale teoretice și empirice ceea ce, cu certitudine, îi sporește valoarea teoretică și aplicativă.

Concluziile și recomandările formulate în prezenta teză sunt orientate în vederea utilizării acestora de către corpul profesoral-didactic și cel studențesc la studierea criminalisticii, a altor discipline specializate din planurile de studii ale învățământului juridic superior, la elaborarea suporturilor de curs, precum și la instruirea inițială și continuă a angajaților organelor de drept din domeniul prevenirii și combaterii criminalității în general și a celei informatice în special. Ele pot

contribui la sporirea eficacității metodelor existente în cercetarea infracțiunilor săvârșite în privința datelor, sistemelor și rețelelor informatice, precum și cu utilizarea acestora.

Lucrarea este utilă atât pentru teoreticieni, în special pentru instituțiile care pregătesc cadre profesionale, antrenate în combaterea fenomenului criminalității informatice, cât și pentru practicieni ai dreptului, cum sunt ofițerii de urmărire penală, procurorii, judecătorii, constituind pentru ei un autentic ghid de îndrumare, oferind, totodată, cunoștințe necesare și utilizatorului obișnuit al internetului sau al unui sistem informatic.

Alte repere conceptuale. Luând în considerare modelul și caracteristica criminalistică a acestor categorii de infracțiuni și a situațiilor tipice în cercetarea acestora, s-a recurs la elaborarea unui sistem de versiuni aplicabile în cadrul urmării penale – atât în anumite circumstanțe ale infracțiunilor informatice, cât și față de activitatea infracțională în ansamblu.

O importanță deosebită prezintă studierea particularităților organizatorice tactice la efectuarea acțiunilor de urmărire penală (cercetarea la fața locului, audierea, ridicarea de obiecte și documente, percheziția), precum și a acțiunilor speciale de investigații în cadrul cercetării infracțiunilor informatice.

Conform lucrărilor științifice consacrate problemelor metodice privind cercetarea anumitor categorii de infracțiuni, în această teză sunt supuse analizei particularitățile pregătirii, dispunerii și efectuării expertizelor judiciare în cauzele penale cu privire la infracțiunile săvârșite asupra și/sau cu ajutorul IT (sistemelor și rețelelor informatice), fiind formulate, în acest sens, anumite concluzii și recomandări.

Aprobarea rezultatelor. Rezultatele cercetărilor efectuate și expuse în prezentul demers științific au fost reflectate în mai multe articole științifice și pot servi drept bază teoretico-metodologică pentru efectuarea unor cercetări ulterioare. Unele concepte și idei au fost prezentate în rapoarte și comunicări la conferințe științifice naționale și internaționale**.**

Implementarea rezultatelor științifice poate fi realizată în procesul de instruire a studenților, masteranzilor, doctoranzilor din cadrul facultăților de drept ale instituțiilor de învățământ universitar, precum și în activitatea practică a organelor de drept.

Sumarul compartimentelor tezei. Având în vedere standardele stabilite, această teză de doctorat are următoarea structură: text de bază 140 de pagini, constituit din adnotări în limbile română, engleză și rusă, lista abrevierilor, introducere, trei capitole divizate în secțiuni, concluzii generale și recomandări, urmat de o bibliografie din 360 titluri, 25 anexe, declarația privind asumarea răspunderii, CV-ul autorului.

Primul capitol, intitulat ***Situația actuală în domeniul cercetării infracțiunilor informatice***, conține, prioritar, o analiză a materialelor științifice relevante (tratate, monografii, cursuri, studii

de drept, culegeri și spețe de practică judiciară), ce reflectă diverse aspecte ale problematicii tezei, materiale publicate atât în Republica Moldova, cât și în România, Federația Rusă și în alte state aparținând diferitor sisteme de drept. De o atenție sporită au beneficiat lucrările semnate de autori ca: Gh. Golubenco, M. Gheorghiță, S. Doraș, T. Vizdoagă, E. Croitor, I. Dolea, D. Roman, S. Brânză și V. Stati, A. Barbăneagră, T. Amza, C. Amza, M. Dobrinoiu, A. C. Moise, F. Encescu, M. Șcheau, S. Lungu, M. Tilea, D. Voinea, I. Vasiu, L. Vasiu, G. Olteanu, E. Stancu, G. Ioniță, D. Ghervase, M. Neamțu, A. Trancă, D. Trancă, N. Lazareva, E.N. Bâstreacov, A. N. Ivanov, V.A. Klimov, V. Meșereakov, B.V. Andreev, P.N. Pak, V. Horst, A. Jmâhov, A. Filippov, D.V. Dobrovolskii, N. Iablokov, T.M. Lopatina, A.V. Vardanian, E.V. Nikitina, M. Menjega, P.V. Hudeakov, D. Ovseanikov, V.I. Aleskerov, I. Maximenko, A.B. Sizonenko, V. Șișkin, T. Vorošilova, A. Kosânkin, V. Davâdov, C.A. Kovaliov, V.B. Vehov, S. Propastin, M. Sussmann, A. Reyes, J. Wiles, D. Kleiman Totodată, a fost urmărită evoluția instrumentelor și instituțiilor naționale, regionale și internaționale în vederea prevenirii și combaterii criminalității informatice.

În urma analizei materialelor științifice, au fost relevate definiții, caracteristici, particularități și viziuni ale autorilor privind infracțiunile informatice în general, precum și metodica cercetării acestor categorii de infracțiuni, în particular.

Cel de-al doilea capitol al studiului, cu titlul ***Caracteristica criminalistică și organizarea cercetării infracțiunilor din domeniul informaticii***, cuprinde unele considerații generale privind noțiunea și clasificarea infracțiunilor informatice, fiind relevate modelul și caracteristica criminalistică ale infracțiunilor informatice, situațiile tipice de urmărire penală și versiunile criminalistice privind cercetarea infracțiunilor informatice, precum și măsurile tactice și strategice de depășire a obstacolelor care împiedică buna desfășurare a cercetării infracțiunilor informatice.

Capitolul al treilea al tezei, intitulat ***Tactica efectuării unor acțiuni de urmărire penală și măsurile speciale de investigații în cercetarea infracțiunilor informatice***, este dedicat analizei particularităților tactice de efectuare a acțiunilor inițiale și a celor ulterioare de urmărire penală, ca: audierea persoanelor implicate în cauzele investigate, cercetarea la fața locului, percheziția, ridicarea și conservarea datelor informatice. Un loc aparte in acest compartiment îl ocupă expertiza și constatarea tehnico-științifică, precum și măsurile speciale de investigații, efectuate în cazurile infracțiunilor vizate în prezentul studiu.

1. SITUAȚIA ACTUALĂ ÎN DOMENIUL CERCETĂRII INFRACȚIUNILOR INFORMATICE

1.1. Infracțiunile informatice ca obiect de cercetare științifică în Republica Moldova și România

Evoluția fenomenului

Calculatoarele au pătruns în viața oamenilor din toate țările, devenind instrumente indispensabile pentru realizarea diferitor activități. Acestea au avut un impact global asupra experienței de zi cu zi, asupra modului de desfășurare a afacerilor, de comunicare interpersonală și de gestiune a informației.

Apariția calculatorului a adus nu numai mari și numeroase avantaje în evoluția rapidă și radicală a noilor tehnologii, dar a deschis și posibilitatea săvârșirii unei game largi de acțiuni ilegale, adică a generat criminalitatea informatică [1].

Pentru prima dată noțiunea de *infracțiune informatică* a fost atestată în legislația SUA (Legea intitulată *Computer crime act of 1978*) [2, p. 107], unde, în anii ’70, autoritățile au depistat o serie de încălcări ale legislației, efectuate în perioada anilor ’50-’70 ai sec. XX. Primul infractor din SUA care a comis o infracțiune prin intermediul sistemelor informatice a fost Alfonce Konfessore. Acesta, în 1969, a prejudiciat statul, prin acțiunile sale, cu 620.000 USD, fiind găsit vinovat de către 20 de instanțe judecătorești de comiterea infracțiunii computerizate.

Inițial, orice infracțiune comisă prin intermediul sistemelor informatice era calificată drept infracțiune informatică, astăzi însă se face o diferențiere între infracțiunile în care sistemul informatic este folosit ca mijloc de comitere a lor și cele în care obiectul atentării sunt datele informatice.

Întrucât anume în SUA au avut loc primele progrese tehnologice în dezvoltarea tehnicii de calcul, este firesc că această țară a fost prima care s-a confruntat cu noul fenomen negativ. Organele de drept luptau cu el prin metodele clasice, calificând acțiunile drept furt, delapidare a averii străine sau ca alte componente de infracțiuni. Însă timpul a demonstrat ineficiența metodelor tradiționale și necesitatea elaborării unor procedee noi și adecvate fenomenului în cauză.

Obiectivul fundamental al politicii de stat a RM, fixat în *Concepția securității naționale a RM* [3], este securitatea națională în calitate de condiție esențială a existenței poporului RM și a realizării obligațiilor pozitive ale statului. Pericolele din domeniul IT fac parte din spectrul amenințărilor la adresa securității naționale, iar combaterea lor este una dintre acțiunile de bază în asigurarea securității informatice.

Astfel, instabilitatea și disfuncționalitatea sistemelor informatice pot să reprezinte amenințări accentuate la adresa securității naționale. Dezvoltarea progresivă a sistemelor electronice de informații din RM, gradul lor înalt de interconexiune cu sistemele informatice internaționale facilitează activitatea factorului criminogen în sfera informațională și fac să sporească vulnerabilitatea sistemelor respective, inclusiv în sferele de importanță primordială pentru securitatea națională.

Pornind de la creșterea rolului pe care îl au IT în domeniul securității statului și potrivit *Strategiei securității naționale a RM* [4], instituțiile abilitate urmează să întreprindă acțiuni pentru asigurarea securității și administrării eficiente a sistemelor informatice naționale – atât la nivel juridic, cât și la nivel funcțional – prin reducerea principalilor factori de risc, precum sunt: atacurile din rețea (cyber-crimes), virușii informatici, vulnerabilitatea softurilor, neglijența sau rea-voința utilizatorilor, conectarea neautorizată a terțelor persoane etc.

Totodată, instituțiile abilitate urmează să elaboreze soluții tehnice speciale privind sporirea fiabilității rețelelor în cazuri critice, precum și să creeze arhive și stocuri de documente electronice în vederea depozitării securizate a bazei de date de importanță națională, în conformitate cu regimul de stocare, păstrare și de evidență, stabilit de legislație, referitor la documentul electronic și la semnătura digitală, la registre și la protecția datelor cu caracter personal [5, p. 187].

Influența digitalului asupra criminalității determină modificarea formelor delincvențiale tradiționale și apariția unor configurații infracționale noi, din moment ce mediul infracțional este receptiv la tot ce presupune minimizarea eforturilor și a riscurilor la obținerea foloaselor ca urmare a activității infracționale. Prin urmare, pe lângă infracțiunile deja arhicunoscute, cum ar fi furtul de informații și spionajul, escrocheriile și fraudele, jocurile de hazard, prostituția, traficul de arme, droguri și organe, hărțuirile, amenințările, pedofilia, pedofilia organizată, criminalitatea organizată, spălarea banilor, terorismul, prozelitismul sectelor, se mai adaugă și cele noi, ca cyberpedofilia, cyberterorismul, hackingul, difuzarea virusurilor informatice, escrocheriile informatice prin intermediul e-mailului, skimmingul, fraudele informatice, e-mail spammingul (procesul de expediere a mesajelor electronice nesolicitate), violarea confidențialității de către organizații, net-strike-ul, gamblingul online, difuzarea informațiilor ilegale (violență, rasism, explozive, droguri, secte satanice, pedofilie etc.) [6].

Interpretări ale fenomenului criminalității informatice în studiile de specialitate publicate în Republica Moldova și în România

Printre lucrările de rezonanță, cu impact istoric profund, un loc aparte îi revine monografiei savantului autohton Gh. Golubenco, intitulate *Criminalistică: obiect, sistem, istorie* [7], în care autorul a scos în evidență cele mai importante aspecte din istoria apariției *Criminalisticii* ca știință, precum și principalele etape în dezvoltarea criminalisticii din RM. De o valoare incontestabilă este analiza, realizată în corpul acestui studiu monografic, a particularităților criminalisticii moderne și a locului ei în sistemul științelor juridice.

Tratatul fundamental al eruditului criminalist autohton S. Doraș, *Criminalistica* [8], reprezintă piatra de temelie a științei *Criminalistica* în spațiul moldav și cartea de căpătâi a specialiștilor din acest domeniu. Autorul descrie aici tehnicile noi de investigare criminalistică, elementele netradiționale de tactică criminalistică, menite a consolida informația necesară identificării, depistării și reținerii persoanelor bănuite de crimă, menționând și importanța interceptării convorbirilor telefonice pentru acțiunile vizate.

Un alt savant autohton, M. Gheorghiță, în lucrarea intitulată *Tratat de metodică criminalistică* [9], a cercetat reperele conceptuale pentru metodica cercetării infracțiunilor, elaborând și analizând minuțios conceptul de *model* și de *caracteristică criminalistică* a infracțiunilor. Un aspect important și de o valoare indiscutabilă al acestui studiu îl reprezintă definirea noțiunii de *învingere a împotrivirii față de urmărirea penală*, și în special, particularitățile *alibiului*, concept care a fost analizat și dezvoltat ulterior, în prezenta teză de doctor, pe dimensiunea infracțiunilor informatice.

O indubitabilă realizare a științei autohtone este și un alt studiu al aceluiași autor, *Tratatul de criminalistică* [10], unde se pune un accent special pe rolul și importanța situațiilor de urmărire penală și a versiunilor criminalistice. Un spațiu aparte este rezervat acțiunilor tactice: cercetarea la fața locului, reținerea bănuitului / învinuitului, percheziția și ridicarea de obiecte și documente, audierea persoanelor etc.

Una dintre primele lucrări din spațiul românesc, în care s-a efectuat o cercetare științifică aprofundată a fenomenului criminalității informatice, este studiul *Criminalitatea informatică*, avându-i ca autori pe T. Amza și C. P. Amza și publicată în România în anul 2003 [11]. În această monografie sunt expuse mai multe definiții și concepte ale delictului informatic, ale criminalității informatice, explicându-se și alți termeni utilizați în legislația internațională. Astfel, în accepția autorilor, criminalitatea informatică reprezintă ansamblul tuturor infracțiunilor în domeniul IT, într-o anumită perioadă de timp și pe un teritoriu bine determinat.

În sus-numitul studiu, sunt prezentate diverse categorii de infracțiuni comise cu ajutorul computerului și al rețelei internet, sunt analizate vulnerabilitățile sistemelor informatice în fața criminalității, precum și preocupările legislative în combaterea fenomenului. Un accent deosebit a fost pus pe caracterizarea personalității criminalilor electronici. Autorii au descris particularitățile cercetării cauzelor ce au ca obiect infracțiunile informatice în România din acea perioadă. Un capitol separat a fost dedicat identificării aspectelor vulnerabile, prevenirii și detectării criminalității informatice. Totodată, au fost analizate problemele legate de păstrarea secretului informației în spațiul cibernetic, fiind descrise posibilele alternative ale autorităților în decriptarea sistemelor folosite de către infractori, precum și metodele utilizate de către aceștia pentru tăinuirea categoriilor respective de infracțiuni. Autorii au cercetat și rolul mass-media în prevenirea criminalității informatice.

Colectivul de cercetători, constituit din S. Lungu, M. Tilea și D. Voinea, remarcă, în articolul *Cercetarea la fața locului în cazul infracțiunilor săvârşite prin mijloace electronice* [12], că, în situația în care organul de urmărire penală intenționează să examineze, în cadrul percheziției sau al ridicării, sistemele și rețelele informatice sau alte dispozitive electronice, existente în încăperea sau asupra persoanei percheziționate, atunci în cuprinsul actelor procesuale cu privire la dispunerea, solicitarea autorizării și autorizarea acțiunii de urmărire penală (ordonanța organului de urmărire penală, demersul procurorului, încheierea și mandatul judecătorului de instrucție), trebuie să fie indicate și dispozitivele electronice care urmează a fi percheziționate și ridicate.

Autorii autohtoni M. Gheorghiță, Z. Brega, L. Vozniuc și T. Stativca, în *Ghidul de expertize judiciare* [13], au relevat problemele pe care le poate soluționa expertiza tehnică a dispozitivelor, adică expertiza asupra componentelor hardware (partea fizică a unui sistem informatic).

Într-o altă lucrare științifico-practică, intitulată *Возможности судебных экспертиз: криминалистическое обеспечение (научно-практическое пособие)* [14], M. Gheorghiță trece în revistă obiectele care pot fi supuse expertizei tehnice a dispozitivelor, precum și sarcinile de bază pe care le poate rezolva expertiza asupra produselor de program.

Una din operele fundamentale de specialitate din spațiul românesc este studiul *Infracțiuni în domeniul informatic* [15], realizat de M. Dobrinoiu, doctor în drept. Autorul a efectuat o analiză aprofundată a termenilor de *sistem informatic* și *internet*, prezentând teoriile existente cu privire la sisteme, la arhitectura sistemelor de calcul, la rețelele de calculatoare. În lucrare sunt cercetate reglementările juridice internaționale și cele din România, diverse aspecte de drept comparat privind criminalitatea informatică, precum și aspecte referitoare la unitatea și concursul de infracțiuni.

Într-un capitol aparte al sus-numitului studiu, au fost descrise particularitățile procedurii penale în cercetarea infracțiunilor informatice atât la nivel internațional, cât și în dreptul intern, inclusiv competența organelor de drept, identificarea și ridicarea de date informatice stocate pe suporți informatici, admisibilitatea probelor produse în cadrul sistemelor informatice în procedura penală, conservarea datelor informatice, percheziția, interceptarea și înregistrarea comunicațiilor desfășurate prin intermediul sistemelor informatice. Totodată, autorul a analizat și unele aspecte criminologice privind infracționalitatea informatică, cum ar fi vulnerabilitatea sistemelor informatice, tipurile de infractori digitali, activismul, hacktivismul și terorismul informatic.

I. Vasiu și L. Vasiu, în monografia *Prevenirea criminalității informatice* [16], au realizat un studiu penal și criminologic asupra infracționalității informatice. Ei au analizat obiectul acestor categorii de infracțiuni, precum și eventualele măsuri destinate prevenirii fenomenului în cauză.

În opinia lui G. I. Olteanu, expusă în lucrarea *Metodologie criminalistică. Cercetarea structurilor infracționale și a unora dintre activitățile ilicite desfășurate de acestea* [17], cercetarea infracțiunilor informatice este deosebit de importantă, în condițiile preocupării speciale a legiuitorului pentru ocrotirea unor interese legitime ale proprietarilor și administratorilor de sisteme informatice, în legătură cu securitatea, inviolabilitatea acestora, garantarea confidențialității datelor, a integrității atât a datelor, cât și a sistemelor informatice.

Cercetătoarea N. Lazareva, în articolul *Уголовно-правовая характеристика преступлений в области информатики и электросвязи* [18], publicat în revista *Studia Universitatis*, a prezentat o analiză detaliată a trăsăturilor juridico-penale, caracteristice infracțiunilor informatice.

Într-o altă lucrare, *Criminalistică. Tradiție și modernism* [19], semnată de cercetătorii români L. Cârjan și M. Chiper, se readuce în discuție activitatea precursorilor români ai criminalisticii, punându-ne la dispoziție o carte de actualitate criminalistică, având în vedere bogăția informației de ultimă oră și noutățile din practica internațională.

Autorul român G. I. Ioniță, în *O scurtă analiză a infracțiunilor din sfera criminalității informatice incriminate în Legea nr. 161/2003 și în noul Cod penal al României* [20], pune accentul pe aspectele subiective din cadrul infracțiunilor informatice, remarcând că, în ceea ce privește acțiunea principală, suntem în prezența intenției directe, dar în privința acțiunii adiacente, aceasta poate fi atât intenție directă, cât și indirectă.

E. Croitor, în studiul intitulat *Categoriile „purtător tehnico-electronic de informație" și „înregistrări" în probatoriul penal* [21], a realizat o analiză a semnificației și admisibilității probelor electronice (informațiilor aflate pe suporturi informaționale, pe suporturi electronice) în procesul penal.

Într-un articol intitulat *Considerații privind fenomenul de criminalitate informatică* [22], semnat de E. Stancu și A. C. Moise, au fost scoase în evidență cele mai relevante semne caracteristice ale infracțiunilor informatice: ele poartă un caracter tehnologic avansat, având în vedere utilizarea IT, a rețelelor informatice și de comunicații, a sistemelor informatice, a purtătorilor de stocare a datelor informatice, ș.a., care constituie instrumente și mijloace de săvârșire a infracțiunilor informatice; ele posedă un nivel înalt de latență, au un caracter transfrontalier. au costuri reduse, în comparație cu beneficiile ilegale care pot fi obținute.

Autorii citați mai sus au elaborat, recent, un tratat intitulat *Criminalistica. Elemente metodologice de investigare a infracțiunilor* [23], în care abordează metodologia criminalistică, ce vizează stabilirea cadrului metodologic general de cercetare a unor categorii de infracțiuni, a activităților procedurale care trebuie desfășurate cu ocazia cercetării criminalistice a unei anumite infracțiuni, precum și clarificarea altor aspecte importante, cum sunt caracterul complex al procesului de urmărire penală, componentele și etapele cercetării criminalistice a unor infracțiuni, elementele metodologice de cercetare a acestor infracțiuni și rolul criminalisticii în prevenirea și combaterea fenomenului infracțional.

G. I. Ioniță, în *Criminalitatea informatică și investigarea criminalistică digitală. Controverse terminologice și de conținut* [24], a realizat o cercetare științifică a noțiunii de *criminalitate informatică*, ajungând la concluzia că aceasta reprezintă orice infracțiune în care un calculator sau o rețea de calculatoare este obiectul unei infracțiuni, sau în care un calculator sau o rețea de calculatoare este instrumentul sau mijlocul de înfăptuire a unei infracțiuni. Totodată, o atenție sporită a fost acordată descrierii anumitor categorii specifice de infracțiuni informatice, cum ar fi terorismul și războiul informatic.

A. C. Moise, în articolul *Pregătirea cercetării la fața locului în cazul infracțiunilor informatice* [25], a trecut în revistă acțiunile preparatorii de bază pe care urmează să le întreprindă ofițerul de urmărire penală în cadrul cercetării infracțiunilor informatice, în procesul de pregătire pentru efectuarea unei acțiuni de urmărire penală, cum ar fi cercetarea la fața locului, reconstituirea faptei, experimentul, percheziția, ridicarea de obiecte și documente etc. În viziunea autorului, este necesar ca măsurile preliminare de bază să fie efectuate de către organul de urmărire penală, odată ajuns la fața locului pentru realizarea acțiunii procesuale preconizate, iar datele urmează a fi fixate în procesul-verbal al acțiunii de urmărire penală.

În lucrarea autorului român A. C. Moise, *Metodologia investigării criminalistice a infracțiunilor informatice* [26], este abordată problema cercetării infracțiunilor informatice ca urmare a creșterii fenomenului criminalității informatice, care se datorează dezvoltării continue a IT și comunicațiilor, acest lucru având un impact important asupra societății contemporane. În

opinia savantului, cercetarea infracțiunilor informatice vizează atât un aspect juridic, caracterizat de legislația în vigoare privind criminalitatea informatică, cât și un aspect tehnico-științific, determinat de metodologii și tehnici de cercetare, utilizate în vederea obținerii probelor digitale. Autorul menționează că probele digitale sunt utilizate în procesul de cercetare în aceleași scopuri ca și probele fizice, iar diferența majoră între cele două tipuri de probe este determinată de faptul că probele digitale reprezintă numai o valoare și nu sunt obiecte tangibile.

Astfel, în lucrarea menționată mai sus se acordă o atenție deosebită clasificării infracțiunilor informatice, descrierii semnelor obiective și subiective ale componenței infracțiunii informatice, analizei etapelor activității de descoperire a criminalității în domeniu, cercetării particularităților efectuării anumitor acțiuni de urmărire penală și măsuri speciale de investigații în cadrul urmăririi penale la cercetarea delictelor informatice.

În monografia sa, *Securitatea informațiilor și internetul – criminalitatea informatică* [27], D. G. Ghervase și-a propus să traseze o paralelă între securitatea informațiilor și internet, interpretând modalitățile de prevenire a fenomenului de criminalitate informatică drept urmare a dezvoltării continue a IT și comunicațiilor și descriind diverse metodologii și tehnici de cercetare a infracțiunilor informatice. Autorul abordează, în această lucrare, o problemă de importanță majoră pentru investigarea criminalistică a infracțiunilor informatice, încercând să clarifice, astfel, răspândirea fenomenului în cauză nu numai pe plan internațional, dar și pe cel intern.

Cercetătorul menționează faptul că, în contextul schimbărilor intervenite în ultimele decenii atât în domeniul social și politic, cât și în cel tehnologic, informația a devenit elementul esențial și versatil pentru protecția și securitatea societății, în sensul că procesul de globalizare se dezvoltă ca un fenomen necesar și ireversibil, fiiind și sursa tuturor schimbărilor economice și politice ale lumii moderne, ceea ce generează noi riscuri și amenințări. IT a afectat și va afecta major conceptele care stau la baza informațiilor, atât pe cele referitoare la arhitectura acestora, cât și pe cele ce țin de metodele și procedeele de protecție, de factorul uman care operează cu diferite sisteme, precum și de impactul unei asemenea tehnologii asupra evoluției societății.

O altă lucrare dedicată securității informatice, cu titlul *Vulnerabilități ale sistemelor informatice: securitatea și securizarea acestora* [28], a fost elaborată de către cercetătorul român M. I. Neamțu. Aici autorul definește noțiunea, elementele și principiile de activitate ale rețelelor de calculatoare, ale aplicațiilor și protocoalelor, ale poștei electronice și WWW, ale sistemelor de fișiere, precum și mecanismele de administrare a acestora, nivelele de comunicație, tipurile de rețele. Totodată, în lucrare atestăm descrierea criminalității informatice, clasificarea riscurilor și incidentelor, vulnerabilităților la care sunt expuse sistemele și rețelele informatice. Autorul a

identificat mai multe tipuri de infractori informatici, clasificați în dependență de motivația acestora pentru comiterea infracțiunilor în cauză.

Criminalistul român M. Ruiu, în lucrarea sa, *Criminalistică*, consacrată cercetării tacticii criminalistice, a studiat specificul percheziției informatice [29], menționând că legiuitorul român a înțeles să acorde, pe de o parte, o protecție juridică sistemelor informatice împotriva diferitor forme de atac informatic sau de modificare a datelor, iar pe de altă parte, a pus la dispoziția organelor judiciare noi mijloace speciale de investigații, în vederea obținerii de probe, printre care se regăsește și percheziția sistemelor informatice. Totodată, s-a precizat că perchezițiile sistemelor informatice ori a suporturilor de stocare a datelor informatice presupune inspectarea acestora de către organele judiciare în vederea descoperirii și strângerii probelor. Autorul a descris particularitățile probelor digitale, precum și importanța implicării specialistului în domeniul IT la administrarea acestora.

În lucrare sunt propuse mai multe recomandări și măsuri preliminare de bază, pe care trebuie să le întreprindă ofițerul de urmărire penală, odată ajuns la fața locului pentru efectuarea acțiunii de urmărire penală, precum și la realizarea nemijlocită a acesteia (cum ar fi modelarea clonelor suporturilor de stocare a informației digitale, fixarea și etichetarea probelor depistate, împachetarea, sigilarea și transportarea acestora). O atenție aparte este acordată modului de cercetare a informațiilor electronice voluminoase, inclusiv în lipsa specialistului în domeniu. Autorul a punctat particularitățile ridicării sistemelor informatice în dependență de faptul dacă sunt sau nu conectate la sursa de alimentare cu energie electrică.

Un an mai târziu, același autor publică lucrarea *Metodologia investigării criminalistice a unor genuri de infracțiuni* [30], în care își propune să semnaleze, din perspectiva unui inventar de probleme, tehnici și tendințe, necesitatea stringentă a reglementărilor globale și a dezvoltării ramurii dreptului spațiului virtual, să abordeze noi direcții în cercetarea acestui fenomen.

Cercetătorii români D. I. Cristescu și V. C. Enescu, în studiul *Prolegomene privind administrarea și expertizarea probelor multimedia (din perspectiva prevederilor noului Cod de procedură penală)* [31], prezintă unele explicații preliminare privind problemele pe care le ridică înregistrările judiciare audio-video și fotografiile (imaginile), adică probele multimedia (analogice ori originale) din perspectiva expertizelor judiciare, ce se pot dispune în legătură cu acestea, ținând seama de prevederile Noului CPP al României.

Autorii investighează atât înregistrările oficiale, realizate de reprezentanții autorităților publice (inclusiv înregistrările audio-video, filmările și fotografiile autorizate de către judecător ori cele realizate de organul de urmărire penală în timpul cercetării la fața locului, percheziției etc., în scopul fixării rezultatelor activității întreprinse), cât și înregistrările neoficiale, atunci când sunt

efectuate de amatori ori profesioniști (reporteri, detectivi particulari, agenți ai societăților de pază și protecție sau depistate în supravegherile electronice, instalate la unele societăți comerciale etc.).

Lucrarea este o sinteză a situațiilor faptice concrete, ce conduc la suspiciuni în privința autenticității înregistrărilor audio-video și a imaginilor depuse în dosarul cauzei, a unor inadvertențe în activitatea de interceptare și înregistrare a convorbirilor telefonice. Astfel, sunt expuse situațiile create de erorile existente în activitatea de redare a conținutului convorbirilor telefonice interceptate și înregistrate, de durata scurtă între momentul când a avut loc efectiv convorbirea telefonică interceptată și înregistrată și momentul când aceasta apare stocată pe suportul de memorie externă, de selectarea unilaterală de către organele și lucrătorii ce reprezintă acuzarea a anumitor convorbiri telefonice sau imagini.

Totodată, autorii studiului atrag atenția asupra faptului utilizării unor metode și mijloace tehnice de interceptare și înregistrare, care au un caracter clasificat, ceea ce nu permite examinarea și verificarea acestora, precum și asupra existenței ipotetice a posibilității de modificare/alterare intenționată sau din neglijență a acurateței și integrității probelor multimedia. Într-un capitol separat sunt analizate constatarea tehnico-științifică și expertiza judiciară privind probele multimedia, inclusiv relevanța mijlocului tehnic, delimitarea dintre aceste două procedee probatorii, obiectivele posibile, materialele ce se pun la dispoziția specialistului sau expertului judiciar, expertiza tehnică a semnăturii electronice ș.a.

Într-o lucrare recentă a cercetătorilor români Em. Stancu și T. Manea, *Tactică criminalistică (I)* [32], este tratată pe larg materia de tactică criminalistică. Aici se regăsesc numeroase exemple din practica judiciară, elemente de noutate privind efectuarea procedeelor probatorii, precum utilizarea reconstrucției locului faptei în varianta tridimensională; interviul cognitiv ș.a.

Autorii români A. Trancă și D. C. Trancă, în monografia *Infracțiunile informatice în noul Cod penal* [33], au cercetat minuțios reglementările noului CP românesc prin prisma CP și a legislației românești anterioare adoptării acestuia, a legislației internaționale, a legislației conexe, precum și practica judiciară a instanțelor judecătorești din România, relevantă pentru criminalitatea informatică.

Totodată, este analizată definiția și evoluția instituției cyber-crime, cercetătorii explicând pe larg terminologia specifică infracțiunilor informatice, delimitările comparative, aspectele de noutate aduse de actualul CP al României. În lucrare este examinată aplicarea practică a prevederilor legislației materiale în domeniu, precum și legea penală mai favorabilă în cazul fiecărei categorii de infracțiuni. Tot aici sunt analizate și caracteristicile criminalistice ale probelor electronice.

Cercetătorii S. Brânză și V. Stati, în *Tratatul de drept penal* [34], similar legiuitorului moldav, au consacrat un capitol separat cercetării aspectelor juridico-penale privind infracțiunile informatice și din domeniul telecomunicațiilor, obiectul analizei constituindu-l totalitatea elementelor și semnelor componenței de infracțiune pentru fiecare infracțiune în parte. Autorii definesc infracțiunile informatice și cele din domeniul comunicațiilor electronice ca fiind fapte socialmente periculoase, săvârșite cu intenție sau din imprudență, care aduc atingere, prin excelență, relațiilor sociale din domeniul informaticii și al comunicațiilor electronice, răspunderea penală pentru care se stabilește la art.259-261[1] CP.

În lucrarea *Codul de procedură penală al Republicii Moldova (comentariu aplicativ)* [35], autorul ei, I. Dolea, a descris acțiunile de urmărire penală și măsurile speciale de investigații, prevăzute de legislația națională, inclusiv cele specifice cercetării infracțiunilor informatice, abordate și prin prisma practicii judiciare a CtEDO.

În afară de studiile prezentate *supra*, pot fi menționate și altele, semnate de autori din RM și România și consacrate diferitor probleme referitoare la aspectele juridico-penale ale criminalității informatice, și anume: colectivul de autori S. Brânză, X. Ulianovschi, V. Stati ș.a. în lucrarea *Drept penal. Partea specială* [36], V. Dobrinoiu, I. Pascu, M. A. Hotca ș.a. în *Noul Cod Penal comentat* [37], M. Dobrinoiu în *Analiza juridică a infracțiunii de fals informatic* [38], I. Vasiu și L. Vasiu în lucrarea *Frauda informatică* [39], A. T. Drăgan în *Frauda informatică în sistemul infracțiunilor contra patrimoniului în noul Cod penal român* [40], Gh. Alecu în *Subiecții activi și pasivi ai infracțiunilor comise prin sisteme informatice, în viziunea noului Cod Penal* [41], I. C. Spiridon în *Reflecții cu privire la legislația română în domeniul criminalității informatice* [42], M. Dobrinoiu în *Accesul ilegal la poșta electronică* [43], F. Encescu în *Considerații asupra disputei dintre teoreticienii și practicienii dreptului privind încadrarea juridică penală a skimming-ului* [44], M. Dobrinoiu în *Infracțiunea de alterare a integrității datelor informatice* [45], M. A. Hotca și M. Dobrinoiu în *Infracțiuni prevăzute în legi speciale* [46] ș.a.

1.2. Studierea infracțiunilor informatice reflectată în literatura de specialitate din alte state

M. A. Sussmann, în articolul *The critical challenges from international high-tech and computer-related crime at the millennium* [47], menționează că criminalitatea informatică are un caracter transfrontalier, neavând limite teritoriale, ceea ce îi permite infractorului să comită infracțiunea de pe teritoriul unui stat față de persoane din alte state.

Cercetătorii ruși, E.N. Bâstreakov, A.N. Ivanov, V.A. Klimov, în studiul *Расследование компьютерных преступлений: учебное пособие* [48], definesc caracteristica criminalistică a

infracțiunilor informatice drept un sistem de date referitoare la elementele tipice ale acestor infracțiuni și ale legăturilor uniforme dintre acestea, relevante pentru soluționarea sarcinilor puse în fața organului de urmărire penală. În opinia lor, structura spațiului cibernetic include: încăperile în care se află sistemele informatice și tehnica complexă care asigură funcționarea acestora (sistemele de comunicații, energia electrică, ș.a.); mijloacele de prelucrare automatizată a informației (mașinile de calcul și sistemele lor); canalele de comunicații electronice și de transmitere a datelor (inclusiv undele audio- și electromagnetice); suporturile pentru stocarea datelor informatice și înseși datele informatice. Autorii consideră că în cadrul cercetării infracțiunilor informatice pot fi evidențiate trei situații tipice, iar victimă a infracțiunii informatice, de cele mai multe ori, se dovedește a fi persoana juridică.

Un grup de practicieni americani din cadrul Departamentului de Justiție al Statelor Unite, sub conducerea lui John Ashcroft, a elaborat, în anul 2001, un ghid cu privire la investigația electronică la fața locului, intitulat *Electronic Crime Scene Investigation. A Guide for First Responders* [49]. În acest ghid, grupul de autori analizează tipurile și trăsăturile criminalistice ale probelor electronice, inclusiv problemele cu care se confruntă organul de drept la administrarea și aprecierea acestora, caracterul latent al lor, necesitatea implicării specialistului în domeniul IT în procesul de investigare. Sunt identificate și descrise majoritatea dispozitivelor locale, precum și cele de rețea care pot conține probe electronice. O atenție deosebită este acordată utilitarelor și echipamentelor necesare unui investigator pentru ridicarea probelor electronice de la fața locului, cum ar fi: documente, instrumente de asamblare și dezasamblare, obiecte pentru împachetarea și transportarea dispozitivelor electronice etc. Totodată, în ghidul respectiv sunt prezentate principiile, politica și procedura securizării și evaluării locului acțiunii procesuale, inclusiv audierea preliminară a persoanelor.

În ceea ce privește procedura colectării nemijlocite a probelor electronice, practicienii americani elucidează bunele practici referitoare la documentarea inițială la fața locului, ridicarea probelor tradiționale, precum și pașii care urmează a fi parcurși în dependență de starea sistemului informatic. În final, sunt oferite mai multe recomandări cu privire la împachetarea, transportul și păstrarea dispozitivelor electronice, un capitol aparte fiind destinat analizei probelor electronice, care urmează a fi administrate în dependență de categoria infracțiunii cercetate.

Autorul american R. Moore, în lucrarea *To view or not to view: Examining the plain view doctrine and digital evidence* [50], pune în discuție specificul volatil al probelor electronice. De la momentul săvârșirii infracțiuni până la efectuarea acțiunilor de urmărire penală, de colectare a probelor electronice, se pot produce multiple conectări și deconectări ale sistemului informatic, diverse operațiuni în sistemul de operare sau asupra acestuia (spre exemplu, defragmentarea

informației, reinstalarea sistemului operațional, ștergerea, modificarea sau suprascrierea datelor informatice), folosirea sistemului informatic de către numeroși alți utilizatori ș.a.m.d. În consecință, toate acestea conduc la pierderea iremediabilă a urmelor electronice relevante.

În autoreferatul *Основы методики расследованя преступлений в сфере компьютерной информации* [51], V.A. Meșereakov susține că structura spațiului cibernetic include încăperile în care se află sistemele informatice, precum și tehnica complexă care asigură funcționarea acestora; mijloacele de prelucrare automatizată a informației; canalele de comunicații electronice și cele de transmitere a datelor; suporturile de stocare a datelor informatice; înseși datele informatice nemijlocite.

Un colectiv de autori, constituit din B.V. Andreev, P.N. Pak și V.P. Horst, în lucrarea *Расследование преступлений в сфере компьютерной информации* [52], au efectuat o cercetare pertinentă a fenomenului criminalității informatice – atât din punct de vedere penal, cât și din cel procesual-penal. Ei au propus diverse interpretări științifice ale anumitor noțiuni din legislația rusă ce țin de infracțiunile informatice, spre exemplu: distrugerea și ștergerea informației computerizate, accesul la date informatice etc.

În opinia autorului american S. Smith, expusă în lucrarea *The Concept of Security in a Globalized World* [53], criminalitatea informatică, în sens restrâns, reprezintă totalitatea infracțiunilor în care drept obiect juridic de bază apar raporturile juridice în domeniul creării, păstrării, prelucrării și transmiterii securizate a informației computerizate, iar obiectul nemijlocit îl constituie datele informatice, precum și mijloacele de securizare a datelor informatice.

Cercetătorul rus A.I. Golovin, în *Криминалистическая систематика* [54], referindu-se la tăinuirea probelor în cauzele de criminalitate informatică, opinează că una din cauzele reușitei actului de opunere a rezistenței în descoperirea infracțiunilor informatice este latența sporită a acestor categorii de infracțiuni. Numeroase acțiuni din domeniul IT, precum și datele informatice pot fi ușor depersonalizate. Totuși datele informatice nu sunt lipsite de anumite semne care să le individualizeze, chiar dacă, încă de la etapa pregătirii infracțiunii, făptuitorul întreprinde măsuri pentru ca aceasta să nu fi identificată, cercetată și descoperită.

În lucrarea *Компьютерная преступность за рубежом и ее предупреждение* [55] a cercetătorului rus A.A. Jmâhov, au fost analizate aspectele juridico-penale și criminologice ale criminalității informatice în diferite state, inclusiv în Federația Rusă. În opinia autorului, criminalitate informatică reprezintă orice infracțiune în care un calculator sau o rețea de calculatoare este obiectul unei infracțiuni, sau în care un calculator sau o rețea de calculatoare este instrumentul sau mijlocul de înfăptuire a unei infracțiuni.

A.G. Filipov, în lucrarea intitulată *Криминалистика: Учебник для высших юридических учебных заведений* [56], a analizat particularitățile cercetării infracțiunilor informatice, descriind instructajul membrilor grupului de urmărire penală, participanți la efectuarea acțiunilor de urmărire penală, explicând utilizarea terminologiei specifice la întocmirea procesului-verbal al acțiunii procesuale, diverse modalități de depistare a probelor electronice distruse sau ascunse, etichetarea componentelor sistemului informatic ce urmează a fi ridicat, propunând soluții hardware și software (partea logică a unui sistem informatic) de oprire a programelor care rulează pe calculatorul supus examinării, prezentând procedura ridicării sistemului informatic care este deconectat de la sursa de alimentare cu energie electrică, a documentelor care pot conține informație probatorie relevantă pentru soluționarea cauzelor penale având drept obiect al cercetării infracțiuni informatice sau tangente acestora, atenționând asupra pericolului substanțelor și materialelor inflamabile, explozibile și toxice, aflate în încăperea în care sunt prezente sisteme informatice, relevând conservarea probelor electronice.

N.G. Șuruhnov, în lucrarea *Криминалистика: Учебное пособие* [57], observă că printre instrumentele caracteristice infracțiunilor informatice, utilizate la crearea piedicilor organului de urmărire penală, se includ: folosirea softurilor care fac imposibilă identificarea persoanei sau utilizarea accesării prin servere intermediare, precum și utilizarea unor *remailers*-uri, calculatoare ce primesc mesaje și le redirecționează către adresa electronică destinată, ștergând toate datele despre expeditor.

J. Baylis, în lucrarea sa *International and global security in the post-cold war era in The Globalization of World Politics* [58], relevă faptul că în ultimii ani criminalitatea informatică se caracterizează și prin unele trăsături politice, reprezentanții serviciilor speciale, ai structurilor de forță din diverse state, organizațiile extremiste și teroriste angajând specialiști de înaltă calificare din domeniul IT.

Cercetătorul rus D.V. Dobrovolskii, în studiul său *Актуальные проблемы борьбы с компьютерной преступностью* [59], a generalizat problemele cu care se confruntă organul de urmărire penală și organul care efectuează activitatea specială de investigații la cercetarea infracțiunilor informatice. În accepția sa, criminalitatea informatică reprezintă ansamblul tuturor infracțiunilor din domeniul IT, săvârșite într-o anumită perioadă de timp și pe un teritoriu bine determinat.

În lucrarea *Криминалистика* [60] a autorului rus N.P. Iablokov, au fost prezentate formele actului de modificare neautorizată a datelor informatice, identificându-se o nouă categorie de infractori informatici, cum ar fi vandalii informatici. Autorul a prezentat 3 situații tipice la cercetarea infracțiunilor informatice.

În același timp, s-a atras atenția asupra unor particularități de cercetate a acestui gen de infracțiuni, și anume: necesitatea invitării specialistului la realizarea acțiunilor de urmărire penală, pericolul „curselor” pregătite de către făptuitor, care să conducă la autodistrugerea informației electronice, pașii pe care trebuie să-i întreprindă ofițerul de urmărire penală, pentru a stabili dacă un sistem informatic este deconectat de la sursa de alimentare cu energie electrică, influența negativă a câmpurilor electromagnetice și electrostatice asupra dispozitivelor electronice ridicate și transportate la sediul organului de urmărire penală, importanța stabilirii identității victimei, a martorului sau a bănuitului/învinuitului pentru audierea acestuia.

A. Reyes și J. Wiles, în lucrarea *The Best Damn Cybercrime and Digital Forensics Book Period* [61], au descris o parte din tipurile surselor de date în legătură cu traficul informatic, cum ar fi: firewall-urile (un ansamblu de componente hardware și software care se interpune între două rețele pentru a regla și controla traficul dintre ele) și router-ele (dispozitiv utilizat pentru interconectarea mai multor rețele locale de tipuri diferite, dar care utilizează același protocol de nivel fizic); sistemele de detectare a intruziunii – IDS (sistemele care monitorizează traficul de rețea și detectează încercările de a obține acces neautorizat la un sistem informatic); instrumentele de analiză criminalistică a rețelei.

În opinia lui N.N. Egorov, expusă în monografia *Вещественные доказательства: уголовно-процессуальный и криминалистический аспект* [62], specialistul trebuie invitat să participe la audiere, atunci când organul de urmărire penală deține informații că persoana audiată posedă cunoștințe vaste referitoare la întrebările speciale și are o experiență bogată în domeniu. În asemenea situații, persoana audiată începe să explice activ schema complicată a obiectelor și multiplele legături dintre ele, fapt prin care se solicită un nivel înalt de cunoaștere din partea organului de urmărire penală într-o anumită ramură, precum și capacitatea lui de a înțelege noțiunile.

În ghidul *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensics Investigators* [63], elaborat de D. Kleiman, este relevată importanța specialistului din domeniul IT în cadrul procesului penal referitor la cercetarea infracțiunilor informatice, inclusiv în pregătirea tuturor softurilor, mijloacelor tehnice și echipamentelor necesare efectuării percheziților informatice; în întreprinderea măsurilor în vederea depistării și realizării copiei fișierelor temporare - probe volatile (memoria RAM, cache, componentele periferice), această categorie de fișiere distrugându-se odată cu întreruperea funcționării sistemului informatic; în examinarea diferitor probe electronice, în funcție de tipul infracțiuni informatice: lista adreselor URL vizitate, mesajele e-mail și lista adreselor e-mail memorată în agenda suspectului, documentele procesate, grafice (în cazul pornografiei infantile), înregistrări chat, registrul sistemului de operare, jurnale

prezentatoare de evenimente (event viewer logs), jurnale de aplicație, fișiere de derulare a documentelor imprimate; realizarea copiei suportului de stocare a informației.

Doctorul în drept T.M. Lopatina, în lucrarea *Криминологические и уголовно-правовые основы противодействия компьютерной преступности* [64], a realizat o cercetare temeinică a problemelor legate de contracararea criminalității informatice, propunând diverse măsuri de ordin criminologic și penal. Autoarea definește criminalitatea informatică ca fiind un ansamblu de infracțiuni, săvârșite pe un anumit teritoriu într-o anumită perioadă de timp, care atentează la acumularea, prelucrarea, stocarea și distribuirea informației computerizate, precum și infracțiunile săvârșite cu utilizarea calculatorului în vederea obținerii unui beneficiu material sau de altă natură. Totodată, T.M.Lopatina analizează și principiile activității speciale de investigații la cercetarea acestor categorii de infracțiuni.

Cercetătorii A.V. Vardanean și E.V. Nikitina, în *Расследование преступлений в сфере высоких технологий и компьютерной информации* [65], au descris specificul efectuării acțiunilor de urmărire penală în cadrul cercetării infracțiunilor din domeniul tehnologiilor avansate, precum și a infracțiunilor informatice, punând un accent deosebit pe realizarea nemijlocită a acțiunii procesuale, în cadrul căreia urmează a fi ridicate sistemele informatice.

Cercetătorul american M. Cross, în lucrarea *Scene of the Cybercrime* [66], a desemnat totalitatea de infracțiuni din domeniul informației computerizate prin termenul *criminalitate informatică*, deoarece expresia în cauză reflectă integral această categorie de infracțiuni, săvârșite în domeniul respectiv prin intermediul dispozitivelor informatice, al rețelelor de comunicații electronice și IT.

A.P. Kuznețov și N.V. Garipova au realizat o cercetare aprofundată cu privire la stabilirea obiectului infracțiunilor informatice, în lucrarea intitulată *Проблемы определения непосредственного объекта в преступлениях в сфере компьютерной информации* [67], concluzionând că obiectul juridic cuprinde relațiile sociale referitoare la utilizarea normală și securizată a sistemelor informatice.

În lucrarea *Уголовно-правовые, криминологические и криминалистические проблемы расследования преступлений в сфере высоких технологий и компьютерной информации* [68], V.A. Dulenko, R.R. Mamleev și V.A. Pestrikov au realizat o cercetare a noțiunii, importanței și a posibilităților tehnologiilor contemporane, analizând categoriile și particularitățile IT. Studiul include descrierea caracteristicilor juridico-penale, criminologice și criminalistice ale infracțiunilor din domeniul tehnologiilor avansate; sunt expuse sarcinile actuale ce țin de profilactica, descoperiea și expertizarea activității ilegale în domeniul IT și informației computerizate.

Distinct, sunt analizate infracțiunile respective, precum și metodele și mijloacele de identificare și de investigare a acestora, punându-se un accent deosebit pe definirea probelor virtuale (electronice, netradiționale). Autorii au detaliat procedurile preparatorii de bază în cadrul efectuării acțiunilor de urmărire penală, cum ar fi: stabilirea planului locului unde urmează a fi efectuată acțiunea procesuală, studierea identității suspectului. În lucrare sunt descrise și principiile fundamentale ale efectuării activității speciale de investigații.

Americanii T. J. Holt și A.M. Bossler, în lucrarea *Cybercrime in progress: theory and prevention of technology-enabled offenses* [69], s-au referit la criminalitatea informatică, analizând-o din punct de vedere criminologic și subliniind necesitatea adaptării teoriilor existente la specificul IT și al spațiului virtual. Întrucât conceptele criminologice existente privind criminalitatea tradițională sunt de o valoare limitată, autorii au pus în discuție problema genezei criminalității informatice, provocând dezbateri din care s-a impus necesitatea formării unor teorii noi, aplicabile doar acestui tip de criminalitate.

Cercetătorii D.V. Litvinov, S.V. Skrâli și A.V. Teamkin, în monografia colectivă *Исследование механизмов противодействия компьютерным преступлениям: организационно-правовые и криминалистические аспекты* [70], au analizat principiile fundamentale organizatorico-juridice, necesare asigurării securității informatice a sistemelor informatice, elborând recomandări cu privire la măsurile de prevenire a criminalității în domeniul informaticii.

În articolul *О характеристике способов совершения сетевых компьютерных преступлений* [71], A.L. Osipenko, referindu-se la obstacolele pe care le poate crea făptuitorul în vederea împiedicării bunei desfășurări a urmăririi penale, menționează că nu doar distrugerea informației computerizate poate conduce la ascunderea urmelor infracțiunii: cu acelaşi scop poate fi efectuată blocarea sau modificarea informației, prin cel din urmă caz infractorul orientând cercetarea într-o direcție greșită. Această ultimă metodă este cea mai periculoasă, întrucât infractorul își poate masca identitatea prin modificarea datelor din registrele electronice, prin schimbarea adresei IP, precum și a pachetelor de date, în consecință fiind create probe false.

În *Социальная и психологическая харакеристика личности компьютерного преступника* [72], T.V.Voroșilova analizează trăsăturile caracteristice ale personalității infractorului informatic. Astfel, în opinia ei, un rol deosebit în descoperirea oricărei infracțiuni informatice îl joacă și profilul psihologic al personalității infractorului. În aceste condiții, trebuie identificat sexul, vârsta, statutul social, situația familială și materială, locul de trai, apartenența la o anumită cultură. Analiza aprofundată a acestei informații va permite stabilirea și restrângerea

cercului de suspecți, a motivelor infracțiunii, va contribui la înaintarea versiunilor și identificarea acțiunilor necesare descoperirii infracțiunii.

O altă monografie în domeniul vizat aparține autorului rus M.M. Menjega, fiind intitulată *Методика расследования создания и использования вредоносных программ для ЭВМ* [73]. Această lucrare reprezintă o cercetare criminalistică complexă a problemelor privind crearea, utilizarea și răspândirea programelor malițioase, destinate sistemelor informatice. Sunt cercetate anumite categorii de infracțiuni, legate de utilizarea acestor produse program, iar în privința unora dintre ele sunt elaborate recomandări, precum și propuneri de perfecționare a legislației în domeniu.

Autorul a analizat particularitățile caracteristicii criminalistice a creării, utilizării și răspândirii produselor program malițioase, inclusiv obiectul faptei criminale, circumstanțele comiterii infracțiunii (respectiv, locul și timpul comiterii infracțiunii), personalitatea infractorului (tipurile de infractori informatici în dependență de motivația acestora, categoriile de vârstă) și a victimei (care, de cele mai multe ori, este persoană juridică), specificul motivelor și scopurilor infracțiunii, modalitățile de săvârșire a faptei, urmele tipice ale infracțiunii.

În lucrare au fost relevate situațiile tipice de descoperire și cercetate a acestor infracțiuni, efectuarea acțiunilor de verificare la etapa inițierii urmăririi penale, planificarea acțiunilor de urmărire penală, precum și conlucrarea dintre organele de drept implicate în cercetarea faptei. Au fost elaborate recomandări suplimentare cu privire la pregătirea și tactica efectuării anumitor acțiuni de urmărire penală la etapa incipientă a procesului penal de cercetare a faptelor de creare, utilizare și răspândire a produselor program malițioase pentru sistemele de calcul, cum ar fi cercetarea la fața locului, percheziția, ridicarea de obiecte și documente, audierea, dispunerea efectuării expertizei. Autorul elucidează greșelile tipice, comise în cadrul urmăririi penale a acestor categorii de infracțiuni, precum și instrumentele utilizate de către infractorii informatici față de organul de urmărire penală, în vederea împiedicării bunei desfășurări a urmăririi penale.

Cercetătorii P.V. Hudeakov și D.V. Ovseanikov au elaborat un ghid privind cercetarea infracțiunilor în domeniul informației computerizate, intitulat *Особенности производства следственных действий при расследовании преступлении в сфере компьютерной информации* [74], în care au fost supuse analizei aspectele juridico-penale și caracteristicile criminalistice ale infracțiunilor din domeniu, specificul pornirii urmăririi penale și al etapei preliminare de cercetare a cauzei. Au fost descrise momentele-cheie în efectuarea anumitor acțiuni de urmărire penală la cercetarea cauzelor respective și au fost prezentate particularitățile audierii martorilor, a victimelor și a persoanelor suspecte în cadrul procesului penal, fiind propuse

recomandări specifice acestei acțiuni de urmărire penală în dependență de profilul psihologic al persoanei audiate, de funcția ocupată, precum și de categoria infracțiunii informatice săvârșite.

Acești autori au invocat necesitatea efectuării anumitor acțiuni specifice de urmărire penală la examinarea cauzelor penale privind infracțiunile informatice, și anume: ridicarea și examinarea sistemelor informatice, a dispozitivelor periferice, a suporturilor de stocare a datelor informatice, a produselor program, precum și a documentelor elaborate cu ajutorul mijloacelor tehnico-electronice. Au fost remarcate erorile tipice, comise de către reprezentanții organelor de drept asupra datelor informatice, fiind formulate anumite recomandări metodologice în vederea depășirii acestor situații. Totodată, au fost relevate sarcinile pe care urmează să le îndeplinească expertizele tehnice în domeniul vizat în dependență de categoria obiectului examinat.

Autorii ruși V.I. Aleskerov și I.A. Maximenko au publicat, în anul 2011, monografia intitulată *Уголовно-правовая и криминалистическая характеристика современных видов преступлений в сфере компьютерной информации* [75]. În lucrare sunt prezentate tipurile, trăsăturile și caracteristica procesual-penală și criminalistică a infracțiunilor de bază din domeniul informației computerizate, categoriile infracțiunilor legate de intervenția în funcționarea calculatorului, infracțiunile săvârșite prin utilizarea sistemului informatic. Totodată, sunt expuse și caracteristicile criminalistice ale probelor electronice (informațiile computerizate), sunt descrise principalele mijloace de comitere a infracțiunilor respective și principiile fundamentale de protecție a informației.

O altă lucrare, destinată pregătirii profesionale a angajaților organelor de drept în vederea prevenirii și combaterii criminalității informatice, este monografia *Особенности раскрытия преступлений в сфере компьютерной информации* [76], semnată de autorii ruși A.B. Sizonenko și V.N. Șișkin, care au definit aici noțiunea de *informație*, au prezentat bazele legale, ce reglementează IT și protecția informației, au clasificat categoriile de informații protejate, precum și instituțiile responsabile de combaterea acestui fenomen în Federația Rusă. O atenție sporită a fost acordată analizei caracteristicii procesual-penale și speciale de investigații a infracțiunilor din domeniul informației computerizate. Un capitol aparte a fost dedicat tacticii de depistare, fixare și ridicare a informației computerizate în cadrul efectuării măsurilor speciale de investigații. Sunt elucidate și particularitățile și principiile activității speciale de investigații și ale anumitor acțiuni de urmărire penală.

Asociația șefilor de poliție din Anglia, Țara Galilor și Irlanda de Nord a elaborat un ghid de bune practici pentru probele digitale *Good Practice Guide for Digital Evidence* [77], în care sunt analizate principiile referitoare la probele electronice, la planificare, la acțiunile care urmează a fi întreprinse de către organul de urmărire penală atât până la sosirea la fața locului, cât și aflându-se

la locul infracțiunii. Trebuie menționate și recomandările cu privire la colectarea probelor electronice online (live), o atenție aparte fiind acordată examinării, interpretării și aprecierii probelor specifice infracțiunilor informatice.

I.V.Smolikova susține, în monografia sa *Великие и выдающиеся, знаменитые и известные личности об уголовном судопроизводстве* [78], că juristul nu dispune și nici nu poate dispune de cunoștințe în toate domeniile, așa că, pentru a-și îndeplini sarcinile, el trebuie să implice specialiștii din domeniile care nu-i sunt cunoscute sau în care are cunoștințe insuficiente. Specializarea și progresul actual al tehnicii nu permit reprezentantului unui domeniu să fie competent în altul.

O altă lucrare în domeniu este *Организация взаимодействия МВД стран СНГ по предупреждению преступлений в сфере информационно-коммуникационных технологий* [79], consacrată cooperării regionale în vederea prevenirii și combaterii criminalității din sfera informaticii. Autorii ei, A.S. Klementiev și O.S. Boiko, au cercetat fenomenul criminalității în domeniul IT și tehnologiilor comunicaționale, precum și problemele prevenirii acestuia, analizând reglementările juridice ale cooperării dintre Ministerele de Interne ale statelor CSI în privința prevenirii infracțiunilor informatice. Un capitol aparte este dedicat studiului perfecționării bazelor organizatorice privind cooperarea statelor membre CSI. Totodată, autorii au descris și cele mai relevante semne caracteristice ale infracțiunilor informatice.

În monografia *Преодоление противодействия расследованию преступлений в сфере компьютерной информации* [80], autorul ei, Kosânkin A.A., menționează că reducerea consemnată a numărului de infracțiuni din domeniul informaticii nu semnifică micșorarea cantitativă a infracțiunilor de acest gen, ci se datorează dificultății descoperirii lor. Acest fapt denotă că metodele, mijloacele și tehnicile utilizate de către infractori pentru a-și tăinui infracțiunile devin mai efective. În același timp, activitatea organelor de drept, orientată spre înlăturarea piedicilor apărute în cadrul procesului penal, nu-și atinge scopul. Din aceste motive problema care cere o soluție imediată este stabilirea metodelor, mijloacelor și tacticilor efective de depășire a obstacolelor apărute în cadrul cercetării infracțiunilor în domeniul informației computerizate.

În ultimii ani, acțiunile de zădărnicire a bunei desfășurări a urmăririi penale în domeniul vizat se modifică foarte mult, se perfecționează, ceea ce face ca metodele și tehnicile anterioare, utilizate pentru învingerea acestora, să fie ineficiente. În acest sens, autorul realizează o analiză a trăsăturilor fundamentale specifice infracțiunilor informatice, descriind și clasificând obstacolele care perturbă desfășurarea normală a procesului penal, în funcție de factorii care generează apariția acestora. În lucrare sunt relevate scopurile pe care le urmărește infractorul prin

influențarea activității de urmărire penală a infracțiunilor săvârșite în domeniul supus analizei, precum și calitățile caracteristice persoanelor, care creează obstacole în efectuarea investigațiilor.

În ghidul ştiinţifico-practic, intitulat *Использование специальных познаний при раскрытии и расследовании преступлений в сфере высоких технологий*, autorii lui, A.V. Narijnâi şi A.H. Pihov [81], au menționat că răspândirea criminalității în domeniul tehnologiilor avansate îi obligă, inevitabil, pe angajații organelor de drept să studieze în detaliu posibilitățile sistemelor informatice și ale utilizării lor în lupta cu această categorie de infracțiuni. Accesibilitatea resurselor informaționale, viteza mare de prelucrare a bazelor de date, volumul extrem de mare al datelor, precum și lejeritatea formării, schimbului și utilizării acestora, au condiționat actualitatea problemei pe care trebuie să o soluționeze organele de drept.

Autorii au analizat unele semne caracteristice infracțiunilor informatice și au descris anumite reguli și recomandări cu privire la acțiunile preparatorii pentru efectuarea acțiunilor de urmărire penală, în vederea administrării probelor la cercetarea acestor categorii de infracțiuni. Au fost analizate și particularitățile cercetării dispozitivelor electronice de comunicație mobilă.

O analiză separată a infracțiunilor în domeniul comunicațiilor electronice a fost efectuată de către cercetătorii ruși V.I. Aleskerov și F.A. Kuț în lucrarea *Преступления, совершаемые в телекоммуникационых сетях, как разновидность преступлений в сфере компьютерной информации* [82]. Potrivit acestora, actualmente asigurarea protecției comunicațiilor electronice reprezintă nu doar o prerogativă a statului, dar și o sarcină de bază în activitatea oricărei instituții, serviciu, organizații și întreprinderi. Orice încălcare în domeniul comunicațiilor electronice poate genera perturbarea activității unei rețele informatice și cauza un prejudiciu material considerabil. Totodată, practica națională și cea internațională remarcă apariția unor noi fapte în domeniul vizat, săvârșite prin intermediul mijloacelor de comunicații electronice, a căror diversitate este într-o permanentă creștere. În lucrare este definită noțiunea de criminalitate informatică, sunt analizate unele aspecte juridico-penale ale infracțiunilor informatice, precum și caracteristicile criminalistice ale probelor electronice (informația computerizată).

În monografia *Методика расследования экстремистских преступлений, совершённых в компьютерных сетях*, autorul ei, V.O. Davâdov [83], elucidează esența și rolul suportului informațional în descoperirea și cercetarea infracțiunilor extremiste, săvârșite cu utilizarea sistemelor și rețelelor informatice (ca o subcategorie a infracțiunilor informatice); realizează caracteristica criminalistică, bazată pe o vastă cercetare empirică; generalizează starea de fapt a practicii de urmărire penală; formulează recomandări metodice cu privire la dobândirea și utilizarea informației probatorii și a altor informații criminalistice relevante, în vederea descoperii și cercetării infracțiunilor din categoria respectivă.

Această lucrare se înscrie printre primele cercetări științifice complexe din spațiul post-sovietic, consacrate colectării și analizei informației criminalistice în cadrul cercetării infracțiunilor legate de extremism, săvârșite cu utilizarea sistemelor și rețelelor informatice. V.O. Davâdov analizează aspectele problematice și lacunele legislative, care reglementează utilizarea mijloacelor electronice, actualitatea fortificării luptei împotriva faptelor de extremism, inclusiv cu utilizarea celor mai noi tehnologii de comunicare socială, necesitatea creării unui sistem de cunoștințe criminalistice referitoare la particularitățile asigurării informaționale a investigațiilor, precum și insuficiența recomandărilor metodice privind efectuarea acestor investigații, necesare organelor de urmărire penală și organelor care organizează activități speciale de investigații. Autorul concluzionează, în baza celor relatate mai sus, că o cercetare în domeniul vizat reprezintă o sarcină prioritară a criminalisticii contemporane.

În opinia cercetătorului rus Musienko O., expusă în *Особенности криминалистической характеристики преступлений, совершаемых в сфере компьютерной информации и сотовой связи* [84], caracteristica criminalistică permite elaborarea și utilizarea eficientă a metodicii de cercetare a oricărei categorii de infracțiuni, inclusiv a celor informatice.

Grupul de autori din cadrul Agenției Europene pentru Securitate a Rețelelor și a Informațiilor (ENISA), în frunte cu Ph. Anderson, au elaborat, în anul 2015, un ghid cu privire la probele electronice, intitulat *Electronic evidence - a basic guide for First Responders* [44]. Aici sunt definite probele electronice, sursele din care provin acestea (computerele, suporturile de stocare a datelor informatice, echipamentele mobile, dispozitivele de rețea), principiile cu privire la colectarea probelor electronice (integritatea datelor, auditul/controlul, suportul specialiștilor, instruirea adecvată, legalitatea). ENISA propune diverse recomandări cu privire la acțiunile ce trebuie întreprinse de către organul de urmărire penală atât până la sosirea la fața locului (pregătirea instrumentelor, a sistemului informatic criminalistic și a utilitarelor), cât și în timpul aflării nemijlocite la locul faptei. Ghidul descrie procedura de examinare a probelor electronice, inclusiv extragerea și analiza acestora. Separat, sunt elaborate propuneri cu privire la evaluarea și prezentarea probelor electronice.

O altă monografie, semnată de criminaliștii ruși S.A. Kovaliov și V.B. Vehov, *Особенности компьютерного моделирования при расследовании преступлений в сфере компьютерной информации* [85], este consacrată studierii particularităților modelării computerizate în cercetarea infracțiunilor din domeniul informaticii. Lucrarea se întemeiază pe cele mai recente realizări științifice în domeniu, pe utilizarea la scară largă a mijloacelor și metodelor moderne de modelare la calculator, pe practica pozitivă a organelor de drept din

Federația Rusă, fiind abordate problemele îmbunătățirii activităților de cercetate a infracțiunilor în domeniul respectiv.

S.A. Kovaliov și V.B. Vehov menționează că, în prezent, majoritatea operațiunilor tehnologice vizează prelucrarea informației, realizată cu ajutorul produselor software și hardware și cu utilizarea unor metode moderne în domeniul IT. Realitățile de astăzi impun crearea de noi mijloace tehnice, metode, tehnici și recomandări, bazate pe utilizarea tehnologiilor avansate și a metodelor de modelare, capabile să influențeze esențial eficacitatea și calitatea cercetării infracțiunilor, inclusiv a celor informatice. Obiectivul principal al acestui progres tehnologic ar trebui să fie introducerea în activitatea criminalistică a unui sistem electronic de management al documentelor, elaborat sub forma unor sisteme informaționale automatizate, apte să funcționeze în cadrul rețelelor informatice și de comunicații electronice, create pentru nevoile organelor de drept.

Într-o altă lucrare, *Организационные и правовые проблемы борьбы с хищениями денежных средств с использованием вредоносных компьютерных программ* [86], autorii ruși P.A. Pimenov și I.V. Goroșko abordează problema luptei cu o categorie nouă de infracțiuni, foarte complexe din punct de vedere organizațional și tehnic, și anume sustragerea mijloacelor financiare de pe conturile bancare și a mijloacelor de plată electronice, prin utilizarea IT și a produselor program malițioase, răspândite pe larg în rețeaua Internet. În monografie se cercetează evoluția, terminologia, baza normativă și tipurile sistemelor electronice de transfer al mijloacelor bănești; aspectele criminologice ale infracționalității în domeniul vizat (dinamica și tendințele extinderii, cauzele nivelului ridicat al latenței acesteia) și problemele actuale ale organelor de drept în lupta cu acest fenomen (stabilirea timpului și locului de comitere a infracțiunii, organizarea examinării sistemelor informatice și a produselor program, asigurarea informațională și analitică a activității de contracarare a acestor categorii de sustrageri).

În lucrare sunt analizate unele semne caracteristice ale infracțiunilor în cauză, dificultățile întâmpinate de către organul de urmărire penală în cadrul efectuării anumitor acțiuni procesuale, inclusiv a expertizelor. Autorii propun mai multe variante de stabilire a locului săvârșirii infracțiunii. Un capitol separat este consacrat studierii caracteristicilor sustragerii mijloacelor financiare prin utilizarea produselor program malițioase, precum și ale organizării activității infracționale și ale situațiilor tipice.

V.D. Zelenskii și G.M. Meretukov, în *Криминалистика: Учебник* [87], au delimitat două categorii specifice de infractori informatici: a) tipul motivat ideologic, caracteristic ultimei perioade de timp, care, de cele mai multe ori, are scopul de a provoca panică, fiind numiți teroriști informatici, și b) tipul bolnav psihic, care suferă de forme noi de maladie psihică – patologii informaționale sau fobii de computer.

Autorii americani S. Bowles și J. Hernandez-Castro, în lucrarea *The first 10 years of the Trojan Horsedefence* [88], au analizat evoluția virusului „Cal Troian", precum și protecția de tip „Cal Troian". Astfel, potrivit acestora, denumirea de „Apărare Cal Troian" își are originea, aparent, în primele cauze documentate în anul 2003 în Marea Britanie și SUA, în care inculpații au negat comiterea faptelor, susținând că acestea au fost comise de programe malițioase de tip „Cal Troian", o serie dintre inculpați fiind achitați în urma constatării prezenței, în sistemul informatic, a unor asemenea programe informatice, întrucât, în aceste condiții, nu a putut fi identificat, dincolo de orice îndoială rezonabilă, făptuitorul real.

Lucrarea *Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации* a autorilor ruși V.I. Aleskerov și O.N. Kolokolcikova [89] reprezintă unul dintre cele mai recente ghiduri științifico-practice, destinat angajaților subdiviziunilor specializate în domeniul prevenirii și combaterii criminalității informatice, din cadrul organelor de drept din Federația Rusă. Acești autori analizează informația ca element de bază în descoperirea infracțiunilor informatice, descriu caracteristica criminalistică a acestor infracțiuni, efectuează un studiu aparte privind infracțiunile săvârșite în rețelele de comunicații electronice. Un element important al lucrării îl constituie descrierea modului de descoperire a infracțiunilor săvârșite prin utilizarea virușilor electronici și acumularea probatoriului pe aceste cauze. Totodată, au fost relevate particularitățile cooperării dintre organul de urmărire penală și organul care efectuează activitatea specială de investigații în cadrul înfăptuirii acțiunilor de urmărire penală, inclusiv a măsurilor speciale de investigații.

În recenta monografie a colectivului de autori, alcătuit din I.G. Smirnova, C.N. Evdokimov, O.A. Eghereva și alții, intitulată *Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ* [90] și consacrată descrierii fenomenului de criminalitate cibernetică, sunt analizate problemele de ordin legislativ, procesual-penal și criminalistic în combaterea acestor infracțiuni, precum și soluțiile pentru depășirea acestora. Dintre aspectele de ordin criminalistic, în lucrare sunt menționate: caracterul preponderent organizat al acestor infracțiuni; necesitatea dezvoltării metodelor netradiționale în activitatea organelor de urmărire penală și a organelor care efectuează activitatea specială de investigații; oportunitatea creării structurilor specializate în cercetarea criminalității cibernetice.

Astfel, acești autori au elaborat bazele metodologice ale cercetării infracțiunilor cibernetice, inclusiv în vederea asigurării securității informatice, au analizat aspectele organizatorice și normative în cadrul cooperării internaționale în acest domeniu, au efectuat o analiză criminologică a acestui fenomen (noțiunea, dinamica infracțiunilor, structura și motivele acesteia, măsurile de prevenire), precum și una juridico-penală, în care sunt reflectate elementele componente ale

infracțiunii. O atenție deosebită a fost acordată cercetării criminalistice și procesual-penale, fiind relevate caracteristicile criminalistice și particularitățile investigației criminalității cibernetice, în baza modelului examinării fraudelor informatice, dar și a activității speciale de investigații.

Autorul rus S.V. Propastin, în una din lucrările sale, intitulată *Тактика допроса по делам о неправомерном доступе к компьютерной информации* [91], a analizat practica organelor de drept cu privire la particularitățile tactice de audiere în cauzele cu privire la accesul neautorizat la informația computerizată, realizând un studiu al materialelor cauzelor penale din domeniul respectiv și identificând scopurile și sarcinile studierii persoanei audiate, alegerea și pregătirea locului audierii, stabilirea cercului de participanți la audiere, alegerea și pregătirea mijloacelor tehnice, elaborarea planului audierii, constatarea obiectului audierii, efectuarea nemijlocită a audierii, fixarea mersului, conținutului și a rezultatelor acestei acțiuni de urmărire penală.

Una dintre cele mai recente lucrări științifice, publicate în Federația Rusă, care abordează aspectele criminologice și criminalistice ale infracțiunilor informatice, este manualul *Криминалистика. 4-е издание, переработанное и дополненное*, elaborat de T.V. Averianova, R.S. Belkin, I.G. Koruhov și E.R. Rosinskaia [92]. În funcție de motivația infractorului, au fost stabilite următoarele tipuri de infractori informatici: tipul materialist, tipul motivat ideologic și tipul investigator. În lucrare sunt prezentate statisticile cu privire la proporționalitatea numărului de infractori informatici, precum și cele referitoare la victime, delimitate după sex și calitate. Totodată, sunt relevate cele trei situații tipice care pot apărea la cercetarea infracțiunilor informatice. Autorii pledează pentru implementarea modelării electronice criminalistice, deoarece aceasta permite depășirea problemelor legate de analiza criminalistică a unui obiect complex sau voluminos.

M.V. Savelieva și A.B. Smușkin, în manualul *Криминалистика: учебное пособие* [93], susțin că, în cercetarea infracțiunilor informatice, în cadrul acțiunilor de urmărire penală urmează a fi ridicate toate dispozitivele și mijloacele tehnice, destinate pentru conectarea la rețele informatice. Totodată, trebuie ridicate toate suporturile de stocare a informației electronice (flash-urile USB, discurile magnetice, discurile optice etc.), întrucât pe ele pot fi stocate produsele program sau părțile componente ale acestora, pregătite pentru comiterea infracțiunii. Potrivit autorilor în cauză, informația electronică poate fi ridicată atât împreună cu suportul de stocare a datelor electronice, cât și fără acesta.

Referitor la aspectele juridico-penale (semnele și elementele componenței de infracțiune, calificarea infracțiunii) privind infracțiunile informatice s-au expus mai mulți cercetători ruși în diverse manuale și monografii, cum ar fi: N.G. Kadnikova, în *Комментарий к Уголовному кодексу Российской Федерации (постатейный)* [94], V.M. Lebedeva, în *Комментарий к*

Уголовному кодексу Российской Федерации [95], N.A. Ovcinnikova, în *Комментарий к Уголовному Кодексу РФ: расширенний уголовно-правовой анализ с материалами судебно-следственной практике* [96], S.I. Uleziko, în *Комментарий к Уголовному кодексу Российской Федерации с постатейными материалами и судебной практикой* [97], A.A. Vitviţkii, în *Уголовное право. Особенная часть* [98], A.I. Ciuceaeva, în *Новое в Уголовном кодексе* [99], T.I. Vaulina, în *Уголовное право. Особенная часть: учебник для вузов* [100], I.Ă. Zvecearovskovo, în *Уголовное право России. Особенная часть* [101], I.V. Graciova și L.D. Ermakova, în *Комментарий к Уголовному кодексу Российской Федерации* [102], O.N. Korşunova, în *Курс криминалистики* [103], A.V. Naumov, în *Комментарий к Уголовному кодексу РФ* [104], I.I. Skuratova și V.M. Lebedeva, în *Комментарий к Уголовному кодексу Российской Федерации* [105], V.A. Mazurov, în *Компьютерные преступления: классификация и способы противодействия* [106], M.V. Bogomolov, în *Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации* [107], N. Sivițkaia, în *Признаки объективной стороны несанкционированного доступа к компьютерной нформации* [108], S. Kojenevskii, în *Методы гарантированного уничтожения данных на жестких магнитных дисках* [109], V. Losev, în *Преступления Против информационной безопасности* [110], A.I. Raroga, în *Уголовное Право Российской Федерации. Особенная Часть* [111], I.E. Kozacenko, Z.A. Neznamova și G.P. Novoselov, în *Уголовное право. Особенная часть* [112], Iu. Gulibin, în *Преступления в сфере компьютерной информации* [113], E.I.Panfilova și A.N. Popov, în *Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе*, R.I. Gadelișin și V.K. Kuznețov, în *Криминалистика: учебное пособие* [114] ș.a.

1.3. Instituțiile și instrumentele naționale, regionale și internaționale din domeniul prevenirii și combaterii criminalității informatice

Încă din anii ’70, în structura organelor de drept ale statelor dezvoltate au început a fi create subdiviziuni pentru combaterea infracțiunilor informatice [115, p. 173]. După cum a menționat expertul internațional în domeniul armonizării legislației cu privire la criminalitatea informatică Stein Schjolberg, spațiul cibernetic, în calitate de al cincilea spațiu comun, după cel terestru, acvatic, aerian și cosmic, necesită coordonare, cooperare și măsuri normative specifice la nivel internațional [116].

Criminalitatea informatică transfrontalieră a impus o evaluare efectivă a cooperării judiciare internaționale în domeniul vizat, nefiind suficientă, în acest sens, numai elaborarea unei legislații

adecvate la nivel intern, motiv pentru care se poate aprecia că abordarea strict legislativă a acestei probleme este insuficientă pentru stabilirea unor direcții de acțiune eficiente [117, p. 20].

Cooperarea internațională prevede utilizarea diferitor forme de interacțiune, ceea ce presupune colaborarea statelor în diverse direcții, inclusiv prin crearea organelor de combatere a criminalității informatice.

La 18 ianuarie 2013 în Haga a fost inaugurat Centrul European pentru Combaterea Criminalității Informatice (EC3) [118], având drept obiectiv acumularea și prelucrarea datelor referitoare la infracțiunile informatice, evaluarea pericolelor din internet, elaborarea și aplicarea metodelor avansate de profilaxie și investigare în domeniu, pregătirea cadrelor noi, precum și acordarea ajutorului necesar organelor de drept din UE [90, p. 28].

Agenția Europeană pentru Securitatea Rețelelor și a Informațiilor (ENISA) [119] este un centru de expertiză pentru securitatea informatică în Europa, cu sediul în Grecia. Agenția colaborează îndeaproape cu statele membre și cu sectorul privat, pentru a oferi consultanță și soluții. Printre acestea se numără: exercițiile de securitate informatică, dezvoltarea strategiilor naționale de securitate informatică, cooperarea și consolidarea capacităților, dar și studii privind adoptarea sigură a cloud-ului, abordarea problemelor legate de protecția datelor, tehnologiile de îmbunătățire a confidențialității datelor, elaborarea și punerea în aplicare a politicii și legislației UE în domeniu.

Comisia Europeană dezvoltă activ platforma de studiu privind cercetarea infracțiunilor informatice (European training platform on cybercrimeinvestigation) în cooperare cu statele membre UE, cu Europolul, cu universitățile și sectorul privat. Comisia acordă asistență Europolului și statelor membre UE în utilizarea platformei europene pentru criminalitatea informatică (European Cybercrime Platform), care include un sistem online de mesaje cu privire la această categorie de infracțiuni (Internet Crime Reporting Online System), fișierul analitic „Cyborg" (Analysis Work File Cyborg), care este utilizat în combaterea grupărilor criminale ce acționează în internet, Forumul experților judiciari în domeniul respectiv (Internet and Forensic Expert Forum) [90, p. 28].

Complexul Global de Inovare INTERPOL (IGCI) din Singapore are misiunea de coordonare în detectarea și prevenirea infracțiunilor digitale. Și-a început activitatea în anul 2014 și utilizează la nivel mondial experiența informatică a organelor de drept și a partenerilor importanți din sectorul privat [120].

Țările dezvoltate ale lumii își creează sau își extind, în cadrul forțelor armate și serviciilor speciale, subdiviziuni care urmează să asigure posibilitățile de avansare în spațiul cibernetic [90, p. 25]. Astfel, în SUA, pe lângă Centrul Național de Securitate Cibernetică (National Cyber

Security Centre) din componența forțelor armate americane, este formată Comenduirea cibernetică unificată (Unified U.S. Cyber Command), care trebuie să fie capabilă a coordona pe plan global eforturile tuturor structurilor Pentagonului în cadrul desfășurării activităților militare, a oferi suport instituțiilor federale civile, precum și a coopera cu organizații similare din alte state [121, p. 26].

Anterior, în SUA a fost creat Centrul de Alertă din Statele Unite cu privire la Fraudele din Internet (http://www.ifraudalert.org), care recepționa rapoartele referitoare la sustragerea datelor cardurilor bancare, cooperând activ cu organele de drept și cu sectorul privat, reprezentat de ISP și instituțiile financiar-bancare [122, p. 129].

În mod similar EC3, în cadrul Biroului Federal de Investigații din SUA, activează, din anul 2000, Centrul IC3 [123], fiind cunoscut anterior, până-n anul 2003, sub denumirea de Centrul de plângeri împotriva fraudei pe internet și având misiunea de a recepționa rapoartele privind criminalitatea informatică,

În Australia a fost creat un grup de coordonare a securității poștei electronice (ESCG), sarcina de bază a acesteia reprezentând crearea unui spațiu virtual operativ securizat, atât pentru sectorul public, cât și pentru cel privat [104, p. 84].

În anul 2001, în structura Ministerului de Interne al Federației Ruse a fost creată Direcția „K" [89, p. 8, 76, p. 127-128]. Obiectivele prioritare ale acestei subdiviziuni sunt: combaterea pornografiei infantile, combaterea accesului neautorizat la informația computerizată, a producerii și utilizării produselor program malițioase, a încălcării dreptului de autor și a drepturilor conexe în domeniul IT, a infracțiunilor în sistemul de plată electronică și al serviciilor bancare la distanță, a escrocheriilor în rețeaua internet, a infracțiunilor în rețelele publice de comunicații, a procurării ilegale a mijloacelor tehnice pentru obținerea ascunsă a informației.

Trebuie menționată practica pozitivă a Chinei, unde, în vederea combaterii criminalității informatice, sunt create grupuri operative specializate a „poliției cibernetice".

În România expertizele criminalistice în domeniul informatic le efectuează următoarele instituții: Institutul de Criminalistică din cadrul IGP [124, p. 527], Institutul Național de Expertize Criminalistice din cadrul Ministerului Justiției și Institutul pentru Tehnologii Avansate din cadrul Serviciului Român de Informații [26, p. 164].

Serviciul de combatere a criminalității informatice din cadrul Secției de combatere a infracțiunilor de terorism și a criminalității informatice a Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism din România [125, p. 3] este instituția de bază din statul vecin, competentă să cerceteze cazurile de criminalitate informatică.

O structură corespunzătoare există și în cadrul Direcției de Combatere a Criminalității Organizate (subdiviziune specializată a Inspectoratului General al Poliției Române). Astfel, Direcția respectivă include Serviciul de combatere a criminalității informatice [126], care desfășoară activități investigative și de cercetare penală pentru combaterea infracțiunilor informatice cu mijloace de plată electronice, a infracțiunilor contra confidențialității și integrității datelor, a celor privind sistemele informatice și pornografie infantilă. La rândul său, Serviciul are în subordine două birouri [127, p. 1]: Biroul de combatere a infracțiunilor informatice și a celor cu mijloace de plată electronică și Biroul de investigare și cercetare a sistemelor informatice.

În RM experții judiciari, autorizați pentru efectuarea expertizei informaționale a tehnicii de calcul, activează în cadrul [128]: Centrului tehnico-criminalistic și expertize judiciare al IGP al MAI, al CNA, al Centrului Național de Expertize Judiciare de pe lângă Ministerul Justiției [129, p. 197].

Competența cercetării infracțiunilor informatice în țara noastră aparține organului de urmărire penală al MAI, în raza de activitate a căruia a fost săvârșită sau a fost descoperită infracțiunea, ori se află bănuitul, învinuitul sau majoritatea martorilor. Totuși, potrivit art.270^2 din CPP, în cazul infracțiunilor prevăzute la art. 259–261^1 CP (Infracțiunile informatice și din domeniul telecomunicațiilor), dacă valoarea prejudiciului cauzat prin infracțiune depășește valoarea de 50000 de unități convenționale, cercetarea acestora ține de competența Procuraturii pentru Combaterea Criminalității Organizate și Cauze Speciale. Totodată, această procuratură specializată conduce urmărirea penală în cauzele în care urmărirea penală este efectuată de către organul de urmărire penală al Centrului pentru combaterea crimelor informatice din cadrul INI al IGP al MAI.

În anul 2010 în cadrul PG a fost creată o subdiviziune specializată, în baza Hotărârii Parlamentului RM privind aprobarea structurii PG nr.77 din 04.05.2010, denumită Secția tehnologii informaționale și investigații ale infracțiunilor în domeniul informaticii. Ulterior, în temeiul Ordinului Procurorului General interimar din 31.05.2016 nr.587 privind reorganizarea și stabilirea structurii interne a PG, în cadrul Direcției urmărire penală și criminalistică a fost creată Secția tehnologii informaționale și combatere a crimelor cibernetice, care: generalizează și contribuie la unificarea practicii în domeniul cercetării cazurilor de criminalitate informatică; acordă ajutor practic și metodologic în domeniu; organizează, coordonează și controlează activitatea procurorilor; prezintă propuneri privind perfecționarea legislației și a actelor normative în domeniu; la decizia Procurorului General, conduce și exercită urmărirea penală, reprezintă învinuirea în instanță în cauze de criminalitate informatică; monitorizează executarea sau, după

caz, execută comisiile rogatorii în cazurile de criminalitate informatică; asigură colaborarea internațională în domeniul prevenirii și combaterii criminalității informatice.

Comunitatea internațională a elaborat acte la diferite nivele, care reglementează cooperarea statelor și organizațiilor în combaterea criminalității informatice.

Atât pentru UE, cât și pentru majoritatea statelor lumii, o importanță principială o are Convenția CE privind criminalitatea informatică, care a fost adoptată de către CE la 23 noiembrie 2001 în Budapesta [130]. Aceasta a fost ratificată de 53 de state – membre ale UE, precum și de Canada, SUA și Japonia. RM a ratificat Convenția respectivă la 02 februarie 2009, prin Legea nr.6 [131]. Convenția prevede măsuri atât la nivel de stat-parte, cât și la nivel internațional.

În Convenție au fost concretizate eforturile comunității internaționale de a stabili faptele care trebuie să fie incriminate în legislațiile naționale, normele procedurale aplicabile în domeniul criminalității informatice și mijloacele de cooperare internațională rapidă, care sunt impuse de specificul infracțiunilor săvârșite prin intermediul sistemelor informatice [132, p. 102].

Art. 23 din Convenție stabilește obligația pentru statele-părți de a colabora în cea mai mare măsură posibilă. În plus, constată faptul că ea nu se aplică numai în cadrul cercetării infracțiunilor informatice, dar și în orice investigare unde trebuie să fie colectate probe în format electronic.

Pentru a eficientiza realizarea investigărilor internaționale, a comunicării dintre state, Convenția a subliniat importanța utilizării mijloacelor rapide de comunicare și a obligat părțile să desemneze puncte de contact 24/7, care să fie disponibile fără limită de timp. Ideea unei asemenea rețele a punctelor de contact se bazează pe rețeaua similară din cadrul Grupului G8 [26, p. 352, 357].

Începând cu anul 2010, autoritățile naționale au elaborat mai multe proiecte de ajustare a legislației RM la rigorile Convenției privind criminalitatea informatică. În prezent, este supus examinării în Parlament controversatul proiect de lege pentru modificarea și completarea unor acte legislative (Legea privind Serviciul de Informații și Securitate al RM – art.7; Codul penal – art.178, 2081, 259, ș.a.: ș.a.) [133], numit în societatea civilă „Legea Big Brother”. Proiectul în cauză a fost supus unor dezbateri publice intensive, fiind și expertizat de către diverși experți internaționali, inclusiv de către Comisia de la Veneția [134]. Deși, în linii mari, proiectul de lege este oportun, totuși constatăm multiple neajunsuri, care urmează a fi înlăturate la aprobarea finală a acestuia.

Astfel, este necesară revizuirea prevederilor ce reglementează procedura de „percheziție a sistemelor informatice”, încât să nu se creeze impedimente nejustificate organului de urmărire penală, legate de persoanele prezente la acțiune, de timpul și durata efectuării acesteia, de

posibilitatea copierii informației volatile (de exemplu, memoria RAM), de aplicabilitatea art.125 alin.(4) CPP etc.

„Interceptarea informatică", propusă în proiect în calitate de o nouă măsură specială de investigații, este dublată de altă măsură prevăzută de art.134^1 CPP – „Monitorizarea conexiunilor comunicațiilor telegrafice și electronice", care permite colectarea în timp real a datelor referitoare la traficul informatic și a datelor referitoare la conținut. Din aceste motive se impune racordarea conținutului art.134^1 CPP la denumirea acestuia, astfel încât să reglementeze doar ridicarea datelor referitoare la traficul informatic. Totodată, având în vedere practica anterioară negativă a RM cu privire la interceptările comunicărilor telefonice, în cazul interceptării informatice, legiuitorul trebuie să țină cont de obiecțiile CtEDO (cauza Iordachi contra RM).

Referitor la obligația ISP de a conserva tot traficul informatic și la procedura de sancționare, propusă în proiect, pentru neexecutarea acesteia, este de menționat că, la 08.04.2014, Curtea de Justiție a UE a emis Hotărârea în cauzele conexate C-293/12 și C-594/12 – Digital Rights Ireland și Seitlinger și alții, prin care declară nevalidă Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15.03.2006 privind prelucrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețelele de comunicații publice, din care motiv decade obligația ISP de a păstra, pentru anumite perioade de timp, datele referitoare la traficul de informații.

Totodată, urmează a fi revăzută sau exclusă măsura de sistare a accesului la adresa IP, care poate fi, de cele mai multe ori, disproporțională și chiar abuzivă, deoarece pe o singură adresă IP pot fi câteva zeci sau sute de site-uri, ba chiar și mai multe, aparținând unei sau mai multor persoane. Pe un site poate exista un număr nelimitat de pagini web. În cazul în care doar una din paginile web conține material interzis de lege și se dispune sistarea adresei IP, pe care este amplasată această pagină web, atunci vor fi sistate, concomitent, toate paginile web, dar și toate site-urile care se află pe serverul cu aceeași adresă IP, care ar putea să nu aibă nici o legătură cu pagina web ce conține material interzis. Blocarea site-urilor web prin intermediul ISP constituie o măsură de cenzură a conținutului online, măsură ce ridică probleme serioase în ceea ce privește respectarea drepturilor omului, în general, și a dreptului la liberă exprimare, în particular.

În concluzie, menționăm necesitatea revizuirii proiectului în ansamblu, inclusiv prin instituirea unui control efectiv din partea procurorului și judecătorului de instrucție asupra măsurilor și procedurilor noi propuse în acest proiect de lege.

Având în vedere că în spațiul cibernetic pot activa grupuri criminale, este aplicabilă, tangențial, Convenția Națiunilor Unite împotriva criminalității transnaționale organizate [135] semnată la Palermo în anul 2000 și ratificată de RM la 17 februarie 2005 [136]. Este unul din

instrumentele juridice valoroase, la care a aderat RM și pe care îl aplică în relațiile cu diverse state cu care nu are încheiate până în prezent tratate bilaterale și care nici nu sunt părți la Convenția din 2001, mai ales în cazul infracțiunilor de criminalitate informatică. Convenția Națiunilor Unite din 2000 cuprinde dispoziții referitoare atât la asistența internațională în materie penală, care se poate realiza între statele părți la Convenție, atâta timp cât acestea nu dispun de un alt instrument juridic, aplicabil în această materie, când infracțiunea este comisă de un grup criminal organizat, precum și la modalitatea de transmitere sau primire a cererilor prin mijloace de comunicare rapidă, ca regulă generală, prin poștă, și de foarte puține ori, prin canalele diplomatice [27, p. 108-109].

Un alt tratat aplicabil cooperării juridice internaționale este Convenția Europeană de asistență juridică în materie penală [137], semnată la Strasbourg în anul 1959 și ratificată de RM la 26.09.1997 [138]. Potrivit acesteia, canalele de comunicare trebuie, în principiu, să treacă prin intermediul Ministerelor de Justiție ale părților, totuși, conform art. 15 alin.(2), în caz de urgență, comisiile rogatorii vor putea fi adresate de autoritățile judiciare ale părții solicitante direct autorităților judiciare ale părții solicitate. O altă modalitate este reprezentată de canalele polițienești, cum ar fi Interpolul [26, p. 360]. Totuși, prin regulile sale, Convenția din 1959 nu corespunde cerințelor de celeritate, impuse de natura infracțiunilor informatice, tocmai prin termenele foarte extinse, care sunt prevăzute în cazul mijloacelor clasice de comunicare a unor asemenea cereri de asistență judiciară, precum și prin transmiterea răspunsului la cererile considerate urgente într-un termen de aproximativ câteva luni de zile [27, p. 106-107].

În cadrul celei de a șaptea Adunări Plenare Interparlamentare a statelor-membre CSI din 17.02.1996, a fost adoptat modelul CP al statelor-membre CSI, în capitolul 30 al căruia, intitulat „Infracțiunile împotriva securității informaționale”, au fost prevăzute 7 categorii de infracțiuni distincte, iar în alte capitole – infracțiuni în cadrul cărora sistemele și datele informatice constituie obiect sau instrument al infracțiunii [139].

La 18.10.1996 a fost adoptată Decizia Consiliului Șefilor de State CSI cu privire la Conceptul formării spațiului informațional al CSI cu privire la coordonarea activității de contracarare a infracțiunilor în domeniul IT și comunicațiilor.

Unul din tratatele multilaterale cu aplicabilitate regională este Acordul privind colaborarea statelor-membre ale CSI în lupta cu infracțiunile în domeniul informației computerizate, adoptat și încheiat la Minsk la 01.06.2001 și semnat de către RM la aceeași dată [140].

În acest acord sunt prevăzute faptele infracționale care urmează a fi prevăzute în legislațiile naționale ale statelor-membre, precum și următoarele forme de cooperare la prevenirea infracțiunilor din domeniul dat, cum ar fi: schimbul de informații despre formele și metodele de prevenție; planificarea și realizarea măsurilor coordonate și a operațiunilor de prevenire a

criminalității în domeniul informației computerizate; cooperarea în domeniul pregătirii profesionale și al instruirii cadrelor, inclusiv prin intermediul desfășurării activității de stagiu a specialiștilor, organizarea conferințelor, a seminarelor și cursurilor de instruire; crearea sistemelor informaționale, care să asigure sarcinile de prevenire a infracțiunilor în domeniu; realizarea unor cercetări științifice comune în domeniul vizat privind problemele de interes comun; schimbul de acte normative, literaturii tehnico-științifice în domeniul combaterii criminalității informatice ș.a. [79, p. 14-15]

În corespundere cu Programul interstatal privind măsurile comune de combatere a criminalității pentru anii 2011-2013, cooperarea Ministerelor de Interne ale statelor-membre CSI în sfera respectivă este orientată spre: combaterea infracțiunilor săvârșite cu utilizarea IT; prevenirea infracțiunilor legate de răspândirea materialelor pornografice în rețelele informatice și de comunicații electronice; întreprinderea măsurilor organizatorico-tehnice cu privire la crearea și utilizarea efectivă a sistemelor informatice moderne, pentru schimbul de informații dintre organele de drept ale statelor-membre CSI ș.a. [141].

În sfârșit, dar nu și în ultimul rând, trebuie menționată importanța cooperării dintre autoritățile de aplicare a legii și ISP [142, p. 4-8].

1.4. Concluzii la Capitolul 1

1. În vederea realizării scopului științific propus, s-a purces la o antrenare a unui număr impresionant de studii și elaborări științifice, care abordează subiecte directe, referitoare la metodica de cercetare a infracțiunilor din domeniul informaticii (inclusiv cu privire la noțiunea și clasificarea infracțiunilor date, modelul și caracteristica criminalistică, situațiile tipice și versiunile criminalistice, particularitățile tactice de efectuare a acțiunilor de urmărire penală și a măsurilor speciale de investigații în vederea descoperirii acestui gen de infracțiuni).

O atenție deosebită a fost acordată analizei lucrărilor autorilor din RM, România, Federația Rusă și SUA, elaborate de către cadrele didactico-științifice din diferite instituții de învățământ superior și de către alți cercetători în domeniu, care au servit drept surse de documentare și suport științifico-teoretic în elucidarea unor subiecte tratate în prezentul studiu.

2. În literatura de specialitate autohtonă, spre deosebire de cea din alte state, metodica cercetării infracțiunilor din domeniul informaticii este abordată în linii mari, din care motiv se impune o necesitate stringentă de a efectua studii aprofundate în problema vizată. Analiza recomandărilor științei criminalistice și a specificului legislației regionale și naționale a contribuit la realizarea primului studiu științific aprofundat din acest domeniu în RM.

3. Dat fiind faptul că spațiul cibernetic reprezintă cel de-al cincilea spațiu comun, după cel terestru, acvatic, aerian și cosmic, investigarea criminalității informatice necesită coordonare, cooperare și măsuri normative specifice la nivel internațional (inclusiv referitoare la colaborarea operativă și crearea organelor regionale de combatere), întrucât doar elaborarea unei legislații adecvate la nivel intern este, în acest sens, insuficientă.

2. CARACTERISTICA CRIMINALISTICĂ ȘI ORGANIZAREA CERCETĂRII INFRACȚIUNILOR DIN DOMENIUL INFORMATICII

2.1. Noțiunea de infracțiune informatică și criminalitate informatică. Clasificarea infracțiunilor informatice.

Definiția infracțiunilor și a criminalității informatice

Autorii autohtoni S. Brânză și V. Stati definesc infracțiunile informatice drept fapte socialmente periculoase, săvârșite cu intenție sau din imprudență, care aduc atingere, prin excelență, relațiilor sociale din domeniul informaticii și al telecomunicațiilor, răspunderea penală pentru care se stabilește la art.259-261[1] CP [34, p. 345].

În CP a fost inclus un capitol separat, dedicat incriminării infracțiunilor în domeniu, și anume Capitolul XI din Partea Specială „Infracțiuni informatice și infracțiuni în domeniul telecomunicațiilor". Totodată, este de menționat faptul că noțiunea de „telecomunicații" este una desuetă, fiind definită anterior în art.2 din Legea telecomunicații [143], care a fost abrogată în anul 2008. De aceea este necesară înlocuirea acestui termen cu expresia „comunicații electronice".

Deși pare a fi o chestiune simplă, noțiunea de *criminalitate informatică* încă mai trezește numeroase discuții controversate. Într-o primă accepție, criminalitatea informatică este definită drept un ansamblu de infracțiuni, al căror obiect este informația computerizată [144, p. 9]. Potrivit art.3 din Legea nr.467 din 21.11.2003 cu privire la informatizare și la resursele informaționale de stat [145] și pct.1 din Hotărârea Guvernului cu privire la Pagina oficială a Guvernului RM în rețeaua Internet nr.1464 din 24.12.2007 [146], *informația* reprezintă cunoștințele despre persoane, subiecte, fapte, evenimente, fenomene, procese, obiecte, situații și idei.

A doua interpretare prezintă criminalitatea informatică ca pe un ansamblu de infracțiuni, săvârșite pe un anumit teritoriu într-o anumită perioadă de timp, atentând la acumularea, prelucrarea, stocarea și distribuirea informației computerizate, precum și infracțiunile săvârșite prin utilizarea sistemelor informatice în vederea obținerii unui beneficiu material sau de altă natură [64, p. 39].

Dintr-o a treia perspectivă, criminalitatea informatică reprezintă ansamblul tuturor infracțiunilor în domeniul IT [59, p. 45, 147], într-o anumită perioadă de timp și pe un teritoriu bine determinat [11, p. 13].

A patra accepție caracterizează criminalitatea informatică drept totalitatea infracțiunilor în care calculatorul sau rețeaua de calculatoare este obiectul infracțiunii, sau în care calculatorul sau rețeaua de calculatoare reprezintă instrumentul sau mijlocul de înfăptuire a infracțiunii [55, p. 18]. Se pare că această interpretare este acceptată de mai mulți savanți români [148, p. 26, 24, p. 396],

precum și de către autoritățile române [149, p. 51]. Concepția respectivă o atestăm și în Recomandarea CE nr. R (89) 9 [150, p. 13]. Totuși, potrivit autorilor ruși V.I. Aleskerov și F.A. Kuț [82, p. 12], interpretarea în cauză este admisibilă din punct de vedere criminalistic, dar nu și din perspectiva dreptului penal, deoarece ar putea crea dificultăți la calificarea infracțiunii.

Autorul M. Cross [66, p. 9] prezintă criminalitatea informatică într-o accepție ce include toate infracțiunile săvârșite în domeniul informației computerizate prin intermediul dispozitivelor și rețelelor de comunicații electronice (*rețeaua informatică* reprezintă un ansamblu de noduri de prelucrare a datelor interconectate în scopul transportului de date [151]) și IT [152, p. 7].

Unii autori, ca S. Smith [53], I.G. Smirnova, C.N. Evdokimov, O.A. Eghereva și alții [90, p. 51], propun examinarea conceptului în cauză sub două aspecte – atât în sens larg, cât și în sens îngust. Având în vedere multitudinea de opinii cu privire la criminalitatea informatică, precum și prevederile Convenției privind criminalitatea informatică considerăm potrivită abordarea respectivă.

În această ordine de idei, precizăm că criminalitatea informatică, în *sens îngust*, reprezintă totalitatea infracțiunilor săvârșite pe un anumit teritoriu într-o anumită perioadă de timp, ce afectează relațiile sociale în domeniul informaticii și al comunicațiilor electronice, precum și securitatea statului, a minorului, a proprietății intelectuale și drepturilor conexe, inviolabilitatea vieții private, a secretului corespondenței electronice, a autenticității instrumentelor de plată, comise cu utilizarea sistemelor informatice, răspunderea penală pentru care se stabilește la art.177, 178, 185^1-185^3, 208^1, 237, 259-261^1 și 346 CP.

În *sens larg* însă, criminalitatea informatică include ansamblul infracțiunilor săvârșite pe un anumit teritoriu într-o anumită perioadă, ce afectează relațiile sociale în domeniul informaticii și comunicațiilor electronice, securitatea statului, a minorului, a proprietății intelectuale și drepturilor conexe, inviolabilitatea vieții private, a secretului corespondenței electronice, a autenticității instrumentelor de plată, precum și alte raporturi juridice, în care datele, sistemele și rețelele informatice, serviciile și rețelele de comunicații electronice reprezintă nu doar obiectul faptei prejudiciabile, dar sunt utilizate în calitate de mijloace și instrumente de săvârșire a infracțiunii.

Clasificarea infracțiunilor informatice

În anul 1994 Organizația Națiunilor Unite a elaborat un *Manual* care tratează problema prevenirii infracțiunilor informatice, printre cele mai frecvent invocate fiind următoarele infracțiuni informatice [153, p. 8]:

1) frauda prin manipularea calculatorului;
2) falsul informatic;

3) alterarea sau modificarea datelor sau a produselor program (*Produsul program* reprezintă o listă de instrucțiuni, scrisă într-un limbaj de programare, într-o anumită secvență, care spune calculatorului ce trebuie să facă [151]. Aceste programe se clasifică în: a) sisteme de operare – grupuri de programe care permit folosirea calculatorului; b) aplicații – programele care execută instrucțiunile utilizatorului și cele incorporate în hardware [154]);
4) accesul neautorizat la sisteme informatice (*Sistemul informatic* reprezintă un ansamblu de programe și echipamente, care asigură prelucrarea automată a datelor [151]. În accepția Convenției CE privind criminalitatea informatică [130], precum și a Legii privind prevenirea și combaterea criminalității informatice [155], expresia *sistem informatic* desemnează orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în conexiune, unul sau mai multe elemente ale căruia asigură prelucrarea automată a datelor) și servicii informatice prin executarea unui program;
5) reproducerea neautorizată a programelor informatice protejate de lege.

Convenția CE cu privire la criminalitatea informatică clasifică infracțiunile informatice, după cum urmează [130]:

1) Infracțiuni împotriva confidențialității, integrității și disponibilității datelor și sistemelor informatice: accesarea ilegală, interceptarea ilegală, afectarea integrității datelor, afectarea integrității sistemului, abuzurile asupra dispozitivelor;
2) Infracțiuni informatice: falsificarea informatică, frauda informatică;
3) Infracțiuni referitoare la conținut: pornografia infantilă;
4) Infracțiuni referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe;
5) Infracțiuni de natură rasistă și xenofobă [156]: distribuirea materialelor rasiste și xenofobe prin intermediul sistemelor informatice, amenințarea bazată pe o motivație rasistă și xenofobă, insulta având ca temei o motivație rasistă și xenofobă, negarea, discriminarea grosolană, aprobarea sau justificarea genocidului ori a infracțiunilor împotriva umanității.

Uniunea Internațională a Telecomunicațiilor a constatat că clasificarea elaborată de către CE nu este completă și consecventă, deoarece ea nu se bazează pe un criteriu unic pentru diferențierea acestor categorii de infracțiuni, propunând, în „Understanding Cybercrime: A Guide For Developing Countries", o altă clasificare a infracțiunilor informatice [26, p. 29]:

1) *Infracțiuni împotriva confidențialității, integrității și disponibilității datelor și sistemelor informatice*: accesul ilegal, spionajul datelor, interceptarea ilegală, afectarea integrității datelor, afectarea integrității sistemului;

2) *Infracțiuni referitoare la conținut*: materiale erotice și pornografice, pornografia infantilă, rasismul, incitarea la ură prin discurs, promovarea violenței, infracțiuni privitoare la religie, jocurile de noroc ilegale on-line, defăimarea și informațiile false, spam-ul și amenințările în legătură cu spamul (mesaj electronic nesolicitat expediat într-o cantitate mare [26, p. 146]), alte forme de conținut ilegal;
3) *Infracțiuni referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe, precum și infracțiunile referitoare la marca comercială;*
4) *Infracțiuni informatice*: frauda informatică, falsul informatic, furtul de identitate, abuzurile asupra dispozitivelor;
5) *Infracțiuni combinate*: terorismul cibernetic (cyberterrorism-ul), război cibernetic (cyberwarfare), spălarea de bani pe Internet, phishing-ul.

În viziunea autorilor ruși V.I. Aleskerov și O.N. Kolokolcikova [89, p. 29], toate infracțiunile din domeniul informatic pot fi divizate în două categorii mari:

- *Infracțiuni legate de accesul la activitatea sistemelor informatice*: accesul neautorizat la informația computerizată, elaborarea și răspândirea virușilor, introducerea virușilor în produsele program, încălcarea regulilor de exploatare a sistemelor și rețelelor informatice, furtul informației computerizate, distrugerea informației computerizate, falsificarea informației computerizate.
- *Infracțiuni săvârșite cu utilizarea sistemelor informatice* [82]:
  a) infracțiuni în rețelele de comunicații electronice prin fir, săvârșite față de operatorii de comunicație fixă (prin fir) prin influențarea mijloacelor tehnice ale operatorilor; arendarea numerelor și canalelor cu ulterioara neachitare a serviciilor; infracțiuni săvârșite cu utilizarea resurselor de comunicație prin fir, prin accesul neautorizat la stațiile de telefonie și generarea traficului;
  b) infracțiuni în rețele de comunicații electronice fără fir, săvârșite în privința operatorilor de comunicație mobilă (fără fir) prin utilizarea ilegală a canalelor de telefonie; inițierea traficului pe „numere scurte”; încheierea contractelor fictive cu privire la prestarea serviciilor de comunicații; infracțiuni săvârșite cu utilizarea mijloacelor de comunicație mobilă, concretizate în: fraude telefonice, câștig la loterie, SMS de la bancă, SMS de solicitare a ajutorului, SMS de la organele de drept [157], transferul eronat de mijloace, cod de la operator;
  c) infracțiuni în rețeaua Internet: răspândirea virușilor; fraude cu utilizarea rețelei Internet; activitatea ilegală de organizare și efectuare a jocurilor de noroc în rețeaua Internet; acces ilegal la serviciile de televiziune prin cablu și satelit.

În literatura românească de specialitate, la infracțiunile informatice mai sunt atribuite și faptele de efectuare a operațiunilor financiare în mod fraudulos, de acceptare a operațiunilor financiare efectuate în mod fraudulos, de spionaj industrial [158], de falsificare de titluri de credit sau instrumente de plată, de punere în circulație a unor valori falsificate, de deținere de instrumente în vederea falsificării de valori [33], precum și terorismul și războiul informatic [24, p. 397].

Având în vedere specificul legislației naționale, acordurile internaționale în domeniul vizat, la care RM este Parte, precum și definiția noțiunii de *criminalitate informatică* în sens larg, considerăm că infracțiunile informatice pot fi divizate în următoarele categorii:

1. Infracțiuni împotriva confidențialității, integrității și disponibilității datelor și sistemelor informatice:
    a) încălcarea inviolabilității vieții personale, săvârșită cu utilizarea sistemelor informatice (art.177 CP);
    b) violarea dreptului la secretul corespondenței electronice (art.178 CP);
    c) accesul ilegal la informația computerizată (art.259 CP);
    d) producerea, importul, comercializarea sau punerea ilegală la dispoziție a mijloacelor tehnice sau a produselor program, a parolelor, codurilor de acces sau a datelor similare (art.260 și 260^4 CP);
    e) interceptarea ilegală a unei transmisiuni de date informatice (art.260^1 CP);
    f) alterarea integrității datelor informatice dintr-un sistem informatic (art.260^2 CP);
    g) perturbarea funcționării sistemului informatic (260^3 CP);
    h) încălcarea regulilor de securitate a sistemului informatic (art.261 CP).
2. Infracțiuni informatice:
    a) falsul informatic (art.260^5 CP);
    b) frauda informatică (art.260^6 CP).
3. Infracțiuni referitoare la conținut: pornografia infantilă săvârșită cu utilizarea sistemelor informatice (art.208^1 CP);
4. Infracțiuni referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe, săvârșite cu utilizarea sistemelor informatice (art.185^1-185^3 CP);
5. Infracțiuni de natură rasistă și xenofobă: fapte orientate în mod intenționat spre aţâțarea vrajbei, discriminării sau dezbinării naționale, etnice, rasiale sau religioase, săvârșite cu utilizarea sistemelor informatice (art.346 CP);
6. Infracțiuni îndreptate împotriva autenticității instrumentelor de plată, săvârșite cu utilizarea sistemelor informatice (art.237 CP);

7. Alte infracțiuni, în care datele, sistemele și rețelele informatice, serviciile și rețelele de comunicații electronice sunt utilizate în calitate de mijloace și instrumente de săvârșire a infracțiunii.

În ceea ce privește statistica cauzelor penale, examinate pe teritoriul RM, constatăm că pe parcursul anilor 2003-2017 au fost înregistrate 1249 de cauze penale cu privire la cercetarea infracțiunilor informatice în sens restrâns, dintre care doar 157 sunt infracțiuni prevăzute de art.259-260^{6} CP. În Anexa nr. 1 din prezenta lucrare este propus un tabel ce reflectă numărul cauzelor penale pornite în această perioadă în țara noastră.

2.2. Modelul și caracteristica criminalistică ale infracțiunilor informatice

Cercetarea infracțiunilor informatice este deosebit de importantă, dată fiind preocuparea specială a legiuitorului pentru ocrotirea unor interese legitime ale proprietarilor și administratorilor de sisteme informatice, în legătură cu securitatea, inviolabilitatea acestora, garantarea confidențialității datelor, a integrității atât a datelor, cât și a sistemelor informatice [17, p. 388].

Au trecut timpurile în care doar hackerii erau profesioniști, având cunoștințe performante în ceea ce privește echipamentele informatice și săvârșind minuni cu ajutorul codurilor de program. Acum orice adolescent studios, curios, dar nu prea împovărat cu principii morale, este capabil de a crea utilizatorilor obișnuiți o mulțime de probleme.

Un intrus, pentru a avea acces la informații confidențiale, uneori nici nu are nevoie de competențe și abilități speciale. În multe cazuri, este suficient „suportul” oferit de factorul uman, care poate fi o bucată de hârtie, lipită pe monitor sau pusă sub sticlă lângă tastatură, în care să fie scrisă parola. Parolele, de obicei, nu se disting prin prea multă originalitate. Și în hățișurile Internetului întotdeauna poate fi găsit un program care își va asuma munca de rutină pentru decodificarea celor mai uzuale parole.

Prima încercare reușită de definire a termenului de „investigare informatică”, „investigare criminalistică informatică”, „investigare digitală”, „investigare criminalistică digitală” a fost realizată în perioada 7-8 august 2001, când la Utica s-a desfășurat primul Atelier de lucru anual având ca subiect cercetarea criminalistică digitală [24, p. 397]. Astfel conceptul de „criminalistică digitală” a fost definit ca reprezentând „utilizarea metodelor derivate și dovedite științific cu privire la conservarea, colectarea, validarea, identificarea, analiza, interpretarea, documentarea și prezentarea dovezilor digitale, provenite din surse digitale, în scopul facilitării sau continuării reconstrucției evenimentelor caracterizate ca fiind de natură penală sau pentru a ajuta anticiparea

acțiunilor neautorizate, identificate ca fiind perturbatoare pentru operațiunile planificate" [159, p. 16].

Orice infracțiune, ca fenomen social, reprezintă un anumit sistem de acțiuni ilicite și de consecințe ale acestora, interdependente și reciproc condiționate, care, de obicei, evoluează conform unor legi concrete. Pentru cunoaşterea obiectivă şi deplină a caracterului infracţiunii cercetate, este necesar a se stabili majoritatea elementelor care fac parte din modelul criminalistic al infracţiunilor de o anumită categorie [9, p. 45].

Noțiunea de *model* a apărut ca un *know-how* în criminalistică, fiind abordat – în mod serios și la nivel de concept – de către savantul autohton M. Gheorghiță, încă prin anii '90. Autorul a descris foarte argumentat și diferența dintre noțiunea de *caracteristică* și *model criminalistic* [9, p. 52].

Potrivit Dicționarului explicativ, *modelul* reprezintă un sistem teoretic, cu ajutorul căruia pot fi studiate indirect proprietățile și transformările altui sistem mai complex; schemă teoretică elaborată în diferite științe pentru a reprezenta elementele fundamentale ale unuia sau mai multor fenomene sau lucruri; șablon, prototip; reprezentare simplificată a unui sistem sau proces [160].

În viziunea cercetătorului M. Gheorghiță, modelul criminalistic al infracțiunilor presupune un sistem fundamentat științific de date (probe), interdependente și condiționate reciproc, despre cele mai tipice urme, însușiri, indicii și intermedieri ale actelor ilicite și infractorilor de o anumită categorie, care se manifestă în legitățile pregătirii, săvârșirii și tăinuirii infracțiunilor și care permit a face concluzii privind căile optime de cercetare și descoperire [10, p. 726].

Astfel, modelul criminalistic al infracțiunilor devine, după cum menționează mai mulți criminaliști, un „etalon", „clișeu", „matriță", care se suprapune pe caracteristica criminalistică a cauzei cercetate.

Modelul criminalistic poate fi utilizat pentru algoritmizarea procesului de cercetare și descoperire a categoriilor de infracțiuni și pentru determinarea caracteristicilor criminalistice ale infracțiunilor concrete.

Astfel, modelul criminalistic al infracțiunilor informatice reprezintă un ansamblu de informații sistematizate cu privire la specificul probelor digitale, la particularitățile infracțiunilor și infractorilor informatici, care se reflectă în cadrul pregătirii, săvârșirii și tăinuirii infracțiunilor informatice și care permit algoritmizarea procesului de cercetare și descoperire a acestor categorii de infracțiuni.

La rândul său, caracteristica criminalistică servește pentru constituirea, precizarea și completarea modelului criminalistic al unei anumite categorii de infracțiuni [10, p. 727].

Caracteristica criminalistică permite elaborarea și utilizarea eficientă a metodicii de cercetare a oricărei categorii de infracțiuni, inclusiv în domeniul informaticii și comunicațiilor electronice [84, p. 45, 7], precum și elaborarea versiunilor temeinice în privința circumstanțelor necunoscute [83, p. 30].

Caracteristica criminalistică presupune descrierea însuşirilor, proprietăţilor, semnelor distinctive ale unui fenomen, eveniment, obiect, ale unei persoane în cadrul cercetării cauzei penale concrete [9, p. 54], care reprezintă produsul activității ofițerului de urmărire penală și are menirea de a obține o imagine mai deplină și mai obiectivă despre actul infracțional depistat și despre persoanele care l-au comis [10, p. 728].

Autorii ruși E.N. Bâstreakov, A.N. Ivanov, V.A. Klimov interpretează caracteristica criminalistică a infracțiunilor informatice drept un sistem de date cu privire la elementele tipice ale acestor infracțiuni și ale legăturilor uniforme dintre acestea, semnificative pentru soluționarea sarcinilor ce stau în fața organului de urmărire penală [48, p. 7].

Caracteristica criminalistică a infracțiunilor informatice constituie un sistem vast de informații și concluzii științifice cu privire la urmele tipice, la modalitățile și mecanismul de săvârșire a infracțiunii, la personalitatea infractorului, la proprietățile și specificul infracțiunii, la obiectul faptei infracționale, circumstanțele comiterii infracțiunii, la particularitățile motivelor și scopurilor [73, p. 8], toate acestea asigurând optimizarea investigării și implementarea în practică a mijloacelor și metodelor criminalistice [161, p. 56], precum și înaintarea versiunilor criminalistice, identificarea direcțiilor de bază ale urmăririi penale în vederea adoptării unor decizii procesuale legale și întemeiate.

Anterior, în lucrarea „Modelul și caracteristica criminalistică ale infracțiunilor informatice și din domeniul telecomunicațiilor” [162, p. 248], am ajuns la concluzia că, printre cele mai relevante semne caracteristice ale infracțiunilor informatice, pot fi relevate următoarele:

- criminalitatea informatică este o categorie distinctă a criminalității;
- este într-o conexiune strânsă cu alte genuri de infracțiuni, astfel încât cele informatice deseori sunt săvârșite în vederea înlesnirii altor categorii de infracțiuni (sustrageri, șantaj [163], spionaj, trădare de patrie, spălare de bani [164], ș.a.) [90, p. 69];
- poartă un caracter tehnologic avansat, având în vedere utilizarea IT, a rețelelor și sistemelor informatice, a purtătorilor de stocare a datelor informatice (*date informatice* constituie orice reprezentare de fapte, informații sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic [155]) ș.a., care constituie instrumente și mijloace de săvârșire a infracțiunilor informatice;

- se caracterizează printr-un nivel înalt de latență [80, p. 178, 79, p. 5, 22, p. 58, 87, p. 677], cauzat de diverși factori obiectivi (nedorința victimelor de a apela la organele de drept, caracterul ascuns față de majoritatea utilizatorilor, dificultatea constatării infracțiunilor respective din cauza numărului insuficient de specialiști din cadrul instituțiilor abilitate cu prevenirea și combaterea acestora). Infractorul digital se ascunde după tastatură și riscul de a fi descoperit este destul de mic [34, p. 342];
- denotă un caracter bine organizat și este strâns legată cu criminalitatea organizată (atacurile de DDoS, banking, phishing, botneturi, ș.a.) [79, p. 5]. Spre exemplu, fraudele informatice în sistemul de plată electronică sunt atât de complexe, încât este imposibil, practic, ca o singură persoană să săvârșească fapta respectivă din momentul elaborării produsului program în vederea comiterii infracțiunii și până la obținerea banilor, în *Anexa* nr. 2 fiind prezentat un model tipic de asemenea infracțiune. Specificul comiterii infracțiunilor informatice în participație constă în faptul că participanții nu se cunosc între ei, iar comunicarea, planificarea și coordonarea activității infracționale se efectuează doar prin intermediul rețelei internet [86, p. 42];
- este o criminalitate profesională, deoarece persoanele care săvârșesc aceste infracțiuni posedă o specializare infracțională, dețin cunoștințele necesare în domeniul IT, respectă anumite reguli și „legi”, utilizează o terminologie specifică. Spre exemplu, la achitarea serviciilor prestate de către membrii grupului criminal, nu se utilizează bani „murdari”, obținuți din infracțiune; înregistrarea conturilor bancare se face pe persoane interpuse; nu se utilizează mijloace de comunicare nesecurizate/necriptate (cum ar fi ICQ sau Skype); sunt folosite pseudonime în forumurile specializate; se practică utilizarea în grup a VPN-urilor, care asigură conexiunea securizată în rețea de tip tunel criptat, precum și mascarea adreselor IP (cea mai populară rețea anonimă este TOR - The Onion Routing sau cu ajutorul proxy serverelor). Reguli de acest gen sunt elaborate în baza experienței criminale, iar încălcarea lor facilitează, într-o anumită măsură, investigațiile organelor de drept [86, p. 69];
- are un caracter transfrontalier [47, p. 451, 27, p. 102-104, 22, p. 58], fără limite teritoriale, ceea ce îi permite infractorului de pe teritoriul unui stat să comită infracțiunea față de persoane din alte state;
- sunt transnaționale: infractorii, pentru a-și înlesni săvârșirea faptelor criminale pe teritoriul a două sau mai multe state, sunt impuși să-și unească eforturile cu grupări criminale internaționale.

- sunt cele mai dinamice în evoluție, fapt asigurat de permanenta perfecționare a noilor IT, de apariția unor noi participanți, de extinderea spațiului cibernetic [165, p. 9];
- are costuri reduse, în comparație cu profiturile ilegale care pot fi obținute [26, p. 45, 22, p. 59]. Spre exemplu, într-un comunicat al PG din RM a fost menționat faptul că organele de urmărire penală din RM, împreună cu autoritățile competente ale SUA, au efectuat o serie de acțiuni de urmărire penală, inclusiv măsuri speciale de investigații, în rezultatul cărora au fost identificați 5 cetățeni, care, începând cu anul 2011, comercializau prin rețeaua Internet un produs program, numit „Citadel", destinat infectării sistemelor informatice și colectării datelor despre conturile bancare și a datelor cu caracter personal. În felul acesta, procurorii au constatat că, prin acțiunile lor, suspecții au infectat peste 5 milioane de computere la nivel mondial, cauzând instituțiilor financiare din SUA și Europa daune materiale, estimate la suma de peste 10 milioane USD [166].
- și-a însușit semnele specifice criminalității economice, dat fiind că majoritatea infracțiunilor informatice sunt săvârșite în sectoarele bancar, financiar și corporativ;
- în ultimii ani, criminalitatea informatică își asumă și caracteristici politice [58, p. 497], dat fiind că reprezentanții serviciilor speciale, ai structurilor de forță din diverse state, organizațiile extremiste și teroriste angajează specialiști de înaltă calificare din domeniul IT [167];
- locul comiterii infracțiunii informatice, de regulă, nu coincide cu locul manifestării consecințelor [81, p. 38], întrucât infractorul nu este obligat să fie prezent la locul faptei [26, p. 45].

Până în prezent CSJ nu s-a expus referitor la aplicarea legislației în cazul infracțiunilor informatice în vederea asigurării unei practici judiciare unice.

Personalitatea infractorului, scopul și motivele infracțiunii informatice

O preocupare prioritară a criminologilor este identificarea cauzelor ce conduc la apariția comportamentului criminal. Până în prezent, analiza practicilor criminale au permis elaborarea și formularea unor teorii și concepții, care vin să explice geneza infracționalității, printre acestea fiind teoriile de orientare bioantropologică, psihologico-psihiatrică și teoriile de orientare sociologică [168, p. 100-134].

În acest sens, intervin discuțiile despre „profesionalizarea și „specializarea" infractorilor, ca efect al procesului de conectare rapidă a țării noastre la filierele criminalității internaționale, ceea ce a determinat un adevărat import de tehnologie infracțională modernă [169, p. 91-95].

Referitor la criminalitatea informatică, se impune necesitatea adaptării teoriilor existente specificului IT și spațiului virtual. În literatura de specialitate, întrucât conceptele criminologice existente privind criminalitatea tradițională sunt de o valoare relativă, când a demarat discuția despre o eventuală explicație a genezei criminalității informatice, au fost enunțate idei privind necesitatea formării unor teorii noi, aplicabile doar acestui tip de criminalitate [69], între care:

1. Teoria neutralizării digitale (Teoria devierii digitale). Această teorie a fost propusă, în 2015, de Goldsmith și Brewer, care au analizat, pentru prima dată, modul în care IT creează pentru diferiți indivizi noi oportunități de a se antrena în activitățile criminale din mediul online și offline. Accesul la internet și utilizarea acestuia se caracterizează prin faptul că indivizii sunt expuși unui spațiu virtual, în care aceștia sunt detașați de identitatea lor adevărată. Utilizatorii își pot crea online personalitatea pe care o doresc, iar anonimitatea de care beneficiază îi eliberează, la nivelul subconștientului, de simțul responsabilității și îi poate încuraja să săvârșească acțiuni pe care nu le-ar comite în lumea reală.

2. *Teoria tranziției spațiului.* Părintele acestei teorii este considerat K. Jaishankar [170], care a constatat că oamenii au un comportament diferit în mediul online față de cel din viața reală, teoria sa fiind întemeiată pe următoarele teze: persoanele care, din cauza statutului sau poziției pe care o au în societate, își reprimă dorința de a comite infracțiuni în lumea reală sunt predispuse să comită infracțiuni în mediul online; multitudinea identităților pe care le pot folosi, anonimitatea și lipsa atragerii la răspundere în mediul online reprezintă factori care motivează infractorii să comită infracțiuni informatice; comportamentul criminal al infractorilor în spațiul cibernetic poate fi transpus în spațiul fizic real și invers; acțiunile riscante comise periodic de infractori în spațiul online și caracterul dinamic, din punct de vedere temporal și spațial, al internetului le dau posibilitatea de a nu fi atrași la răspundere; specificul IT permite persoanelor necunoscute să se asocieze în spațiul cibernetic în vederea planificării și comiterii infracțiunilor în lumea reală, iar pentru partenerii din lumea fizică – să se grupeze pentru a săvârși infracțiuni în spațiul cibernetic; datorită regimurilor guvernamentale, este mare probabilitatea ca infracțiunile informatice să fie săvârșite mai degrabă de persoane care locuiesc în societăți închise, decât cele din societățile deschise; conflictul permanent dintre normele și valorile lumii reale și cele din spațiul virtual poate duce la creșterea criminalității informatice.

La descoperirea oricărei infracțiuni informatice un rol deosebit îl joacă și specificul psihologiei personalității infractorului [89, p. 10]. Astfel, se impune să ținem cont de sexul, vârsta, statutul social, situația familială și cea materială, de locul de trai, apartenența la o anumită cultură [72, p. 5]. Analiza aprofundată a acestei informații va permite stabilirea și restrângerea cercului de

suspecți, a motivelor infracțiunii, înaintarea versiunilor și identificarea acțiunilor procesuale, necesare descoperirii infracțiunii.

Interacțiunile digitale, difuzarea și utilizarea intensă a IT generează un șir întreg de modificări antropologice stabile la nivelul factorilor psihici, cognitivi și motivaționali. De fapt, infractorul digital este același infractor comun, descris și explicat prin prisma teoriilor criminologice clasice și contemporane, dar căruia îi sunt specifice noi trăsături de caracter și competențe social-profesionale, datorate evoluției societății spre o nouă eră, cea informațională. Astfel, nucleul central al personalității infractorului suportă anumite schimbări de natură calitativă, și nu neapărat cantitativă.

În aceste condiții, apar noi abilități în stilul comunicativ, dar, mai ales, în procesele de gândire, pentru care se solicită o flexibilitate și rapiditate tot mai mare în trecerea operativă de la dimensiunea reală la cea virtuală, de la o relație mediată de un spațiu emotiv-fizic la o relație mediată de un spațiu emotiv-artificial.

Mediul telematic contribuie la alterarea percepției infracțiunii din perspectiva făptuitorului, căruia îi este specifică incapacitatea sau capacitatea redusă de previzibilitate a caracterului ilegal al faptei sale sau, mai cu seamă, a efectelor prejudiciabile, induse prin propria sa acțiune/inacțiune. Cu atât mai mult, îi sunt caracteristice aceste trăsături infractorului digital, pentru care computerul constituie un „mediator” între el și victimă sau/și obiectul lezat. Interacțiunea la nivel digital cu aceleași obiecte și persoane nu este pe deplin conștientizată și impactul distructiv al faptei sale social-periculoase nu este totalmente conceput sau parțial realizat.

Cele mai alterate elemente, în acest sens, sunt percepția ilegalității comportamentului, estimarea riscurilor de a fi descoperit, de a fi denunțat, percepția daunei provocate victimei, posibilitatea de a fi sancționat social sau legal [6].

În literatura de specialitate, persoanele care comit infracțiuni informatice, de cele mai multe ori, sunt numite „hackeri” (persoane care cu ajutorul computerelor pătrund ilegal în sistemul victimei, în scopul de a explora, a se informa sau din simplă curiozitate [11, p. 59, 41]), „crackeri” (persoane care pătrund în sistemele informatice ale unei organizații, instituții, companii prin violarea sistemelor de securitate informatică [171, p. 3, 11, p. 60]), „pirați electronici”, „escroci”, „hoți”, „bandiți electronici”, „programatori obsedați”, „hoți cu chei electronice”, [90, p. 227], „gulere albe”, „spioni electronici” (persoane care distrug sistemul de acces al computerului, pentru a obține informații ce pot fi utilizate în scopuri politice, militare sau economice [172, p. 64, 173, p. 722, 6]), „phreakeri” (persoane care accesează ilegal rețelele de comunicare prin intermediul telefoanelor mobile [15, p. 309]).

În cazul anumitor subcategorii de infracțiuni informatice, infractorii informatici pot fi numiți în dependență de rolul și funcțiile pe care le au în comiterea infracțiunii, spre exemplu, în Anexa nr. 3 la prezenta lucrare este realizată o clasificare a infractorilor informatici, proprie cazurilor de fraudă informatică, propusă de autorii V. A. Pimenov și I. V. Goroșco [86, p. 45].

Infractorii informatici sunt organizați în grupări regionale, editează mijloace electronice personale de informare în masă (reviste, forumuri, periodice, etc.), organizează conferințe on-line, dispun de dicționare de terminologie specifică, care se dezvoltă mereu și sunt distribuite prin buletine informative care, de asemenea, propagă informații necesare pentru perfecționarea metodicii de accesare ilegală a sistemelor și de violare a securității. Limbajul comun constituie cel mai important element de coeziune și de identitate pentru grupurile cibernetice deviante. Infractorii împărtășesc un adevărat lexicon, puternic influențat de limba engleză [92, p. 907] și de terminologia tehnică, reprezentând o importantă structură a identității subculturale a hackingului.

Tipologia infractorilor informatici, realizată de A. N. Kosenkov și G. A. Ciornâi, distinge următoarele categorii [174, p. 91]:

1) *Infractori specializați*. Acest tip de infractori își orientează activitatea spre săvârșirea anumitor categorii de infracțiuni informatice, și chiar săvârșesc de sine stătător fapta respectivă, având cunoștințele „profesionale" necesare. De regulă, aceștia sunt persoane cu vârsta de 14-20 de ani [175, p. 907].

2) *Infractori nespecializați*. Infractorii în cauză comit orice gen de infracțiuni informatice, utilizând dispozitivele electronice necesare, fără a deține cunoștințele tehnice în domeniu sau posedă cunoștințe generale.

Motivul și scopul reprezintă un element-cheie al caracteristicii criminalistice a infracțiunilor informatice. Relevăm faptul că scopul și motivul acestor categorii de infracțiuni nu poate exista de sine stătător, separat de personalitatea infractorului informatic, din care considerente este necesară examinarea acestor elemente corelate între ele și simultan. Astfel, în dependență de motivația infractorului, pot fi delimitate următoarele tipuri de infractori informatici [174, p. 92]:

1. *Tipul materialist* [73, p. 38-39, 92, p. 907], care se regăsește în majoritatea infracțiunilor informatice. Criminalitatea informatică cauzează anual prejudicii materiale pentru economia globală, în volum de aproximativ 900 de miliarde de euro [118].

2. *Tipul violent*, care determină persoanele-țintă la sinucidere sau le amenință cu moartea (*cyberbullying* „intimidare", *cyberstalking* „urmărire electronică") [22]. În acest context, un exemplu recent este cazul jocului „Balena Albastră", în care minorii și adolescenții din diferite țări [176], inclusiv din RM, erau influențați psihologic de către „curatori" să se sinucidă [177].

3. *Tipul predispus sexual* se manifestă, spre exemplu, prin răspândirea materialelor pornografice. PG, în comun cu Centrul pentru combaterea crimelor informatice a INI, au documentat activitatea mai multor persoane, care făceau schimb de imagini și înregistrări video cu pornografie infantilă, având ca „personaje" copii cu vârste cuprinse între 4 și 12 ani, abuzați sexual de persoane majore de sex masculin, precum și minori implicați în raporturi sexuale reale, fotografiați și filmați de persoane adulte. Printre suspecți a fost identificat un slujitor de cult, un producător de reviste lunare, un student și doi directori de întreprinderi, precum și un angajat al administrației unui centru comercial din capitală.

4. *Tipul dezorientat social*, a cărui intenție este de a încălca normele sociale și a influența distructiv relațiile în cauză [178, p. 115, 48, p. 76]. În literatura de specialitate [28, p. 42], asemenea infractori poartă denumirea de *vandali* [60, p. 684, 6], sau *huligani* [73, p. 40-41, 92, p. 907];

5. *Tipul motivat ideologic* (îndeosebi în cazul infracțiunilor de extremism [83, p. 40]) sau *politic* [179, p. 9, 92, p. 907], caracteristic ultimei perioade de timp. De cele mai multe ori, scopul lor este de a produce fobie, fiind numiți *teroriști* [28, p. 42, 87, p. 680] și *extremiști* [26, p. 43]. Spre exemplu, în cadrul cauzei penale nr. 2015928176, s-a stabilit că pe 20.05.2015, inculpatul B.S., învinuit în săvârșirea infracțiunii de corupere a alegătorilor, prevăzute de art.181[1] CP, a procurat, pe un termen de un an, domeniul www.alegerimoldova.com, indicând date de contact false și creând o platformă-web, prin intermediul căreia determina alegătorii, înregistrați pe site, să voteze un anumit candidat la alegerile locale. Acesta îi asigura pe utilizatorii site-ului cu privire la deplina anonimitate și securitate a acțiunilor ilicite pe care urmau să le comită. La concret: cu 2 zile înainte de data alegerilor locale, administratorul platformei urma să le transmită alegătorilor prin e-mail o scrisoare cu datele candidatului pentru care urmau să voteze. Ulterior, alegătorul trebuia să fotografieze buletinul de vot, completat conform instrucțiunilor, și să-l transmită inculpatului, care le promitea câte 50 de lei pentru fiecare buletin de vot încărcat [180].

6. *Tipul obsedat de statut*. Acești infractori comit infracțiunea în vederea obținerii, în societatea cibernetică, a unui statut social neformal mai înalt. De regulă, aceștia sunt *hackerii* [28, p. 42, 181, p. 110, 73, p. 40];

7. *Tipul investigator* [181, p. 110, 73, p. 39-40, 92, p. 907]. Motivarea lor de bază constă în analiza produselor program și a mijloacelor tehnice, a sistemelor informatice, pentru a depista breșele și a căuta mijloacele de înlăturare a acestora. În februarie 2016, a fost reținut un tânăr de 21 de ani, originar din raionul Anenii Noi, care, în perioada anilor 2015-2016, utilizând produse program, special elaborate pentru spargerea sistemelor informatice, a accesat ilegal baze de date, site-uri oficiale ale mai multor companii private, companii prestatoare de servicii Internet și

comunicații telefonice, bănci comerciale, precum și ale unor instituții de stat din țară, ulterior publicând o parte din aceste informații pe blogul personal. Tânărul a declarat că a efectuat faptele date din motive de interes investigativ [182].

8. *Tipul bolnav psihic*, care suferă de forme noi de maladie psihică – patologii informaționale sau fobii de computer [6, 87, p. 680].

Vârsta infractorilor informatici variază într-un diapazon destul de mare (14-45 ani): 33% - sunt persoane cu vârsta până la 20 de ani, 54% - între 20-40 ani, 13% - peste 40 de ani. Cu toate acestea, categoriile de vârstă pot varia în dependență de categoria infracțiunii informatice săvârșite, spre exemplu, în cazul creării, utilizării și răspândirii produselor program ilegale, persoanele cu vârsta între 11-21 de ani constituie circa 64% din numărul total, cele cu vârsta de 21-25 ani – 22% și cele cu vârsta peste 25 ani – 14% [73, p. 23-24].

Majoritatea celor implicați în aceste tipuri de infracțiuni o constituie bărbații – 83%, iar în cazul infracțiunilor de extremism, săvârșite cu folosirea tehnologiilor avansate, numărul lor atinge cota de 97% [83, p. 36, 175, p. 908, 92, p. 907]. Mărimea prejudiciului cauzat de către o persoană de sex masculin depășește de 4 ori pe cel cauzat de către o persoană de sex feminin [90, p. 230].

52% din infractori au avut o pregătire specială în domeniul prelucrării automatizate a informației [114, p. 213]. Majoritatea infractorilor (77%) au avut un nivel mediu de dezvoltare intelectuală, 21% - peste cel mediu și doar 2% sub cel mediu. Doar 7 cazuri din 1000 de infracțiuni informatice au fost săvârșite de programatori profesioniști [90, p. 230].

În peste 85% din cazuri, infractorii au acționat în grup [83, p. 36].

Se consideră că violența în grupurile delincvențiale este o normalitate, dar, în cazul grupurilor deviante digitale, aceasta este practic nulă, cu excepția violenței verbale [6].

În 98% din cazuri, infractorii informatici descoperiți de către organele de urmărire penală sunt persoane fără antecedente penale [80, p. 75].

Potrivit legislației penale a RM, subiect al infracțiunilor informatice în sens restrâns, poate fi o persoană fizică responsabilă, care în momentul comiterii faptei a atins vârsta de 16 ani, cu excepția art.260 CP, când vârsta poate fi de 14 ani. Persoana juridică (cu excepția autorității publice) este subiect în majoritatea categoriilor infracțiunilor analizate [183], cu excepția celor prevăzute la art.177 alin.(1-1^1), 178, 185^2 alin.(1), 260^2, 260^5, 260^6 și 346 CP. În unele situații, subiectul infracțiunilor analizate are o calitate specială, fiind o persoană care fie că nu este autorizată în temeiul legii sau al unui contract, fie că depășește limitele autorizării, fie că nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic, ori să desfășoare cercetări științifice sau să efectueze orice altă operațiune într-un sistem informatic (art.259). Totodată, în ipoteza infracțiunii prevăzute la art.261 CP, subiect poate

fi numai persoana în ale cărei obligații intră respectarea regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informației ori a regulilor de protecție a sistemului informatic [34, p. 345].

În opinia autorului D. Ciuvaga [6], pe care noi nu o agreăm, infractorii digitali reprezintă o categorie tipologică de infractori cu aptitudini intelectuale dezvoltate și cu un nivel avansat de cunoștințe tehnice în domeniul informatic. Ei manifestă un profil preponderent non-violent, au o capacitate sporită de planificare a acțiunilor în vederea exploatării tuturor oportunităților informaticii. Este subiectul care este predispus a acționa în solitudine, având tendința minimă de a se percepe drept criminal, este o personalitate mai mult introvertită, prezentând trăsăturile unui individ slab integrat social și dezangajat moral. Incidența bolilor psihice și a tulburărilor de personalitate în rândul infractorilor digitali este redusă, ei suferind mai mult de diverse fobii sau manii.

În urma analizei sentințelor de condamnare emise de instanțele de judecată din țara noastră pe parcursul anilor 2003-2017, am constatat că circa 55% din infracțiunile examinate au fost comise din motive de cupiditate, 35% sunt infracțiuni cu tentă sexuală, 3% - au fost comise de persoane dezorientate social, 2% - de infractori investigatori și 5% - de alte categorii de motivații infracționale. Vârsta infractorilor informatici din RM variază între 16 și 55 ani: 24% sunt persoane cu vârsta sub 25 de ani, 52% - au vârsta cuprinsă între 25 și 35 ani, 24% - peste 35 de ani. 92% din infracțiunile informatice examinate în instanțele de judecată din RM au fost săvârșite de persoane fizice, dintre care doar 5% constituie persoane de sex feminin. 93% din infractorii informatici condamnați pe teritoriul RM nu au avut anterior antecedente penale. A se vedea, în acest sens, Anexa nr. 1 la prezenta lucrare.

În opinia noastră, infractorii informatici sunt persoane cu capacități deosebit de flexibile de trecere operativă de la dimensiunea reală la cea virtuală, de la o relație mediată de un spațiu emotiv-fizic la o relație mediată de un spațiu emotiv-artificial; ei au o percepție alterată sau diminuată asupra ilegalității comportamentului lor, a daunei provocate, a riscurilor de a fi denunțați, descoperiți și sancționați, cu sau fără cunoștințe tehnice în domeniul IT, fiind numiți în dependență de rolul și funcțiile pe care le au în comiterea infracțiunii, cu un profil predominant non-violent, având un limbaj comun cu terminologie specifică și cu o motivație infracțională diversificată (fie materială, sexuală, ideologică, politică, obsedată de statut social sau de investigație). În majoritatea covârșitoare a cazurilor, ei sunt de sex masculin, cu vârsta cuprinsă între 16 și 55 de ani, acționează în grup, neavând, de regulă, antecedente penale.

Locul comiterii infracțiunilor informatice

Stabilirea locului și momentului săvârșirii infracțiunii informatice constituie o problemă criminalistică și practică esențială.

Fapta criminală poate fi comisă pe teritoriul unui stat, iar consecințele ei pot să se manifeste într-o altă țară. Pe lângă aceasta, având în vedere principiile de funcționare a rețelei Internet, urmele infracțiunii se pot afla pe serverul ISP, care s-ar putea afla fizic pe teritoriul unui al treilea stat [73, p. 14].

Examinând particularitățile caracteristice funcționării sistemelor informatice, deducem că, pe de o parte, locul comiterii infracțiunii reprezintă însăși rețeaua informatică și de comunicații electronice, în cadrul căreia se efectuează introducerea, modificarea, copierea, blocarea, transmiterea, păstrarea, prelucrarea sau ștergerea datelor informatice, pe de altă parte, locul săvârșirii infracțiunii informatice îl constituie spațiul unde se află sistemul informatic, prin intermediul căruia se săvârșește fapta. Anume în acest spațiu se află volumul de bază al informației, ce caracterizează procesul săvârșirii infracțiunii (modalitatea, instrumentele, mijloacele ș.a.), adică probele [90, p. 221].

Specific infracțiunilor informatice este faptul că asupra lor nu influențează factorii naturali sau climaterici [184, p. 113], adică ele pot fi săvârșite în orice locație, unde funcționează un sistem informatic [73, p. 14].

În opinia unor savanți [51, p. 15, 48], componența spațiului cibernetic include:

1) încăperile în care se află sistemele informatice, precum și tehnica complexă care asigură funcționarea acestora (sistemele de comunicații, energia electrică, ș.a.).

2) mijloacele de prelucrare automatizată a informației (mașinile de calcul și sistemele lor);

3) canalele de comunicații electronice și de transmitere a datelor;

4) suporturile electronice (suport material ale cărui calități fizice permit imprimarea, păstrarea și prelucrarea informației documentate [145], numit în literatura de specialitate *purtător tehnico-electronic de informație* [21, 185] sau *suport de stocare a datelor informatice*);

5) datele informatice nemijlocite.

Spre exemplu, înaintea și în timpul comiterii unei fraude informatice, diverși participanți la infracțiune efectuează multiple acțiuni separate, în rezultatul cărora se întâmplă diverse evenimente în diferite locuri. În dependență de aceasta, se disting mai multe variante de stabilire a locului săvârșirii infracțiunii [86, p. 103]:

- adresa *de iure* a proprietarului mijloacelor bănești sustrase (a victimei);
- adresa *de facto* a proprietarului mijloacelor bănești sustrase;
- adresa aflării operatorului transferului mijloacelor bănești, al cărui client este victima;
- adresa aflării operatorului utilizat în calitate de intermediar (buffer) de către infractori;

- adresa persoanei pe numele căreia este înregistrat contul la operatorul intermediar;
- adresa oricărui alt operator utilizat de către infractori în transferul ilegal de bani;
- locul aflării bancomatului, a filialei instituției financiare, a punctului de convertire în mijloace electronice de plată, a filialei de transfer bănesc și de primire a banilor în numerar;
- adresa persoanei pe numele căreia este înregistrat cardul bancar utilizat la lichefierea mijloacelor bănești;
- locul de aflare fizică a resurselor din rețeaua internet (servere, site-uri), utilizate la răspândirea virusului, folosirea nemijlocită a produsului program destinat pentru comiterea infracțiunii, gestionarea centrului de control al botnetului (mai multe dispozitive conectate la internet, fiecare dintre care rulează unul sau mai mulți roboți), ascunderea accesului neautorizat la informația computerizată, ș.a.

Lista prezentată nu este una exhaustivă și poate suferi modificări în dependență de stabilirea circumstanțelor cauzei.

De regulă, locul comiterii infracțiunii, precum și cel al survenirii consecințelor faptei nu coincid, fiind, în proporție de 79%, diferite [103, p. 689]. Totodată, 51% din infracțiunile informatice sunt comise de la domiciliul infractorului, 27% din cazuri – de la locul de muncă (de studii), 13% - din locuri publice și doar 7% sunt comise la locul aflării victimei [85].

În cadrul unei cercetări empirice [83, p. 117] referitoare la locul comiterii infracțiunilor cu privire la extremism, săvârșite cu utilizarea IT, s-a constatat că acesta îl constituie: domiciliul bănuitului – în 46% din cazurile examinate; domiciliul altor persoane – 19,9% din cazuri (inclusiv în vederea ascunderii datelor sale); locul de muncă al bănuitului – 16,5% (utilizarea calculatorului personal de la serviciu sau al colegilor de serviciu, a computerelor de folosință comună); locurile de utilizare publică a sistemelor informatice (sală de calculatoare, cafenea-internet, locuri de recreare, sală de lectură, aeroport, autogară, transport public [186] ș.a.).

În rețeaua internet sunt numeroase „reprezentanțe” sau „piețe de desfacere” (piața neagră), destinate comercializării produselor (inclusiv a produselor program create pentru comiterea infracțiunilor informatice) și serviciilor ilegale, comunicării dintre infractorii informatici, căutării de lucru, solicitărilor, schimbului de experiență și instruirii, recrutării noilor participanți. Cele mai veritabile site-uri sunt cele private (inaccesibile publicului), iar pentru dobândirea accesului către aceste resurse este necesară obținerea unei recomandări sau achitarea unei plăți considerabile. Pentru obținerea unor informații generale cu privire la activitatea și propunerile pieței negre, pot fi recomandate următoarele resurse din internet, cum ar fi www.forum.zloy.bz, www.darkmoney.cc, www.forum.antichat.ru, www.forum.beznal.cc [86, p. 44].

În urma analizei sentințelor de condamnare, emise de instanțele de judecată din țara noastră pe parcursul anilor 2003-2017, am constatat că circa 67% din infracțiunile examinate au fost comise de la domiciliul infractorilor, 16% de la locul de muncă al acestora, 14% din locurile publice, și numai 3% de la domiciliul victimei (Anexa nr. 1).

În concluzie, considerăm că locul comiterii infracțiunilor informatice este determinat de caracterul predominant transfrontalier al acestei categorii de infracțiuni și, în majoritatea cazurilor, este diferit de locul survenirii consecințelor faptei. Acesta reprezintă atât însăși rețeaua informatică și de comunicații electronice, cât și locul aflării sistemului sau rețelei informatice. Specific infracțiunilor respective este faptul că, de regulă, ele sunt săvârșite de la domiciliul infractorului, de la locul său de muncă sau din locuri publice.

Timpul săvârșirii infracțiunilor informatice

Studiul materialelor cauzelor penale a arătat că timpul comiterii infracțiunilor informatice este identificat în 96% din cazuri, în 73% din această categorie de infracțiuni – cu precizie până la un minut, în 17% - până la o oră, iar în 6% din cazuri – până la o zi. Aceasta se datorează înregistrării automate a operațiunilor relevante și fixării evenimentelor legate de prelucrarea datelor [85].

În general însă, timpul nu influențează modalitatea de comitere sau tăinuire a infracțiunii informatice [73, p. 19].

De cele mai multe ori, atacurile cibernetice sunt săvârșite în perioada zilelor de odihnă, precum și în orele matinale, atunci când serviciile de securitate sunt mai pasive, iar solicitarea ajutoarelor este mai dificilă, precum și la finele zilei lucrătoare (sau zilei bancare). Un exemplu de fraudă reușită este sustragerea sumei de 25 mln de ruble rusești de la o societate comercială din Moscova, transferul fiind efectuat la 7 martie, aproximativ la ora 16, atunci când nu doar era sfârșitul zilei de muncă, dar când și tot personalul era preocupat de pregătirea sărbătoririi zilei internaționale a femeilor. Astfel, în cazul fraudelor informatice de sustragere camuflată a mijloacelor bănești din conturile electronice, opțiunea timpului de comitere a infracțiunii va depinde de [86, p. 64]:

- specificul efectuării plăților electronice de către victimă;

- eventuala reacție a utilizatorului legal al calculatorului infectat, în cazul în care el va avea acces la istoricul plăților sau va recepționa un mesaj electronic sau de tip SMS cu privire la operațiunea de plată;

- posibila reacție a angajatului băncii care verifică ordinele de plată.

Modalități de comitere a infracțiunilor informatice

În urma analizei articolelor expuse în capitolul XI din Partea Specială a CP, constatăm că cele mai frecvente modalități de comitere a faptei prejudiciabile, în cazul infracțiunilor informatice, sunt:

a) introducerea datelor informatice;
b) distrugerea informației și ștergerea datelor informatice;
c) deteriorarea informației (datelor informatice);
d) modificarea informației (datelor informatice);
e) blocarea informației și restricționarea accesului la datele informatice;
f) copierea informației;
g) dereglarea funcționării calculatoarelor, a sistemului informatic sau a rețelei informatice;
h) transferul (transmiterea) datelor informatice;
i) „acces", „acces la informație", „acces ilegal la informație".

Introducerea datelor informatice presupune inserarea într-un sistem informatic a unor date care nu existau înainte în respectivul sistem. Datele pot fi inserate în mod direct de către făptuitor, prin utilizarea tastaturii ori a altor echipamente periferice [37, p. 314, 843].

Unii oameni de știință consideră că *distrugerea informației* presupune ștergerea ei de pe suportul fizic [52, p. 38], precum și modificarea neautorizată a componentelor sale [60], care schimbă esențial conținutul [187, p. 235]. Alții sunt de părerea că ar semnifica influențarea infracțională nemijlocită asupra informației, adică încetarea existenței acesteia sau aducerea ei într-o stare care exclude - în totalitate și definitiv - utilizarea ei conform destinației sale funcționale, întrucât informația nu mai poate fi restabilită prin reparație, restaurare [104, p. 664] sau prin ștergerea din memoria suportului material [105, p. 699]. O categorie de specialiști susțin că distrugerea informației computerizate reprezintă imposibilitatea utilizării ei după destinație, în totalitate sau în parte [188, p. 583]. Totuși, din punct de vedere teoretic, este posibilă restabilirea oricărei informații prin metoda extragerii acesteia din adâncul memoriei [106, p. 97, 37, p. 314]. Cu toate acestea, mulți dintre utilizatori nu au, de regulă, abilități și posibilități de a extrage și de a restabili informația, de aceea ștergerea informației computerizate, chiar dacă există posibilitatea restabilirii acesteia prin mijloace tehnice [107, p. 45], urmează a fi apreciată drept distrugere a informației. Totodată, este de menționat că vom fi în prezența acestei modalități de infracțiune chiar și în cazul în care proprietarul, posesorul sau utilizatorul deține o copie a informației respective pe un alt suport material [108, p. 69]. Există numeroase produse program (cum ar fi: HARA-KIRI, RedBut, BestCrypt, StrongDisk Pro, Cipher, Eraser, DBAN etc.) [109, 189], dar și metode tehnice (mecanică, termică, chimică, radiațiilor și fizică), care au ca obiectiv principal distrugerea informației computerizate [190, p. 74].

Deteriorarea informației (datelor informatice) se manifestă prin influențarea infracțională nemijlocită asupra informației și presupune o înrăutățire considerabilă a stării acesteia, informația devenind inutilizabilă parțial sau temporar, iar acest fapt poate fi remediat prin reparație, restaurare sau prin alt procedeu de readucere a informației computerizate la starea sa inițială. Deteriorarea informației, de cele mai multe ori, poate fi cauzată de atacul unui virus [191, p. 82], care, deseori, este mascat sub un joc [192].

Autorii români M. Dobrinoiu [37, p. 314, 839], A. C. Moise [26, p. 80] și I. C. Spiridon [42, p. 240] susțin că *modificarea datelor informatice* presupune introducerea de noi secvențe sau extragerea anumitor porțiuni, care au drept rezultat formarea unor noi date informatice, diferite de cele inițiale și, mai ales, neconforme cu ceea ce reflectau acestea. Unii cercetători consideră că modificarea informației reprezintă introducerea oricăror modificări [193, p. 47], alții – introducerea oricăror modificări, cu excepția adaptării, perfecționării produselor program și a bazelor de date [105, p. 700, 194, p. 160]. A treia categorie opinează că aceasta semnifică modificarea organizării logice și fizice a bazelor de date [187, p. 235]. În ce ne privește, susținem opinia că modificarea informației constă în schimbarea conținutului ei în comparație cu informația care era inițial la dispoziția proprietarului (posesorului, utilizatorului) [105, p. 700, 195, p. 484], indiferent de categoria modificărilor operate și de conținutul informației modificate [107, p. 45]. Este de menționat faptul că modificarea informației poate fi efectuată și de viruși [196, p. 19].

Blocarea informației, în opinia unor autori [105, p. 700, 110, p. 41], constă în îngrădirea artificială – fizică sau logică [37, p. 315, 840] – a accesului utilizatorului la informația computerizată, fără distrugerea acesteia. O parte din ei sunt de părerea că aceasta ar însemna crearea condițiilor (inclusiv cu ajutorul unor produse program) care exclud posibilitatea folosirii informației computerizate de către proprietarul legitim al acesteia [187, p. 236], într-un interval de timp rezonabil [26, p. 81]. Noi considerăm că blocarea informației reprezintă imposibilitatea permanentă sau temporară de a efectua orice operațiuni asupra informației computerizate, cu păstrarea intactă a acesteia.

În ceea ce privește *copierea informației*, opiniile doctrinare de asemenea nu sunt unanime. Astfel, în viziunea unor autori, copierea informației prin intermediul pixului sau fotografierea textului de pe ecran nu constituie copierea informației [111, p. 237]. Alții consideră copierea informației ca fiind producerea unui alt exemplar al bazei de date sau al mapei sub orice formă materială, precum și copierea lor în memorie pe un suport informațional [187, p. 235], inclusiv copierea pe suport material, imprimarea pe suport de hârtie [111, p. 235]. Sunt autori care înțeleg copierea informației ca fiind repetarea și memorarea informației pe orice suport [105, p. 700] sau ca transcriere, reproducere și publicare a informației, cu păstrarea informației originale [104, p.

664]. Susținem părerea potrivit căreia copierea informației urmează a fi interpretată drept producerea unei copii a informației pe orice suport material [107, p. 45], cu păstrarea intactă a informației originale [36, p. 497].

Dereglarea funcționării calculatoarelor, sistemului informatic sau a rețelei informatice este considerată în doctrină drept o abatere de la modul normal de funcționare, manifestată prin refuzul de a oferi informația sau prin acordarea unei informații distorsionate [104, p. 664]. Există păreri care o echivalează cu crearea erorilor de funcționare a lor în conformitate cu destinația, pe o perioadă permanentă sau temporară [105, p. 701]. Interpretarea ei drept o diminuare a funcționalității anumitor elemente ale calculatorului, ale sistemului sau rețelei informatice [112, p. 558] este o altă opinie asupra acestui subiect. În ceea ce ne privește, susținem părerea specialiștilor [36, p. 497] care explică această sintagmă ca desemnând deteriorarea calculatoarelor, a sistemului sau a rețelei informatice, având ca efect oferirea unei informații incorecte, refuzul de a oferi informația, scoaterea din funcțiune sau întreruperea funcționării etc.

Transferul (transmiterea) datelor informatice se realizează de la distanță, folosindu-se facilitățile oferite de conectarea sistemului vizat la o rețea informatică sau la internet. Transmiterea se poate realiza prin: transferul sistemului informatic respectiv de fișiere sau programe infectate de pe suporți externi; transmiterea de mesaje e-mail având ca atașament fișiere infectate; descărcarea de fișiere sau programe purtătoare de cod malițios din internet [37, p. 843].

Noțiunea de *acces* este definită în Legea comunicațiilor electronice [197] ca fiind punerea la dispoziția unui terț autorizat, conform legii și în anumite condiții, a spațiilor, echipamentelor sau serviciilor, în mod exclusiv sau neexclusiv, în scopul furnizării serviciilor de comunicații electronice. Accesul la informația computerizată presupune intrarea în întreg sistemul informatic sau numai într-o parte a lui [130, 42, p. 71]. Totodată, acesta presupune obținerea posibilității reale de a distruge, de a deteriora, de a modifica, de a bloca, de a copia etc. informația computerizată [102, p. 376]. Accesul reprezintă orice formă de pătrundere la sursa de informație prin utilizarea mijloacelor tehnico-electronice de identificare, care permit manipularea informației computerizate [52, p. 37]. Din punct de vedere tehnic, el poate fi realizat prin mai multe tipuri de acțiuni, cum ar fi: autentificarea, evitarea, citirea, copierea sau furtul informației [17, p. 389, 149, p. 58]. Specialiștii din domeniul prevenirii și combaterii infracțiunilor informatice disting diverse tipuri de *cyber atacuri*, și anume [15, p. 161-166]: atacuri prin parolă [198], atacurile de acces liber, atacurile care exploatează bibliotecile partajate, atacurile prin deturnarea TCP, deturnarea sesiunii, atacurile prin inginerie socială [199] [200], obținerea de date informatice.

Hotărârea Plenului CSJ cu privire la practica judiciară în cauzele penale privind minorii (pct.13^1) [201], oferă o interpretare a modalităților normative de comitere a faptei prejudiciabile de

pornografie infantilă prevăzută la art.208[1] CP, și anume: producerea (fabricarea sau combinarea de imagini sau alte reprezentări), distribuirea (asigurarea pe orice căi a accesului contra cost sau gratuit), difuzarea (expunerea publică, cu sau fără scop de vânzare), importarea (aducerea în propria țară a imaginilor sau a altor reprezentări produse în străinătate), exportarea (scoaterea în afara țării a respectivelor reprezentări produse în țară), oferirea (prezentarea cuiva a imaginilor sau altor reprezentări), vinderea (cedarea stăpânirii definitive asupra respectivelor reprezentări în schimbul unei sume de bani), procurarea (obținerea în posesie a imaginilor sau altor reprezentări), schimbarea (cedarea unor imagini sau altor reprezentări, pentru a lua în locul acestora alte asemenea reprezentări), utilizarea (vizionarea respectivelor reprezentări), deținerea (ținerea în posesie sau în păstrare) a unor imagini sau altor reprezentări ale unui sau mai mulți copii, implicați în activități sexuale explicite, reale sau simulate, ori a unor imagini sau altor reprezentări ale organelor sexuale ale unui copil.

În urma analizei literaturii de specialitate, au fost relevate și alte clasificări cu privire la categoriile (grupurile) de modalități de comitere a infracțiunilor informatice, și anume:

1) accesul nemijlocit la purtătorii informatici și la mijloacele tehnico-electronice care conțin date informatice sau sustragerea acestor purtători sau mijloace [85];

2) accesul la distanță la purtătorii informatici și la informația computerizată ocrotită de lege. Acesta se poate manifesta prin „curățarea urnei” (adică căutarea datelor lăsate de către utilizator în urma folosirii calculatorului); „abordajul informațional” (*brute Force*, când infractorul alege codul de acces cu utilizarea diverselor produse program); *„*alegerea pe îndelete*”* (căutarea punctelor slabe ale sistemelor de protecție); „breșă” (infractorul caută breșe în anumite sectoare ale produselor program); „mascaradă” (folosirea codurilor de acces ale utilizatorilor legali, dobândite prin mituire și stoarcere de informații); „mistificare” (folosirea codurilor de acces ale utilizatorilor legali, obținute prin înșelăciune); „schimbarea datelor”; „calul troian” (introducerea în calculatorul străin a produselor program speciale); „salam” (dobândirea mijloacelor financiare grație deducerilor din multiple operațiuni); „virușii electronici” (soft care se conectează de sine stătător la alte produse program și efectuează diverse acțiuni nedorite, odată cu rularea produsului program infectat) [90, p. 213].

3) falsificarea datelor de intrare / ieșire și a comenzilor de control;

4) modificarea neautorizată a produselor program existente pentru sisteme informatice și crearea softurilor destinate pentru comiterea infracțiunilor [85];

5) răspândirea ilegală a suporturilor de stocare a informațiilor electronice;

6) modalități complexe.

Cardul de plată [202, p. 51], inclusiv datele acestuia, sunt din ce în ce mai utilizate în ziua de azi. Fiind portofelul electronic al majorității persoanelor, tentația e mare: fraudele săvârșite cu utilizarea datelor din cardurile de plată au sporit ca număr și ca valoare. Fraudarea prin utilizarea datelor unui card de plată se poate face prin [203] achiziționarea de bunuri și servicii sau extragerea directă de mijloace bănești. Obținerea ilegală a datelor unui card bancar se poate realiza prin una din următoarele modalități: *skimming* (activitatea de copiere a datelor valide de pe banda magnetică a unui card autentic prin intermediul unui dispozitiv de citire a cardurilor, fără știrea posesorului legitim, cu intenția de a fi folosite în scopuri frauduloase) [204, p. 183, 205, p. 7]; *phishing* (crearea mesajelor transmise prin poșta electronică și paginile web, care sunt reproduceri exacte ale unor site-uri existente, pentru a induce în eroare utilizatorii să divulge date personale, financiare sau date privind parola) [206, p. 164, 207]; *carding* (modificarea codului-sursă al unei pagini originale a unui site comercial, așa încât informațiile introduse de deținătorul legitim al datelor de cont să fie direcționate către infractor, fără știrea celui dintâi) [26, p. 293]; sau *generarea de numere de carduri* (generarea unei liste de numere de carduri, pornind de la un singur număr de card, prin aplicarea algoritmului matematic al lui Luhn, pe care-l folosesc emitenții legali de carduri) [26, p. 294].

În cazul fraudelor informatice, săvârșite la procurarea online a bunurilor (spre exemplu, orice gen de echipament, utilaj, tehnică, îmbrăcăminte, accesorii și altele) sau a serviciilor (cum ar fi plățile comunale, biletele pentru orice gen de transport, rezervările hoteliere, foile turistice, publicitatea etc.) cu utilizarea datelor cardurilor de plată străine, cumpărătorul (infractorul) urmează să parcurgă câteva etape, care pot să difere neesențial de la un caz la altul, în dependență de dorințele vânzătorului online (administratorului platformei de comerț electronic). Etapele de bază sunt:

1) alegerea produsului sau serviciului dorit;
2) completarea datelor cu privire la cumpărător și/sau beneficiar;
3) efectuarea operațiunii de plată electronică.

La fiecare dintre aceste etape infractorul lasă urme care trebuie depistate, ridicate, analizate și utilizate la descoperirea infracțiunii.

Preliminar, la prima etapă, infractorul va căuta site-ul vânzătorului electronic care dispune de produsele sau serviciile pe care și le dorește, va verifica disponibilitatea acestora, precum și informațiile pe care urmează să le ofere vânzătorului [208, p. 219].

Infractorii folosesc un număr redus de instrumente destinate mascării datelor din sistemul informatic utilizat (spre exemplu, aplicații de ascundere a adresei IP), deoarece încă nu s-a trecut la executarea nemijlocită a infracțiunii și pentru a nu complica procesul de căutare a produselor

sau a serviciilor prin utilizarea acestor instrumente.

Datele cu privire la aceste acțiuni de căutare pot fi găsite pe serverul care găzduiește site-ul comerciantului electronic, denumite și *jurnale* sau *loguri*, un exemplu de asemenea jurnale este reflectat în Anexa nr. 4 din prezenta teză. Astfel, administratorul site-ului poate deține informații cu privire la:

a) căutările preliminare: produsul sau serviciul căutat; cantitatea bunurilor căutate; culoarea, dimensiunea, precum și alte caracteristici ale produsului căutat; perioada prestării serviciului căutat; numărul de beneficiari ai serviciului căutat; alte detalii cu privire la serviciul căutat; timpul căutării bunului sau a serviciului; adresa IP și alți parametri ai sistemului informatic utilizat la căutarea produselor sau a serviciilor.

b) alegerea produsului sau serviciului dorit;

c) completarea datelor cu privire la cumpărător și/sau beneficiar;

d) efectuarea operațiunii de plată electronică frauduloasă.

Odată constatată săvârșirea operațiunilor frauduloase de plată, organul de urmărire penală trebuie să întreprindă neîntârziat următoarele acțiuni: să identifice datele comerciantului electronic (administratorului site-ului de comerț online); să stabilească datele cu privire la numele de domeniu al site-ului de comerț electronic; să fixeze datele serverului care găzduiește site-ul de comerț online; să efectueze identificarea abonatului, proprietarului sau utilizatorului adresei IP a serverului; să colecteze rapid sau să ridice informația de la ISP (de la comerciantul electronic/administratorul site-ului de comerț online); să analizeze datele informatice administrate de pe serverul-gazdă.

În cauza penală nr.2014928507 de învinuire a lui G.S. (a.n.1989) în săvârșirea infracțiunilor de la art. 243 și art. 260^6 CP (spălarea banilor și fraudă informatică), s-a stabilit că, în perioada anilor 2012-2014, învinuitul, împreună cu alte persoane, utilizând datele cardurilor bancare străine (emise de instituţiile financiar-bancare din Japonia, India, Germania etc.), fără știrea și acordul titularilor acestor carduri și prin intermediul rețelelor informatice (din RM, România, Germania, Franța, Spania etc.), și folosind serviciile de vânzare a biletelor online, a procurat bilete de avion către diverse destinaţii (Paris, Istambul, Antalya, Bucureşti, Londra, Minsk, Lisabona, Moscova, Punta Cana, Colombo, Varadero, Chișinău etc.), pe numele a circa 50 de persoane, în sumă de circa 400000 MDL, precum și servicii hoteliere din oraşele enumerate. Prin aceeaşi schemă ilegală, învinuitul efectua plăţi on-line pentru procurarea florilor, cadourilor, a combustibilului, produselor alimentare etc, estimate la circa 16 mii lei, precum și plăţi de reîncărcare a conturilor numerelor de telefon în sumă de peste 70 mii lei. Totodată, organul de urmărire penală a stabilit faptul că, deși în momentul săvârșirii infracțiunii făptuitorul a mascat adresa IP a sistemului

informatic utilizat de către el, prin utilizarea diverselor Proxy servere (din diverse state), la momentul căutărilor preliminare pe site-ul www.zbor.md, conform criteriilor identice cu privire la călătorie (aeroporturile de decolare și aterizare a avionului, data decolării și aterizării, data returului, numărul pasagerilor, vârsta pasagerilor minori, timpul căutării și altele), făptuitorul a utilizat o altă adresă IP a sistemului informatic, alocată ISP din RM „StarNet" S.R.L., care a fost înregistrată pe adresa sa din mun. Chișinău, unde infractorul locuia temporar [209].

La cea de a doua etapă, de completare a datelor cu privire la cumpărător și/sau beneficiar, de regulă, atunci când infractorul trece nemijlocit la procurarea bunurilor sau a produselor, acesta utilizează diverse instrumente de mascare a datelor sistemelor și rețelelor informatice, utilizate la comiterea infracțiunii. Însă, oricum s-ar ascunde infractorul, el urmează să ofere și informație veridică, dat fiind că, la cea de-a doua etapă, la completarea formularelor online, comercianții solicită diverse date despre cumpărător [210, p. 223].

Spre exemplu, la procurarea biletelor de avion pe site-ul www.zbor.md, administratorii cer introducerea datelor pasagerului (numele, prenumele, data nașterii, sexul, naționalitatea); ale pașaportului pasagerului (țara emitentă, numărul și data expirării); ale persoanei care efectuează rezervarea (numele, prenumele, e-mailul și numărul de telefon).

Din exemplul prezentat în Anexa nr. 5 ce poate observa că, dacă numele și prenumele persoanei care efectuează rezervarea pot fi modificate, atunci datele pasagerului și ale pașaportului acestuia trebuie să fie veridice, deoarece biletul emis trebuie să corespundă datelor reale ale pasagerului în momentul îmbarcării, în caz contrar, acest bilet nu va putea fi folosit. Mai mult decât atât, nici datele de contact ale persoanei care efectuează rezervarea nu pot fi manipulate totalmente, dat fiind faptul că pe adresa electronică indicată se remite biletul electronic, iar la numărul de telefon indicat urmează a fi clarificate diverse chestiuni legate de emiterea biletului și de călătorie.

Unii vânzători online pot cere și alte date, spre exemplu, adresa livrării cumpărăturii, persoana de contact, mesajul cumpărătorului etc.

În cauza penală nr. 2016928137 de învinuire a lui M.V. (a.n. 1984) în săvârșirea infracțiunii prevăzute de art.260^6 CP (fraudă informatică), care, la 14.05.2014 M.V. a efectuat o tranzacție de procurare a bunurilor, în valoare de 95,97 Euro – 51 de trandafiri (olandezi, de culoare albă, cu lungimea de 60-70 cm) – pe numele altei persoane, prin intermediul companiei „Livrare Flori" S.R.L., utilizând serviciile website-ului www.livrareflori.md, iar comanda fiind livrată la aceeași dată. Totodată, organul de urmărire penală a constatat că făptuitorul a indicat adresa reală din mun. Chișinău, numărul de telefon al beneficiarului, precum și numele acestuia [211].

La această etapă, organul de urmărire penală trebuie să acumuleze probe suplimentare cu

privire la săvârșirea infracțiunii prin investigarea beneficiarilor produselor/serviciilor, efectuând: analizarea rețelelor de socializare în vederea stabilirii interferențelor, a conexiunilor dintre toți beneficiarii (spre exemplu, infractorii ar putea fi prietenii comuni din rețelele de socializare ai tuturor beneficiarilor); stabilirea, prin intermediul operatorilor de telefonie fixă și mobilă, a numerelor de telefon utilizate de către toți beneficiarii; colectarea sau ridicarea informației privind convorbirile telefonice din perioada respectivă, în vederea identificării numerelor de telefon comune; percheziționarea domiciliilor infractorilor, în vederea depistării și ridicării documentelor și înscrisurilor cu privire la produsul sau serviciul procurat, a calculatoarelor (blocurilor de sistem, laptopurilor, tabletelor), a telefoanelor mobile etc.; percheziționarea informatică (cercetarea, examinarea, expertiza) a calculatoarelor și echipamentelor mobile ale beneficiarilor, în vederea stabilirii persoanelor care le-au expediat biletele electronice, a mesajelor electronice relevante, a corespondenței efectuate prin intermediul produselor program (de exemplu: Skype, Facebook, Odnoklassniki, Outlook, Messenger, The Bat, Thunderbird, Viber, WhatsApp etc.); audierea lor cu privire la modul de procurare a produsului sau a serviciului, precum și a persoanelor implicate la procurarea nemijlocită, și alte date importante pentru justa soluționare a cauzei [212, p. 258].

Pentru efectuarea operațiunii frauduloase de plată online, infractorul utilizează doar o parte din informațiile conținute pe cardul de plată [213, 210, p. 227], și anume: (1) numărul cardului de plată, (2) data de expirare a cardului, (3) numele deținătorului cardului de plată și (4) codul de securitate al cardului, în corespundere cu prezentarea efectuată în Anexa nr. 5.

În cauza penală nr. 2015928175 de învinuire a lui B.A. (a.n. 1986) în săvârșirea infracțiunilor de obținere ilegală și divulgare a informațiilor ce constituie secret bancar, prevăzute de art. 245^{10} CP și a tentativei de fraudă informatică, prevăzute de art. 27, art. 260^{6} CP, organul de urmărire penală a stabilit că B.A., activând în calitate de barman în incinta unui restaurant din mun. Chișinău, a primit de la clienții restaurantului sau, după caz, de la chelneri, cardurile de plată pentru achitarea serviciilor prestate și, prin intermediul POS-terminalului, asigurându-se că, în acel moment, clienții nu observă acțiunile sale, a colectat, prin copiere pe suporturi de hârtie, informații despre datele cardurilor de plată, cum ar fi numerele, codurile de securitate (destinate pentru verificarea validității cardului de plată în cazul efectuării tranzacțiilor CNP), data expirării și numele titularilor cardurilor de plată, fără știrea și acordul deținătorilor acestor carduri, clienți ai restaurantului. Ulterior, utilizând sisteme informatice și rețele informatice, precum și alte mijloace electronice, inclusiv contul său din jocul „LineAgeII”, a utilizat datele respective, fără știrea și acordul titularilor acestor carduri, efectuând tranzacții on-line de convertire a banilor în mijloace de plată electronică, în cadrul jocurilor electronice [214].

Mijloacele și instrumentele utilizate la comiterea infracțiunilor informatice

În cazul unor infracțiuni informatice, stabilirea mijloacelor de săvârșire a infracțiunii (mijloacele tehnice speciale, sistemul sau rețeaua informatică) este obligatorie [34, p. 343].

Mijloacele tehnice speciale reprezintă niște dispozitive tehnice, atașate la canalele de comunicații electronice, sau niște dispozitive concepute sau adaptate pentru a colecta și înregistra transmisiile fără fir [36, p. 498]. Drept exemplu de mijloace tehnice speciale pot servi: microfoane fără fir, repetoare radio, stetoscoape radio, camere video ascunse, cu transferul de informații prin radio etc.

Infracțiunile informatice sunt săvârșite întotdeauna cu utilizarea mijloacelor tehnico-electronice. Structura acestor mijloace este complexă, incluzând atât sistemele informatice în accepția lor tradițională, cât și dispozitivele care funcționează în baza procesoarelor și a algoritmelor speciale și permit accesul la rețele informatice (ultrabook-uri, notebook-uri, netbook-uri, tablete, telefoane mobile, book reader-uri și altele ș.a.), IT (routerele WiFi, CDMA și WiMax, Bluetooth, rețele/modeme 3G și 4G, GSM, GPRS, EDGE etc.), suporturile de stocare a informației electronice pe discurile optice (CD, DVD, BD), pe dispozitive în bază de memorie flash (USB stickurile, cartelele de memorie ale telefoanelor mobile, aparatelor foto, camerelor video, cartele SIM ș.a.), precum și produsele program cu diverse destinații [83, p. 117].

În ceea ce privește sustragerea mijloacelor bănești prin utilizarea IT (produsele program concepute sau adaptate pentru fraudele informatice), acestea au început să fie observate de către specialiști prin anii 2005-2006 [215]. În anul 2007, a fost depistat „celebrul" produs program de tip Troian „Zeus" („Zbot"), devenind în curând cel mai răspândit. În 2009, a apărut „SpyEye", în anul 2010 - „Carberp" și „HodProt" („Origami"). Unele dintre ele sunt folosite până în ziua de azi de către grupările criminale – cel puțin, versiunile noi ale „Zeusului" sau virușii creați pe baza acestora [216]. În prezent, sunt actuale produsele program de tip Troian, cum ar fi „Corkow", „Ranbyus", „Lurk", „Shiz", „BifitAgent", totodată dezvoltându-se activ „troienii" specializații pentru dispozitivele mobile.

Considerăm că unii autorii [73, 86, 217] definesc eronat produsele program, concepute sau adaptate pentru comiterea anumitor categorii de infracțiuni, drept *softuri malițioase*. Or, orice soft ar putea fi folosit atât în scopuri legale, cât și ilegale, asemeni cuțitului de la bucătărie, care nu poate fi denumit „cuțit rău intenționat sau malițios".

Desigur, sustrageri din sistemele de plată electronică, cu utilizarea produselor program, special concepute sau adaptate pentru fraude informatice, au avut loc și mai înainte. Totuși aceste infracțiuni purtau un caracter predominant individual și deseori se comiteau în prezența factorului

uman, într-o formă sau alta, sau cu utilizarea diverselor metode de inginerie socială, iar produsele program respective se răspândeau doar către anumiți adresați.

Printre produsele program utilizate de către infractorii informatici se regăsesc: *virusul* (o serie de coduri de program, care au proprietatea de a se atașa la fișiere executabile sau fișiere-obiect [45, p. 62] și de a se propaga către alte programe de calculator [26, p. 22] și alte sisteme informatice [218, p. 57]), *virusul sectoarelor de boot* (infectează Master Boot Record al hard discului [219, p. 19]), *virusul script* (shell-virus, java-virus ș.a.), *macrovirusul* pentru Word și Excel, *viermele* (are aceleași proprietăți ca cele ale unui virus, cu deosebirea că el nu se poate reproduce [26, p. 22] și există independent de alte programe [11, p. 115]), *backdoor*-ul (mijloc ascuns de acces la distanță), *keylogger-ul* (un software sau hardware care înregistrează fiecare tastă pe care o apasă utilizatorul [26, p. 147]), *spyware-ul, sniffer-ul* (un software sau hardware destinat monitorizării traficului dintr-o rețea [26, p. 149]), *adware-ul* (programul care furnizează conținutul publicității într-o manieră surprinzătoare și nedorită de utilizator [219, p. 52]), diverse produse program concepute pentru fraude [86, p. 35].

Programului de tip *Calul Troian* („Troienii”, „troi”) i s-a atribuit această denumire prin analogie cu mitul antic despre construirea unui cal gigantic din lemn, în care s-au ascuns ostașii greci, pătrunzând astfel în Troia și cucerind-o. În mod similar, deghizat în ceva inofensiv (liste de directoare, un program de arhivare, un joc sau chiar un program de localizare și distrugere a virușilor) [37, p. 840], *Troianul* se instalează pe ascuns în sistemul informatic sau în dispozitivul mobil, în vederea îndeplinirii anumitor sarcini, cum ar fi [86, p. 38]: identificarea faptului utilizării mijloacelor de plată electronică (aplicațiile de tip „bancă-client”, utilizate pentru accesul la conturile bancare sau mijloacele de plată electronică; semnele de utilizare a internet banking (efectuarea de tranzacții bancare prin intermediul Internetului), a produselor program ale operatorilor, destinate pentru transferul mijloacelor bănești); primirea copiilor datelor de autentificare și ale altor date, necesare pentru efectuarea transferurilor bănești, precum și informația cu privire la starea contului, a transferurilor realizate, la plăți și beneficiar; efectuarea, dacă e posibil, a transferurilor bănești neautorizate prin utilizarea mijloacelor de plată electronice existente în sistemul informatic sau prin dispozitivul mobil infectat; ștergerea urmelor de utilizare neautorizată a mijloacelor de plată electronică, de activității efectuate, precum și pe sine însuși [220, p. 336].

La 12-15.05.2017, a fost înregistrat un atac cibernetic fără precedent în lume, având în vedere aria de acțiune, pericolul și consecințele acestuia, prin intermediul malware-ului Ransomware de tip WannaCry (WannaCryptor) [221], ce împiedică accesul la fișiere sau chiar la întregul sistem informatic infectat, până la plata unei „recompense” (ransom). Pentru a complica

procesul de recuperare a fișierelor, ransomware-urile blochează accesul la fișiere (documente, fotografii, muzică, video etc.) prin criptarea asimetrică a acestora. Această amenințare se propagă prin intermediul unor mesaje e-mail, care conțin atașamente și link-uri, atacatorii utilizând tehnici de inginerie socială, pentru a determina utilizatorii să acceseze resursele malițioase [222].

În cazul contrafacerii (falsificării) de carduri bancare, se presupune folosirea dispozitivelor special concepute, similare celor utilizate de instituțiile financiare emitente, care imprimă pe banda magnetică a cardului ori stochează în microprocesor (chip) informațiile necesare creării impresiei de autenticitate [46, p. 660], a cardurilor cu bandă magnetică, cu sau fără cip, noi sau utilizate, pe care vor fi înscrise datele bancare obținute ilegal, a sistemelor informatice cu soft special, necesar pentru funcționarea dispozitivului de înscriere a datelor pe carduri, a datelor valide ale cardurilor bancare originale clonate [26, p. 294].

O altă resursă importantă, deseori utilizată de către infractorii informatici, este Deep Web-ul (Internetul ascuns, Hidden Web, Invisible Web sau Deepnet), un spațiu din internet ascuns, pentru care sunt necesare anumite acreditări și logări, precum și Darknet-ul (Internetul întunecat, Dark Web, exemple de site-uri de acest gen a se vedea pe http://deepweblinks.org/ [223]), o rețea peer-to-peer, în care fiecare utilizator se conectează direct la alt utilizator. Printre cele mai „celebre" Darknet-uri sunt Freenet și TOR [122, p. 112]. Există mai multă literatură online cu privire la specificul și tehnicile de investigare a Darknet-ului [224, 225], Deepweb-ului [226, 227, 228], TOR-ului [229] etc.

Personalitatea victimei în cazul infracțiunilor informatice

Un rol deosebit în structura caracteristicii criminalistice îl joacă studiul personalității victimei. Informația despre victimă este importantă din punct de vedere criminalistic, deoarece contribuie la caracterizarea personalității infractorului, la stabilirea motivelor lui, la limitarea cercului de suspecți.

Victimele infracțiunilor informatice pot fi divizate în trei categorii de bază: proprietarii sistemelor, ai rețelelor sau datelor informatice; clienții, care utilizează serviciile acestora, precum și alte persoane. Victimele infracțiunilor informatice, îndeosebi cele din prima categorie, de cele mai multe ori, ezită să comunice organului de urmărire penală despre fapta comisă, din următoarele temeri și îngrijorări: că angajații organelor de drept nu sunt suficient de competenți în domeniul dat; că cheltuielile de investigație vor depăși suma prejudiciului cauzat și va avea de suferit imaginea companiei; că ca fi divulgat, în cadrul examinării judiciare, sistemul de organizare a securității companiei; că organul de urmărire penală va stabili și ilegalități comise de

către însăși victimă; că în rezultatul investigațiilor se va constata incompetența profesională a angajaților; în sfârșit, din cauza insuficienței culturii juridice și altele [92, p. 907].

În literatura de specialitate [48, p. 33] se opinează că victimă a infracțiunii informatice, de cele mai multe ori, devine persoana juridică (72%) [73, p. 31]. Totuși, dată fiind computerizarea masivă a vieții private, se remarcă o tendință de echilibrare a numărului de persoane fizice și juridice, victime ale acestor categorii de infracțiuni.

Băncile comerciale, de regulă, sunt afectate din motive de cupiditate a infractorilor informatici, care, de cele mai multe ori, sunt angajații proprii ai instituției financiare, persoanele care cunosc bine structura instituției sau cele care fac uz de situația de serviciu [73, p. 31-32].

Criteriul de bază, care caracterizează victima, este insuficiența cunoștințelor fundamentale în domeniul securității informatice sau disciplina scăzută a angajaților. De multe ori, chiar acțiunile victimei determină implicarea sa într-o infracțiune.

Potrivit legislației naționale, victimă a infracțiunii informatice poate fi orice persoană fizică sau juridică (inclusiv statul), care este proprietarul, posesorul sau utilizatorul informației computerizate, al sistemului [37, p. 843] sau al rețelei informatice, al datelor informatice interceptate, parolelor sau codurilor de acces etc.; poate fi persoana al cărui patrimoniu a fost prejudiciat [41]; ISP; minorul care fie că este implicat în activități sexuale explicite, reale sau simulate, fie că îi sunt reprezentate organele sexuale într-o manieră lascivă sau obscenă, inclusiv în formă electronică; titularul dreptului de autor și/sau al drepturilor conexe; autorul sau succesorul proprietății industriale; solicitantul protecției obiectului de proprietate intelectuală.

În corespundere cu Legea cu privire la informatizare și resursele informaționale de stat [145], *proprietarul sistemului sau rețelei informaționale* este o persoană fizică, persoană juridică sau statul, care exercită integral dreptul de posesiune, folosință și dispoziție asupra resurselor și sistemelor informaționale, tehnologiilor și mijloacelor de asigurare a acestora; *posesorul* este o persoană fizică, persoană juridică sau statul, cu drept de posesiune și folosință asupra resurselor și sistemelor informaționale, tehnologiilor și mijloacelor de asigurare a acestora, în condițiile stabilite de titularul drepturilor respective; *utilizatorul* este o persoană fizică sau persoană juridică ce efectuează acțiuni de prezentare, primire, păstrare și alte acțiuni de utilizare a informației documentate în sistem informațional automatizat.

Un prejudiciu material considerabil, cauzat de criminalitatea informatică, este adus relațiilor din domeniul financiar-bancar, îndeosebi serviciilor bancare la distanță, a căror clasificare este redată în Anexa nr. 6 din prezenta lucrare. Totodată, în dependență de tipurile mijloacelor electronice de plată, utilizate de către clienții băncilor, sistemul serviciilor bancare la distanță, tradițional, se divizează în felul următor [86, p. 22]:

1) *sistemul „Bancă-client”* – presupune utilizarea de către clientul băncii („clientul gras”) a unui produs program, pus la dispoziție de către bancă și instalat în sistemul informatic al clientului;

2) *sistemul de Internet banking* – vizează administrarea contului și efectuarea operațiunilor prin intermediul site-ului băncii, cu ajutorul unei interfețe web, setată pentru fiecare client („clientul slab”); este cel mai utilizat sistem de plată electronică la distanță, dar și cel mai des afectat din punct de vedere al fraudelor informatice;

3) *sistemul de banking mobil* – preconizează utilizarea de către clientul băncii a unui produs program, instalat pe telefonul său mobil, fiind folosite rețelele de comunicații electronice;

4) *tehnologia serviciilor bancare la distanță cu utilizarea dispozitivelor de autodeservire bancară* – bancomate, terminale de plată și chioșcuri.

Deși în textul Convenției privind criminalitatea informatică este utilizat termenul de „minor”, la implementarea acesteia în legislația penală a RM a fost introdusă noțiunea „copil”. În lipsa unei definiții în lege, nu este clar dacă acești doi termeni sunt identici. Totodată, CPP definește expresia de „persoană minoră” ca desemnând persoana care nu a împlinit vârsta de 18 ani, similar art. 9 pct. 3 din Convenție [212, p. 245].

Totodată, Convenția stabilește că termenul *materiale pornografice* având ca subiect copiii desemnează orice material pornografic, care reprezintă într-un mod evident: un minor care se dedă unui comportament sexual explicit; o persoană majoră, prezentată ca o persoană minoră, care se dedă unui comportament sexual explicit; imagini realiste reprezentând un minor care se dedă unui comportament sexual explicit. Cu toate că, la ratificarea Convenției în cauză, RM nu a înaintat vreo rezervă în această privință, ultimele două situații nu au fost reflectate în legislația națională.

În afară de aceasta, stabilirea faptului dacă imaginile sunt reprezentate de manieră lascivă sau obscenă (spre deosebire de materialele erotice) este pusă în sarcina Agenției de Stat pentru protecția moralității de pe lângă Ministerul Culturii, conform pct.8 lit.g) din Regulamentul Agenției [230].

Urmele tipice (probele electronice) în cazul infracțiunilor informatice

După cum menționează Iu.V. Gavrilin și V.V. Șipilov, probatoriul în cazul infracțiunilor informatice este specific și de aceea este necesară elaborarea unor metode și mijloace criminalistice noi. Urmele acestor categorii de infracțiuni trebuie divizate în două tipuri:

1) *urme tradiționale* (urmele ideale, urme-substanțe, urme-obiecte) și

2) *netradiționale*, reprezentând probele electronice [231], care mai sunt numite în literatura de specialitate și *virtuale* [73, p. 57, 181, p. 73, 68, p. 184].

La prima categorie sunt atribuite urmele de mâini, picioare, particule de piele, alte urme biologice, urme traseologice (ale instrumentelor de spargere), documente, înregistrări ale sistemelor de monitorizare video, metadatele (datele care descriu alte date) convorbirilor telefonice etc. Ele se pot forma în procesul activității membrilor grupului criminal în mediul extern [232, p. 653, 233, p. 33], depistându-se, fixându-se se ridicându-se prin metode criminalistice tradiționale [234, p. 81, 235]. Așa-numitele *probe electronice*, care sunt atribuite la a doua categorie, se produc în mediul informatic și reprezintă rezultatul transformării informației computerizate în urma ștergerii, copierii, blocării, modificării sau a oricărei alte intervenții în funcționarea mijloacelor de stocare, prelucrare sau transmitere a datelor informatice, a rețelei de comunicații electronice sau informatice [86, p. 112].

La rândul lor, probele electronice pot fi divizate și ele în două subcategorii [73, p. 60]:

a) *locale*, formate pe suporturi electronice, cum ar fi discurile solide (Hard Disk) [21], discurile optice (CD, DVD, BD), cartelele de memorie (Secure Digital Card – SD, Micro SD Card, Compact Flash Card), stickurile USB, discurile cu bandă magnetică, dispozitivele periferice (fax, scanner, imprimantă, cameră web, mașină de calcul și control, cititor de carduri), telefoanele mobile, aparatele audio, video și foto, consolele de jocuri și alte dispozitive electronice (cipuri, tochen, GPS, ceasuri electronice). La etapa incipientă a procesului penal, urmele electronice locale din dispozitivele victimei sunt probele cele mai importante și mai accesibile [49, p. 15, 18-22].

b) *de rețea*, constituite pe suporturile sistemelor informatice și ale altor dispozitive de comunicații electronice (Port, MAC, Bandwidth, Network Attached Storage, Network Interface Controller, Network Hub, Network Switch, Router, Server, Firewall, Access Point), utilizate pentru conectarea la rețeaua informatică locală (LAN) și globală (WAN). În această subcategorie se includ și datele deținute de către ISP, de hosting (calculator conectat la o rețea și care pune la dispoziție altor calculatoare din rețea unele resurse ale sale), de telefonie, operatori de transferuri ale mijloacelor bănești [44, p. 4], precum și din resursele internet [77, p. 7-8]. Analiza practicii arată că cele mai multe infracțiuni informatice sunt comise prin Internet (65%) [73, p. 61].

Potrivit *Ghidului introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică*, probele digitale sunt informații cu valoare doveditoare pentru organele judiciare, care sunt stocate, prelucrate sau transmise prin intermediul unui sistem informatic [149, p. 74]. Ele cuprind probe informatice, probe audio digitale, cele produse sau transmise prin telefoane mobile, faxuri digitale etc. Una din particularitățile acestor categorii de probe este că, aparent, ele nu sunt evidente, fiind conținute în echipamente informatice [29, p. 210, 236], și nu sunt obiecte tangibile [237, p. 683].

Probele electronice posedă următoarele caracteristici criminalistice:

- sunt practic invizibile unui simplu utilizator și, de regulă, pot fi colectate, analizate și interpretate doar de către un specialist în domeniu [122, p. 12, 49, p. 2-3, 44, p. 7, 31, p. 42], cu instrumente criminalistice specifice;
- pot fi modificate sau distruse, neintenționat, prin utilizarea sistemului (spre exemplu, suprascrierea datelor, deconectarea calculatorului) [122, p. 12, 49, p. 2, 31, p. 41];
- pot fi copiate nelimitat, cu ușurință, pe diverse dispozitive electronice și transmise rapid la orice distanță [89, p. 19, 122, p. 12, 49, p. 6];
- își schimbă foarte ușor forma [82, p. 13, 75, p. 6];
- în cazul ridicării (copierii) informației computerizate, spre deosebire de obiectele materiale, aceasta poate rămâne și pe suportul original [89, p. 19, 75, p. 6];
- sunt volatile, adică, în timp, devin din ce în ce mai dificil de obținut, iar uneori, practic imposibil [238, p. 1, 122, p. 12, 49, p. 6, 31, p. 42];
- în majoritatea cazurilor, prezintă o anumită valoare și constituie obiect de vânzare-cumpărare [89, p. 19, 75, p. 6].

Deși între probele electronice și cele tradiționale există o diferență esențială, totuși lor li se aplică aceleași reguli procesuale privind admisibilitatea, administrarea și aprecierea [122, p. 150].

În concluzie, putem menționa că probele electronice sunt informații cu valoare doveditoare, fiind stocate, prelucrate sau transmise prin intermediul unui sistem informatic. Ele se produc în mediul informatic și reprezintă rezultatul transformării informației computerizate în urma ștergerii, copierii, blocării, modificării sau a oricărei alte intervenții în funcționarea mijloacelor de stocare, prelucrare sau transmitere a datelor informatice sau a rețelei de comunicații. Printre particularitățile acestor categorii de probe se înscriu și cele care demonstrează că, aparent, ele nu sunt evidente, sunt volatile, conținându-se în echipamente informatice, și nu sunt obiecte tangibile.

2.3. Situațiile tipice de urmărire penală și versiunile criminalistice

Situațiile tipice de urmărire penală

Prin *situația de urmărire penală* se înțelege starea de fapt: circumstanțele reale în care acționează organul de urmărire penală într-un moment concret al cercetării, circumstanțele ce determină o anumită ordine și un anumit mod de acțiune în scopul realizării cu succes a sarcinilor trasate [10, p. 312]. Noțiunea de *situație de urmărire penală*, în prezent, se bucură deja de o stabilitate reală în criminalistică și treptat începe să influențeze luarea deciziilor într-un șir mai mare de probleme științifice și practice [10, p. 314].

Printre legitățile activității criminalistice de descoperire și cercetare a infracțiunilor se înscrie și apariția și repetarea permanentă a *situațiilor tipice de urmărire penală*, ce denotă caracterul situațional al cercetării diverselor infracțiuni [7, p. 96], din care nu fac excepție nici cele din domeniul informaticii.

Drept urmare, atât în tactica criminalistică, cât și în metodica de cercetare a infracțiunilor din domeniul informaticii, un rol important le revine situațiilor tipice de urmărire penală.

Situațiile tipice constituie începutul (baza) tacticii de urmărire penală și al metodicii de cercetare, care corespund într-un mod mai complet cerințelor actuale ale practicii de combatere a fenomenului infracțional [10, p. 316].

Alegerea unei anumite acțiuni de urmărire penală ține de competența organului de urmărire penală, care, de regulă, se conduce de situația concretă a investigației [103, p. 689].

Astfel, la cercetarea infracțiunilor informatice pot fi relevate patru situații tipice [89, p. 53, 239, 48, 60, p. 684, 56, p. 691, 92, p. 907-908]:

1) Proprietarul, posesorul sau utilizatorul legal al informației computerizate (datelor informatice), al sistemului sau rețelei informatice, al transmisiei de date informatice, al canalului sau serviciului de comunicații electronice a descoperit de sine stătător încălcarea integrității, accesibilității, inviolabilității sau confidențialității acestora, a identificat făptuitorul și a denunțat infracțiunea;

2) Proprietarul, posesorul sau utilizatorul legal al informației computerizate (datelor informatice), al sistemului sau rețelei informatice, al transmisiei de date informatice, al canalului sau serviciului de comunicații electronice a descoperit de sine stătător încălcarea integrității, accesibilității, inviolabilității sau confidențialității acestora, dar nu a identificat făptuitorul, denunțând infracțiunea la organele de drept;

3) Încălcarea integrității, accesibilității, inviolabilității sau confidențialității informației computerizate (datelor informatice), a sistemului sau rețelei informatice, a transmisiei de date informatice, a canalului sau serviciului de comunicații electronice și făptuitorul infracțiunii au devenit cunoscute publicului larg sau au fost descoperite nemijlocit de către organele de drept;

4) Încălcarea integrității, accesibilității, inviolabilității sau confidențialității informației computerizate (datelor informatice), a sistemului sau rețelei informatice, a transmisiei de date informatice, a canalului sau serviciului de comunicații electronice au devenit cunoscute publicului larg sau au fost descoperite nemijlocit de către organele de drept, dar nu este cunoscut făptuitorul infracțiunii.

În dependență de situația tipică, la etapa inițială a procesului penal, organul de urmărire penală va întreprinde acțiuni de urmărire penală și măsuri speciale de investigații specifice.

Mijloace eficiente în lupta cu criminalitatea sunt evidențele criminalistice, care presupun un sistem științific argumentat de fixare, clasificare, sistematizare, păstrare și folosire a datelor referitoare la persoanele și obiectele ce au importanță criminalistică și pot fi folosite în scopul clarificării circumstanțelor cazurilor penale [240, p. 119].

În prezent, organele de drept nu dispun de vreo bază de date centralizată privind informația operativă în cauzele de criminalitate informatică [241, 242, p. 132]. În vederea asigurării informaționale și analitice a organelor care efectuează activitatea specială de investigații, este rezonabil ca o astfel de bază de date să conțină informații cu privire la [86, p. 125]:

- toate operațiunile de plată electronică frauduloase (reușite și nereușite);
- conturile (bancare, telefonice, electronice) care au avut legătură directă cu infracțiunile informatice, inclusiv ale victimelor, de buffer și pentru lichefierea mijloacelor bănești;
- persoanele implicate în aceste infracțiuni;
- adresele IP prin intermediul cărora au fost efectuate conexiunile în procesul de pregătire, săvârșire și ascundere a infracțiunii (și anume ale serverelor și sistemelor informatice utilizate la gestionarea centrelor de control al botnetului, la răspândirea virușilor, la accesarea neautorizată a informației computerizate și altele);
- numele de domeniu (un șir de caractere care corespund unei adrese IP numerice, aferente unui server conectat permanent la Internet) ale site-urilor utilizate la pregătirea și comiterea infracțiunii;
- numerele de telefon, adresele poștelor electronice, conturile din softurile de comunicare rapidă, adresele MAC ale dispozitivelor ș.a., având legătură directă;
- viruși, botneturi etc.;
- subdiviziunile organelor de drept care au efectuat investigațiile, instituțiile de expertiză care au examinat sistemele și rețelele informatice.

Pe lângă datele textuale formalizate, baza de date ar trebui să preconizeze și posibilitatea de a salva date media: texte, imagini, înregistrări video și audio, documente electronice de orice gen: spre exemplu, fișiere de tip log ale dispozitivelor de rețea și ale sistemelor informatice; înregistrări video și imagini foto de la bancomate; capturi de ecran efectuate cu produsele program, destinate pentru comiterea infracțiunii; copii ale documentelor scanate ale dropilor; concluzii ale specialiștilor și experților în urma efectuării constatărilor și expertizelor judiciare; copii ale produselor program, destinate pentru comiterea infracțiunii și ale codurilor; copii offline ale paginilor web; chei electronice și certificate etc.

Utilizarea unor astfel de date va permite identificarea conexiunilor dintre infracțiuni, săvârșite în diferite locuri, stabilirea legăturilor dintre diferite persoane, fapte și circumstanțe, chiar în baza unor semne minore.

Desigur, va fi necesară și respectarea condițiilor prevăzute de Legea privind protecția datelor cu caracter personal [243] și de Legea cu privire la registre [244], inclusiv cu notificarea la Centrul Național pentru Protecția Datelor cu Caracter Personal a bazei de date respective, în cadrul căreia urmează a fi prelucrat un volum mare de date cu caracter personal.

Modelarea electronică criminalistică permite soluționarea problemelor legate de analiza criminalistică a unui obiect complex sau voluminos [92, p. 906], având drept scop, inclusiv, punerea în aplicare a tuturor activităților criminalistice la un nivel tehnologic avansat.

Versiunile în cazul infracțiunilor informatice

Primul savant care a abordat problematica aplicării de către organul de urmărire penală a raționamentelor logice, a regulilor de elaborare și de verificare a versiunilor a fost E. Annuschat, în anul 1927, în lucrarea sa *Arta descoperirii infracțiunii și legile logicii* [7, p. 41].

Variantele posibile, în care infracțiunile și împrejurările acestora pot fi înfățișate, în baza datelor deținute la o anumită etapă de cercetare și care urmează a fi verificate, sunt numite *versiuni de urmărire penală* [8, p. 284].

Versiunea criminalistică, în accepția criminalistului autohton M. Gheorghiță, înseamnă explicația verosimilă referitor la natura, conținutul, unele circumstanțe ale actului infracțional, modul de comitere și acoperire, participanții, forma de vinovăție, mobilul și scopul urmărit, cauzele care au favorizat săvârșirea infracțiunii, bazate pe datele administrate în cauză [10, p. 322], aceasta fiind o teorie bine elaborată în știința criminalistică [245, p. 4].

În monografia *Drepturile Persoanei în probatoriul penal,* savantul autohton, I. Dolea vorbește și despre noțiunea prezumției de fapt, care nu poate fi confundată cu versiunea. Prezumția de fapt este o generalizare aplicabilă ca punct de reper (o regulă generală) la cercetarea anumitor situații tipice. Versiunea, la rândul ei, se întemeiază pe această regulă, în toate cazurile fiind însă concretă și luându-se în considerare circumstanțele cauzei concrete [246, p. 123].

Așadar, activitatea de elaborare a versiunilor este însoțită de crearea unor explicații presupuse despre faptă în ansamblu (versiuni generale) sau despre anumite circumstanțe ale faptei cercetate (versiuni particulare) [247, 10, 9].

Drept urmare, în cadrul cercetării infracțiunilor informatice, structura dinamică a etapei de formulare a versiunilor de către organul de urmărire penală trebuie să parcurgă mai multe etape:

1) cercetarea tuturor informațiilor relevante, administrate în cadrul urmăririi penale;

2) stabilirea circumstanței/circumstanțelor necunoscute;

3) identificarea și unificarea problemelor și situațiilor;

4) formarea bazei *de facto* a versiunilor criminalistice din informația probatorie relevantă, grupată în jurul circumstanțelor nestabilite;

5) formarea bazei teoretice a versiunilor din sursele de informații suplimentare (spre exemplu: datele despre caracteristicile criminalistice ale acestei categorii de infracțiuni, experiența personală și colectivă a conducătorilor și colaboratorilor etc.);

6) formularea versiunilor cu ajutorul bazelor faptice și teoretice.

Pot fi relevate câteva subsisteme ale versiunilor tipice [83, p. 104]:

I. Versiunile cu privire la fiecare faptă (episod) de infracțiune informatică.

1) Versiuni generale:

- a avut loc o infracțiune informatică în circumstanțele comunicate de denunțător;
- a avut loc o infracțiune informatică în alte circumstanțe decât cele comunicate de către denunțător;
- a avut loc altă infracțiune săvârșită cu utilizarea sistemelor și rețelelor informatice;
- a avut loc o înscenare a unei infracțiuni informatice.

2) Versiuni particulare, cu privire la:

- pregătirea comiterii infracțiunii informatice;
- modalitatea săvârșirii infracțiunii;
- săvârșirea infracțiunii de către un grup de persoane, acțiunile acestora până și după comiterea infracțiunii, particularitățile distribuirii rolurilor;
- caracterul instrumentelor și mijloacelor utilizate;
- ascunderea urmelor infracțiunii;
- locul comiterii faptei;
- timpul și împrejurările săvârșirii infracțiunii;
- particularitățile comportamentului victimei, al martorilor oculari până la, în timpul și după comiterea infracțiunii.

II. Versiunile cu privire la diferite episoade ale infracțiunii informatice, săvârșite de către același grup criminal organizat:

1) Versiuni referitoare la aria de acțiune a grupului criminal organizat:

- într-o localitate din RM;
- în diferite localități din RM;
- pe teritoriul a două sau mai multe state.

2) Versiuni ce țin de implicarea grupului criminal organizat (a membrilor lui) în săvârșirea altor infracțiuni:

- care deja se investighează – la nivel local sau regional – de către subdiviziunile MAI;
- care deja se investighează de către alte organe de urmărire penală (CNA, SV Procuratură);
- ale căror semne încă nu au fost descoperite de către organele de drept;
- descoperite în anii precedenți;
- nedescoperite în anii precedenți.

III. Versiunile cu privire la componența și caracteristicile grupului criminal organizat:

- identitatea organizatorului, a autorului și complicilor, precum și locul aflării acestora;
- momentul creării grupului criminal organizat;
- numărul membrilor activi;
- specialiștii care participă nemijlocit în procesul de utilizare a sistemelor și rețelelor informatice.

IV. Versiunile cu privire la etapa de pregătire a infracțiunii informatice:

- referitoare la obținerea (procurarea, crearea) sistemelor și rețelelor informatice, a mijloacelor de comunicație, a transportului, a surselor și modalităților de plată a traficului de rețea ș.a.;
- referitor la influențarea participanților la proces, în vederea împiedicării investigării normale, precum și consecințele acesteia.

V. Versiunile cu privire la existența altor surse de informație probatorie relevantă neidentificată, și anume privind:

- existența martorilor oculari și a altor martori ai infracțiunii cercetate sau a altor activități infracționale ale grupului criminal organizat și locul aflării acestora;
- existența într-un anumit loc (inclusiv în rețea sau în sistemul informatic, în purtătorii de informație electronică) a urmelor infracțiunii;
- existența la o anumită persoană a probelor materiale și a documentelor relevante pentru justa soluționare a cauzei.

VI. Versiunile cu privire la circumstanțele (cauzele și împrejurările) care au favorizat săvârșirea infracțiunii, și anume:

- referitoae la crearea și activitatea grupului criminal organizat;
- cu privire la săvârșirea altor categorii de infracțiuni.

Pe lângă versiunile specifice analizate *supra*, mai pot fi amintite și versiunile legate de personalitatea infractorului, de circumstanțele în care a fost comisă fapta, de mărimea prejudiciului cauzat etc. [248, p. 624]

Următoarea etapă presupune verificarea versiunilor înaintate prin efectuarea acțiunilor de urmărire penală, inclusiv a acțiunilor speciale de investigații, și constă în:

- deducerea din fiecare versiune criminalistică pe caz a tuturor acțiunilor posibile;

- luarea deciziilor tactice;

- realizarea practică a planului urmăririi penale în vederea obținerii datelor care confirmă sau infirmă versiunile;

- aprecierea tuturor probelor administrate, în baza concluziilor referitoare la caracterul autentic sau fals al versiunilor verificate.

Specific pentru procesul penal cu privire la cercetarea infracțiunilor informatice (în sens restrâns) este faptul că, în conformitate cu prevederile art.276 CPP, pentru pornirea urmăririi penale nu este necesară plângerea prealabilă a victimei, cu excepția infracțiunilor prevăzute la art.185^2 (Încălcarea dreptului asupra obiectelor de proprietate industrială) și la art.185^3 CP (Declarații intenționat false în documentele de înregistrare ce țin de protecția proprietății intelectuale).

Pe parcursul anului 2017, din cele 127 de sesizări cu privire la săvârșirea infracțiunilor informatice, a fost dispusă urmărirea penală în 113 cazuri. Astfel, au fost emise 14 ordonanțe de refuz în pornirea urmării penale: în 6 cazuri (43%) – pe motivul unor pretinse fapte de fraudă informatică (art.260^6 CP); în 5 cazuri (36%) – pe motivul încălcării inviolabilității vieții personale (art.177 CP) și în câte un caz (câte 7%) – pe motivul încălcării dreptului asupra obiectelor de proprietate industrială (art.185^1 CP), pe motivul fabricării sau punerii în circulație a cardurilor sau a altor instrumente de plată false (art.237 CP), precum și pe motivul accesului ilegal la informația computerizată (art.259 CP). Motivele care au stat la baza emiterii ordonanțelor de refuz au fost: în 8 cazuri (57%) – că fapta nu întrunește elementele infracțiunii; în 5 cazuri (36%) – că există alte circumstanțe prevăzute de lege care condiționează excluderea sau, după caz, exclud urmărirea penală și 1 caz (7%) – că nu există faptul infracțiunii. Articolele din CP, în baza cărora a fost pornită urmărirea penală, sunt expuse în Anexa nr. 1 din prezenta lucrare [249].

2.4. Măsuri tactice și strategice de depășire a obstacolelor care împiedică buna desfășurare a cercetării infracțiunilor informatice

Apărută la începutul anilor '90, teoria învingerii împotrivirii urmăririi penale ține de criminalistică și este inclusă în această știință ca o doctrină particulară. La elaborarea ei au contribuit mai mulți criminaliști (R. Belkin și alții) [250].

Activitatea organelor de urmărire penală, de cele mai multe ori, se complică prin faptul că infracțiunile sunt comise deseori de persoane care au anumite cunoștințe din diverse surse și unele deprinderi criminale, bunăoară, cum sunt cele specifice IT, iar săvârșirea infracțiunii, de regulă, e

precedată de o pregătire minuțioasă. În virtutea acestui fapt, realizarea eficientă a sarcinilor cercetării reclamă din partea organelor de urmărire penală și a celor speciale de investigații o înaltă *măiestrie tactică*, care, la rândul ei, reprezintă un sistem de teze generale și procedee/recomandări argumentate științific [251, p. 8], bazate pe dispozițiile legii procesual-penale și pe practica în domeniu, a căror aplicare e menită să asigure eficacitatea/comportarea [8, p. 266] activității organelor de drept în timpul cercetării faptelor infracționale și examinării acestora în instanța de judecată, ținând cont de particularitățile și de situațiile în care infracțiunea a fost comisă [10, p. 291].

Una din sarcinile de bază ale cercetării criminalității informatice este stabilirea tuturor circumstanțelor săvârșirii infracțiunii. Totuși la realizarea acesteia deseori se opun persoanele care doresc ca infractorul să se eschiveze de la răspunderea penală.

În dependență de factorii ce condiționează apariția obstacolelor care perturbă desfășurarea normală a procesului penal, acestea pot fi clasificate în [80, p. 13]:

1) *obiective*, care apar și acționează independent de voința persoanei (spre exemplu, condițiile meteorologice nefavorabile, care au favorizat distrugerea urmelor infracțiunii);

2) *subiective*, create de către făptuitor, de către alte persoane în interesele acestuia, precum și de greșelile/omisiunile organului de urmărire penală;

3) *relativ obiective*, care nu depind de voința anumitor persoane, însă pot fi luate în calcul de către acestea. Drept exemplu pot fi invocate particularitățile suporturilor de stocare a datelor electronice, care stau la baza distrugerii informației.

Totodată, impedimentele care apar la investigarea infracțiunilor comise pot fi clasificate în *legale* (dreptul bănuitului/învinuitului de a nu da declarații, dreptul părților de a înainta cereri și demersuri, lipsa răspunderii bănuitului/învinuitului în cazul depunerii declarațiilor false, obligația organului de urmărire penală de a verifica versiunile apărării) și *ilegale* (declarațiile false ale martorilor, victimei). Cele legale, la rândul lor, pot fi *vădite,* spre exemplu, refuzul de a da declarații, și *camuflate,* în care suspectul își manifestă dorința de a contribui la stabilirea adevărului pe caz și disponibilitatea de a acorda ajutorul necesar organului de urmărire penală, dar intenția sa adevărată este de a direcționa urmărirea penală pe o pârtie greșită. Impedimentele camuflate reprezintă o cursă periculoasă pentru organul de urmărire penală.

De cele mai multe ori, declarații false sunt depuse de către bănuit/învinuit (72%), martori (18%), victimă (10%). Această situație se datorează strategiei de comportament, alese de către infractor, posibilităților lui, precum și specificului infracțiunii investigate [80, p. 26]. În majoritatea cazurilor, în cadrul audierii sale, bănuitul/învinuitul va tatona nivelul cunoștințelor în domeniul IT a persoanei care îl audiază, ulterior, în baza acestei informații, el se va prezenta drept

o persoană insuficient de capabilă pentru utilizarea sistemelor informatice sau pentru a avea intenții infracționale.

Spre exemplu, Apărarea Cal Troian urmărește aplicarea regulii „in dubio pro reo" în calitate de complement al prezumției de nevinovăție, contestând identificarea făptuitorului și având în practica judiciară șanse de succes doar în măsura înțelegerii de către practicieni și instanțe a realităților societății digitale, mai cu seamă în cauzele în care trimiterea în judecată s-a făcut exclusiv pe baza probelor digitale incriminatoare, prelevate din sistemul informatic al suspectului ori inculpatului (de exemplu, fotografii cu minori în ipostaze sexuale explicite) și fără a adresa corespunzător și a elimina aspectele privind un eventual control de la distanță asupra sistemului informatic ori privind virușii existenți care ar fi putut comite fapta în mod automatizat, precum și în cauzele în care percheziția informatică nu este completată și de alte procedee probatorii, precum supravegherea operativă, documentarea profilului persoanei investigate, operațiuni financiare în legătură cu fapta și altele similare, menite a-l plasa pe inculpat „la tastatură" în momentul comiterii faptei ori a proba distinct fapta sub aspectul laturii subiective, așa cum o indică, de altfel, manualele de bune practici în cercetarea infracțiunilor de criminalitate informatică [252, p. 168, 253, p. 162].

Scopul cererilor și al demersurilor părții apărării, de regulă, este de a impune versiunea ei, prezentând faptele suspectului ca fiind inofensive, și, totodată, de a supraîncărca organul de urmărire penală cu un volum mare de informație, pentru a-l dezorienta. Doar examinarea acestora, în vederea admiterii sau respingerii lor, răpește mult timp și sustrage organul de drept de la activitatea de bază a investigației. O altă tehnică aplicată constă în derutarea organului de urmărire penală prin terminologie, precum și prin procesele utilizate în sisteme informatice, înaintându-se, în acest scop, demersuri cu privire la efectuarea diferitor expertize.

Ascunderea urmelor infracțiunii este urmărită nu doar prin distrugerea informației computerizate; în același scop poate fi efectuată blocarea sau modificarea informației. În cel din urmă caz, infractorul va orienta investigarea într-o direcție greșită [254, p. 3]. Această metodă este cea mai periculoasă, pentru că infractorul își poate masca identitatea prin modificarea datelor din registrele electronice, prin schimbarea adresei IP, precum și a pachetelor de date, fiind create, astfel, probe false [71, p. 152].

Orice nedescoperire a infracțiunii și neidentificare a făptuitorului acesteia permite infractorului să-și continue activitatea, iar practica negativă îi permite să înțeleagă erorile pe care nu trebuie să le admită la săvârșirea unei infracțiuni analogice.

Influențarea activității de urmărire penală a infracțiunilor săvârșite în domeniul supus analizei, de regulă, urmărește scopurile [80, p. 52, 255, p. 146]:

- de a prezenta infracțiunea săvârșită drept o activitate socialmente nepericuloasă, adică non-penală, comisă din curiozitate;
- de a reda fapta comisă drept o consecință întâmplătoare, fără vreo intenție infracțională, a lipsei unor cunoștințe aprofundate a făptuitorului în domeniul tehnologiilor avansate. Apărarea, prin invocarea nepriceperii utilizatorului, susține, spre exemplu, că acesta nu a avut intenția de a pune la dispoziție materialele ilegale, descărcate prin sistemele de partajare de fișiere [256] și că nu a știut că programul de partajare punea automat la dispoziție în rețea documentele descărcate [257];
- de a demonstra că acțiunile făptuitorului sunt rezultatul unei constrângeri insurmontabile și au fost săvârșite exclusiv în interesul societății;
- de a convinge organul de urmărire penală de onestitatea persoanei suspecte, care, la fel ca și acesta, dorește să stabilească adevărul și, în consecință, să-și confirme nevinovăția;
- de a demonstra părtinirea și rea-credința persoanei care efectuează urmărirea penală, nedorința ei de a stabili toate circumstanțele cauzei;
- de a prezenta suspectul drept o victimă a infracțiunii, datorată evoluției nefavorabile a circumstanțelor cauzei;
- de a argumenta necesitatea efectuării anumitor acțiuni procesuale, în vederea îndreptării procesului penal spre un punct mort;
- de a argumenta inadmisibilitatea efectuării anumitor acțiuni (inclusiv procesuale), pentru ca unele împrejurări ale săvârșirii infracțiunii să rămână neidentificate;
- de a crea impresia incompetenței persoanei care efectuează urmărirea penală (cum ar fi lipsa abilităților de a cerceta o cauză complexă);
- de a crea o opinie publică pozitivă despre suspect.

La cercetarea infracțiunilor informatice, cele mai răspândite forme de opunere de rezistență sunt [255, p. 146]:

1) *Tăinuirea infracțiunii și a probelor* (63%). În jumătate din cazurile de infracțiuni informatice, infractorii tind să-și concentreze eforturile pe crearea obstacolelor în vederea ridicării și cercetării suporturilor de stocare a informației electronice. În acest scop, recurg la substituirea suporturilor respective, pentru a crea impresia, la examinarea acestora, că nu a fost săvârșită infracțiunea.

Una din cauzele reușitei activității de opunere a rezistenței contra descoperirii infracțiunilor informatice este latența sporită a acestor categorii de infracțiuni. Numeroase acțiuni din domeniul IT, precum și datele informatice pot fi ușor depersonalizate. Totuși datele informatice nu sunt lipsite de anumite semne care să le individualizeze. Încă de la etapa pregătirii infracțiunii,

făptuitorul întreprinde măsuri pentru ca aceasta să nu fie identificată, cercetată și descoperită [54, p. 161]. Baza informațională este foarte complicată pentru citire, de regulă, necesită decodificare și doar după aceasta poate fi utilizată în investigație.

2) *Înscenarea* (27%). Cele mai răspândite înscenări în cazurile de criminalitate informatică sunt:

- simularea faptului că informația a fost afectată în rezultatul utilizării proaste a acesteia de către persoanele care aveau drept de acces la ea;
- virusarea din neatenție de către persoanele care aveau drept de acces la informația computerizată;
- defecțiunea suportului de stocare a informației electronice, sub pretextul unor motive independente de voința persoanelor;
- imitarea unei alte fapte prejudiciabile, pentru a sustrage atenția organului de urmărire penală [71, p. 152].

„Hackerii", care au abilități tehnice și profesionale mai bune decât alte categorii de infractori informatici, preferă utilizarea înscenărilor, iar în unele cazuri și a tăinuirii infracțiunii.

3) *Formarea unei opinii publice favorabile infractorului* (3%). Aceasta se realizează nu doar prin utilizarea mijloacelor tradiționale de informare în masă (periodice, televiziune și radio), dar și prin publicații în rețeaua internet. Ea este caracteristică persoanelor care încalcă regulile de exploatare a sistemelor și rețelelor informatice.

4) *Influențarea directă a organului de urmărire penală* (7%). Organele de drept sunt învinuite pe nedrept în depășirea atribuțiilor de serviciu, în efectuarea defectuoasă a urmăririi penale și altele. De regulă, partea apărării contestă pe toate căile posibile (la procuror, la procurorul ierarhic superior, la judecătorul de instrucție etc.) legalitatea, temeinicia și corectitudinea efectuării acțiunilor procesuale, în ideea că un alt reprezentant al organului de urmărire penală, cunoscând cauzele înlăturării de la efectuarea urmăririi penale a colegului său, va fi mai cooperant cu partea apărării și va accepta mai ușor propunerile acesteia referitor la desfășurarea procesului penal.

5) *Șantajarea victimei* are loc prin începerea/continuarea atacurilor cibernetice asupra resurselor ei informatice, prin răspândirea informațiilor confidențiale despre ea, care i-ar putea afecta reputația.

În cazul constatării de către apărător a unor greșeli admise de către organul de urmărire penală, această constatare poate avea două finalități: fie că, în cel mai bun caz, avocatul le va arăta organului de urmărire penală, fie că partea apărării va trece sub tăcere erorile admise, până la momentul favorabil pentru ea din punct de vedere tactic, chiar până la cercetarea judecătorească a

cauzei, în speranța folosirii lor pentru a „distruge dosarul” și a obține o sentință de achitare sau de încetare a procesului penal [258, p. 184].

Persoanelor, care creează obstacole la efectuarea investigațiilor cu privire la infracțiunile în domeniul informației computerizate (bănuiți – 61%, învinuiți – 42%, martori – 26%, părți vătămate – 7%, apărători – 21%, alți participanți la proces – 10%), le sunt caracteristice următoarele calități [80, p. 77]:

- au un nivel sporit de rezistență la stres;
- posedă abilitatea de concentrare în situații critice;
- sunt foarte critici în aprecierea situațiilor apărute;
- sunt echilibrați emoțional;
- sunt siguri în capacitățile lor intelectuale;
- au un nivel intelectual înalt.

Printre persoanele care împiedică buna desfășurare a procesului penal sunt: infractorul, apărătorul acestuia, rudele făptuitorului, prietenii, colegii de serviciu, persoanele care au temerea de a nu fi răspândită informația ce le poate afecta imaginea (spre exemplu, în iunie 2011, hackerii au reușit să obțină acces la datele cardurilor bancare a 360 000 de persoane, ceea ce a fost confirmat recent de către oficialii băncii, iar colaboratorii băncii nu au informat despre acest fapt organele de drept timp de trei săptămâni, ceea ce a expus clienții la prejudicii și mai mari) [259].

Este specific faptul că, în ultima perioadă, pentru infracțiunile cercetate în prezenta lucrare, obstacolele în investigarea infracțiunii sunt create de către persoane necunoscute infractorului. Aceasta se referă la *hackeri*, care sunt predispuși să execute, în semn de „solidaritate”, anumite mișcări în internet, în vederea periclitării atragerii la răspundere a altor „colegi de breaslă”.

Printre instrumentele utilizate la crearea piedicilor în fața organului de urmărire penală, caracteristice infracțiunilor informatice, putem releva [255, p. 146]:

- produsele program utilizate la comiterea infracțiunii, care nu lasă urme, le șterg instant și/sau criptează informația [73, p. 63, 11, p. 153-154, 213-228];
- softurile care fac inadmisibilă identificarea persoanei sau utilizarea de servere intermediare, atunci când este imposibilă distrugerea urmelor [11, p. 158, 57, p. 556];
- programele care, în opinia infractorului, nu pot fi identificate de către sistemele de securitate;
- remailers-urile, care reprezintă calculatoare ce primesc mesaje și le redirecționează către adresa electronică de la destinație, ștergând toate datele despre expeditor [57, p. 556];
- datele informatice păstrate la distanță [73, p. 63, 11, p. 156];
- manevrele de distragere a atenției (de exemplu, atacurile cibernetice);

- alte posibilități tehnice de tăinuire a infracțiunii, asigurate cu diverse metode și mijloace (cum ar fi situația în care victimei îi este inconvenabilă atragerea atenției asupra infracțiunii săvârșite, având în vedere faptul că-i poate afecta reputația).

Metodele și mijloacele de învingere a rezistenței opuse trebuie selectate în dependență de caracterul și specificul obstacolelor. În literatura juridică, pentru desemnarea activității organului de urmărire penală, orientate spre învingerea împotrivirii la efectuarea procesului penal, sunt folosiți doi termeni: „neutralizarea obstacolelor" [260, p. 75] și „depășirea obstacolelor" [261, p. 77].

Depășirea obstacolelor în cercetarea infracțiunilor informatice presupune realizarea următoarelor sarcini și măsuri [255, p. 146]:

- asigurarea confidențialității la colectarea informațiilor despre infracțiunea comisă și despre suspecți, despre acțiunile procesuale planificate sau realizate [262, p. 236] (prin limitarea/interzicerea conectării/deconectării la rețeaua internet a sistemelor informatice ce constituie obiectul infracțiunii; prin continuarea activității online a victimei pentru a nu atrage atenția la investigațiile efectuate; prin planificarea cronologiei activităților procesuale, așa încât acțiunile față de persoanele care pot divulga datele investigațiilor să fie realizate în ultimă instanță; prin efectuarea percheziților sau ridicărilor în perioada de timp când poate fi evitată prezența masivă a martorilor; prin supunerea unui controlul permanent a tuturor mesajelor electronice, expediate de către subdiviziunea care efectuează investigația pe caz; prin stabilirea defecțiunilor în sistemul de securitate a informației din sistemele informatice ale victimei, precum și a pericolelor ascunse în sistemele informatice accesate neautorizat);
- colectarea datelor despre persoanele care au acces la documente și care pot întreprinde acțiuni în vederea distrugerii probelor (organul de urmărire penală, precum și judecătorul de instrucție va trebui să ofere cât mai puțină informație despre investigațiile efectuate și persoanele suspecte în actele procesuale care vor fi prezentate persoanelor terțe – ISP, operatorii de telefonie etc.);
- stabilirea informațiilor necesare pentru pornirea urmăririi penale, precum și pe parcursul procesului penal;
- identificarea surselor din care pot fi dobândite probe;
- planificarea efectuării măsurilor speciale de investigații, îndreptate în vederea obținerii informațiilor, care pot fi utilizate la învingerea impedimentelor cu privire la cercetarea cazului. Asemenea date se pot referi la personalitatea infractorului, la persoanele care pot acorda ajutor făptuitorului, la informațiile privind activitățile planificate de către infractorul informatic [80, p. 154];

- colaborarea ofițerului de urmărire penală cu organul care efectuează activitatea specială de investigații, orientarea acestuia în privința informațiilor care trebuie să fie colectate, monitorizarea continuă a activității lui și verificarea corectitudinii informațiilor prezentate [263, p. 240];
- anticiparea posibilelor piedici care pot apărea la colectarea materialelor, precum și a comportamentului infractorului [264, p. 190], planificarea și realizarea acțiunilor de zădărnicire [9] a acestora, inclusiv a măsurilor de ordin tehnic (identificarea softurilor speciale, destinate pentru prevenirea accesului neautorizat la informație, instalarea filtrelor);
- planificarea și efectuarea activităților de depășire a obstacolelor deja existente, cu implicarea specialistului în domeniul IT;
- organizarea și întreprinderea acțiunilor îndreptate în vederea învingerii piedicilor legate de efectuarea urmăririi penale trebuie pusă în sarcina ofițerului de urmărire penală sau a conducătorului acțiunilor grupului de urmărire penală [265, p. 216];
- efectuarea concomitentă a câtorva măsuri procesuale care se dublează, în vederea constatării existenței cazurilor de influențare nepermisă a angajaților organelor de drept și anihilării acestora, identificarea surselor de influențare, stabilirea scopului și sarcinilor acesteia, infiltrarea unor informații false cu privire la activitățile planificate de către suspect, alegerea unei măsuri preventive mai severe;
- efectuarea ridicării sistemelor și dispozitivelor informatice, utilizate la comiterea infracțiunii, chiar la etapa incipientă a procesului penal, aceasta fiind o măsură-cheie, menită să prevină apariția și efectul negativ al obstacolelor la investigație [266, p. 167];
- colectarea probelor suplimentare: organul de urmărire penală trebuie să acorde o atenție sporită identificării făptuitorului real, spre exemplu, în cazul când nu se poate prezuma din simpla prezență a materialelor ilegale în sistemul informatic aparținând suspectului ori inculpatului că acesta se face vinovat de comiterea faptei, în lipsa unor probe suplimentare de altă natură decât informatică [252, p. 168].

Luând în considerare complexitatea și rafinamentul activității de zădărnicire a cercetării infracțiunilor informatice, măsurile de învingere a acestora trebuie să fie organizate minuțios și la cel mai înalt nivel, cu utilizarea operațiunilor tactice [267, p. 295].

În acest sens, de cele mai multe ori, este necesară utilizarea posibilităților tehnice ale sistemelor informatice și ale produselor program pentru blocarea accesului ilegal al persoanelor interesate la informația computerizată, aflată în rețelele informatice.

Operațiunile tactice, specifice acestor categorii de infracțiuni, sunt [80, p. 165]:

- ridicarea purtătorilor de stocare a informației computerizate, în legătură cu care au fost săvârșite faptele ilegale;
- înaintarea acuzării bănuitului și audierea acestuia.

Autorul rus N.A. Ivanov menționează despre „alibiul digital”, și anume, despre activitatea suspectului la calculator în momentul săvârșirii infracțiunii [217]. Practica denotă că stabilirea faptului absenței persoanei bănuite la locul săvârșirii infracțiunii în timpul când s-a produs infracțiunea încă nu înseamnă că persoana respectivă nu are nici o atribuție la fapta săvârșită. Persoana putea să nu apară în calitate de executor nemijlocit al infracțiunii, ci să fie complice al acesteia în calitate de organizator sau instigator. Posibilitățile tehnice moderne, aflate „în serviciul” infractorilor, de exemplu, mijloacele de telefonie mobilă, internet, Skype etc., permit organizatorului infracțiunii să țină sub control situația criminală, să coordoneze acțiunile complicilor, să le dirijeze, pe măsura parvenirii din partea lor a unor semnale urgente, și să elaboreze, în baza analizei lor, indicațiile de rigoare. Înaintarea (declararea) alibiului are ca scop zădărnicirea efortului organului de urmărire penală de a se stabili adevărul în cauză și încercarea de a influența sistemul probatoriu în folosul său.

Tot mai des, bănuiții, când fac referință la „alibiul digital”, îl motivează prin faptul că, în momentul săvârșirii infracțiunii, ei lucrau de la calculatorul personal (sau se foloseau de telefoanele mobile personale, se aflau în perimetrul de observație a camerelor de supraveghere, se conectau la rețelele informatice prin autorizare personală), care, în realitate, se afla în altă parte. Acesta și poate fi numit „alibi digital”. În asemenea cazuri, organul de urmărire penală trebuie să efectueze, înainte de toate, acțiunea tactică de audiere a persoanei care invocă „alibiul digital”. Aici, organul de urmărire penală urmează să stabilească legătura directă între localizarea bănuitului în momentul săvârșirii infracțiunii și sistemul electronic aflat la distanță, în alt loc, făcând loc apariției noțiunii de „urme virtuale” [181, 268]. În astfel de situații, sub incidența urmelor materiale cad amprentele papilare de pe tastatură, urme lăsate de secrețiile sudoripare, etc. Timpul formării acestor urme este extrem de greu de stabilit, din cauza interacțiunii permanente a persoanei cu dispozitivele externe ale sistemului informatic. Urmele ideale rămân totuși a fi în mintea și conștiința persoanei, cea care nemijlocit manipulează cu un sistem informatic concret.

În urma analizei logice a tuturor informațiilor într-un un caz concret, organul de urmărire penală elaborează versiunile:

1) bănuitul (învinuitul) are „alibiu digital”;
2) bănuitul (învinuitul) nu are „alibiu digital”;
3) „alibiul digital” al bănuitului (învinuitului) a fost falsificat.

Atragerea specialistului la identificarea unei sau altei versiuni este indispensabilă. Astfel, organul de urmărire penală poate apela la cunoștințele specialistului în momentul audierii, chiar și la pregătirea întrebărilor care vor fi adresate bănuitului. În timpul audierii, al cercetării la fața locului poate și chiar este indicat să participe specialistul, pentru a explica și a ajuta la identificarea circumstanțelor aferente cazului, la fixarea și ridicarea probelor, precum și la monitorizarea celor relatate de către bănuit, așa încât să se evite dezorientarea organului de urmărire penală. Organul de urmărire penală, în asemenea cazuri, trebuie să determine profilul necesar de cunoștințe speciale ale specialistului pe care îl va atrage în cadrul acțiunilor procesuale, deoarece este imposibil ca respectivul să posede cunoștințe complete în toate domeniile informațiilor computerizate [269].

De asemenea, în procesul de verificare a versiunilor „alibiului digital", organul de urmărire penală va preciza dacă bănuitul real are aptitudini profesionale speciale în domeniul IT (deținerea diplomelor, verificarea notelor obținute, descrierea competențelor și experienței de către colegii de serviciu, stimulările angajatorului, stagiul de lucru, posedă anumite *hobby*-uri în domeniu). În scopuri criminalistice, putem obține „portretul psihologic" și chiar date de identificare (nume, data, anul nașterii), precum și numere de telefoane, adrese electronice ale persoanei care invocă „alibiul digital" din informația plasată de către aceasta în rețeaua internet, și anume, în rețelele sociale (de exemplu, Facebook, Instagram, Odnoklassniki, Vkontakte, etc). Toată această informație este publică, se regăsește în rețeaua internet, ceea ce nu necesită autorizare, facilitând astfel considerabil lucrul organului de urmărire penală.

După demascarea „alibiului fals" (una din formele cele mai răspândite de împotrivire), bănuitului, învinuitului i se propune să relateze obiectiv despre cele săvârșite și rolul lui în infracțiunea cercetată [9, p. 91].

Prin urmare, alibiul este o apărare, prin care se susține imposibilitatea participării la desfășurarea unei activități ilicite a făptuitorului, deoarece el s-ar fi aflat, în perioada de timp când s-a desfășurat activitatea ilicită cercetată, în alt loc, așa încât nu putea face ceea ce i se incriminează, pentru că nu putea fizic să o facă. Pe bună dreptate, alibiul este dovada de nevinovăție constatată că, la data săvârșirii infracțiunii, cel învinuit se afla în altă parte decât la locul săvârșirii [270], însă nu și în cazul infracțiunilor informatice. Infractorul informatic mereu lasă urme, oricât ar încerca să „camufleze" prezența sa în mediul online. Mai mult ca atât, este cunoscută tendința acestuia de a fi recunoscut și de a pretinde un loc mai înalt în ierarhia delincvenților, scop pentru care făptuitorul se laudă cu cele întâmplate/săvârșite în spațiul virtual, pentru a obține „aprecierea" altor delincvenți sau a celor inițiați în domeniul de activitate de care este interesat infractorul informatic.

2.5. Concluzii la Capitolul 2

1. Conceptul de *criminalitate informatică* urmează a fi examinat sub două aspecte, atât în sens larg, cât și în sens restrâns. Astfel, în *sens restrâns,* ea reprezintă totalitatea infracțiunilor săvârșite pe un anumit teritoriu într-o anumită perioadă de timp, îndreptate împotriva relațiilor sociale în domeniul informaticii și al comunicațiilor electronice, a securității statului, minorului, a proprietății intelectuale și drepturilor conexe, a vieții private, secretului corespondenței electronice, precum și a autenticității instrumentelor de plată, comise cu utilizarea sistemelor informatice, răspunderea penală pentru care se stabilește la art.177, 178, 185^1-185^3, 208^1, 237, 259-261^1 și 346 CP.

Criminalitatea informatică în *sens larg* reprezintă ansamblul infracțiunilor săvârșite pe un anumit teritoriu într-o anumită perioadă de timp, îndreptate împotriva relațiilor sociale în domeniul informaticii și comunicațiilor electronice, a securității statului, minorului, a proprietății intelectuale și drepturilor conexe, a vieții private, secretului corespondenței electronice, autenticității instrumentelor de plată, precum și împotriva altor raporturi juridice, în care datele, sistemele și rețelele informatice, serviciile și rețelele de comunicații electronice reprezintă nu doar obiectul faptei prejudiciabile, dar sunt utilizate în calitate de mijloace și instrumente de săvârșire a infracțiunii.

2. Modelul și caracteristica criminalistică a infracțiunilor informatice constituie un sistem vast de informații și concluzii științifice cu privire la urmele tipice, modalitățile și mecanismul de săvârșire a infracțiunii, la personalitatea infractorului, la proprietățile și specificul infracțiunii, la obiectul faptei infracționale, la circumstanțele comiterii infracțiunii, particularitățile motivelor și scopurilor, care asigură optimizarea cercetării și implementarea în practică a mijloacelor și metodelor criminalistice, înaintarea versiunilor criminalistice, identificarea direcțiilor de bază ale urmăririi penale în vederea adoptării unor decizii procesuale legale și întemeiate.

3. Printre cele mai relevante semne caracteristice ale infracțiunilor informatice sunt: legătura cu alte genuri de infracțiuni (îndeosebi, cu criminalitatea organizată și cea economică), caracterul tehnologic avansat, nivelul înalt de latență, caracterul bine organizat, profesional, transfrontalier și transnațional, aceste infracțiuni fiind cele mai dinamice în evoluție, având costuri reduse pentru săvârșire, caracterizându-se prin trăsături politice, extremiste și teroriste.

4. Infractorii informatici sunt persoane cu o flexibilitate înaltă de trecere operativă de la dimensiunea reală la cea virtuală, de la o relație mediată de un spațiu emotiv-fizic la o relație mediată de un spațiu emotiv-artificial, ei se caracterizează printr-o percepție alterată diminuată asupra ilegalității comportamentului lor, a daunei provocate, a riscurilor de a fi denunțați,

descoperiți și sancționați, cu sau fără cunoștințe tehnice în domeniul IT, fiind categorizați în dependență de rolul și funcțiile pe care le au în comiterea infracțiunii, cu un profil predominant non-violent, având un limbaj comun, cu terminologie specifică, și o motivație infracțională diversificată (fie materială, sexuală, ideologică, politică, obsedată de statut sau de investigație). În majoritatea covârșitoare a cazurilor, ei sunt de sex masculin, cu vârsta cuprinsă între 16 și 55 de ani, acționează în grup, neavând, de regulă, antecedente penale.

5. Probele electronice sunt informații cu valoare doveditoare, care sunt stocate, prelucrate sau transmise prin intermediul unui sistem informatic. Ele se produc în mediul informatic și reprezintă rezultatul transformării informației computerizate în urma ștergerii, copierii, blocării, modificării sau a oricărei alte intervenții în funcționarea mijloacelor de stocare, prelucrare sau transmitere a datelor informatice sau a rețelei de comunicații. Printre particularitățile acestor categorii de probe se remarcă faptul că, aparent, ele nu sunt evidente, sunt volatile, fiind conținute în echipamente informatice, nu sunt obiecte tangibile și au, de obicei, o anumită valoare materială.

6. În prezent, organele de drept din RM nu dispun de o bază de date centralizată a informației operative privind cauzele de criminalitate informatică, care să conțină date cu privire la operațiunile frauduloase de plată electronică, conturi implicate, adrese IP conexe, nume de domenii cu tangențe la infracțiunile date, viruși, botneturi, date media indexate (fișiere de tip log, imagini foto, capturi de ecran, coduri program și alte) etc. Introducerea unor astfel de date va permite identificarea conexiunilor dintre infracțiunile săvârșite în diferite locuri, stabilirea legăturilor dintre diferite persoane, fapte și circumstanțe, chiar și în baza unor semne minore.

7. Pe lângă stabilirea tuturor circumstanțelor săvârșirii infracțiunii, printre sarcinile de bază în cercetarea infracțiunilor informatice, se înscrie și identificarea tuturor formelor posibile de opunere de rezistență, specifice infractorilor digitali (cum ar fi: tăinuirea infracțiunii și a probelor, înscenarea, formarea unei opinii publice favorabile infractorului, influențarea directă a organului de urmărire penală, șantajarea victimei), a instrumentelor utilizate la crearea piedicilor, stabilirea specificului acestora și aplicarea metodelor și mijloacelor de învingere a lor.

3. TACTICA EFECTUĂRII UNOR ACȚIUNI DE URMĂRIRE PENALĂ ȘI MĂSURILE SPECIALE DE INVESTIGAȚII LA CERCETAREA INFRACȚIUNILOR INFORMATICE

3.1. Aspecte generale privind efectuarea unor acțiuni inițiale și ulterioare de urmărire penală

Examinarea criminalistică a sistemelor informatice trebuie să prezinte o serie de caracteristici specifice, necesare asigurării unui grad înalt de corectitudine a concluziilor rezultate în urma acestei examinări, și anume: autenticitate (dovada sursei de proveniență a probelor); credibilitate (lipsa dubiilor în privința credibilității și solidității probelor); completitudine (prelevarea tuturor probelor existente și integritatea acestora); existența unor proceduri pre-definite pentru situațiile întâlnite în practică; lipsa interferențelor și a contaminării probelor ca rezultat al investigației; posibilitatea repetării testelor realizate, cu obținerea unor rezultate identice; anticiparea posibilelor critici ale metodelor folosite; acceptarea faptului că metodele utilizate la un moment dat pot face subiectul unor modificări și anticiparea problemelor legate de admisibilitatea probelor [149, p. 73].

Spre deosebire de alte categorii de infracțiuni, în cadrul cărora administrarea probatoriului se efectuează concentric (de la periferii spre centru), adică inițial sunt acumulate probele existente, aflate departe de suspect, iar în final sunt ridicate probele aflate nemijlocit în zona de activitate a făptuitorului, în opinia noastră, în cazul infracțiunilor informatice, regula respectivă parțial decade.

Acest fapt se datorează specificului volatil al probelor electronice. Din momentul săvârșirii infracțiuni până la efectuarea acțiunilor de urmărire penală, de colectare a probelor electronice pot fi efectuate multiple conectări și deconectări ale sistemului informatic, diverse operațiuni în sistemul de operare sau asupra acestuia (spre exemplu, fragmentarea informației, reinstalarea sistemului operațional, ștergerea, modificarea [50, p. 58] sau suprascrierea datelor informatice), folosirea sistemului informatic de către alți utilizatori și altele. Toate acestea duc la pierderea iremediabilă a urmelor electronice relevante.

Atunci când există suspiciuni cu privire la implicarea unei persoane în săvârșirea infracțiunii informatice, organul de urmărire penală și organul care realizează activitatea specială de investigații au sarcina preliminară de a stabili toate circumstanțele cauzei, cu implicarea proprietarului sistemului informatic și fixarea probelor, inclusiv: a) încălcarea integrității sau confidențialității informației computerizate; b) prejudiciul cauzat; c) mecanismul săvârșirii infracțiunii; d) corelația dintre făptuitor, faptă și urmări [271, p. 144].

Tactica efectuării investigațiilor este direct legată de specificul mecanismului de săvârșire a acestor categorii de infracțiuni [245]. Un exemplu de sarcini de bază ale cercetării unei categorii de infracțiuni informatice (cu utilizarea virușilor) este descris în Anexa 7 din prezenta lucrare.

Cercetarea infracțiunilor informatice este una din cele mai costisitoare investigații, în care statul trebuie să investească resurse financiare considerabile – atât în mijloace tehnice și produse program, cât și în instruirea profesională a persoanelor implicate în combaterea fenomenului în cauză.

Activitatea de descoperire a infracțiunilor informatice poate fi divizată în câteva etape interdependente și consecutive [26, p. 203, 44, p. 15-19, 77, p. 9-11, 27, p. 84-86, 124, p. 529]: a) *identificarea incidentului*; b) *pregătirea investigării* (pregătirea echipei de investigații, pregătirea instrumentelor de investigare, obținerea documentelor necesare desfășurării procesului de investigare, formularea unui plan de acțiuni); c) *colectarea probelor* (securizarea, evaluarea și înregistrarea locului infracțiunii, căutarea probelor, audierea persoanelor implicate, conservarea probelor); d) *examinarea probelor* (evaluarea și extragerea informațiilor relevante din datele colectate); e) *analiza probelor* (studierea datelor și determinarea relevanței lor pentru caz); f) *prezentarea rezultatelor* (rezumarea pașilor întreprinși și a concluziilor obținute în timpul cercetării cazului).

Cercetarea la fața locului, percheziția sistemelor informatice, ridicarea de obiecte și documente etc., în cazul infracțiunilor informatice, prezintă multe similitudini din punct de vedere tehnic [26, p. 212].

Obiectele specifice acțiunilor procesuale din cadrul cercetării infracțiunilor informatice pot fi divizate în câteva grupuri, și anume: a) *încăperile* (în care se află sistemele și rețelele informatice, dispozitivele de comunicații, servere și altele); b) *dispozitivele informatice* (sistemele informatice în înțelesul lor tradițional; dispozitivele care funcționează în baza procesoarelor, ce permit accesul la rețele informatice: ultrabook-uri, notebook-uri, netbook-uri, tablete, telefoane mobile, book reader-uri și altele; dispozitive de tehnologii comunicaționale fără fir: GSM, GPRS, EDGE, 3G și 4G, modeme, routere CDMA și WiMax etc.); c) *suporturile de stocare a datelor informatice* (discurile optice: CD, DVD, Blu-Ray; dispozitive pe bază de memorie flash: USB stickurile, cartelele de memorie ale telefoanelor mobile, ale aparatelor foto, ale camerelor video, cartele SIM ș.a.) și d) *documentele* [83, p. 116].

Acțiuni preparatorii de bază la efectuarea activității de urmărire penală

În cadrul cercetării infracțiunilor informatice, în procesul de pregătire pentru efectuarea unei acțiuni de urmărire penală, cum ar fi cercetarea la fața locului, percheziția, ridicarea de obiecte și

documente etc., ofițerul de urmărire penală va întreprinde anumite acțiuni preparatorii de bază [272, p. 200, 273, p. 3, 274].

Astfel, se va asigura conservarea locului și a probelor temporare și fragile [25, p. 328], ce urmează a fi investigate până la sosirea persoanelor care vor efectua cercetarea acestora [73, p. 93].

Ofițerul de urmărire penală va stabili cercul de persoane care urmează să participe la efectuarea acțiunii de urmărire penală, sarcinile, algoritmul și consecutivitatea efectuării acțiunilor de către fiecare participant (membrii grupului de urmărire penală, specialistul în domeniul IT, specialistul-criminalist, specialistul care efectuează înregistrările foto și video, persoanele antrenate în asigurarea securității locului efectuării acțiunii de urmărire penală [83, p. 113]), numărul acestora variind în dependență de suprafața spațiului sau de numărul de încăperi care urmează a fi cercetate/percheziționate [74, p. 36].

În procesul de pregătire pentru efectuarea unei acțiuni de urmărire penală, se va efectua și instructajul membrilor grupului de urmărire penală, care vor participa la realizarea acțiunii respective. În cadrul instructajului, membrilor grupului li se va atrage, în special, atenția la legislația pertinentă [44, p. 9]; la particularitățile infracțiunii cercetate; la obiectele și documentele care urmează a fi depistate și ridicate; la modul de lucru cu echipamentul; la modalitatea de asigurare a confidențialității sursei de informare operativă; vor fi atenționați la comportamentul celorlalți participanți la acțiune, la necesitatea de a fi prudenți cu mijloacele tehnice depistate și dea interzice terțelor persoane de a le atinge [56, p. 693]; le vor fi explicate drepturile și obligațiile procesuale [275, p. 8].

Ofițerul de urmărire penală va organiza invitarea specialistului din domeniul IT [103, p. 690, 232, p. 659] și va asigura prezența acestuia la instructajul descris mai sus. Printre sarcinile lui de bază sunt: stabilirea tipului și destinației sistemului informatic; examinarea dispozitivelor și conexiunilor cu alte sisteme informatice; stabilirea stării sistemului informatic în momentul respectiv, a tipului sistemului de operare, a activităților realizate în sistemul de operare în momentul indicat; luarea deciziilor cu privire la acțiunile următoare asupra sistemului informatic; luarea măsurilor pentru obținerea accesului la informația computerizată sau pregătirea sistemului informatic pentru transportare [74, p. 39, 60, p. 89-90]; conservarea probelor volatile; consultarea ofițerului de urmărire penală cu privire la ordinea efectuării acțiunii; închiderea computerului pentru transport; etichetarea, înregistrarea, împachetarea, transportul și prelucrarea probelor [25, p. 328-329]. Totodată, se va dispune pregătirea de către specialist a tuturor softurilor, mijloacelor tehnice [29, p. 215], precum și a altor echipamente necesare [63, p. 150, 122, p. 39-40, 49, p. 23-

24, 44, p. 9-11], în Anexa nr. 8 la prezenta lucrare fiind expusă lista instrumentelor care trebuie să le conțină o trusă criminalistică pentru cercetarea infracțiunilor informatice.

În măsura posibilităților, se va obține informația referitoare la sistemul de organizare a procesului de funcționare a sistemelor și rețelelor informatice, care urmează a fi examinate [81, p. 41], precum și a sistemelor de operare utilizate, pentru ca specialistul să știe de ce produse program și dispozitive tehnice va avea nevoie la efectuarea acțiunii procesuale [103, p. 691].

O sarcină esențială este și stabilirea planului locului unde urmează a fi petrecută acțiunea procesuală [68, p. 171].

Nu în ultimul rând, la pregătirea pentru efectuarea acțiunii de urmărire penală, ofițerul de urmărire penală va studia personalitatea suspectului, îndeosebi nivelul cunoștințelor lui profesionale în domeniul IT [68, p. 172].

Măsuri preliminare la efectuarea acțiunilor de urmărire penală

Odată ajuns la fața locului, ofițerul de urmărire penală, desemnat pentru efectuarea acțiunii procesuale preconizate, va întreprinde anumite măsuri preliminare de bază [272, p. 205], cum ar fi: stabilirea perimetrului efectuării acțiunii procesuale, a numărului și schemei de amplasare a tehnicii de calcul [175, p. 910]; înlăturarea persoanelor terțe de la fața locului [29, p. 212], precum și prevenirea apariției acestora pe parcursul efectuării acțiunii procesuale [175, p. 910]; asigurarea securității locului efectuării acțiunii de urmărire penală (teritoriul cercetat, persoana reținută, locul aflării sistemului informatic, serverul rețelei informatice care conține baza de date cu privire la operațiunile efectuate, locul deconectării sursei de alimentare cu energie electrică) [83, p. 114, 175, p. 914, 92, p. 913]. De regulă, serverul se află într-o încăpere separată, având sistem de răcire a aerului [175, p. 914, 92, p. 913].

Totodată, ofițerul de urmărire penală, ajuns la fața locului, va ține cont de faptul că infractorul poate activa anumite dispozitive, pregătite în prealabil, pentru distrugerea informației electronice, cum ar fi câmpuri magnetice puternice (spre exemplu, în mânerul ușii prin care poate fi scos echipamentul electronic) [276, p. 635]; va colecta informație preliminară de la angajații întreprinderii, care urmează a fi luată în calcul în cadrul cercetării; va verifica posibilitatea accesului persoanelor neautorizate în încăperile în care se află dispozitivele electronice critice; va identifica persoana care administrează rețeaua și fiecare sistem informatic, deoarece s-ar putea ca suspecții să încerce să afirme că acestea nu le aparțin sau că nu au fost folosite de către ei. Organul de urmărire penală trebuie să aibă o evidență strictă a persoanelor asupra cărora a fost găsit fiecare dispozitiv în parte și cui îi aparțin lucrurile respective [49, p. 26].

Reprezentantul organului de urmărire penală va asigura stabilirea existenței rețelelor locale, topologia acestora, precum și a calculatoarelor conectate la aceste rețele, care se află în afara ariei locului examinat [175, p. 910], în vederea prevenirii transmiterii informației prin rețeaua locală și a elaborării planului acțiunilor de urmărire penală [103, p. 691]; stabilirea denumirii și a caracteristicilor dispozitivului de comunicații utilizat; efectuarea fotografiilor și a înregistrărilor video panoramice și de orientare [83, p. 115, 49, p. 27]. Consemnarea, în varianta foto sau video, are relevanță și pentru a arăta starea în care se găsea echipamentul în momentul ridicării, prevenind astfel plângerile legate de o eventuală deteriorare a acestuia [29, p. 213]. Aparatul foto/video urmează să fie setat astfel, încât să fie vizibilă data și timpul realizării fotografiei/înregistrării [44, p. 9].

Reguli de ordin general la efectuarea acțiunilor de urmărire penală

În cadrul efectuării acțiunilor de urmărire penală (cercetarea la fața locului, percheziția, ridicarea de obiecte și documente etc.), în cercetarea infracțiunilor informatice, organul de urmărire penală trebuie să respecte anumite reguli generale.

Cercetarea, percheziționarea încăperii începe cu respectarea procedurilor criminalistice generale de examinare a spațiului și de colectare a probelor tradiționale [29, p. 212]: amprente digitale de pe tastieră, întrerupătoare și alte componente ale sistemului informatic [81, p. 43, 49, p. 26, 248, p. 626], urme de picioare, încălțăminte, ale instrumentelor de spargere, înscrisuri și alte probe materiale [89, p. 55].

În cazul cercetării infracțiunilor informatice, săvârșite cu utilizarea instrumentelor de plată electronică, pe lângă carduri bancare implicate, înregistrări, bonuri și facturi de la oficiile poștale, de la bancomate, de la comercianți, organul de urmărire penală trebuie să caute și să ridice dispozitive specifice elementelor exterioare ale unui bancomat, ca dispozitivele pentru scrierea de date pe banda magnetică a cardurilor [26, p. 297].

Este necesar ca specialiștii criminaliști să fie prudenți la utilizarea prafurilor și reactivelor chimice pentru descoperirea și fixarea urmelor, așa încât particulele acestora să nu aungă pe suprafața și în interiorul dispozitivelor electronice. Totodată, trebuie interzisă utilizarea prafurilor de aluminiu, pentru a nu deteriora echipamentele și datele.

Sistemul informatic trebuie examinat în starea în care a fost depistat (conectat sau deconectat). În cazul în care calculatorul a fost găsit deconectat, acesta se va ridica, fără a fi conectat la sursa de alimentare cu energie electrică [49, p. 25].

Este interzisă manipularea sistemului informatic și a datelor informatice stocate, când nu se cunoaște rezultatul acestor acțiuni.

Specialiștii în domeniul IT trebuie să utilizeze doar produse program și mijloace tehnice certificate, înregistrate din punct de vedere al protecției drepturilor de autor [29, p. 215], adică să dispună de licență [175, p. 912]. Trebuie limitată sau exclusă utilizarea mijloacelor tehnico-criminalistice, al căror principiu de funcționare constă în utilizarea câmpurilor magnetice, electromagnetice, a razelor roentgen, a razelor ultraviolete și altor emisii, deoarece acestea pot afecta datele informatice, stocate în dispozitivele electronice.

La fixarea caracteristicilor și proceselor funcționării sistemelor și rețelelor informatice în procesul-verbal al acțiunii de urmărire penală, se utilizează terminologia specifică, cu explicarea semnificației acesteia [56, p. 698].

În procesul de examinare a dispozitivelor electronice se respectă principiul cercetării concentrice (de la general la particular), descriindu-se, inițial, particularitățile externe ale dispozitivului electronic: culoarea, mărimea, tipul, categoria, denumirea, marca, modelul, numărul de identificare, seria, existența înscrisurilor, a deteriorărilor și urmelor [239, p. 123, 277, p. 11].

Pentru optimizarea investigării unui volum mare de informații poate fi aplicată funcția căutării după cuvinte cheie [90, p. 273].

Este interzisă orice manipulare directă asupra calculatorului ridicat, indiferent de circumstanțele cauzei. Trebuie să fie excluse conectările sistemului informatic până la transmiterea acestuia către instituția de expertiză, fără asigurarea măsurilor de protecție necesare. Astfel, pentru examinarea datelor informatice, trebuie, înainte de toate, să fie făcută o copie de rezervă (clona discului, copia oglindă) a informației electronice. Clona informației constituie o copie identică a suportului original de stocare a datelor informatice (întregul conținut al discului, sector cu sector, inclusiv fișierele temporare, fișierele de schimb, fișierele șterse, chiar și informația aflată pe porțiunile avariate ale discului, etc. [29, p. 215]). Această măsură va exclude eventualitatea cauzării daunelor de către softurile de autodistrugere a informației.

Atunci când în sistemul informatic este instalată o măsură de protecție (spre exemplu, o parolă), conectarea lui poate conduce la distrugerea datelor informatice, deoarece este posibil ca făptuitorul să fi instalat diverse „capcane” de autodistrugere. Totodată, calculatorul poate conține unele comenzi care produc pierderea datelor [60, p. 691], ele pot fi mascate sub numele unor comenzi uzuale ale sistemului de operare folosit [149, p. 78]. Din aceste considerente, nu se permite pornirea sistemului informatic respectiv prin utilizarea propriului său sistem de operare.

Astfel, în vederea analizării și/sau descrierii conținutului discurilor rigide ale calculatorului, sistemul informatic va fi pornit cu ajutorul unui suport, pregătit în prealabil de către specialist, de încărcare a sistemului de operare extern prin intermediul BIOS Setup [277, p. 12]. În situația în care a fost instalată o parolă de acces către BIOS, aceasta va fi concretizată în cadrul audierii

angajaților companiei sau va fi dezactivată prin intermediul unor mijloace tehnice ori prin deconectarea bateriei (acumulatorului) care alimentează memoria calculatorului, autonomă de sursa de alimentare. În BIOS se vor seta: tipul unității de disc, precum și parametrii de încărcare a sistemului de operare, așa încât sistemul să se încarce, inițial, de pe unitatea de disc pe care se află sistemul de operare extern [74, p. 43].

Toate suporturile magnetice de stocare a datelor trebuie protejate împotriva modificării conținutului lor. Unele tipuri de hard-discuri au contacte speciale care realizează protejarea la scriere [29, p. 214].

Totodată, probele electronice pot exista și ca fișiere distruse sau ascunse [248, p. 628, 56, p. 696], iar datele, legate de aceste fișiere, pot fi salvate doar cu ajutorul produselor program specializate. Cele mai simple softuri sunt de tipul SafeBack. Purtătorii magnetici pe care urmează a fi copiată informația, trebuie să fie pregătiți în prealabil, asigurându-ne că nu există vreo informație pe ele [74, p. 26].

Odată cu terminarea clonării, trebuie verificată integritatea datelor prin una din următoarele metode [44, p. 6]: CRC [277, p. 12], MD5, SHA-1 [26, p. 234], SHA-256 [122, p. 135].

După ce a fost realizată copia identică a suportului de stocare a informației al dispozitivului examinat, se va efectua verificarea prezenței virușilor. Specialistul trebuie să nu admită „tratarea" fișierelor infectate. Faptul stabilirii prezenței virușilor doar se fixează. Fișierele infectate vor fi prezentate intacte expertului, pentru a stabili categoria virușilor, modul de răspândire, consecințele utilizării acestora, timpul instalării și nivelul de calificare al persoanei care l-a elaborat și/sau l-a instalat [74, p. 34].

De regulă, verificarea se efectuează cu cel puțin 3 produse antivirus diferite (spre exemplu, Bitdefender, Kaspersky, Norton, Avira ș.a.). Specialistul în domeniul investigării virușilor va efectua așa-numita inginerie inversă (de la engl. „reverse engineering"). În urma acestei analize se va restabili și se va studia codul-sursă al produsului program, structura, funcționalitatea, posibilitățile, setările, adresele centrelor de dirijare, precum și alte legături.

Simpla prezență într-un sistem informatic, conectat la rețeaua Internet, a unor materiale ilegale – spre exemplu, fotografii înfățișând minori în ipostaze sexuale explicite – nu poate justifica prezumția că deținătorul ori utilizatorul de drept al sistemului informatic, chiar dacă este singura persoană care a avut acces fizic la sistem, este și făptuitorul real, fiind necesară eliminarea prin probe a ipotezelor alternative de comitere a faptei penale de către terțe persoane ori, în mod automatizat, prin acțiunea unui program de tipul virușilor informatici [278, p. 50].

Una din cele mai frecvente strategii de apărare în cazul infracțiunilor informatice o constituie apărarea tip *Cal Troian*, în care bănuitul sau învinuitul neagă faptul că ar fi autorul

faptei și susține fie că infracțiunea a fost săvârșită de către un terț individ, prin controlul de la distanță a sistemului informatic, infectat cu un program de tip virus sau Cal Troian ce oferea acces („back door”) atacatorului real, fie că fapta a fost comisă în mod automat de către un program, care executa automat un set predefinit de instrucțiuni – în ambele situații, fără știrea utilizatorului sau a deținătorului legitim al sistemului informatic [252, p. 167].

Conceptul de *Apărare Cal Troian* își are originea în primele cauze documentate, în perioada anului 2003, în Marea Britanie și SUA [279], în care inculpații au negat săvârșirea faptelor incriminate, susținând că acestea au fost comise de programe de tip Cal Troian, așa încât o serie dintre inculpați au fost achitați, în urma constatării prezenței în sistemul informatic a unor asemenea programe informatice de control la distanță ș.a. și a imposibilității de a identifica făptuitorul real în aceste condiții [88]. În același context, a fost semnalată chiar și o formă de șantaj, ce consta în ,,plantarea” unor date informatice conținând pornografie infantilă pe un sistem informatic vulnerabil și constrângerea ulterioară a titularului respectivului sistem de a transfera o sumă de bani [280, p. 24].

Trebuie exclusă posibilitatea învinuirii organului de urmărire penală de virusarea intenționată a sistemului informatic al bănuitului/învinuitului, de incompetență la efectuarea acțiunilor de urmărire penală sau neglijență, dat fiind faptul că aceste circumstanțe ar putea să pună la îndoială toată munca expertului și concluziile acestuia.

Este necesar a interzice accesul și apropierea suspectului de sistemul informatic original, mai ales dacă persoana are pregătire specială în domeniul informatic [29, p. 212], precum și a refuza ajutorul altor persoane neautorizate. Ei pot cripta sau distruge informația chiar în prezența organului de urmărire penală. Din aceste motive, le poate fi permis accesul numai la clona suportului de stocare a informației electronice [74, p. 24].

Organul de urmărire penală urmează să ridice doar mijloacele tehnice pe care sunt sau pot exista informații relevante pentru cauză [65, p. 96].

În cazul în care se impune dezasamblarea sistemului informatic, fiecare componentă a acestuia trebuie etichetată, înainte de modificarea configurației în vederea ridicării probelor. În privința cablurilor, se etichetează atât cablul, cât și suporturile de unde a fost debranșat [29, p. 214, 49, p. 31, 56, p. 695, 92, p. 911].

Ridicarea sistemelor informatice se efectuează doar în stare deconectată [65, p. 97]. Ofițerul de urmărire penală urmează să se asigure că dispozitivul pe care intenționează să-l ridice este deconectat (cablul de alimentare este decuplat de la sursa de alimentare cu energie electrică, nu se aude ventilatorul intern, nu luminează niciun indicator, nu există imagini pe ecran, sistemul nu este cald) [49, p. 27, 60, p. 691].

Dispozitivele ridicate se împachetează, așa încât să fie prevenită deteriorarea, modificarea și distrugerea acestora de lovituri, de temperaturi ridicate sau scăzute, precum și de oscilațiile acestora, ce ar putea cauza vreun scurtcircuit provocat de condensat, de particule mici și prafuri, de mijloacele tehnico-criminalistice de detectare a undelor magnetice, de radiații ultraviolete și infraroșii, de câmpurile electromagnetice [57, p. 563] și electrostatice, de plieri sau zgârieturi ale dispozitivelor de stocare a datelor informatice (cum ar fi dischete, suporturi optice și altele). Totodată, împachetarea trebuie să asigure prevenirea conectării sistemului informatic la sursa de alimentare cu energie electrică și dezasamblarea echipamentului [74, p. 42, 175, p. 915].

La sistemele informatice și alte dispozitive electronice împachetate se va atașa o foaie de hârtie (numită *foaie de însoțire/custodie*), pe care se vor face următoarele mențiuni: numărul cauzei penale [281, p. 3], acțiunea de urmărire penală în cadrul căreia au fost ridicate, numărul de ordine conform procesului-verbal [92, p. 914], data împachetării, locul împachetării, descrierea succintă a conținutului, numele, prenumele și semnătura fiecărui participant la acțiunea de urmărire penală. În acest mod urmează a fi etichetate toate obiectele care se ridică de la fața locului.

În cazul utilizării pentru sigilare a benzii adezive, aceasta urmează a fi aplicată în așa fel, încât, dacă se va încerca scoaterea ei, va fi afectată integritatea foii de hârtie atașate, menționate *supra* [282, p. 25], ceea ce poate motiva contestarea informației ce se află acolo [29, p. 215].

Este de menționat că discurile magnetice solide sunt foarte sensibile la vibrații, iar deteriorarea lor mecanică conduce la inaccesibilitatea totală a datelor [83, p. 133].

În cazul imposibilității de a transporta concomitent tot echipamentul ridicat, se va asigura paza bunurilor rămase la fața locului într-o încăpere separată [175, p. 915, 92, p. 914].

Recomandări de bază la efectuarea acțiunilor de urmărire penală

Organul de urmărire penală trebuie să ia în considerare și anumite recomandări tactice, valabile pentru acțiunile de urmărire penală sub formă de cercetare la fața locului, percheziție și ridicare de obiecte și documente, efectuate în cadrul investigării infracțiunilor informatice.

Astfel, pentru examinarea încăperilor, metoda propusă în literatura de specialitate [283, p. 188] este cea excentrică, adică de la cel mai important obiect (server, sistem informatic) către periferii.

În cazul în care există un număr considerabil de sisteme și/sau rețele informatice care urmează a fi examinate în cadrul acțiunii de urmărire penală [175, p. 914], în literatura de specialitate se recomandă să fie formate mai multe subgrupuri de participanți la acțiune, conduse de către diferiți ofițeri de urmărire penală, care vor efectua separat cercetarea obiectelor sau

încăperilor [83, p. 113]. Considerăm însă că utilizarea acestui procedeu creează mai multe probleme procesuale, cum ar fi: asigurarea prezenței, în fiecare subgrup, a persoanei în privința căreia se face acțiunea de urmărire penală ori a celor care reprezintă interesele persoanei respective; întocmirea procesului-verbal al acțiunii de urmărire penală.

Pentru identificarea făptuitorului sau a complicilor lui, se recomandă ridicarea dispozitivelor de înregistrare și fixare video de pe teritoriul întreprinderii sau cel adiacent acesteia [12, p. 239].

Atunci când organul de urmărire penală intenționează să examineze un volum mare de informații, fie din lipsa specialistului în domeniul IT [29, p. 213], fie din intenția de a analiza aprofundat informația existentă în sistemele informatice, se impune dispunerea unei expertize asupra lor, deoarece aceste investigații informatice durează un timp mai îndelungat, uneori necesitând o pregătire prealabilă a specialistului sau condiții de laborator [284].

Ofițerul de urmărire penală trebuie să țină cont că în calculator pot fi instalate softuri speciale de securitate, care, în cazul când nu sunt introduse anumite coduri sau sunt introduse coduri greșite, declanșează distrugerea informațiilor existente. În asemenea situații, este oportun a obține benevol, în măsura posibilităților, aceste coduri.

Se recomandă efectuarea a două copii (clone) ale dispozitivelor de stocare a datelor informatice, pe una dintre ele realizându-se analiza propriu-zisă, cealaltă fiind o copie de rezervă [149, p. 79]. O copie certificată a acesteia se păstrează la procuror, în locuri speciale, în plic sigilat și va fi pusă la dispoziția instanței la solicitarea ei [31, p. 49].

Pot exista diferențe neesențiale între conținutul documentelor dublate, însă acestea pot reprezenta o valoare probatorie semnificativă. Identificarea lor poate fi ușor realizată cu ajutorul redactoarelor moderne de text [74, p. 26].

Ordinea stopării funcționării softurilor care rulează pe sistemul informatic, precum și a deconectării sistemului informatic se coordonează nemijlocit cu specialistul [26, p. 218].

Dacă suspectul insistă să ajute organul de urmărire penală în procesul de închidere sau ridicare a componentelor sistemului informatic, acesta poate să explice operațiunile pe care dorește să le execute și chiar să le descrie pe hârtie. Organul de urmărire penală nu va aplica indicațiile suspectului, ci le va remite specialiștilor/experților ce efectuează analiza probelor, care vor putea fi avertizați, în acest mod, de eventualele capcane introduse de suspect [29, p. 213].

În cazul ridicării blocului de sistem, restul elementelor sistemului informatic – monitorul, tastiera, mouse-ul – nu se supun ridicării.

În situația în care există unele suporturi care nu au conectate cabluri, se recomandă să fie etichetate ca „neutilizate” [29, p. 214, 49, p. 32].

La împachetarea sistemelor informatice și ale altor dispozitive electronice se vor utiliza, în măsura posibilităților, cutiile originale ale producătorului, alte cutii sau saci [74, p. 46]. Cutia în care se află dispozitivul ridicat trebuie, la rândul ei, să fie împachetată într-o sacoșă din polietilenă. Purtătorii magnetici este necesar să fie împachetați și transportați în containere ecranate [175, p. 915] sau în huse din aluminiu care previn influențarea negativă a câmpurilor magnetice și electromagnetice și asigură protecția electrostatică a acestora [29, p. 214, 60, p. 692], din aceste motive, dacă la acțiunea procesuală participă specialistul, se recomandă ca împachetarea și sigilarea obiectelor electronice să fie pusă în sarcina acestuia [81, p. 36]. Banda adezivă nu trebuie să fie aplicată pe suprafața suportului de stocare a datelor informatice.

La transportarea și păstrarea sistemelor informatice, a purtătorilor de stocare a informației electronice, se vor întreprinde măsuri în vederea evitării șocurilor, a vibrațiilor excesive, a emisiilor radio sau a radiațiilor electromagnetice [29, p. 214] (spre exemplu, monitoarele urmează a fi transportate pe scaun, cu ecranul în jos, fiind fixate cu centurile de siguranță [49, p. 36]); a excluderii interacțiunii acestora cu substanțe chimice active, a respectării regulilor de păstrare a mijloacelor tehnice, evitându-se umiditatea excesivă și praful; se va exclude expunerea la soare sau în autoturisme cu temperaturi ridicate [285, p. 30]; nu se va admite aranjarea în stive mai mult de trei sisteme informatice, se va asigura depozitarea în încăperi încălzite, fără rozătoare [74, p. 47, 175, p. 916].

Ridicarea informației electronice împreună cu suportul de stocare a datelor informatice în cadrul acțiunilor de urmărire penală

Informația electronică poate fi ridicată atât împreună cu suportul de stocare a datelor electronice, cât și fără acesta [74, p. 18, 93, p. 215].

În cazul în care informația computerizată este ridicată împreună cu suportul de stocare a datelor informatice, sunt posibile două situații:

- ridicarea nemijlocită a suportului de stocare a informației (discul rigid, optic sau magnetic și altele) [283, p. 216];
- ridicarea sistemului informatic (blocul de sistem, procesorul) cu HDD-ul conectat. Aceasta este calea cea mai potrivită, mai operativă și mai efectivă, care urmează să fie utilizată de către organele de drept.

În situația în care infracțiunea a fost săvârșită cu mult timp în urmă și nu există bănuieli rezonabile că faptele infracționale continuă și în prezent, sistemul informatic poate fi deconectat de la sursa de alimentare cu energie electrică, fără pericolul de a pierde datele. În caz contrar, acțiunea de urmărire penală urmează a fi planificată astfel, încât să fie efectuată atunci când

sistemul informatic este deconectat de la sursa de alimentare, spre exemplu, în orele matinale. Totuși, trebuie luat în calcul faptul că serverele, de regulă, funcționează încontinuu.

Deseori, suporturile de stocare a datelor informatice se află în alt loc, decât cel al sistemului informatic prin intermediul căruia se accesează, în altă cameră sau chiar în alt imobil.

În procesul-verbal al acțiunii de urmărire penală urmează a fi fixate: constatarea stării funcționale a dispozitivului și ordinea deconectării acestuia; locul concret de aflare a obiectului ridicat, precum și poziționarea acestuia față de alte obiecte, cu anexarea schemelor și planurilor necesare [57, p. 564]; modul de conexiune a tuturor dispozitivelor între ele, cu indicarea particularităților acestora (culoarea, numărul, mărimea, particularitățile individuale ale cablurilor, muftelor, marcajul); stabilirea existenței rețelei informatice și de comunicații electronice, a canalului utilizat; tipul ambalajului și stabilirea modului de transportare a obiectelor ridicate [65, p. 97].

Ridicarea informației electronice fără suportul de stocare a datelor informatice

Acest procedeu este mult mai complicat decât ridicarea informației împreună cu suportul acesteia, în afară de aceasta, informația ridicată este incompletă. Totuși procedura respectivă poate fi aplicată în practică, spre exemplu, în situațiile în care activitatea sistemului sau a rețelei informatice nu poate fi stopată în legătură cu implicarea lor în procese complexe neîntrerupte, a utilizării în calitate de server, iar sistarea poate cauza prejudicii și cheltuieli materiale considerabile, precum și alte consecințe inacceptabile.

În situația în care la etapa incipientă nu a fost posibilă aflarea parolelor și a codurilor produselor program, atunci dispozitivul urmează a fi ridicat, în vederea examinării lui în condiții de laborator, cu implicarea specialiștilor, pentru a identifica parolele și codurile de acces.

În unele situații (când există bănuiala că documentele puteau fi imprimate sau când este necesară identificarea imprimantei la care a fost elaborat documentul), este necesară ridicarea și a imprimantei. În memoria acesteia poate fi stocată informația cu privire la documentele și timpul imprimării, fapt care poate fi stabilit în cadrul expertizei [74, p. 21].

În cadrul ridicării informației din sistemul informatic, în unele cazuri, se impune copierea conținutului discului cu aplicații specializate [272, p. 215]. Dacă la efectuarea acțiunii de urmărire penală participă specialistul în domeniul IT, această sarcină îi revine lui.

În procesul-verbal al acțiunii procesuale este necesară fixarea, inclusiv, a următoarelor date: softurile care rulează în momentul efectuării acțiunii de urmărire penală; rezultatele activității softurilor depistate; manipulările prin intermediul mijloacelor tehnice, al produselor program, mediile de stocare, precum și rezultatele obținute [272, p. 215].

Este indicată și elaborarea unor modele (formulare) de procese-verbale, specifice cercetării, percheziționării și ridicării sistemelor și rețelelor informatice, a datelor electronice [81, p. 48].

În literatura românească de specialitate [29, p. 210], precum și în legislația României, investigațiile efectuate asupra suporturilor de stocare a datelor informatice sunt numite *percheziție a sistemelor informatice*, iar în cea americană – *Computer Forensics* [286, p. 1].

Examinarea sistemelor informatice aflate în funcțiune

În situația în care sistemul informatic este în funcțiune, organul de urmărire penală urmează să întreprindă anumite măsuri specifice [89, p. 56].

Dacă anterior, în literatura de specialitate (spre exemplu: M. Ruiu [29, p. 214]), se considera necesară deconectarea alimentării cu energie electrică pentru salvarea eficientă a datelor informatice până la începerea acțiunii procesuale, acum, odată cu implementarea masivă în sistemele informatice a surselor de alimentare cu energie electrică fără fir, această măsură a pierdut din eficacitate [81, p. 40].

În dependență de starea monitorului (conectat, deconectat sau regim de suspendare), se va efectua ori investigația „live" (cu descrierea datelor de pe suprafața de lucru a ecranului), sau „Post mortem" (descrisă mai jos), conform anexei nr. 9 [29, p. 212, 83, p. 123, 49, p. 30-31, 92, p. 911].

Prin intermediul „Managerului de activități" (tastarea concomitentă Ctrl-Alt-Del), pot fi vizualizate procesele și produsele program care rulează în sistemul informatic. Totuși, softurile destinate distrugerii informației pot rula, în cazuri excepționale, în regim ascuns.

Oprirea programelor care rulează în computer se efectuează, mai ales, în cazul aflării probelor în pericol imediat (de exemplu, procesul formatării unui disc) [29, p. 213], inclusiv cu ajutorul „Managerului de activități", concomitent păstrând toată informația activă și registrele de activitate [74, p. 40], iar în situațiile excepționale, chiar și cu deconectarea sistemului. Multe softuri pot fi oprite prin tastarea concomitentă Ctrl-C, sau Ctrl-Break, sau Ctrl-Q. Deseori, pentru închiderea unui program, este necesară tastarea comenzii EXIT sau QUIT, iar uneori este de ajuns apăsarea tastei Esc sau clic cu cursorul pe pictograma de închidere a programului [56, p. 694].

Asigurarea accesului ulterior la informație, la lista discurilor logice, inclusiv cele virtuale și de rețea, este realizată prin introducerea login-ului utilizatorului și parolei acestuia [74, p. 40].

Specialistul în domeniul IT trebuie să întreprindă măsurile necesare în vederea depistării și realizării copiei fișierelor temporare - probe volatile (memoria: RAM, cache, componentelor periferice) [287, p. 5, 77, p. 9-10]. Această categorie de fișiere se distruge odată cu întreruperea funcționării sistemului informatic [63, p. 139]. Datele stocate în fișierele temporare pot fi extrem

de folositoare, îndeosebi dacă fișierul inițial a fost criptat sau documentul a fost imprimat, dar niciodată nu a fost salvat [74, p. 26]. Fișierele temporare conțin date și cu privire la softurile care rulează.

Pentru copierea informației temporare sunt utilizate diverse produse program destinate pentru diferite sisteme informatice, pe care le va pregăti specialistul în prealabil. Colectarea informațiilor respective urmează a fi efectuată într-o anumită consecutivitate și cu ajutorul mai multor utilitare [83, p. 130, 122, p. 73-74, 44, p. 11-13], o listă exemplificativă, în acest sens, fiind prezentată în Anexa nr. 10.

Informații relevante se pot stoca și în memoria operativă a sistemului informatic (memoria Dump/RAM), a dispozitivului periferic și a anumitor suporturi externe de stocare a informației. Fixarea datelor din memoria operativă poate fi efectuată prin imprimarea pe suport de hârtie [60, p. 692] sau prin copierea cu ajutorul softurilor specializate. În anexa nr.11 din prezenta lucrare este descrisă, cu titlu de exemplu, una din căile de obținere a memoriei Dump în sistemul de operare „Windows 8".

O altă categorie de fișiere temporare sunt Swap File-urile, care funcționează asemeni discului de memorie, reprezentând o bază enormă de date și conținând diverse fragmente temporare de informații. În Swap File pot fi depistate chiar și textele documentelor întregi [74, p. 26]. Stabilirea existenței fișierelor de tip log și copierea acestora, inclusiv a fișierelor de tip Swap, pot fi restabilite cu ajutorul produselor program specializate (Hetman Partition Recovery, Lazesoft Data Recovery, File Rescue Plus ș.a.) [83, p. 124].

Ofițerul de urmărire penală trebuie să stabilească existența fișierelor criptate în computer (spre exemplu, cu ajutorul softurilor Bitlocker, FileVault, eCryptFS, Steganos, PGP – Pretty Good Privacy, Folderlock, SafeHouse, TrueCrypt, ultimul sistat în anul 2014 etc.). Dacă examinatorul nu cunoaște parola de decriptare a fișierelor criptate, practic este imposibilă identificarea acesteia în timp util. Totuși, investigatorul va putea încerca parolele pe care știe că le folosește persoana suspectă: cuvintele, cifrele, precum și combinațiile acestora, depistate în apropierea sistemului informatic, în agendele acestuia etc., lista celor mai des folosite parole (cum ar fi: 123456, password, qwerty, superman, football, admin ș.a.) [122, p. 142].

În situația în care discurile sau containerele criptate sunt montate, urmează a fi efectuată copierea acestora, atâta timp cât mai există acces la ele. Dacă montarea a fost efectuată cu ajutorul Bitlocker, atunci trebuie salvată cheia de recuperare, prin utilizarea comenzii „manage-bde -protectors -get" [122, p. 78].

Totodată, organul de urmărire penală trebuie să identifice numărul și tipurile sistemelor de operare, instalate în sistemul informatic examinat, operație care poate fi efectuată cu ajutorul

datelor din registre (File registry); trebuie să determine ISP-ului, precum și adresa IP alocată, cu indicarea alăturată a timpului fixării acesteia; să fixeze timpul sistemului (BIOS) și timpul în sistemul de operare (conform datelor din registrele electronice) [83, p. 125], inclusiv timpul setat în telefonul mobil sau tabletă, comparând ora și data cu un ceas de referință; să descrie toate probele potențiale, de exemplu, dacă investigatorul deschide un fișier cu extensie „.jpg", care ar putea fi o fotografie pornografică a unui copil, el trebuie să înregistreze în procesul-verbal numele fișierului, locul unde fișierul este localizat pe hard disc, data și marcajul de timp, precum și alte proprietăți ale fișierului [220, p. 582].

În funcție de tipul infracțiuni informatice, se vor examina diferite probe electronice, cum ar fi: lista adreselor URL vizitate; mesajele e-mail și lista adreselor e-mail, memorată în agenda suspectului; documentele procesate; grafice (în cazul pornografiei infantile); înregistrări chat; registrul sistemului de operare; jurnale prezentatoare de evenimente (event viewer logs); jurnale de aplicație; fișiere de derulare a documentelor imprimate [63, p. 188].

Toate căutările și paginile web vizitate sunt disponibile în istoricul browser-ului (un program de „navigare" virtuală în web [288]), care poate fi vizualizat prin tastarea CTRL-H, în sistemele de operare Windows și Linux, sau prin Command-H, în Mac OS. Motoarele de căutare (un program apelabil de căutare, care accesează Internetul în mod automat și frecvent și care stochează într-o bază de date titlul, cuvintele-cheie și, parțial, chiar conținutul paginilor web [289]) Google și Bing păstrează istoricul căutărilor timp de câțiva ani. Google păstrează istoricul accesărilor utilizatorului la adresa http://www.google.com/history, iar Windows Live (Bing) le afișează la link-ul http://www.bing.com/profile/history.

Ofițerul de urmărire penală va fixa rezultatele acțiunilor întreprinse și reacția sistemului la acestea [272, p. 254], va stabili existența conectării dispozitivelor externe, a suporturilor de stocare a informației.

Odată cu constatarea existenței dispozitivelor de conectare la distanță, se va deconecta cablul de rețea, așa încât să nu fie posibilă modificarea sau distrugerea informației. Existența rețelelor informatice poate fi stabilită și prin prezența mai multor sisteme informatice sau a componentelor de rețea (cartelă de rețea și cabluri, echipamente wireless LAN, routere, hub-uri, comutatoare, servere) [49, p. 16-17, 32].

Totodată, printre indicii stocării datelor la distanță pot fi: existența fișierelor partajate, e-mailul păstrat pe IMAP sau Exchange server, servicii cloud etc. Datele respective trebuie copiate atâta timp cât calculatorul se află în rețea [122, p. 80].

O sarcină importantă este stabilirea locului aflării serverului la care este conectat sistemul informatic examinat, precum și numărul de alte sisteme informatice, conectate la acest server, cu asigurarea examinării concomitente ale acestora.

Deconectarea sistemului informatic poate fi efectuată prin închiderea obișnuită sau prin întreruperea alimentării cu energie electrică, în timp ce acesta funcționează [290, p. 44]. În cazul închiderii obișnuite, se produc următoarele efecte: spațiul memoriei virtuale a hard-discului se pierde, sunt lansate procese de distrugere a probelor, sistemul de fișiere și fișierele rămân intacte. În urma întreruperii alimentării cu energie electrică, efectele produse sunt următoarele: datele volatile sunt șterse, sistemul de fișiere poate fi deteriorat, accesul viitor la date poate fi pierdut. Întreruperea se va face prin extragerea cablului de alimentare cu energie electrică de la echipament, dar nu de la priză [49, p. 31].

În cadrul investigațiilor efectuate asupra sistemului informatic, toate acțiunile organului de urmărire penală, precum și ale specialistului, urmează a fi explicate tuturor participanților la această acțiune procesuală, într-un limbaj accesibil [175, p. 912].

Ulterior, ofițerul de urmărire penală urmează să realizeze acțiunile specifice ridicării sistemelor informatice, deconectate de la sursa de alimentare cu energie electrică și care nu sunt în funcțiune, descrise mai jos.

Examinarea sistemelor informatice care nu sunt în funcțiune

Dacă sistemul informatic nu este în funcțiune, organul de drept va efectua investigația „Post mortem” [89, p. 57], care constă în: fixarea locului aflării calculatorului și a dispozitivelor periferice; descrierea detaliată a ordinii conectării între dispozitivele respective, cu realizarea fotografierii sau filmării acestor conexiuni [56, p. 695]; deconectarea dispozitivelor periferice de la calculator [49, p. 31]; realizarea de către specialist [63, p. 140] a copiei suportului de stocare a informației (copia oglindă, clona discului) cu ajutorul softurilor specializate (spre exemplu, EnCase, FTK, SafeBack, SMART, ProDiscover) sau softului „dd”, care este o componentă a sistemului de operare de tipul Unix/Linux [83, p. 124], precum și a dispozitivelor de blocare a înregistrărilor pe suportul de date informatice [86, p. 118, 277, p. 12]; împachetarea separată a suporturilor de stocare a informației electronice în pungi antistatice [49, p. 35]; împachetarea fiecărui dispozitiv și cablu de conexiune.

Examinarea notebook-urilor (inclusiv a ultrabook-urilor, netbook-urilor), tabletelor și a telefoanelor mobile moderne, pe lângă particularitățile descrise mai sus, prezintă și anumite trăsături specifice. În aceste dispozitive, o parte considerabilă a datelor informatice se păstrează în memoria operativă, dependentă de sursa de energie. În cazul deconectării sursei de energie de la

un astfel de dispozitiv, de regulă, are loc pierderea ireversibilă a datelor. Starea (regimul) „deconectat” *de facto* reprezintă regimul de „hibernare”, atunci când energia electrică se utilizează doar pentru menținerea memoriei operative.

Dacă, în momentul efectuării acțiunii procesuale, dispozitivul este activ, atunci se impune [83, p. 126]: să nu fie atins ecranul acestuia, deoarece el este un element funcțional, iar fiecare atingere este percepută drept o comandă [49, p. 28]; fixarea foto și video a conținutului ecranului [175, p. 912]; stabilirea aplicațiilor care rulează (de regulă, pictogramele aplicațiilor care rulează apar în josul ecranului la atingerea butonului „Acasă”); determinarea tipului conexiunii la rețeaua internet (3G, 4G, Wi-Fi), prin vizualizarea pictogramei respective în partea de sus a ecranului sau prin atingerea pictogramei „setări” din rubrica „date mobile” și „Wi-Fi”, cu închiderea ulterioară a acestor interfețe wireless; deconectarea prin ținerea apăsată timp de câteva secunde a butonului de pornire/deconectare „Power”; interzicerea extragerii acumulatorului dispozitivului.

Atunci când sistemul informatic este în regim de „hibernare”, organul de urmărire penală va putea să aleagă: îl va opri imediat ori îl va activa, fixând conținutul ecranului și deconectându-l ulterior.

Pentru deconectarea notebook-ului nu este suficientă întreruperea de la sursa de alimentare cu energie electrică, deoarece, în asemenea situație, el va trece la energia acumulatorului, din aceste considerente este necesară și extragerea acumulatorului. Nu este recomandată închiderea capacului laptopului, dat fiind faptul că se activizează funcția de hibernare, ceea ce duce la modificarea informației pe disc [83, p. 127].

La cercetarea telefoanelor mobile, pot fi obținute datele despre identificatorii echipamentului, datele convorbirilor telefonice și, după caz, înregistrările acestor convorbiri, conținutul mesajelor (inclusiv poșta electronică), agenda telefonică, istoricul vizitării site-urilor (căutărilor în internet), programările din calendar, fotografii și înregistrări video. De asemenea, poate fi stabilită și geolocația dispozitivului (locul aflării persoanei-utilizator al acestui dispozitiv) în anumite perioade de timp. Această posibilitate este oferită atât de către operatorii de telefonie mobilă (în cazul apelurilor telefonice și/sau conectării la rețeaua 3G/4G), cât și de către informația existentă chiar pe dispozitiv (spre exemplu, cea indicată în fotografiile realizate prin intermediul acestui telefon sau în unele aplicații instalate, cum ar fi setările implicite „Google Map”).

Verificarea IMEI-ului telefonului mobil sau al tabletei poate fi efectuată de către organul de urmărire penală prin introducerea următoarelor caractere **#06#*, care funcționează și în lipsa cartelei SIM [81, p. 44]. IMEI-ul conține 15 cifre, care indică modelul și țara de origine a echipamentului mobil de comunicație (primele 8 cifre) și producătorul (restul cifrelor).

Deblocarea (resetarea) codului PIN poate fi obținută, spre exemplu, prin introducerea comenzii ***05*<Codul PUK >*<noul cod PIN>*<confirmarea noului cod PIN># și altele. Astfel de aplicații (comenzi) pot fi obținute de la Centrele de deservire ale operatorilor de telefonie mobilă [291]. Parola PIN și PUK poate fi depistată pe suportul din care a fost detașată cartela SIM, în cadrul audierii proprietarului/utilizatorului dispozitivului, din înscrisuri, prin încercarea de deblocare a codului PIN, utilizând combinațiile frecvent întâlnite, prin interpelarea operatorului de telefonie mobilă, prin exploatarea defectelor sau a vulnerabilităților sistemului, cunoscute în autentificare, prin intermediul programelor sau mijloacelor tehnice „backdoor" sau prin alte metode.

De regulă, pe cartela SIM este imprimat numărul unic de identificare – ICCID, format din 20 de cifre (prefixul de identificare industrial, codul țării, numărul de identificare al producătorului, numărul de identificare al contului individual). Totodată, cartela SIM poate stoca informații privind ICCID, MSISDN, numărul de apelare rapidă, ultimele numere formate, SMS, IMSI, informații de localizare (LOCI), cheia de criptare (Kc).

Introducerea de diferite cartele SIM poate conduce la ștergerea datelor din dispozitivul de comunicație. De aceea, uneori (dacă nu se cunoaște codul PUK sau în vederea evitării alterării datelor), se impune realizarea unei cartele SIM înlocuitoare, imitând cartela originală, iar pentru obținerea unor astfel de cartele pot fi folosite diverse instrumente criminalistice, cum ar fi: Forensic SIM Toolkit, GSM.XRY.SIM ID Cloner, TULP 2G SIMIC [26, p. 320].

Echipamentele utilizate cu telefonul mobil sau tableta, cum ar fi suporturile de date detașabile, cartela SIM, pot constitui potențiale probe, mai valoroase chiar decât telefonul însuși. Acestea se ridică, fără a fi detașate de la telefon sau tabletă. Proprietarul sau utilizatorul dispozitivului de comunicații poate fi interogat pentru a se afla codurile de securitate sau parolele [26, p. 314].

În vederea împiedicării traficului de date, a parvenirii mesajelor și apelurilor noi, a suprascrierii datelor existente, putem evidenția câteva modalități de izolare a dispozitivului de astfel de comunicație [26, p. 315]: închiderea telefonului sau a tabletei (în această situație, se activează codurile de autentificare, care pot să nu fie cunoscute investigatorului); utilizarea unui container „Faraday" sau a foliilor de aluminiu (ceea ce provoacă creșterea consumului de energie de la acumulator, datorită încercării zadarnice de conectare la rețea); utilizarea opțiunii „Airplane Mode" (metoda respectivă creează un risc din cauza interacțiunii cu tastele sau ecranul dispozitivului).

Producătorul, modelul telefonului, codul IMEI pot fi găsite în cavitatea în care se află acumulatorul. Detașarea acumulatorului poate afecta starea telefonului, mai ales conținutul

memoriei volatile, valoarea timpului menținut, și poate activa codurile de autentificare. Caracteristicile dispozitivelor mobile de comunicații pot fi stabilite și prin intermediul unor site-uri specializate, cum ar fi www.gsmarena.com [292].

În majoritatea cazurilor, este oportună deconectarea telefoanelor mobile, cu toate acestea acumulatorul nu trebuie extras. Totuși, în anumite cazuri, ofițerul de urmărire penală poate decide menținerea telefonului în stare funcțională, dacă informația parvenită ulterior ar putea avea importanță pentru cauză. În această din urmă situație urmează a fi încărcată periodic bateria acestuia [83, p. 127].

Atunci când telefonul a fost depistat închis, data și ora, diferențele față de ceasul de referință vor fi înregistrate imediat ce telefonul va fi deschis pentru prima dată în cadrul examinării.

Se va asigura încărcarea acumulatorului până la împachetarea și sigilarea dispozitivului.

Cercetarea (percheziționarea, ridicarea) suporturilor de stocare a datelor informatice include următorul algoritm [83, p. 129]: stabilirea tipului, modelului, destinației și parametrilor tehnici ai dispozitivului; stabilirea elementelor ce îl individualizează, a inscripțiilor, deteriorărilor fizice ș.a.; aprecierea stării tehnice a dispozitivului (mărimea, integritatea, existența mecanismelor de protecție a informației); stabilirea existenței, numărului și stării tehnice a prizelor de conectare la dispozitiv; identificarea semnelor de falsificare a purtătorului de informații și a protecției; verificarea, cu ajutorul programului specializat, a prezenței softurilor malițioase [217]; căutarea fișierelor ascunse, criptate și șterse.

Cercetarea documentelor electronice se efectuează în vederea descoperirii semnelor exterioare (rechizitelor) ale documentului și analiza conținutului acestuia. Algoritmul acțiunilor de examinare trebuie să fie realizat în următoarea consecutivitate [83, p. 131]:

1) fixarea formatului (de exemplu: *.doc, *.docx, *.xls, *.txt, *.pdf, *.jpg etc.);

2) stabilirea atributelor fișierului: aplicația cu ajutorul căreia a fost creat, numele fișierului, mărimea acestuia, data și timpul creării (sau al ultimei modificări, ștergeri), etichetarea fișierului (de sistem, din arhivă, ascuns, doar pentru citire, doar pentru înregistrare, ș.a.);

3) determinarea softului care permite vizualizarea conținutului;

4) accesarea conținutului documentului pe ecran, fotografierea sau înregistrarea video;

5) identificarea rechizitelor obligatorii ale documentului: datele utilizatorului care l-a elaborat, locul aflării (adresa electronică), data elaborării (sau copierii pe purtătorii de informații), mărimea documentului (numărul simbolurilor, paginilor, biților), rechizitele adresatului;

6) fixarea datelor suplimentare: numărul documentului în pachet (baza de date, folder), numărul telefonului (faxului), etc.;

7) analiza elementelor de editare a documentului: parametrii paginii, stilul textului, denumirea și mărimea fontului, conținutul textului ș.a.;

8) imprimarea documentului pe suport de hârtie și anexarea acestuia la procesul-verbal.

În cadrul acțiunilor de urmărire penală, efectuate în legătură cu cercetarea unei infracțiuni informatice, pot fi depistate și ridicate diverse ***documente importante pentru cauză***, cum ar fi: registrele de evidență a personalului [175, p. 913, 92, p. 912] și a orelor de lucru [57, p. 564, 87, p. 679], a accesului la sistemele informatice și bazele de date electronice [173, p. 721], a defecțiunilor tehnice constatate, a lucrărilor de reparație și de mentenanță petrecute [272, p. 259]; documentele purtătoare de urme privind infracțiunea comisă (facturi și agende telefonice, parole și coduri de acces, agende personale ș.a.) [60, p. 692, 175, p. 913, 92, p. 912]; documentele cu urme ale dispozitivelor periferice [56, p. 697] (dacă în timpul efectuării acțiunii procesuale imprimanta printează niște documente, trebuie așteptată definitivarea activității imprimantei, iar documentele printate urmează a fi descrise și ridicate [83, p. 116]); documente ce descriu mijloacele tehnice și produsele program, licențele și contractele de utilizare a acestora [60, p. 692, 173, p. 721, 87, p. 679]; documente și acte normative cu privire la reglementarea utilizării sistemelor și rețelelor informatice [56, p. 697]; documentele personale ale suspectului [56]; literatură și alte înscrisuri, care pot conține mențiuni, efectuate de către infractor, privind circumstanțele elaborării instrumentelor și mijloacelor infracțiunii [90, p. 238].

În concluzie, constatăm că, în cadrul cercetării infracțiunilor informatice, la efectuarea acțiunilor de urmărire penală sub formă de cercetare la fața locului, percheziție, ridicare de obiecte și documente, în procesul de pregătire de efectuare a acestora, organul de urmărire penală urmează să întreprindă anumite acțiuni preparatorii de bază specifice, iar odată ajuns la fața locului pentru realizarea acțiunii procesuale, ofițerul de urmărire penală trebuie să realizeze diverse măsuri preliminare, caracteristice cercetărilor informatice, să asigure respectarea unor reguli de ordin general și să țină cont de anumite recomandări de bază. Totodată, ofițerul de urmărire penală trebuie să decidă, în fiecare caz concret, ridicarea informației electronice, împreună sau fără suportul de stocare a datelor informatice, respectând anumite reguli specifice. Mai mult decât atât, examinarea sistemelor informatice se efectuează după anumite procedee și într-o anumită consecutivitate, în dependență de starea acestora (aflate sau nu în funcțiune, conectate sau nu la sursa de alimentare cu energie electrică). Ridicarea notebook-urilor, a tabletelor și a echipamentelor mobile, cercetarea suporturilor de stocare a datelor informatice și a documentelor electronice, de asemenea, se efectuează conform anumitor reguli și se caracterizează prin particularități specifice.

3.2. Audierea persoanelor în cadrul cercetării infracțiunilor informatice

Juristul nu dispune și nici nu poate dispune de cunoștințe în toate domeniile, de aceea, în vederea îndeplinirii sarcinilor sale, el trebuie să implice specialiștii din domeniile care nu-i sunt cunoscute sau în care are cunoștințe insuficiente. Specializarea și progresul actual al tehnicii nu permit reprezentantului unui domeniu să fie absolut competent în altul [78, p. 288].

În opinia cercetătorului N.N. Egorov, specialistul trebuie invitat să participe la audiere, atunci când organul de urmărire penală cunoaște că persoana audiată posedă cunoștințe vaste privind întrebările speciale și are o experiență bogată în domeniu. În aceste situații, ea începe să explice activ schema complicată a obiectelor și multiplele legături între ele, ceea ce solicită organului de urmărire penală un nivel înalt de cunoștințe într-o anumită ramură, precum și capacitatea de a înțelege noțiunile respective [62, p. 197]. Specialistul ar putea acorda un ajutor considerabil, în acest sens, nu-i va permite persoanei audiate să preia inițiativa, va reuși să mențină audierea în limitele obiectului cauzei și să se facă trimiteri la probele existente.

Totuși, prezența unei alte persoane decât cea audiată și cea care efectuează audierea, ar putea crea obstacole în stabilirea contactului psihologic. În cazul dat, se impune obligatoriu consultarea prealabilă a organului de urmărire penală cu specialistul, în vederea pregătirii de audiere.

În vederea stabilirii circumstanțelor relevante pentru cauze, în cadrul audierii martorilor, organul de urmărire penală va ține cont de întrebările-tip, specifice pentru cercetarea acestei categorii de infracțiuni [74, p. 7]. Astfel, în cadrul audierii martorului, urmează a se stabili: persoanele care au manifestat interes față de informația computerizată, față de soft și mijloacele tehnice; persoanele străine, care au vizitat încăperea în care se află sistemele informatice; fixarea cazurilor de prelucrare de către angajații companiei a informației care nu ține de competența lor; existența perturbărilor în activitatea produselor program, sustragerea purtătorilor de informație electronică și a sistemelor informatice; fixarea cazurilor de perturbare a funcționării sistemelor și rețelelor informatice, a mijloacelor de protecție; verificarea produselor program în privința virusării acestora, analiza rezultatelor ultimelor verificări; frecvența actualizării softurilor, identificându-se prin ce modalitate și de către cine au fost actualizate; procedura de procurare, reparare și modernizare a sistemelor informatice, cine a fost implicat și când; procedura de lucru, modul de prelucrare și transmitere a informației computerizate; persoanele care sunt conectate la această rețea informatică, precum și competențele acestora, modalitatea de realizare a conexiunilor; modul de realizare și mijloacele de protecție a informației; posibilitatea cauzării prejudiciului de neglijența angajaților, de defecțiunile sistemului sau ale rețelei informatice; caracterul modificărilor informației; proprietarul (utilizatorul legal) al informației copiate

(distruse, modificate, blocate). În cazul martorilor oculari, se vor mai concretiza: circumstanțele în care martorul a văzut infractorii (fapta infracțională); modul săvârșirii infracțiunii; rolul fiecărui participant implicat în infracțiune; cunoașterea scopului urmărit de către făptuitori; existența anterioară a unor cazuri similare; particularitățile fizice ale făptuitorului.

În cazul victimei, martorului sau a bănuitului/învinuitului, tactica audierii trebuie să ia în considerare personalitatea acestora [91, 60, p. 693].

În situația în care victima infracțiunii este o persoană juridică, trebuie audiați în calitate de martori toți angajații implicați în fapta cercetată, cum ar fi: administratorul de rețea, operatorul sistemelor informatice, programatorii, persoanele responsabile de securitatea informatică, angajații responsabili de deservirea tehnică a sistemelor informatice, contabilul, managerul și alții [90, p. 236]. În dependență de funcția ocupată în cadrul întreprinderii-victimă, angajații vor fi audiați cu privire la anumite circumstanțe ale cauzei [74, p. 8].

La audierea victimei (persoană fizică), urmează a se constata: sistemele informatice utilizate de către victimă; nivelul cunoștințelor referitoare la proprietățile sistemelor informatice și ale dispozitivelor complexe; cunoașterea specificului produselor program, instalate la calculator, și a mijloacelor tehnice; ISP cu care a încheiat contract de prestare a serviciilor, precum și condițiile contractuale; modul în care a aflat despre infracțiunea săvârșită și sursa de informare; condițiile în care a avut loc contactul vizual cu făptuitorul infracțiunii.

Întrebări specifice există și la audierea operatorilor sistemelor informatice (regulile de completare a registrelor, ordinea primirii-predării schimburilor; regimul de lucru al operatorilor; ordinea identificării operatorilor; regulile de păstrare, distrugere a listing-urilor, categoriile de persoane care au acces la ele; procedura de acces în încăperile în care se află sistemele informatice, categoria de angajați cărora le este permisă utilizarea acestora și altele), a programatorilor (lista softurilor utilizate și clasificarea acestora în licențiate/personale; parolele de protecție a softurilor și frecvența de modificare a acestora; caracteristicile tehnice ale rețelelor informatice și administratorul lor; procedura de procurare și actualizare a softurilor; existența în softuri a fișierelor în care se înregistrează intrările și care este conținutul acestora etc.), a administratorului rețelei informatice (existența mijloacelor tehnice speciale de protecție a informației; ordinea de acces a utilizatorilor la rețeaua informatică; procedura de autentificare a utilizatorilor sistemelor informatice și regimul de lucru al utilizatorilor rețelei informatice; ordinea de acces a angajaților la sisteme informatice în afara programului; modul de acordare și modificare a parolelor utilizatorilor; caracteristica măsurilor de protecție a informației), a angajaților care se ocupă de deservirea tehnică (lista și caracteristicile tehnice ale sistemelor informatice instalate la întreprindere; lista mijloacelor tehnice de protecție; frecvența deservirii

tehnice, a efectuării lucrărilor profilactice și de reparație; cazuri de conectare neautorizată la rețelele de comunicații telefonice, instalarea dispozitivelor electrice suplimentare), a administratorului - persoană juridică (specificul activității și sediul persoanei juridice; actele cu privire la înregistrarea persoanei juridice și dispunerea ei de licențe; regimul activității, existența pazei, a sistemelor de alarmă, a punctului de control, programul intern, atribuțiile funcționale; volumul activității, caracterul, tipul și prevederile contractelor încheiate, denumirea și locul aflării concurenților; conținutul și volumul informației stocate în calculator, existența codurilor și a parolelor de acces către această informație; probele materiale cu privire la existența, caracterul și volumul prejudiciului cauzat; cine dintre angajați a intrat în contact cu suspectul și în ce condiții, perioada de activitate a lui în această funcție; temeiul juridic de reprezentare a intereselor companiei în cadrul organelor de drept, procura/contractul de prestări servicii; modul de constatare a incidentului; circumstanțele cunoscute; persoanele care pot comunica organului de urmărire penală informații de ordin tehnic și juridic; existența în cadrul companiei a subdiviziunilor specializate de utilizare a rețelelor informatice și serviciilor de securitate, componența și competența acestora; certificarea softurilor de protecție și a mijloacelor tehnice; structura organizatorică a sistemelor și rețelelor informatice; existența regulilor interne de exploatare a sistemelor și rețelelor informatice, procedura de informare a angajaților privind aceste reguli și monitorizarea respectării lor; lista angajaților concediați în perioada respectivă și motivele concedierii; cazuri de pătrundere neautorizată în încăperile în care se află sistemele informatice; cazuri de accesare neautorizată a informației computerizate, virusări ale sistemelor informatice și altele; opinia cu privire la mecanismul de săvârșire a infracțiunii, precum și cauzele și condițiile parvenirii rezultatelor infracțiunii).

În corespundere cu prevederile art.153 din CPP, în cazul în care raportul expertului nu este clar sau are unele deficiențe, pentru a căror înlăturare nu sunt necesare investigații suplimentare, ori a apărut necesitatea de a preciza metodele aplicate de către expert sau unele noțiuni, organul de urmărire penală este în drept să audieze expertul după prezentarea raportului de expertiză, respectându-se prevederile art.105-109 din CPP.

În cadrul audierii bănuitului și învinuitului, în fiecare caz concret, organul de urmărire penală trebuie să stabilească, cel puțin, anumite circumstanțe de bază [93, p. 215]. Printre circumstanțele de bază care urmează a fi stabilite la audierea acestora sunt: unde, în ce perioadă și în ce calitate a activat; studiile obținute (instituție, domeniul și perioada); competențele de lucru la calculator, dispunerea de anumite softuri, nivelul de calificare; persoana care l-a instruit cum să utilizeze softul în cauză; codurile și parolele care i-au fost acordate (inclusiv, de lucru în sistemul și/sau rețeaua informatică); produsele program la care are acces și nivelul accesului; tipurile de

operațiuni electronice pe care le executa în momentul săvârșirii infracțiunii; procedura de accesare a sistemului și/sau a rețelei informatice; dacă are restricții de acces în încăperea în care sunt instalate sistemele informatice; dacă i-a fost adusă la cunoștință fișa de post (atribuțiile funcționale); dacă i-au fost aduse la cunoștință regulile de prelucrare a informației și instrucțiunile cu privire la utilizarea și securitatea sistemelor informatice; cazuri de încălcare a regimului de lucru, a procedurii de efectuare a lucrărilor, a ordinii de acces la informația computerizată; modul de distrugere a urmelor infracțiunii.

În dependență de categoria infracțiunii informatice săvârșite, la audierea bănuitului/învinuitului, se va ține cont de anumite întrebări-tip, spre exemplu:

- în cazul infracțiunilor prevăzute la art.259 CP și al altor infracțiuni similare: informația computerizată la care are acces; operațiunile de prelucrare a informației pe care are dreptul să le execute; nivelul drepturilor de acces la informație; modalitatea de accesare neautorizată a informației computerizate; modul de pătrundere în încăperea în care sunt instalate sistemele informatice și de conectare la rețeaua informatică; restricțiile de acces în încăperea unde sunt instalate sistemele informatice; de unde a aflat parolele și codurile de acces la informație; parvenirea propunerilor de la alte persoane de transmitere a informației, softurilor; persoanele care și-au manifestat interesul de a obține parolele și codurile de acces; cunoașterea faptului că informația obținută este protejată de lege; persoanele care l-au informat despre datele informatice stocate în calculator; conținutul informației pe care a accesat-o, a distrus-o, a deteriorat-o, a modificat-o, a blocat-o sau a copiat-o; scopul urmărit la comiterea faptei; proprietarul/utilizatorul legal al informației pe care a accesat-o ilegal; modul de utilizare a informației obținute;
- în cazul infracțiunii prevăzute la art.260 CP și al altor infracțiuni similare: modul de dobândire a mijlocului tehnic/produsului program; limbajele de programare pe care le posedă; scopul producerii, importului, comercializării, transmiterii mijloacelor tehnice/produselor program; specificul și modul de utilizare a mijlocului tehnic/produsului program; stabilirea produselor program al căror autor este necunoscut; cazuri de perturbare a funcționării mijlocului tehnic și a dispozitivelor de protecție a informației într-o anumită perioadă de timp; stabilirea cazurilor de alterare a funcționării produselor program, identificarea virușilor electronici, precum și alte dereglări în funcționarea softurilor; algoritmul de funcționare a produsului program;
- în cazul infracțiunii prevăzute la art.261 CP și al altor infracțiuni similare: dacă ține minte regulile de prelucrare a informației computerizate, de utilizare a sistemelor și rețelelor informatice; atribuțiile sale funcționale în cadrul întreprinderii; documentele și înscrisurile în care a fost fixată activitatea sa în ziua săvârșirii infracțiunii; operațiunile efectuate la calculator de persoana audiată în ziua comiterii infracțiunii; respectarea cerințelor de protecție antivirus; momentul constatării

faptului de însușire, denaturare sau distrugere a informației ori de provocare a altor urmări grave; măsurile întreprinse în vederea neadmiterii agravării situației; existența legăturii dintre încălcarea regulilor de prelucrare, utilizare și/sau securitate a sistemelor informatice cu însușirea, denaturarea sau distrugerea informației ori cu provocarea altor urmări grave.

La procesul-verbal de audiere pot fi anexate schemele întocmite de către persoana audiată în cadrul acțiunii de urmărire penală, cum ar fi configurația sistemului, schema deplasării informației ș.a. [248, p. 629].

În concluzie, accentuăm că la cercetarea infracțiunilor informatice întrebările-tip expuse mai sus sunt extrem de relevante în vederea stabilirii tuturor circumstanțelor cauzei penale, ele vor asigura ca ofițerul de urmărire penală/procurorul să nu scape din vedere anumite împrejurări sau situații, să cerceteze concomitent toate versiunile posibile. Totuși, organul de urmărire penală va lua în calcul și particularitățile fiecărui caz concret, suplimentând întrebările-tip, care urmează a fi adresate persoanei audiate, cu anumite chestiuni specifice cazului.

3.3. Cercetarea la fața locului

Recentele completări, operate la art.118 alin.(1) din CPP [293], prin introducerea noțiunii de „cercetare la fața locului a sistemelor informatice sau a suporturilor de stocare a datelor informatice", vin să reflecte particularitatea „virtuală" a obiectelor respective, subliniază „netradiționalitatea" stocării datelor electronice, ceea ce nu este caracteristic tipurilor de cercetări existente [81, p. 43]. În aceste condiții, organul de urmărire penală trebuie să țină cont de specificul fixării probelor electronice, respectându-se, desigur, normele procesuale cu privire la efectuarea acestei acțiuni de urmărire penală.

Totodată, după cum am menționat anterior, legiuitorul român a reglementat investigațiile asupra dispozitivelor electronice la capitolul acțiunilor de urmărire penală sub formă de percheziție, și anume *percheziția sistemelor informatice* [294]. Condiția obținerii autorizației legale, organul competent să dispună efectuarea acesteia, intervalul de timp în care se poate efectua sunt stabilite de normele procesual-penale generale [295, p. 177].

Cercetarea la fața locului este una din acțiunile de bază ale procesului penal cu privire la investigarea infracțiunilor informatice, ea se efectuează la etapa incipientă a procesului penal și este una din cele mai informative (din punct de vedere criminalistic) acțiuni de urmărire penală inițială, mersul și direcția investigațiilor fiind determinate, în mare măsură, de rezultatele obținute în cadrul cercetării la fața locului. Totodată, trebuie menționat că este foarte dificil a înlătura

ulterior, în cadrul urmăririi penale, erorile și lacunele admise la efectuarea acesteia [83, p. 109, 296, p. 18].

După luarea deciziei de a efectua cercetarea la fața locului, pe lângă acțiunile de bază, valabile pentru toate acțiunile de urmărire penală descrise mai sus, în prezentul capitol, ofițerul de urmărire penală va întreprinde și anumite măsuri, specifice cercetării la fața locului, cum ar fi: asigurarea pazei locului comiterii infracțiunii, până la sosirea ofițerului de urmărire penală; luarea măsurilor de prevenire sau diminuare a urmărilor prejudiciabile ale infracțiunii informatice; asigurarea prezenței, la momentul sosirii sale, a persoanelor care ar putea deține informații necesare despre infracțiune: administratorul rețelei, conducătorul subdiviziunii de securitate internă în cadrul întreprinderii, martorii oculari, operatorii sistemelor informatice, analiștii, contabilii și alte persoane [272, p. 200].

Odată ajuns la fața locului pentru realizarea cercetării, ofițerul de urmărire penală, suplimentar la măsurile de bază valabile pentru majoritatea acțiunilor de urmărire penală, efectuate la cercetarea infracțiunilor informatice, va identifica persoanele care au fost la fața locului până la sosirea organului de urmărire penală, precum și modificările efectuate de către aceste persoane [272, p. 205].

Totodată, în art.118 din CPP au fost introduse prevederi noi, potrivit cărora, la cererea persoanei care deține sau are sub control obiectele ce conțin date informatice, organul de urmărire penală dispune, prin ordonanță motivată, efectuarea de copii, care servesc ca mijloc de probă. Copiile se realizează prin utilizarea metodelor și mijloacelor tehnice ce asigură integritatea și autenticitatea datelor informatice [293].

Particularitățile investigării unei pagini web sau a unui site

De regulă, una dintre primele acțiuni procesuale care urmează a fi efectuată de către organul de urmărire penală la cercetarea unei infracțiuni informatice este cercetarea la fața locului a paginilor web (site-urilor), prin intermediul cărora a fost comisă fapta prejudiciabilă.

Printre obiectivele de bază ale cercetării online sunt: 1) examinarea materialului publicat; 2) stabilirea datelor cu privire la numele de domeniu; 3) identificarea datelor serverului-gazdă [212, p. 244].

Rezultatele cercetării paginii web/site-ului pot fi obținute și printr-o altă acțiune procesuală, și anume, prin constatarea tehnico-științifică asupra acestor resurse informatice. Ambele acțiuni pot fi realizate la orice etapă a procesului penal și nu necesită autorizarea judecătorului de instrucție. La luarea deciziei cu privire la procedeul probatoriu care urmează a fi aplicat, organul de urmărire penală trebuie să se conducă de următoarele două caracteristici [212, p. 245]:

a) rezultatele obținute în cadrul constatării tehnico-științifice parvin la organul de urmărire penală (ordonator) într-o perioadă de timp mai îndelungată, chiar până la câteva luni, spre deosebire de cercetare, care poate dura până la câteva ore;

b) constatarea tehnico-științifică poate oferi informații tehnice suplimentare sau mai detaliate decât cele acumulate în rezultatul cercetării la fața locului.

Din motivele sus-menționate, este oportună invitarea unui specialist în domeniul IT la cercetarea paginilor web sau ale site-urilor, care își expune concluziile în procesul-verbal al acțiunii de urmărire penală.

1. *Examinarea materialului publicat (difuzat, distribuit)* are un rol deosebit în cazul cercetării infracțiunilor referitoare la pornografia infantilă, la atingerile aduse proprietății intelectuale și drepturilor conexe, precum și în cazul altor infracțiuni informatice.

În urma examinării materialului publicat, organul de urmărire penală urmează să stabilească următoarele împrejurări [212, p. 245]:

a) dacă materialul conține imagini sau alte reprezentări ale unui sau mai multor copii, implicați în activități sexuale explicite, reale sau simulate, ori imagini sau alte reprezentări ale organelor sexuale ale unui copil, prezentate într-o manieră lascivă sau obscenă, în cazul pornografiei infantile;

b) *parametrii (proprietățile, atributele, metadatele) materialelor electronice publicate*, îndeosebi cei referitori la timp [31, p. 39], locație, hardware și software (Anexa nr. 12).

Data și timpul creării (compilării, fotografierii, filmării etc.), al modificării sau al altei acțiuni de prelucrare a materialului permite investigatorului să stabilească perioada pregătirii instrumentelor pentru săvârșirea infracțiunii sau, după caz, timpul săvârșirii nemijlocite a infracțiunii.

În cazul materialelor foto/video, în proprietățile fișierului pot fi identificate datele cu privire la echipamentul prin intermediul căruia a fost creat materialul (marca, modelul și setările aparatului). Aceste informații vor orienta organul de urmărire penală, la momentul efectuării percheziților domiciliare, corporale ș.a., în privința obiectelor care urmează a fi descoperite.

În situația în care la prelucrarea materialului au fost folosite anumite software, denumirea și versiunea acestora poate fi prezentă în metadatele fișierului. La examinarea calculatorului făptuitorului de către specialistul/expertul IT, depistarea unor urme ale folosirii acestui produs program va fi o probă suplimentară în dovedirea vinovăției.

Unele echipamente (aparate foto, camere video, telefoane mobile, alte echipamente) au opțiunea localizării GPS, iar la crearea materialului, datele locației sunt inserate în metadate [122, p. 143, 77, p. 9]. Informația despre latitudinea și longitudinea locației poate ajuta organul de

urmărire penală în stabilirea, cu maximă precizie, a locului pregătirii infracțiunii sau al comiterii ei.

Totodată, în proprietățile fișierului pot fi depistate date cu privire la calea (locul) din calculatorul făptuitorului, de unde a fost încărcat (distribuit) materialul (de exemplu: /home/ionescu/Desktop/Poze/IUBI/). Din aceste informații putem stabili datele de login ale utilizatorului sistemului informatic (în cazul de față, „ionescu"), în care au fost create, prelucrate sau păstrate materialele publicate, denumirea mapei în care au fost păstrate fișierele (în speță, „IUBI"). Aceste date, uneori, pot fi foarte relevante pentru identificarea presupusului făptuitor, îndeosebi, în urma audierii victimei și a prezentării acesteia a datelor stabilite.

c) *obiectul/victima infracțiunii*. În cazul infracțiunilor îndreptate împotriva proprietății intelectuale și a drepturilor conexe, organul de urmărire penală trebuie să identifice opera protejată, și anume: denumirea, versiunea, volumul, autorul, formatul, precum și alte particularități ale ei.

Un rol deosebit în examinarea materialelor publicate, în situația examinării unui caz de pornografie infantilă, îl are stabilirea identității victimei, inclusiv a vârstei acesteia la momentul realizării materialului foto/video. În dependență de vârsta persoanei care apare în imagine (persoană minoră sau persoană majoră), fapta urmează a fi încadrată – fie conform art.208/1 din CP („Pornografia infantilă"), fie conform art.90 din CCo („Producerea, comercializarea, difuzarea sau păstrarea produselor pornografice"). Totodată, legislația prevede imperativ faptul că atingerea de către partea vătămată a unei anumite vârste, dacă aceasta are importanță în cauză, trebuie constatată prin certificat de vârstă, iar în caz de incapacitate legată de vârstă sau dacă documentele ce confirmă vârsta prezintă dubiu – prin raportul expertizei medico-legale sau psihiatrice.

d) *împrejurările în care a fost efectuat materialul* pot fi stabilite la examinarea nemijlocită a materialului foto/video. În acest sens, organul de urmărire penală trebuie să acorde atenție și obiectelor/persoanelor din planul doi, cum ar fi: mobilier, numere de înmatriculare ale autoturismelor, denumiri de străzi, relief, denumiri regionale, branduri, mărci comerciale (spre exemplu, o umbrelă cu logoul unei companii care are tangență cu făptuitorul).

e) *paginile web/website-urile, șterse sau modificate* de către făptuitor – fie în mod intenționat, fie în lipsa voinței sale – până la momentul sesizării organului de urmărire penală, pot fi examinate în starea lor inițială, prin intermediul mai multor utilitare. Astfel, motoarele de căutare servesc, în mod frecvent, direct din cache paginile web pe care le-au indexat. De exemplu, Google oferă o legătură „din cache" lângă majoritatea rezultatelor căutării. O altă utilitară este Internet Archive Wayback Machine (www.archive.org) – un serviciu de arhivare a paginilor de internet (înființat în 1996). Acest serviciu oferă și un motor de căutare prin zeci de miliarde de

pagini arhivate, astfel încât utilizatorul are posibilitatea de a consulta materiale care, în prezent, nu se mai află pe internet, în locația lor originală, la o anumită dată (potrivit exemplelor expuse în Anexa nr. 13).

f) *alte mijloace de identificare a victimelor și făptuitorilor*. International Child Sexual Exploitation Image Database (ICSE) [297] a Interpolului este un proiect care certifică creșterea numărului de copii identificați și salvați de la abuzuri. Un instrument de bază îl constituie programele informatice sofisticate de comparare a imaginilor, care pot face conexiuni între victime și locuri. De asemenea, acest instrument permite utilizatorilor autorizați din țările membre ale Interpol să acceseze direct și în timp real baza de date.

Baze de date similare au fost create de către Europol, Inhope Foundation (www.inhope.org) [298], în care sunt adunate adresele web raportate, ce găzduiesc pornografie infantilă [122, p. 129].

Valoarea funcției hash a fișierelor depistate poate fi utilizată de către investigator în scopul căutării acestora în bazele de date respective [299, p. 369-370].

O altă resursă publică în care sunt acumulate date privind paginile web cu activitate malițioasă este www.malwareurl.com [300].

Torentele se întemeiază pe tehnologia P2P, în baza căreia se formează o rețea virtuală de utilizatori, iar pentru a avea acces în această rețea, doritorii trebuie să folosească un program-tip P2P (uTorrent, BitTorrent, eDonkey, Gnutella, FastTrack, KaZaA, Morpheus, FreeNet, WinMx, iMesh, etc.) și să pună la dispoziție celorlalți utilizatori fișiere cu informații pe calculator (filme, muzica, programe, fotografii etc.). În cadrul unui proces penal, aceste produse sunt considerate instrumente de bază ale săvârșirii infracțiunii de încălcare a dreptului de autor și a drepturilor conexe, ale pornografiei infantile, iar protocolul prin intermediul căruia are loc descărcarea fișierelor –drept mijloc al săvârșirii infracțiunii. De altfel, aceste aplicații pot fi folosite și de către organul de urmărire penală, pentru a stabili adresele IP ale sistemelor informatice, utilizate la descărcarea/încărcarea fișierelor cu conținut ilicit, și, în cele din urmă, a persoanelor care stau în spatele acestor sisteme informatice. Astfel, investigatorul urmează să stabilească materialul publicat pe site-ul de torent (fișierul) și să pornească descărcarea acestuia. Imediat după inițierea descărcării, la rubrica „Parteneri” vor apărea adresele IP implicate în punerea la dispoziție a fișierelor ilicite (Anexa nr. 14.).

Totodată, o atenție deosebită trebuie acordată conținutului „invizibil” al unui site, care conține, înainte de toate, limbajul de programare (HTML, CSS, Javascript etc.) folosit la crearea paginii web [122, p. 103]. Codul-sursă al unei pagini web reprezintă un text, care definește conținutul și formatul unei pagini. Pe lângă reprezentarea grafică, pagina web poate conține

informații suplimentare „invizibile”, cum ar fi: comentariile utilizatorilor și administratorilor (parolele de logare, referințele cu privire la identitate sau locație), câmpurile ascunse, referințele către site-urile externe, care pot furniza informații suplimentare pe caz [122, p. 104], autorul paginii web, codul program, metadata și alte informații de identificare, care pot să nu apară în conținutul „vizibil” al paginii web [26, p. 272]. Un exemplu de instrument electronic gratuit pentru examinarea unei pagini web este FireBug (care rulează în browser-ul Chrome).

Conturile din majoritatea rețelelor de socializare sunt create cu utilizarea unei anumite adrese (poște) electronice și/sau număr de telefon, acest fapt poate ușura activitatea organului de urmărire penală în depistarea conturilor folosite de către făptuitor.

Dacă numele contului unei persoane dintr-o rețea de socializare poate fi, de regulă, modificat, atunci numărul de identificare al acestui cont (ID-ul) rămâne neschimbat. Acest ID poate fi stabilit chiar din URL-ul care ne direcționează către contul respectiv. Spre exemplu la Facebook ar fi http://www.facebook.com/photo.php?fbid=**123456789012345** (ID-ul este 123456789012345), iar în Odnoklassniki https://ok.ru/profile/**123456789012** (ID 123456789012). Din rețelele de socializare putem identifica denumirea contului (conform exemplului din Anexa nr. 15), cercul de prieteni/cunoscuți, locații, mesaje, comentarii, imagini și alte date relevante.

Datele noi obținute prin investigațiile efectuate (denumirile de conturi, numerele de telefon, numele de persoane etc.), urmează, la rândul lor, să fie și ele verificate prin intermediul motoarelor de căutare, în vederea obținerii datelor (informațiilor) noi.

2. *Stabilirea datelor cu privire la numele de domeniu* (de exemplu*:* www.usm.md) [212, p. 253] este necesară atât în cazul în care făptuitorul creează un site pentru comiterea infracțiunii, cât și atunci când făptuitorul utilizează o parte (o pagină sau mai multe pagini web) a unui site existent. Dacă, în primul caz, examinarea datelor referitoare la numele de domeniu ne-ar putea direcționa către autorul infracțiunii, atunci în cel de-al doilea caz, vom putea stabili persoana fizică sau juridică (administratorul, fondatorul site-ului), de la care ar putea fi ridicate informații relevante pentru identificarea făptuitorului (adresele de IP la înregistrarea contului/logare, data și timpul înregistrării/logării, informația publicată/modificată/ștearsă, e-mailul, mesajele din cont, mijloacele de plată, datele de contact, inclusiv adresă, telefonul și altele).

a) *numele de domeniu .md.* Potrivit pct.15 lit.b) din Concepția sistemului informațional automatizat, „Registrul resurselor și sistemelor informaționale de stat” [301] Î.S. „MoldData” înregistrează posesorii numelor înregistrate în domenul de nivel superior .md. Totodată, pagina web http://nic.md/RO/wh1.php permite identificarea persoanelor pe numele cărora au fost înregistrate numele de domeniu .md (Anexa nr. 16 din prezenta lucrare).

b) *alte nume de domeniu* pot fi verificate prin diverse utilitare online, ce oferă informații atât cu privire la deținătorul numelui de domeniu, cât și cu privire la serverul care găzduiește site-ul, situații pe care le vom analiza mai jos.

3. *Fixarea datelor serverului-gazdă* [212, p. 255]. Sistemele de operare permit identificarea adresei IP a unui site prin comanda: „ping" + numele de domeniu al site-ului investigat (Anexa nr. 17). Ulterior, după obținerea adresei IP, datele cu privire la ISP căruia i-a fost alocată această adresa IP vor fi identificate prin intermediul registratorilor internaționali, în dependență de regiunea unde ISP prestează serviciile internet: AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC.

Totodată, există utilitare care efectuează activitățile descrise mai sus în mod automatizat, oferind toată informația necesară cu privire la numele de domeniu, adresa IP a serverului, ISP precum și alte date relevante, doar prin introducerea numelui de domeniu.

Cele mai des utilizate unelte online de acest gen sunt www.whois.domaintools.com și http://www.ip-adress.com/whois/, prin intermediul cărora se vor obține: data creării serverului, adresa IP a serverului, ISP căruia îi este alocată adresa IP a serverului, datele registratorului, titlul website-ului găzduit pe server, datele persoanei pe numele căreia este înregistrat numele de domeniu, data creării/înregistrării și expirării numelui de domeniu, datele DNS, numele de domenii ale altor site-uri, găzduite pe același server și alte date.

Această ultimă informație este foarte relevantă, în cazul în care pe același server sunt găzduite mai multe site-uri, care pot ajuta la identificarea organizatorului infracțiunii, dat fiind că, de regulă, făptuitorul arendează un server întreg, pentru a avea acces deplin la el, inclusiv în vederea ascunderii/ștergerii urmelor infracțiunii. Serverul poate fi folosit și pentru alte activități ale făptuitorului, legale sau ilegale. Deseori infractorii au bloguri/forumuri în care își împărtășesc experiența într-un anumit domeniu, în diverse scopuri, și unde nu-și ascund identitatea. Aceste bloguri/forumuri pot fi găzduite pe același server cu site-ul implicat în săvârșirea infracțiunii.

Procesul-verbal al cercetării la fața locului a unei pagini web sau site [212, p. 258].

Motoarele de căutare și site-urile de arhive pot să nu reușească să indexeze un anumit site sau pagină web, importante pentru stabilirea circumstanțelor infracțiunii, fapt care poate avea drept consecință imposibilitatea organului de urmărire penală de a demonstra că o anumită pagină web sau website, la momentul cercetării acestuia, avea un anumit conținut. Ținând cont de aceste constatări, investigatorul urmează să efectueze capturi de ecran („screenshot") ale unei anumite pagini cu ajutorul unor combinații de taste (tastarea concomitentă CTRL-PRNT SCRN) [56, p. 694] sau aplicații: „Snipping Tool", „FastStone Capture, Jing", „Skitch", „Snagit" etc.

Unele browsere (Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome, Opera, Nintendo, Flock) au extensii (suplimente), destinate funcției de a capta imaginea parțială (partea vizibilă a unei pagini web, nederulată pe ecranul calculatorului) sau integrală (derulată din partea de sus a paginii web până la finalul acesteia). Exemple de astfel de extensii sunt „Nimbus Screen Capture", „Easy Screenshot", „ScreenShotLink", „Instances Screen Capture", „Screenshoter", „Screengrab" și altele.

Totodată, examinatorul urmează să efectueze captura în așa fel, încât să fie vizibile și datele cu privire la linkul paginii capturate, pentru a fi clar cărei pagini web i-a aparținut captura.

Totuși, în situația în care pentru comiterea infracțiunii a fost folosit întregul site sau din alte motive, organul de urmărire penală are nevoie să efectueze capturi de ecran la toate paginile web ale site-ului sau o parte considerabilă a acestora, care pot fi uneori până la câteva zeci de mii, atunci există aplicații care efectuează copia off-line a site-ului, fără a fi necesară deschiderea manuală a fiecărei pagini web. Ulterior investigatorul va putea să acceseze această copie ori de câte ori va avea nevoie, în starea în care se afla la momentul cercetării site-ului și fără a fi conectat la rețeaua internet. Printre aplicații de acest gen sunt „HTTrack website copier" [122, p. 120] (cel mai des utilizată), „Cyotek WebCopy", „SiteSucker" ș.a.

Rezultatele obținute în urma efectuării capturilor de ecran, precum și a copiilor site-urilor se înregistrează pe un suport optic de stocare a informației de tip CD sau DVD, care se va anexa la procesul-verbal de cercetare la fața locului (a paginii web sau a website-ului). Imprimarea acestora pe suport de hârtie poate fi ineficientă și incomodă pentru analiza ulterioară a probelor.

Persoana care întocmește procesul-verbal trebuie să descrie amănunțit faptele constatate, măsurile luate (fiecare acțiune, fiecare apăsare de taste sau mouse), mijloacele tehnice utilizate, condițiile și modul de aplicare a lor, precum și rezultatele obținute [92, p. 911].

3.4. Percheziția, ridicarea de obiecte și documente. Conservarea imediată a datelor cu privire la traficul informatic

În cazul cercetării infracțiunilor informatice, este oportună efectuarea operativă a percheziției, în măsura posibilităților, chiar imediat după pornirea urmăririi penale, deoarece acest fapt va asigura depistarea și ridicarea probelor, a mijloacelor și instrumentelor infracțiunii [90, p. 237, 232, p. 665]. Cadrul procesual penal cu privire la efectuarea percheziției și ridicării de obiecte și documente este reglementat în art.125-132 CPP.

În situația în care organul de urmărire penală intenționează să examineze, în cadrul percheziției sau ridicării, sistemele și rețelele informatice, alte dispozitive electronice, existente în

încăperea sau asupra persoanei percheziționate, atunci în cuprinsul actelor procesuale cu privire la dispunerea, solicitarea autorizării și autorizarea acțiunii de urmărire penală, trebuie să fie indicate și dispozitivele electronice care urmează a fi percheziționate și ridicate [12, p. 206, 302], în vederea asigurării dreptului la secretul corespondenței, la viața intimă, familială și privată [303, p. 74].

În procesul de pregătire pentru efectuarea percheziției sau ridicarea de obiecte și documente, suplimentar la acțiunile preparatorii de bază descrise în prezentul capitol, ofițerul de urmărire penală [74, p. 35]: va constata ce fel de echipament se află în încăperea care urmează a fi percheziționată, precum și cantitatea acestuia; va stabili dacă sunt folosite dispozitive de alimentare autonomă, precum și consecințele deconectării energiei electrice; va studia personalitatea proprietarului (utilizatorului) sistemului informatic, aptitudinile lui profesionale în domeniul IT; va stabili ora efectuării acțiunii de urmărire penală și măsurile de asigurare a confidențialității acesteia.

Totuși, alegerea timpului depinde de factori diferiți, precum ar fi: tipul sistemului și al rețelei informatice; prezența sau lipsa personalului; în zilele de odihnă, de regulă, sistemele informatice sunt deconectate de la rețea [304, p. 224]. Cel mai reușit interval de timp pentru realizarea acestei acțiuni de urmărire penală sunt orele matinale – între 06:00 și 08:00. În această perioadă, de regulă, sistemele informatice sunt deconectate, ceea ce diminuează riscul distrugerii informației electronice. Lipsa personalului (angajaților) însă complică obținerea documentelor tehnice necesare [103, p. 697].

În cadrul efectuării percheziției sau ridicării de obiecte și documente, pe lângă regulile generale cu privire la efectuarea acțiunilor de urmărire penală descrise în acest capitol, organul de urmărire penală trebuie să respecte și anumite reguli specifice.

Odată ajunși la fața locului, membrii echipei trebuie să pătrundă rapid și inopinat în încăpere, în vederea preîntâmpinării distrugerii datelor informatice [74, p. 37]. Persoanelor prezente trebuie să le fie interzisă atingerea și folosirea dispozitivelor electronice și de comunicații: computere, suporturi de stocare a informației, telefoane mobile, tablete, fax și altele [89, p. 56, 103, p. 702]. Imediat după ce membrii echipei au intrat în încăpere, trebuie să fie asigurată paza sistemelor informatice, precum și a sursei de energie electrică [295, p. 136].

Dacă există suficiente temeiuri de a presupune că persoana prezentă în încăperea în care se efectuează percheziția are asupra sa mijloace de comunicare, purtători de informație electronică, obiecte destinate pentru distrugerea datelor informatice, inițial ,urmează a fi efectuată percheziția ei corporală, în vederea depistării și ridicării acestor obiecte [232, p. 665-666].

Atunci când există temeiuri de a bănui că despre efectuarea acțiunii procesuale cunosc complicii infractorului, care se află în afara ariei acțiunii procesuale, trebuie neîntârziat deconectate conexiunile de rețea de la dispozitivele electronice (decuplarea cablurilor de rețea, deconectarea modemelor și routerelor, oprirea utilizării regimului Wi-Fi și transmiterii pachetelor de date) [83, p. 115]. Nu trebuie conectate dispozitivele informatice, depistate în stare deconectată. Este necesară efectuarea fotografiilor și/sau înregistrărilor video a tuturor dispozitivelor informatice (sau, cel puțin, întocmirea unei scheme detaliate privind montajul), îndeosebi, al cablurilor periferice [83, p. 115, 49, p. 31], în vederea asigurării posibilității reconstruirii modului de funcționare a întregului sistem [92, p. 911].

Totodată, organul de urmărire penală trebuie să ia în considerare, pe lângă recomandările de bază, valabile pentru majoritatea acțiunilor de urmărire penală efectuate în cadrul cercetării infracțiunilor informatice, și anumite recomandări specifice efectuării percheziției sau ridicării.

În cazul în care infracțiunea a fost săvârșită prin participație, percheziția se efectuează, în măsura posibilităților, după identificarea tuturor coparticipanților la infracțiune, realizându-se, concomitent, la fiecare dintre ei [74, p. 34, 305, p. 923].

Este necesară înlăturarea imediată din încăpere a substanțelor și materialelor inflamabile, explozibile și toxice [89, p. 56, 56, p. 694].

Urmează a fi întocmită lista tuturor specialiștilor în domeniul IT, angajați oficial și neoficial în cadrul întreprinderii (trebuie stabilite, în măsura posibilităților, datele lor de identitate, domiciliul și locul de muncă de bază) [74, p. 42], care urmează a fi audiați cu privire la atribuțiile de serviciu și datele stocate în sistemele informatice [295, p. 136].

Organul de urmărire penală trebuie să nu întreprindă de sine stătător vreo acțiune față de sistemele informatice, în situația în care nu este cunoscut rezultatul acestor acțiuni [89, p. 56].

În cadrul acestor proceduri de urmărire penală, urmează a fi ridicate toate dispozitivele și mijloacele tehnice, destinate pentru conectarea la rețele informatice. De asemenea, trebuie ridicate toate suporturile de stocare a informației electronice (flash-urile USB, discurile magnetice, discurile optice etc.), pe care pot fi stocate produsele program sau părțile componente ale acestora, destinate pentru comiterea infracțiunii [93, p. 216], informațiile obținute în urma săvârșirii infracțiunii [90, p. 238], spre exemplu, niște baze de date [87, p. 675].

O atenție aparte trebuie acordată înscrisurilor pe care pot fi fixate parole, adrese electronice și alte date criminalistice relevante. Deseori astfel de informații, sub formă de foițe mici, stickere sunt pe masa de lucru, lipite de monitorul calculatorului sau pe perete lângă sistemul informatic [83, p. 116], în portmonee și genți, în buzunarele suspectului, în coșul de gunoi, scrumiere, în interiorul cărților și manualelor etc. [26, p. 231].

Totodată, o atenție deosebită trebuie acordată spațiilor de folosință comună din cadrul companiei (veceu, baie, bucătărie, inventarul sanitar), precum și teritoriilor de sub geamurile clădirii, unde făptuitorii ar putea ascunde sau arunca probele căutate [103, p. 705];

În cadrul efectuării percheziției sau ridicării, trebuie audiați toți utilizatorii cu privire la parolele sistemelor informatice ridicate (alăturat, loginul și parola de acces), precum și parola BIOS, codul de deblocare al tastierei, codul de deblocare al ecranului, alte protecții de tip software/hardware, întrebarea secretă și răspunsul pentru parolă [122, p. 212, 49, p. 26]. Fiecare caracter al parolei trebuie notat separat, ținând cont de alfabetul și registrul caracterului.

Considerăm că legiuitorul urmează să instituie reguli procesuale general-valabile cu privire la examinarea sistemelor informatice și a suporturilor de stocare a datelor informatice, efectuată în cadrul oricărei acțiuni de urmărire penală, inclusiv, de cercetare la fața locului, de percheziție, de ridicare a obiectelor și documentelor, de prezentare a obiectelor spre recunoaștere, de reconstituire a faptei, în cadrul experimentului în procedura de urmărire penală și altele. Este necesară crearea posibilității legale de investigare a datelor informatice atât în cadrul urmăririi penale, cât și la etapa judiciară. Este oportună aplicabilitatea normelor de la art.125 alin.(4) CPP, în cazurile ce nu suferă amânare sau cele de delict flagrant (spre exemplu, necesitatea copierii memoriei volatile de tip RAM a sistemului informatic funcțional). Dacă este imposibilă prezența persoanei al cărei sistem informatic urmează a fi examinat sau a persoanei care reprezintă interesele ei, atunci este oportună prevederea invitării nu a reprezentantului autorității executive a administrației publice locale, dar a asistentului procedural, firește, cu completarea art.82 alin.(2) din CPP. Având în vedere specificul timpului săvârșirii infracțiunilor informatice, inclusiv a duratei de copiere a suporturilor de stocare a datelor informatice, este binevenită prevederea posibilității efectuării percheziției informatice, inclusiv, în timpul nopții. Din aceste considerente, este dezirabilă introducerea unui articol nou în CPP, destinat reglementării acțiunilor de urmărire penală, efectuate asupra datelor informatice.

Conservarea imediată a datelor informatice și a datelor referitoare la traficul informatic

În corespundere cu prevederile lit.b) din alin.(4) al art.4 din Legea privind prevenirea și combaterea criminalității informatice [155], PG, în condițiile legislației de procedură penală, dispune, în cadrul desfășurării urmăririi penale, la solicitarea organului de urmărire penală sau din oficiu, conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, în privința cărora există pericolul distrugerii ori alterării, iar ISP sunt obligați să execute, în condiții de confidențialitate, solicitarea autorității competente privind conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, față de care există pericolul distrugerii

ori alterării, pe un termen de până la 120 de zile calendaristice, în condițiile legislației naționale (lit.c) din alin.(1) al art.7). Conservarea imediată a datelor reprezintă o măsură procesuală provizorie, care permite organului de drept să ridice ulterior informația respectivă [42, p. 250].

Astfel, în cadrul cooperării internaționale, autoritatea competentă străină poate solicita autorității competente din RM conservarea imediată a datelor informatice sau a datelor privind traficul informatic, existente într-un sistem informatic de pe teritoriul RM, referitor la care autoritatea competentă străină urmează să formuleze o cerere argumentată în acest sens. Conținutul obligatoriu al cererii de conservare este expus în anexa nr. 18 din prezenta lucrare.

Termenul de conservare a datelor nu poate fi mai mic de 60 de zile și este valabil până când autoritățile competente naționale decid asupra cererii de asistență juridică internațională în materie penală. Transmiterea datelor informatice se va efectua doar în urma acceptării cererii de asistență juridică internațională în materie penală. Chiar dacă legislația în vigoare nu prevede expres, în literatura de specialitate s-a apreciat că această măsură poate fi dispusă de către procuror și în cadrul procesului penal, în cazul în care există o bănuială rezonabilă cu privire la pregătirea sau săvârșirea unei infracțiuni prin intermediul sistemelor informatice [306, p. 95, 277, p. 7].

Potrivit art.7 alin.(1) lit.f) din Legea privind prevenirea și combaterea criminalității informatice, ISP sunt obligați să asigure monitorizarea, supravegherea și păstrarea datelor referitoare la trafic, pe o perioadă de 180 de zile calendaristice, pentru ISP, utilizatorii de servicii și a canalul prin intermediul căruia a fost transmisă comunicația. Prevederi similare se conțin și în Directiva UE 2006/24/EC. Totuși în aprilie 2014, Curtea Europeană de Justiție a stabilit invaliditatea Directivei în cauză, din motive de disproporționalitate și incompatibilitate cu drepturile omului [307].

Conservarea datelor informatice, prevăzută de art. 16-17 din Convenția privind criminalitatea informatică, urmează a fi reglementată în legea procesual-penală, deoarece prevederile în acest sens din Legea cu privire la prevenirea și combaterea criminalității informatice nu sunt incluse în CPP, în corespundere cu art. 2 alin. (4) CPP. Astfel, este necesară completarea CPP și a Legii cu privire la asistența juridică internațională în materie penală [308].

Considerăm că modificările și completările actelor legislative propuse vor contribui eficient la realizarea sarcinilor pe care și le-a trasat statul nostru – pe plan intern și internațional – de intensificare a luptei cu fenomenul criminalității informatice și de sporire a eficacității măsurilor de combatere a acestuia.

Modificarea în cauză este necesară în vederea asigurării unei reglementări general-valabile privind orice conservare de date informatice, în scopul protejării probelor electronice volatile (susceptibile alterării sau pierderii), al securizării rapide a integrității datelor informatice, pentru a

putea permite organului de urmărire penală ridicarea ulterioară a acestora, al executării asistenței juridice internaționale operative, în materie penală, la administrarea probelor electronice. Totodată, urmează a fi excluse interpretările greșite referitoare la organul competent să dispună conservarea datelor informatice în cazul executării cererilor de conservare a datelor informatice, parvenite din alte state, precum și în afara procesului penal.

3.5. Efectuarea expertizei și a constatărilor tehnico-științifice

Odată aduse în laborator pentru efectuarea cercetării (examinării), constatării tehnico-științifice sau expertizei dispozitivului electronic ridicat, componentele trebuie asamblate, pentru a reconstitui sistemul original. În acest scop, se vor folosi fotografiile, înregistrările video, filmate înainte de ridicarea probelor [29, p. 215], schițele, descrierile din procesul-verbal al acțiunii de urmărire penală, în cadrul căreia au fost ridicate.

La cercetarea infracțiunilor informatice un rol deosebit îl au expertizele tehnice ale calculatoarelor [309, 310], care sunt de câteva tipuri [89, p. 61, 175, p. 917-918, 92, p. 915-917]:

1) *asupra componentelor hardware ale sistemului informatic* (expertiza tehnică a dispozitivelor) [13, p. 82-83]. Obiect al expertizei tehnice a dispozitivelor pot fi [74, p. 52, 14, p. 124]: computerele personale, precum și documentele tehnice ale acestora; dispozitivele periferice; dispozitivele de rețea (servere, cabluri de rețea. ș.a.); sistemele integrate (telefoane mobile, ș.a.); sistemele incorporate în baza controlerului cu microprocesor (dispozitiv de imobilizare, transponder, controler de croazieră); orice componente ale obiectelor menționate mai sus.

2) *asupra produselor program* [14, p. 124-126]. În cazul expertizelor tehnice asupra produselor program, obiect al investigației pot fi: sistemul de operare, aplicațiile, programele incorporate în hardware, mijlocul de elaborare și rulare a softului; aplicația de utilizare generală (redactori de text și grafici, sisteme de gestionare a bazelor de date, tabele electronice, prezentări și altele); aplicația de utilizare specială într-un domeniu al științei tehnice, economiei.

3) *informațională* (a datelor informatice stocate în sistemul informatic). Obiect de investigare în cadrul expertizelor tehnice informaționale (asupra datelor informatice) pot constitui: fișiere-text sau grafice, elaborate cu ajutorul mijloacelor informatice; date în format multimedia; baze de date electronice; cardurile bancare.

4) *asupra rețelei informatice și componentelor acesteia*.

Problemele pe care le pot rezolva categoriile expertizelor enumerate mai sus sunt descrise în anexa nr. 19.

În literatura de specialitate există și alte clasificări ale expertizelor în domeniu [122, p. 131]:

1. *expertiza calculatoarelor*: a) Post mortem (calculatoarele deconectate de la sursa de energie); b) Live (calculatoarele conectate la sursa de energie); c) a aplicațiilor (a produselor software); d) a altor dispozitive (rutere, schimere, console de jocuri ș.a.);

2. *expertiza telefoanelor mobile/tabletelor*: a) Android; b) iOS; c) Windows Phone/Symbian/altele; d) altele (de exemplu, Satnav); e) a cardurilor de memorie;

3. *expertiza rețelelor informatice*: a) live; b) a pachetelor capturate; c) analiza malware-ului.

În prezent, perioada cuprinsă între momentul dispunerii expertizei și parvenirea raportului de expertiză la ordonator este foarte îndelungată. Astfel, timpul de așteptare a efectuării expertizei în subdiviziunile specializate ale instituțiilor de expertiză din domeniu constituie 6-8 luni, după care efectuarea nemijlocită a acesteia durează încă vreo câteva luni [86, p. 121].

Specialiști în domeniul IT, cu o bună pregătire și o experiență necesară în domeniu, se găsesc foarte greu. Angajarea acestora în subdiviziunea de expertiză criminalistică este dificilă din cauza cerințelor sporite, înaintate angajaților organelor de drept, iar nivelul de salarizare nu este unul motivant. Experții, deja încadrați în câmpul muncii, efectuează numeroase și vaste examinări, preponderent pe cauze penale de altă categorie.

La cercetarea infracțiunilor informatice poate apărea necesitatea dispunerii și altor tipuri de expertize, spre exemplu: analiza fizică a unui card (bancar) cu bandă magnetică și/sau cu cip pentru a stabili compoziția plasticului și a cernelii, metoda tipăririi (ecranului sau litografică), datele ștanțate, proprietățile magnetice, hologramele, modul de confecționare [311, p. 38]; expertiza autorului textului, pentru a stabili sexul, vârsta, studiile, limba maternă, profesia, ocupația, starea fizică și psihologică a autorului în momentul elaborării textului, semnele de elaborare a textului în circumstanțe neobișnuite, semnele mascării competențelor lingvistice, întocmirea textului după dictare, coincidențe textuale între autorii X și Y etc. [312, p. 192]; expertiza lingvistică în vederea determinării conținutului unui text sau discurs; expertiza tehnico-criminalistică a documentului [313, p. 130]; expertiza dactiloscopică; expertiza traseologică și altele [314].

În cadrul efectuării expertizelor tehnice asupra cardurilor SIM și a telefoanelor mobile, experții utilizează diverse instrumente de investigare criminalistică, spre exemplu [26, p. 328-329]: Forensic Card Reader, Forensic SIM Toolkit, SIMCom, SIMIS, USIMdetective, PDA Seizure, Pilot-link, Oxygen Phone Manager, BitPim, Cell Seizure, Cell DEK, GSM.XRY, MOBILedit, Secure View, TULP2G, Phone Base 2 ș.a.

3.6. Măsuri speciale de investigații pertinente cercetării infracțiunilor informatice

Prin aplicarea măsurilor speciale de investigații există posibilitatea prevenirii săvârșirii infracțiunii sau tăinuirii acesteia, a fixării procesului criminal, a neadmiterii distrugerii urmelor infracțiunii, a identificării tuturor participanților etc., acestea având, totodată, și un rol important în planificarea acțiunilor de urmărire penală.

În activitatea specială de investigații, legată de cercetarea infracțiunilor informatice, trebuie să se ia în considerare specificul acestor categorii de infracțiuni [64], respectând și următoarele principii [315, 76, p. 129, 68, p. 145-146]:

- strategia și tactica măsurilor speciale de investigații urmează a fi elaborate în baza utilizării noilor realizări în domeniul IT;
- este necesară implicarea specialiștilor de înaltă calificare în domeniul IT;
- trebuie revizuită componența calitativă a subiecților la stabilirea cooperării confidențiale;
- arsenalul tehnicii specializate trebuie completat cu dispozitive moderne, elaborate și aplicate reușit în domeniul IT;
- angajații subdiviziunilor specializate urmează să fie instruiți continuu în aplicarea tehnologiilor moderne și mijloacelor program [316, 44, p. 8, 77, p. 13, 317, p. 126], împreună cu alte persoane implicate (ofițeri de urmărire penală, procurori, judecători) [122, p. 136-137, 318].

În activitatea specială de investigații sunt utilizate diverse produse program, având ca sarcini de bază: controlul procesului tentativelor de acces neautorizat; identificarea programatorului și a specificului softurilor acestuia; stabilirea adreselor IP și a site-urilor pe care le-a folosit utilizatorul; constatarea softurilor utilizate de către persoana vizată; urmărirea activității online a programatorului; identificarea informației codificate sau ascunse; diagnosticarea dispozitivelor privind posibile accesări neautorizate; examinarea suporturilor de stocare a datelor informatice; cercetarea sistemelor informatice și a bazelor de date.

Specific procesului penal cu privire la cercetarea infracțiunilor informatice este că organul de urmărire penală poate dispune efectuarea măsurilor speciale de investigații doar într-un număr redus de cazuri, având în vedere faptul că majoritatea infracțiunilor din această categorie sunt infracțiuni ușoare și mai puțin grave. Ceea ce este paradoxal, o simplă identificare a abonatului, a proprietarului sau utilizatorului unui sistem de comunicații electronice, monitorizarea conexiunilor comunicațiilor telegrafice și electronice, ca măsuri vitale în cercetarea unei infracțiuni informatice, de regulă, nu pot fi efectuate [319, p. 220].

Convenția CE privind criminalitatea informatică stabilește dreptul statelor-părți de a aplica prevederile referitoare la efectuarea măsurilor speciale de investigații specifice doar la anumite

infracțiuni suficient de grave, conform legislațiilor naționale interne. Cu toate acestea, în Raportul explicativ la Convenție este specificat că aplicarea unor asemenea tehnici (cum ar fi colectarea datelor cu privire la trafic, interceptarea datelor referitoare la conținut) sunt adesea cruciale pentru cercetarea unor infracțiuni informatice. De aceea, Părțile ar trebui să ia în considerare aplicarea celor două măsuri în cazul infracțiunilor stabilite în Secțiunea 1 a Capitolului II din Convenție, pentru a oferi un mijloc eficient în cercetarea acestor infracțiuni informatice și a infracțiunilor săvârșite cu ajutorul sistemelor informatice [320, p. 36], fapt despre care nu s-a ținut cont în legislația procesual penală a RM [319, p. 220].

Odată cu ratificarea Convenției CE cu privire la criminalitatea informatică, RM s-a obligat să prevadă în legislația sa internă măsuri specifice cercetării infracțiunilor informatice în sens larg, cum ar fi conservarea datelor informatice (art.16-17), identificarea abonatului (art.18), percheziția (cercetarea) datelor informatice (art.19), colectarea în timp real a datelor referitoare la trafic (art.20) și interceptarea datelor referitoare la conținut (art.21).

Deși Convenția se referă la criminalitatea informatică, ea prevede posibilitatea aplicării acestor măsuri atât la cercetarea infracțiunilor informatice pe care le enumeră la art.2-11, a altor infracțiuni săvârșite prin intermediul sistemelor informatice, cât și la colectarea probelor electronice, indiferent de categoria infracțiunii.

Creșterea considerabilă a posibilităților de păstrare a datelor informatice de către utilizatorii simpli în *cloud*, precum și de accesare prin intermediul IT a datelor aflate la distanță, a creat noi provocări organelor de drept privind obținerea accesului către aceste date, precum și, de cele mai multe ori, la datele abonaților acestor servicii [321, p. 3].

Din aceste considerente, în CPP, precum și în alte acte normative, au fost introduse măsuri procesuale noi, specifice infracționalității informatice.

Reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale

Potrivit art. 30 din CRM [322], statul asigură secretul scrisorilor, al telegramelor, al altor trimiteri poștale, al convorbirilor telefonice și al celorlalte mijloace legale de comunicare. De la aceste prevederi se poate deroga prin lege, în cazurile când aceasta este necesar în interesele securității și bunăstării economice a țării, a ordinii publice și în scopul prevenirii infracțiunilor.

La fel și CPP, la art. 14, confirmă, printre principiile generale ale procesului penal, secretul corespondenței, stipulând faptul că dreptul la secretul scrisorilor, al telegramelor, al altor trimiteri poștale, al convorbirilor telefonice și al celorlalte mijloace legale de comunicare este asigurat de stat. În cursul procesului penal, nimeni nu poate fi lipsit sau limitat în acest drept. Limitarea dreptului în cauză se admite numai în baza unui mandat judiciar, emis în condițiile CPP.

Astfel, legislația procesual-penală, la art. 133 și 134 din CPP, reglementează procedura efectuării măsurii speciale de investigații sub forma reținerii, cercetării, predării, percheziționării și ridicării trimiterilor poștale.

Expresia „trimitere poștală" nu a fost inclusă în art. 6 din CPP în lista termenilor și expresiilor utilizate în CPP, cu toate acestea la alin. (2) al art. 133 din CPP sunt enumerate tipurile de trimiteri poștale care pot fi reținute, cercetate, predate, percheziționate sau ridicate, și anume: *scrisoare* de orice gen (trimitere poștală închisă în plic prin care se transmit anumite comunicări, pct. 2 din Regulile privind prestarea serviciilor poștale [323]); *colet poștal* (bunuri, cu sau fără valoare comercială, expediate prin rețelele poștale, art. 2 din Legea comunicațiilor poștale [324]); *mandat poștal* (serviciu poștal a cărui particularitate constă în completarea unui formular în formă fizică pe baza căruia se execută, conform indicațiilor expeditorului, transferul și remiterea unei sume de bani destinatarului, transmis pe suport de hârtie prin rețeaua poștală sau în format electronic prin rețeaua de comunicații electronice, pct. 2 din Regulile privind prestarea serviciilor poștale); *comunicare prin fax*; *comunicare prin poștă electronică; telegramă, radiogramă, banderolă, container poștal* (legislația actuală nu stabilește astfel categorii de trimiteri poștale, ele fiind prevăzute anterior în Legea poștei [325], abrogată în 2016.

Potrivit Dicționarului explicativ al limbii române [160], prin *banderolă* este desemnată o fâșie de hârtie, lipită în jurul unui ambalaj sau pe locul lui de deschidere, ca mijloc de control al integrității mărfii ambalate. Practica vamală a statelor limitrofe și a celor vecine denotă că în banderole pot fi expediate peste frontiera vamală a statului manuscrise, desene, ștampile, gravuri, hărți geografice, cataloage, aspecte de desene și proiecte de construcții, iar în cazurile expedierii de către persoanele juridice peste frontiera vamală a statului – inclusiv documente tehnice și de proiectare [326, p. 63].

Noțiunea de „trimitere poștală" este definită în art. 2 din Legea comunicațiilor poștale, semnificând un bun ce are înscrisă o adresă, la care urmează să fie distribuit de către furnizorul de servicii poștale. Din această categorie mai fac parte trimiterile de corespondență, precum și cărți, cataloage, ziare, publicații periodice și colete poștale conținând bunuri cu sau fără valoare comercială.

În literatura de specialitate [326], se mai menționează utilizarea expresiei „expediere poștală", specifică legislației anterioare.

Măsura se dispune în sarcina instituției poștale (furnizorul de servicii poștale), indiferent de tipul de proprietate (publică sau privată), executarea ordonanței procurorului fiind obligatorie pentru șeful instituției poștale. Instituția poștală este obligată să asigure condiții tehnice necesare executării de către organele împuternicite a măsurilor speciale de investigații.

Legea comunicațiilor poștale (la art. 2) stabilește că *furnizor de servicii poștale* este persoană fizică sau juridică autorizată, înregistrată în calitate de întreprinzător în RM, a cărei activitate constă, în totalitate sau în parte, în furnizarea serviciilor poștale.

În prezent, în RM sunt 40 de astfel de instituții poștale, lista completă a acestora (denumirea companiei), adresa de corespondență, tipurile de servicii prestate, pagina web a furnizorului pot fi consultate în Registrul public al Furnizorilor de servicii poștale, oferită de către Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației a RM, și anume pe pagina web http://www.anrceti.md/furnizori_comunicatii_postale [327].

Totuși, în cazul comunicărilor prin poștă electronică, ar putea apărea mai multe dificultăți la realizarea acțiunii procesuale. De cele mai multe ori, infractorii utilizează propriile adrese electronice, care nu sunt atribuite companiilor prestatoare de servicii de poștă electronică (cum ar fi: Gmail, Yahoo, Mail.ru etc.). Astfel, în situația în care infractorul deține un server, acesta va putea crea o poștă electronică personală în baza serverului de mail pe care îl deține, infractorul fiind el însuși „șeful instituției poștale" [122, p. 124]. Mai mult decât atât, furnizorii de servicii de poștă electronică nu se regăsesc printre furnizorii de servicii poștale.

Măsura se dispune de către procuror, prin ordonanță motivată (art. 132^4 alin. (1) CPP, pct. 118 din Regulile privind prestarea serviciilor poștale). Elementele obligatorii ale ordonanței respective sunt expuse în anexa nr. 20 din prezenta lucrare.

Totodată, CPP a instituit controlul judecătoresc asupra dispunerii reținerii, cercetării, predării, percheziționării și ridicării trimiterilor poștale, în aceste condiții procurorul va adresa un demers judecătorului de instrucție pentru a obține autorizrea măsurii speciale de investigații (art.14 alin.(2), art. 41 pct. 5), art. 52 alin. (1) pct. 16), art. 132^2 alin. (1) pct. 1) lit. d) din CPP, pct. 118 din Regulile privind prestarea serviciilor poștale).

Mai mult decât atât, legiuitorul a prevăzut faptul că măsura poate fi dispusă doar asupra trimiterilor poștale primite sau expediate de către bănuit sau învinuit, acestea, precum și adresa lui, vor fi indicate judecătorului de instrucție în încheiere [35, p. 364].

Această activitate specială de investigații este o acțiune cu caracter secret [328]. Furnizorul de servicii poștale trebuie să întreprindă acțiuni necesare în vederea neadmiterii divulgării conținutului și metodelor măsurii speciale de investigații (pct. 118 din Regulile privind prestarea serviciilor poștale). În cazul în care parvin cereri privind căutarea unei trimiteri poștale, pentru care organele de drept au emis decizia de a efectua măsuri, furnizorul de servicii poștale informează despre aceasta expeditorul sau destinatarul trimiterii numai cu permisiunea reprezentantului organului de urmărire penală (pct. 120 din Regulile privind prestarea serviciilor poștale).

Procedura reținerii, cercetării, predării, percheziționării sau ridicării trimiterilor poștale, se desfășoară în următoarele etape:

1) ordonanța cu privire la dispunerea măsurii speciale de investigații, precum și autorizația judecătorului de instrucție se transmit șefului instituției poștale (pct. 119 din Regulile privind prestarea serviciilor poștale);

2) în cazul în care parvin trimiteri poștale, indicate în ordonanță, primite sau expediate de către bănuitul sau învinuitul în privința căruia a fost dispusă măsura specială de investigații, șeful instituției poștale le reține, până la examinarea acestora de către organul împuternicit;

3) despre aceasta șeful instituției poștale îi comunică imediat procurorului;

4) reprezentantul organului de urmărire penală, prezentându-se în instituția poștală, aduce la cunoștința șefului acestei instituții, contra semnătură, ordonanța de examinare și ridicare a trimiterilor poștale;

5) reprezentantul organului de urmărire penală deschide și examinează, în prezența șefului instituției poștale, trimiterile poștale parvenite de la bănuit/învinuit sau expediate către acesta;

6) în cazul descoperirii documentelor și obiectelor care au importanță pentru cauza penală, reprezentantul organului de urmărire penală le ridică sau face copiile respective, iar în lipsa unor asemenea documente și obiecte, reprezentantul organului de urmărire penală dispune înmânarea trimiterilor poștale examinate adresantului, cu întocmirea unui proces-verbal în acest sens.

Procesul-verbal cu privire la examinarea și ridicarea trimiterilor poștale se întocmește de către reprezentantul organului de urmărire penală, în prezența conducătorului instituției poștale, pentru fiecare caz de examinare a trimiterilor poștale.

Pe lângă elementele prevăzute la art. 260 și 261 din CPP, procesul-verbal trebuie să mai includă și: cine, unde, când a examinat, ridicat trimiterea poștală sau a dispus înmânarea acesteia adresantului; genul de trimitere poștală; de pe care trimiteri poștale au fost făcute copii; ce mijloace tehnice au fost utilizate; ce s-a depistat; consemnarea faptului prevenirii tuturor participanților și a celor prezenți la acțiunea procesuală despre obligativitatea păstrării secretului corespondenței, nedivulgării informației cu privire la urmărirea penală, precum și despre răspunderea penală prevăzută la art. 178 și 315 din CP.

O situație aparte prezzintă corespondența între deținut și avocatul său, în cauza Campbell c. Regatului Unit [329], Curtea a menționat că asemenea corespondența poate fi citită numai în situații excepționale.

Monitorizarea conexiunilor comunicațiilor telegrafice și electronice

Potrivit alin.(1) al art.134[1] CPP, monitorizarea conexiunilor comunicațiilor telegrafice și electronice și a altor comunicări presupune accesul și verificarea – fără înștiințarea expeditorului sau a destinatarului – a comunicărilor ce au fost transmise instituțiilor care prestează servicii de livrare a corespondenței electronice sau a altor comunicări și a apelurilor de primire și ieșire ale abonatului.

Dacă din denumirea articolului 134[1] CPP („Monitorizarea conexiunilor comunicațiilor telegrafice și electronice") se creează impresia că legiuitorul dorește să reglementeze modul de descoperire și de capturare a activității din rețea, adică a datelor referitoare la traficul informatic, atunci din lecturarea conținutului articolului respectiv constatăm că acesta cuprinde și reglementări cu privire la interceptarea și înregistrarea datelor referitoare la conținut. Acest fapt reiese din alin.(2), care menționează că ofițerul de urmărire penală sau procurorul ia cunoștință imediat, dar nu mai târziu de 48 de ore din momentul recepționării informației, de conținutul comunicării și adoptă o decizie privind ridicarea acesteia sau transmiterea ei pentru livrare ulterioară, cu fotografierea, copierea sau fixarea prin alt mijloc tehnic a conținutului comunicării.

Potrivit Legii cu privire la informatică (art.2), *traficul informatic* reprezintă circulația datelor și a programelor între doi sau mai mulți utilizatori, iar datele referitoare la trafic – în corespundere cu Legea cu privire la prevenirea și combaterea criminalității informatice – constituie orice date având legătură cu o comunicare transmisă printr-un sistem informatic, produse de acest sistem în calitate de element al lanțului de comunicare, indicând originea (numărul de telefon, adresa IP sau alte elemente de identificare ale dispozitivului de comunicații căruia ISP îi acordă servicii [320, p. 6]), destinația (elementele de identificare ale dispozitivului de comunicații către care sunt transmise comunicările [320, p. 6]), itinerarul, ora, data, mărimea, durata sau tipul de serviciu subiacent (tipul de serviciu care este utilizat în cadrul rețelei, de exemplu, transfer de fișiere, poștă electronică sau mesagerie instantanee [320, p. 6]).

Legiuitorul nu delimitează traficul informatic (Traffic data) de conținutul comunicării informatice (Content data), deși Convenția CE cu privire la criminalitatea informatică le dedică articole (art.20 și 21) și reglementări separate acestor două noțiuni. Cu toate acestea, Convenția admite ca în legislațiile naționale ale statelor Părți să fie aplicabile norme comune pentru aceste două instituții [320, p. 36].

Pentru o înțelegere mai simplă, le putem asemui cu ridicarea informațiilor referitoare la descifrările convorbirilor telefonice, în cazul datelor cu privire la trafic, și cu interceptarea comunicărilor telefonice, în cazul datelor referitoare la conținut [320, p. 40, 330]. Din aceste considerente, pledăm pentru operarea modificărilor de rigoare, așa încât interceptarea datelor

referitoare la conținut (excluzând colectarea datelor privind traficul informatic) să fie efectuată doar în cauzele cu privire la săvârșirea infracțiunilor enumerate exhaustiv la art.132^8 alin.(2) CPP.

Constatăm o lacună legislativa, și anume aceea de concurență dintre normele procesuale de la art.133 CPP („Reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale") și cele de la art.134^1 CPP, deoarece ambele articole reglementează modul de ridicare a comunicărilor electronice: „comunicări prin poșta electronică", „comunicații electronice", „corespondență electronică". Or, toate aceste expresii semnifică orice gen de comunicări, efectuate prin intermediul IT: prin poștă electronică (fie prin intermediul browser-ului sau aplicațiilor), prin programe pentru schimb rapid de mesaje (WhatsApp, Viber, Jabber, ICQ, Skype).

Astfel, potrivit Raportului explicativ la Convenția cu privire la criminalitatea informatică [320, p. 35], la comunicările electronice se referă atât cele transmise prin intermediul rețelelor informatice prin cablu, cât și comunicările fără fir, publice sau private, conținutul propriu-zis al comunicării, mesajele, precum și alte informații transmise.

Aceasta situație provoacă confuzia normelor care trebuie aplicate în cazul necesității ridicării conținutului corespondenței electronice, iar deosebirea majoră constă în instituția care urmează a fi implicată în acest proces: instituția poștală sau cea care prestează servicii de livrare a corespondenței electronice.

Din aceste considerente, propunem modificarea alin.(2) al art.133 CPP, prin excluderea cuvintelor „ și prin poșta electronică", iar după îmbinarea „scrisori de orice gen," să fie introduse cuvintele „cu excepția celor electronice,".

Colectarea datelor referitoare la traficul informatic, pe lângă problemele legislative, mai poate ridica și anumite probleme tehnice, cum ar fi: *stocarea datelor* (atunci când există un volum mare de activitate în rețea, mai ales în timpul unor evenimente ostile, cum ar fi atacurile, jurnalele ar putea înregistra multe evenimente într-un timp scurt. Dacă nu este disponibil suficient spațiu de stocare, informațiile despre activitatea recentă ar putea fi suprascrise și pierdute), *traficul criptat* (când traficul informatic este criptat, dispozitivele care monitorizează traficul de-a lungul căii criptate, văd numai caracteristicile de bază ale acestuia, cum ar fi, de exemplu, sursa și destinația adreselor IP, de aceea sursa de date trebuie poziționată acolo unde poate vedea activitatea decriptată) și *alternarea punctelor de acces* (atacatorii intră adesea în rețele, alternând punctele de acces, pentru a evita detectarea de către controalele de securitate care monitorizează punctele de acces importante) [26, p. 257].

Având în vedere caracterul foarte intruziv al colectării și înregistrării comunicărilor electronice asupra vieții private a persoanei [320, p. 37], legiuitorul a prevăzut, la art.132^2 alin.(1) pct.1) lit.e) din CPP, obligativitatea autorizării măsurii respective de către judecătorul de

instrucție, asigurându-se controlul judiciar. Totodată, organul trebuie să respecte toate condițiile cu privire la imixtiunea statului în viața persoanei, stabilite anterior de către Curtea Europeană pentru Drepturile Omului (a se vedea cazurile Klass [331], Kruslin [332] , Huvig [333], Malone [334], Halford [335], Lambert [336]).

Datele cu privire la conexiunile comunicațiilor informatice pot constitui sau pot furniza dovezi importante pentru cauza penală, datorită capacității rețelelor informatice de a transmite cantități mari de date, inclusiv de text scris, imagini și sunet. Atunci când o infracțiune este comisă, mai ales, de la distanță, prin intermediul Internetului, este necesar și esențial să se urmărească ruta comunicațiilor de la victimă către făptuitor. Pot fi corelate ora, data, sursa și destinația comunicațiilor suspectului cu momentul intruziunilor în sistemele informatice ale victimelor, pot fi identificate alte victime [320, p. 37]. În cadrul examinării traficului informatic (de rețea), un investigator poate să facă o conexiune între o adresă IP (alocată de către ISP) și adresa MAC a plăcii de interfață cu rețeaua, putând astfel identifica un anumit computer [26, p. 253].

Actele procesuale cu privire la dispunerea și autorizarea măsurii speciale de investigații trebuie să specifice concret comunicările pentru care urmează a fi colectate datele referitoare la trafic, deoarece Convenția CE privind criminalitatea informatică nu autorizează monitorizarea generală și nediferențiată [320, p. 38]. Asigurarea executării tehnice a monitorizării conexiunilor este pusă în sarcina ISP, și anume a instituției care prestează servicii de livrare a corespondenței electronice, a apelurilor de intrare și ieșire sau a altor comunicări. Deși legislația procesual-penală nu specifică, totuși ISP trebuie să posede o anumită infrastructură sau echipamente pe teritoriul RM, chiar dacă nu este locația activităților sale de bază sau sediul întreprinderii. În caz contrar, va fi necesară întocmirea unei comisii rogatorii în adresa statului în care se află fizic ISP.

Totodată, dacă ISP nu are posibilitate tehnică de a realiza colectarea și înregistrarea datelor referitoare la traficul informatic, această măsură va fi asigurată tehnic de către organul de urmărire penală și/sau organul ce efectuează activitatea specială de investigații, prin conectarea la echipamentul instituției care prestează servicii de livrare a corespondenței electronice, a apelurilor de intrare și ieșire sau a altor comunicări [320, p. 38].

Monitorizarea conexiunilor comunicațiilor telegrafice și electronice are un caracter secret, din care motiv ISP trebuie să fie preîntâmpinat despre confidențialitatea măsurii și interdicția dezvăluirii datelor care i-au devenit cunoscute [320, p. 39].

Legislația internațională, precum și cea națională nu prevede modalitatea tehnică prin care urmează a fi executată monitorizarea conexiunilor comunicațiilor telegrafice și electronice.

Există mai multe tipuri de surse de date privind traficul informatic: firewall-uri (un ansamblu de componente hardware și software care se interpune între două rețele pentru a regla și controla traficul dintre ele) [337, p. 131] și router-e (dispozitiv utilizat pentru interconectarea mai multor rețele locale de tipuri diferite, dar care utilizează același protocol de nivel fizic); detectoarele de pachete și analizatori de protocol (componente hardware sau software destinate să intercepteze sau să înregistreze traficul într-o rețea informatică și să decodeze comunicații care utilizează protocoale diferite) [61, p. 445]; sistemele de detectare a intruziunii – IDS (sistemele care monitorizează traficul de rețea și detectează încercările de a obține acces neautorizat la un sistem informatic) [61, p. 533]; accesul de la distanță (dispozitive, cum ar fi porțile VPN și serverele-modem, care facilitează conexiunile dintre rețele); software-ul de management al securității evenimentului (SEM); instrumentele de analiză criminalistică a rețelei [61, p. 532] – Net Witness (analiza și monitorizarea traficului de rețea), Netresident Tool (captarea, stocarea, analiza și reconstrucția evenimentelor rețelei, cum ar fi mesajele de e-mail, paginile web, fișierele descărcate ș.a.); servere cu protocol dinamic de configurație a gazdei (DHCP), Infinistream Security Fornesics (proiectat pe tehnologia detectoarelor de pachete), CA Network Forensics (descoperirea și investigarea traficului), Wireshark [122, p. 119] (analizator de protocol care capturează traficul de rețea), Snort (detectarea evenimentelor din rețea); software-ul de monitorizare a rețelei; înregistrările furnizate de ISP; aplicații client/server; configurările și conexiunile de rețea ale gazdei [26, p. 253].

Monitorizarea se efectuează asupra conexiunilor comunicațiilor transmise în timp real (live, online) [320, p. 35], în caz contrar, aceasta ar fi o simplă ridicare de obiecte sau documente.

Printre metodele contemporane, utilizate de către subdiviziunile specializate în efectuarea măsurilor speciale de investigații și menite să controleze procesul de schimb de informații în rețeaua internet, trebuie menționate [83, p. 137]: sniffing de rețea, interceptarea traficului de rețea, metoda de interogare falsă ARP, metoda de rutare falsă, interceptarea conexiunilor TCP și altele.

Specificul organizării controlului și înregistrării comunicărilor, efectuate prin utilizarea tehnologiei Skype, constă în interceptarea fluxului de date necriptate. Mai mult decât atât, politica de confidențialitate prevede posibilitatea Skype-ului de a prezenta datele personale, datele traficului și/sau conținutul convorbirilor organelor de drept competente [338].

În cazul în care se confirmă existența unei corespondențe electronice între anumite persoane – în contextul cercetării unor infracțiuni – și organul de urmărire penală dorește acces la conținutul acesteia, el va dispune, iar procurorul va solicita judecătorului de instrucție autorizarea acțiunii de urmărire penală, în cadrul căreia vor fi citite (prelucrate) mail-urile (mesajele și altă corespondență electronică), stocate în dispozitivul electronic [29, p. 216].

Dat fiind faptul că anumite aspecte legale cu privire la interceptarea și cercetarea comunicărilor, efectuate inclusiv prin intermediul poștei electronice (e-mailului), vor fi prezentate mai jos, în secțiunea dedicată analizei monitorizării conexiunilor comunicațiilor telegrafice și electronice, în vederea excluderii dublărilor, vom supune examinării doar unele proceduri tehnice, legate de investigarea poștei electronice.

Poșta electronică este o facilitate de comunicare, oferită grație interconectării sistemelor informatice și cuplării acestora la diferite tipuri de rețele (Internet sau Intranet), care suportă protocoale necesare schimbului de mesaje electronice [43].

Adresa de e-mail are următoarea structură: *nume_utilizator@adresa_server*. *Nume_utilizator* reprezintă numele utilizatorului, iar *adresa_server* – adresa computerului server care stochează mesajele e-mail [339, p. 9].

Din punct de vedere tehnic, un utilizator poate folosi o interfață, denumită client de e-mail (Outlook Express, Microsoft Outlook, Mozilla Thunderbird, Eudora, OperaMail etc) sau poate alege să acceseze direct serverul de mesaje prin web-mail (https://mail.yahoo.com, https://mail.google.com, http://mail.usm.md).

La rândul său, mesajul e-mail este format din mai multe elemente [340, p. 48], care pot fi găsite în anexa nr. 21 din prezenta lucrare.

Mesajul e-mail, trimis de către infractor în adresa victimei, poate fi examinat direct în poșta electronică a acesteia, iar în antetul (proprietățile, header-ul) mesajului, pe lângă datele menționate mai sus, în majoritatea cazurilor, vom depista și adresa IP a sistemului informatic de pe care a fost expediat e-mailul. Totuși unii ISP, cum ar fi Gmail, nu afișează adresa IP a expeditorului mesajului în vederea protejării vieții private a utilizatorilor săi [122, p. 107]. Este de menționat că, de regulă, conținutul antetului este ascuns, asemeni proprietăților documentelor electronice [122, p. 146, 341]. Citirea datelor acestuia se poate realiza în diferite moduri, în funcție de programul utilizat pentru poșta electronică [26, p. 267, 342] și este redată în anexa nr. 22 la prezenta lucrare. Pentru facilitarea analizei datelor conținute în antetul mesajului sunt disponibile diverse utilitare online [343, 344, 345].

Colectarea informației de la furnizorii de servicii de comunicații electronice

Operatorul de telefonie mobilă ne poate oferi informații cu privire la: codul de acces PIN, PUK, numărul de legătură, IMEI și altele. Datele din bazele de date ale numerelor de identificare a dispozitivelor în rețea – EIR pot conține informația cu privire la numerele de serie ale dispozitivelor pentru care, din anumite motive, le-a fost blocat accesul în rețea (spre exemplu, dacă dispozitivul a fost sustras) [81, p. 44].

Totodată, operatorii, pe lângă informațiile cu privire la identificarea datelor abonaților săi (numele, adresa, datele de facturare, serviciile prestate, inclusiv de roaming, numerele de telefon înregistrate, etc.), dispun și de înregistrările convorbirilor telefonice (CDR): apelurile telefonice reușite/eșuate efectuate, apelurile telefonice reușite/eșuate primite, mesajele SMS/MMS trimise, mesajele SMS/MMS recepționate, utilizarea datelor mobile, numerele de telefon de origine (ale apelantului), numerele de telefon finale (ale apelatului), IMEI-urile echipamentelor de comunicație, utilizate și denumirea locației Cell ID, tipul, data, ora și durata comunicării, durata convorbirilor, localizarea geografică a antenei de emisie a celulei.

Localizarea geografică a antenei de emisie a celulei are o importanță deosebită pentru identificarea locului aflării unui anumit echipament mobil într-o anumită perioadă de timp. În cazul utilizării datelor mobile, în CDR-uri va fi vizibilă locația peste fiecare câteva secunde. Totodată, prin intermediul acestei opțiuni, concomitent cu identificarea timpului și locului nemijlocit de comitere al faptei criminale, iar ulterior și a denumirii celulei respective, va fi posibilă identificarea tuturor echipamentelor mobile active în acea perioadă de timp în celula respectivă (adică se poate determina cine a fost într-o anumită zonă la un anumit timp) [26, p. 326].

Pentru analiza și sistematizarea eficientă a informației din CDR-uri, există mai multe produse program (spre exemplu, i2 Analyst Notebook).

Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic

Potrivit art.134^5 alin.(1) din CPP identificarea abonatului, a proprietarului sau utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic constă în solicitarea de la un ISP de a identifica abonatul, proprietarul sau utilizatorul unui sistem de comunicații electronice, al unui mijloc de comunicații electronice ori al unui punct de acces la un sistem informatic sau de a comunica dacă un anumit mijloc de comunicații sau un punct de acces la un sistem informatic este folosit sau este activ în momentul solicitării ori a fost folosit sau a fost activ la o anumită dată.

În sensul Convenției CE privind criminalitatea informatică, potrivit art.18 alin.(3), expresia „date referitoare la abonați” desemnează orice informație – deținută de ISP sub formă de date informatice sau sub orice altă formă – referitoare la abonații acestor servicii, alta decât datele referitoare la traficul informatic sau conținut, și care permite a stabili:

a) tipul de serviciu de comunicații utilizat (de exemplu: telefonie mobilă, redirecționare de apeluri, mesaje voce etc.), dispozițiile tehnice luate în această privință și perioada serviciului;

b) identitatea, adresa poștală sau geografică, numărul de telefon al abonatului și oricare alt număr de contact (inclusiv numărul de telefon, adresa web a site-ului sau numele de domeniu, adresa de e-mail, etc.), precum și datele referitoare la facturare și plată, disponibile în baza unui contract sau a unui aranjament de servicii;

c) oricare altă informație referitoare la locul în care se găsesc echipamentele de comunicație (cum ar fi aparatele de telefon, rețele locale și alele), disponibile în baza unui contract sau a unui aranjament de servicii [320, p. 30].

Formularea „în baza unui contract sau a unui aranjament" trebuie să fie interpretată într-un sens larg și include orice fel de relație, în baza căreia un client folosește serviciile ISP.

Susținem poziția legiuitorului național, care a folosit nu doar noțiunea de *abonat*, dar și cea de *proprietar* și *utilizator*, ceea ce este binevenit. În asemenea situații, ISP sunt obligați să țină evidența (jurnalele) unei game mai largi de clienți: de la persoane care au încheiat contracte de prestări servicii contra cost și dețin abonamente (abonați) până la clienții „PrePay" (proprietari), inclusiv cei care beneficiază de servicii gratuite, precum și persoanele care au dreptul de a utiliza contul abonatului (utilizatori) [320, p. 30].

Totuși, potrivit Raportului explicativ la Convenția CE privind criminalitatea informatică, prevederile respective nu trebuie să fie înțelese în sensul impunerii obligației ISP să păstreze documente (copii de documente) ale abonaților lor sau să verifice corectitudinea informațiilor prezentate de către abonați. Totodată, un ISP nu este obligat să înregistreze informații privind identitatea utilizatorilor cartelelor preplătite (PrePay) pentru servicii de telefonie mobilă și nici nu este impus să verifice identitatea abonaților sau să împiedice utilizarea pseudonimelor de către utilizatorii serviciilor sale [320, p. 31].

Acestei măsuri îi sunt aplicabile garanțiile procesuale de la art.14 din Convenție, care stabilește că organul statului poate apela la ea doar în cazuri concrete, cu privire la anumiți abonați. Spre exemplu, în baza ordonanței prin care a fost dispusă identificarea abonatului, se poate solicita informația cu privire la un anumit număr de telefon sau adresă de e-mail, asociate persoanei investigate. Organul de urmărire penală nu poate obliga ISP să dezvăluie fără discernământ informații privind toți abonații acestuia sau a unui grup de abonați (utilizatori) [346, p. 233].

După cum am menționat anterior, infractorii informatici, în peste 50% din cazuri [85], săvârșesc faptele criminale de la domiciliul lor. În majoritatea cazurilor, domiciliul *de iure* și *de facto* al acestora nu coincide, ceea ce complică identificarea făptuitorului și a locului comiterii infracțiunii, deoarece în bazele de date publice, la care au acces angajații organului care efectuează activitatea specială de investigații, lipsesc informații cu privire la domiciliul *de facto* al persoanei.

Totuși, de cele mai multe ori, infractorii informatici încheie contracte de prestare a serviciilor internet cu operatorii, personal sau prin intermediul persoanelor apropiate, evitând încheierea contractului de către proprietarul imobilului pe care îl închiriază. Astfel, în situația în care se cunoaște numele suspectului, ofițerul de investigații poate obține de la ISP informația cu privire la locația pentru care suspectul a contractat servicii de internet. Totodată, trebuie să se ia în considerare și faptul că acești infractori pot corupe angajații companiilor prestatoare de servicii internet, pentru a fi informați despre interpelările parvenite de la organele de drept [86, p. 45].

Dat fiind faptul că ingerința statului nu este întru atât de intruzivă, identificarea abonatului se realizează doar cu autorizația procurorului, în baza ordonanței de dispunere a măsurii speciale de investigații, elementele obligatorii ale căreia sunt expuse în anexa nr. 20. În anexa nr. 23 la prezenta lucrare, la sugestia experților judiciari din domeniul IT, expusă în cadrul chestionării acestora, a fost elaborat un formular al ordonanței cu privire la dispunerea identificării abonatului, proprietarului sau utilizatorului.

ISP trebuie să fie preîntâmpinat despre confidențialitatea măsurii și interdicția dezvăluirii datelor care i-au devenit cunoscute și răspunderea ce o poartă în cazul încălcării acestei obligații.

Totodată, în corespundere cu Recomandările pentru cooperarea dintre autoritățile de aplicare a legii și ISP împotriva criminalității informatice, adoptate de către CE [142, p. 5], corespondența dintre organele de aplicare a legii și ISP trebuie să cuprindă: numărul de înregistrare, temeiul juridic, informația solicitată concretizată, precum și informații care permit verificarea provenienței cererii (inclusiv numărul de telefon, adresa de poștă electronică a autorității care solicită transmiterea informației) [346, p. 233].

Noțiunea „imediat” trebuie înțeleasă în sensul că organul de urmărire penală va acorda ISP timp suficient pentru a răspunde la interpelare, având în vedere faptul că este posibil ca ISP să fie în situația în care trebuie să răspundă și altor cereri formulate de alte autorități [142, p. 6].

Atât legea procesual-penală, cât și Convenția, pun executarea identificării abonatului în sarcina ISP, care dispune de asemenea date sau le ține la control.

Expresia de la pct.1) al alin.(2) al art.134^5 din CPP „dispune de datele” se referă la posesia fizică a datelor referitoare la abonații, proprietarii sau utilizatorii sistemelor, ai mijloacelor de comunicații electronice ori ai punctelor de acces la sistemele informatice, cărora ISP de pe teritoriul RM le prestează servicii. Totodată, formularea „sau le ține la control” se referă la situația în care datele cu privire la abonați nu se află în posesia fizică a ISP, cu toate acestea, el le poate controla în mod liber de pe teritoriul RM, prin diverse metode și mijloace (de exemplu, utilizând mijloace tehnice de acces la distanță la datele stocate pe un server aflat în posesia fizică a unei alte companii din țară sau de peste hotare) [320, p. 29].

Pe site-ul Agenției Naționale pentru Reglementare în Comunicații Electronice și Tehnologia Informației a RM este publicat Registrul public al furnizorilor de rețele și servicii de comunicații electronice http://anrceti.md/lista_furnizori_servicii_retele_ce [347]. Astfel, conform datelor din 14.12.2017, pe teritoriul RM activau 543 de furnizori de servicii (de telefonie, transport apeluri, transmisii de date, acces la Internet, linii închiriate, programe audiovizuale). În acest Registru putem stabili, denumirea, adresa de corespondență, tipurile de rețele sau servicii de comunicații electronice, numărul și data includerii în Registru, pagina web a furnizorului etc. [346, p. 233]

Convenția specifică expres că solicitarea de a prezenta datele referitoare la abonat poate fi pusă în sarcina ISP, care prestează servicii pe teritoriul statului Parte, adică, atât ISP care posedă o anumită infrastructură sau echipamente pe teritoriul RM, chiar dacă nu este locația activităților sale de bază sau sediul întreprinderii, cât și cel care se află în afara teritoriului țării, dar oferă serviciile sale în RM. În aceste situații, organul de urmărire penală nu va fi obligat să solicite consimțământul altui stat și nici să obțină informațiile respective, făcând uz de asistența juridică internațională în materie penală, prin intermediul organelor de drept ale statului în care se află fizic ISP. Prezenta interpretare a art.18 din Convenție nu prejudiciază jurisdicția națională a statelor Părți [321, p. 6]. Actualmente locația datelor nu este factorul determinant la stabilirea jurisdicției.

Secvența „prestează servicii pe teritoriul Părții" reprezintă situațiile când [321, p. 8]:

- ISP permite persoanelor aflate pe teritoriul statului Parte să se înscrie la serviciile sale (și, spre exemplu, nu blochează accesul la astfel de servicii), precum și
- ISP stabilește legături reale și substanțiale cu statul Parte la Convenție. Acesta își orientează atenția către abonații statului respectiv (cum ar fi promovarea publicității locale ori publicității în limba statului Parte), folosește informația despre acești abonați în activitatea sa, interacționează cu ei.

ISP din SUA au permisiunea de a dezvălui voluntar informații despre abonații săi autorităților competente ale altor state. Spre exemplu, pe parcursul anului 2015, cei mai renumiți furnizori americani (Apple, Facebook, Google, Microsoft, Twitter și Yahoo) au dat curs la peste 82.000 (din cele peste 138.000) de solicitări de identificare a abonatului, înaintate direct de către autoritățile altor state, decât SUA, fără utilizarea comisiilor rogatorii [348, p. 4].

Compania Apple execută solicitările cu privire la identificarea abonatului, cu condiția ca: să parvină de la autoritatea competentă a statului; să fie transmisă prin intermediul poștei electronice oficiale a acestei autorități; solicitantul să completeze o anchetă referitor la caz, șablonul căreia se regăsește pe pagina web http://www.apple.com/legal/privacy/emeia-le-inforequest.pdf [349, p. 1]; să fie transmisă la adresa de e-mail law.enf.emeia@apple.com (acest e-mail este destinat exclusiv

depunerii cererilor de aplicare a legii de către organele de drept și agenții guvernamentali). În ceea ce privește informația cu privire la conținut, cu excepția procedurilor urgente, Apple o dezvăluie doar în baza unui mandat de percheziție și a comisiei rogatorii sau a altei cereri similare.

Solicitările către Facebook și Microsoft din alte state decât Canada sau SUA trebuie transmise către reprezentanțele acestora din Irlanda, care nu va procesa cererile vagi sau vaste, iar pentru dezvăluirea datelor cu privire la conținut este necesară transmiterea unei cereri de asistență juridică internațională în materie penală.

La fel, în baza principiului voluntarietății, Google poate oferi date cu privire la utilizatorii săi autorităților competente ale altor state, cu condiția respectării normelor internaționale, ale Statelor Unite ale Americii, a politicii Google și a legislației statului solicitant [348, p. 5-8].

La rândul său, ofițerul care efectuează această activitate specială de investigații urmează să întocmească un proces-verbal cu privire la consemnarea măsurii, în corespundere cu prevederile art.132^5 din CPP, la care se anexează, în plic sigilat, purtătorul material de informații care conține rezultatele măsurii speciale de investigații [208, p. 220].

Totodată, la întocmirea actelor procesuale cu privire la identificarea abonatului, trebuie să se țină cont de mai multe aspecte tehnice foarte relevante și, de cele mai multe ori, decisive pentru obținerea unor date veridice.

Pentru a putea fi identificate în cadrul rețelei, calculatoarele conectate la Internet, numite host-uri, noduri, sisteme sau servere, trebuie să poată fi identificate printr-o adresă IP [26, p. 260].

În IPv4, standardul curent pentru comunicarea în Internet, adresa IP este reprezentată pe 32 de biți (de ex. 192.168.0.1). Din motivul unui număr limitat de adrese IPv4, internetul este în proces de evoluție către versiunea IPv6, care are o lungime de 128 de biți [350].

După obținerea adresei IP, datele cu privire la ISP, căruia i-a fost alocată această adresă IP, vor fi identificate prin intermediul registratorilor internaționali, în dependență de regiunea unde ISP prestează serviciile internet, cum ar fi: AfriNIC [351], APNIC [352], ARIN [353], LACNIC [354], RIPE NCC [355], conform anexei nr. 24 [356].

Adresele IP sunt dinamice (se modifică la fiecare conectare a calculatorului în rețea) și statice (este atribuită permanent dispozitivului configurat). Pentru o înțelegere mai simplă a semnificației adresei IP, o putem asemui unui număr de telefon mobil, doar că în cazul adreselor IP dinamice, acest număr s-ar fi modificat de fiecare dată când se face un apel telefonic. Astfel, pe parcursul unei zile, o adresă IP poate fi atribuită consecutiv mai multor persoane. Din această cauză, în solicitarea organului de urmărire penală, în drept cu adresa IP, se va indica data și timpul concret (când s-a conectat sistemul informatic la rețea).

Totodată, trebuie să atenționăm și asupra faptului că data și timpul conectării calculatorului la rețea poate să difere de data și timpul din RM, în dependență de locul aflării serverului la care se conectează și/sau data, timpul și fusul orar setat pe server. Din aceste considerente, se vor verifica setările serverului utilizat pentru conectare la internet, indicându-se suplimentar și informația cu privire la timpul zonal (spre exemplu: 123.456.789.012, 26 aprilie 2017, GMT+3) [122, p. 96]. În situația în care suntem în prezența unei adrese IP dinamice, fiind indicate doar data și timpul, fără a specifica fusul orar (în cazul în care este diferit de cel local), ISP ne va furniza informație neveridică. În cel mai bun caz, ISP poate să specifice lipsa conectării la rețea a respectivei adrese IP pentru data și timpul dat, iar în cel mai rău caz, ne va oferi o informație cu privire la un alt utilizator de servicii internet.

Având adresa IP, timpul și data (incluzând timpul zonal) ISP căruia i-a fost alocată adresa IP ne va putea comunica informația cu privire la abonatul, proprietarul sau utilizatorul acestei adrese IP la data și timpul respectiv [346, p. 233].

În cazul numerelor de telefon alocate furnizorilor de servicii de telefonie, este de menționat faptul că pe site-ul oficial al Agenției Naționale pentru Reglementare în Comunicații Electronice și Tehnologia Informației a RM este publicată lista titularilor de licențe pentru utilizarea resurselor de numerotare http://anrceti.md/titulari_lic_resurse_numerotare [357].

Începând din anul 2013 a fost introdusă instituția portabilității numerelor de telefon, ceea ce reprezintă posibilitatea unui abonat de a-și păstra, la cerere, numărul de telefon, atunci când își schimbă furnizorul de servicii publice de telefonie destinate publicului.

Portabilitatea numerelor în RM este prevăzută de Legea comunicațiilor electronice (art.65).

Agenția a elaborat și a aprobat Regulamentul privind portabilitatea numerelor, care stabilește principiile generale ale acestui proces, regulile de portare a numerelor și de rutare a apelurilor, obligațiile furnizorilor implicați în procesul de portare a numerelor, statutul bazei de date centralizate și modalitatea de selectare a administratorului acestei baze.

În septembrie 2012, ÎCS „NP Base” SRL a fost desemnată, prin Hotărârea Consiliului de Administrație al ANRCETI nr. 38/1 din 12.09.2012 [358], în calitate de administrator al bazei de date centralizate. Aceasta are misiunea de a organiza, opera, administra și întreține baza de date, a coordona și controla procesul de portare a numerelor, a oferi suportul necesar furnizorilor în procesul de portare a numerelor.

În aceste condiții, în vederea identificării furnizorului care prestează la moment servicii de telefonie către un anumit număr de telefon, este necesară verificarea numărului în baza de date centralizată a ÎCS „NP Base” SRL, disponibilă pe pagina web http://portare.md/ [359].

3.7. Concluzii la Capitolul 3

1. Încă de la etapa urmăririi penale, apar probleme cu privire la pregătirea organului de drept pentru administrarea probelor electronice. Acest fapt este determinat de nivelul insuficient de pregătire a reprezentanților organului de urmărire penală, de implicarea redusă a specialiștilor în domeniul IT, de necunoașterea posibilităților anumitor acțiuni de urmărire penală (spre exemplu ale expertizei informaționale), din care cauză multiple circumstanțe, care ar fi putut obține un statut probatoriu, rămân în afara materialelor cauzei penale, statul urmând să investească resurse financiare considerabile atât în mijloace tehnice și produse program, cât și în instruirea profesională a persoanelor implicate în combaterea fenomenului în cauză.

2. Este imperios necesară elaborarea unei metodologii noi cu privire la metodica și tactica criminalistică în cercetarea infracțiunilor informatice, care să prevadă:

- acțiunile preparatorii de bază, specifice investigării infracțiunilor informatice, pe care urmează să le întreprindă ofițerul de urmărire penală atât în procesul de pregătire de efectuare a acțiunii de urmărire penală, cât și la efectuarea nemijlocită a acestora, îndeosebi la efectuarea cercetării la fața locului, a percheziției, a ridicării de obiecte și documente etc.;

- regulile generale și speciale referitoare la administrarea probatoriului în cauzele de criminalitate informatică;

- recomandările fundamentale, valabile pentru acțiunile de urmărire penală, efectuate în cadrul cercetării infracțiunilor respective și legate de conservarea probelor, de participanții la acțiunea procesuală, de instructajul membrilor grupului, de participarea specialistului, instrumentele și mijloacele necesare, de asigurarea securității locului și a probelor, de examinarea și ridicarea probelor tradiționale și a celor electronice, de realizarea copiilor probelor digitale, etichetarea, împachetarea, transportarea și păstrarea probelor electronice, de limitele implicării suspectului la examinarea și ridicarea probelor electronice, de evitarea capcanelor de distrugere a informațiilor digitale, de specificul examinării produselor program și a documentelor electronice, de stabilirea și examinarea fișierelor criptate, de conținutul procesului-verbal al acțiunii de urmărire penală;

- regulile specifice situaților de ridicare a informației electronice, împreună sau fără suportul de stocare a datelor informatice;

- procedeele și consecutivitatea examinării sistemului informatic, în dependență de starea acestuia (aflat sau nu în funcțiune, conectat sau nu la sursa de alimentare cu energie electrică);

- particularitățile ridicării notebook-urilor, tabletelor și a echipamentelor mobile, ale cercetării suporturilor de stocare a datelor informatice și a documentelor electronice;

- întrebările-tip pentru audierea persoanelor, specifice cercetării acestei categorii de infracțiuni, care vor asigura ca persoana care efectuează audierea să nu scape din vedere anumite împrejurări sau situații, să cerceteze concomitent toate versiunile posibile, luând în calcul și specificul fiecărui caz concret;

- particularitățile, regulile metodologice și recomandările practice pentru investigarea paginilor web și a site-urilor, specifice pentru fiecare etapă și obiectiv trasat, inclusiv cel legat de examinarea materialului publicat (proprietățile, metadatele materialelor, obiectul infracțiunii, împrejurările în care a fost efectuat materialul, paginile web și site-urile modificate sau șterse, identificarea victimei), de stabilirea datelor cu privire la numele de domeniu, precum și identificarea datelor serverului gazdă;

- sarcinile de bază ale expertizelor tehnice ale calculatoarelor: asupra componentelor hardware ale sistemului informatic (expertiza tehnică a dispozitivelor); asupra produselor program; informaționale (a datelor informatice stocate în sistemul informatic) asupra rețelei informatice și componentelor acesteia.

3. Legiuitorul urmează:

- să instituie reguli procesuale general-valabile cu privire la examinarea sistemelor informatice și suporturilor de stocare a datelor informatice, efectuată în cadrul majorității acțiunilor de urmărire penală, la orice etapă procesuală;

- să transpună în CPP al RM instituția conservării datelor informatice, în vederea asigurării protejării probelor electronice volatile (susceptibile alterării sau pierderii), a securizării rapide a integrității datelor informatice, pentru a putea permite organului de urmărire penală ridicarea ulterioară a acestora, a executării asistenței juridice internaționale operative în materie penală, la administrarea probelor electronice, în conformitate cu prevederile art.16 și 17 din Convenția privind criminalitatea informatică;

- să asigure posibilitatea realizării măsurilor speciale de investigații sub forma identificării abonatului, a proprietarului sau utilizatorului unui sistem de comunicații electronice ori a unui punct de acces la un sistem informatic, a monitorizării conexiunilor comunicațiilor telegrafice și electronice, la cercetarea infracțiunilor informatice, a altor infracțiuni săvârșite prin intermediul sistemelor informatice, precum și la colectarea probelor electronice, indiferent de categoria infracțiunii;

- să racordeze conținutului art.134^1 CPP la denumirea acestuia, așa încât să reglementeze doar ridicarea datelor referitoare la traficul informatic, iar colectarea informațiilor cu privire la conținutul comunicării informatice urmează să fie expusă într-un articol nou, cu prevederi mai

riguroase, specifice interceptării comunicărilor telefonice, ținându-se cont de specificul comunicațiilor electronice;

- să înlăture lacuna legislativă de la art.133 CPP și art.134^1 CPP, prin care ambele reglementează modul de ridicare a comunicărilor electronice: poștă electronică (fie prin intermediul browser-ului sau aplicațiilor), programe pentru schimb rapid de mesaje (WhatsApp, Viber, Jabber, ICQ, Skype). Aceasta situație provoacă confuzia normelor care trebuie aplicate în cazul necesității ridicării conținutului corespondenței electronice, deosebirea majoră constând în instituția care urmează a fi implicată în acest proces: instituția poștală sau instituția care prestează servicii de livrare a corespondenței electronice.

CONCLUZII GENERALE ŞI RECOMANDĂRI

Scopul principal al investigației noastre a constituit cercetarea complexă și multilaterală a conceptului asupra metodicii de cercetare a infracțiunilor din domeniul informaticii.

În urma analizei și generalizării materiei expuse în teză, formulăm următoarele ***concluzii***:

1. ***Soluționarea problemei științifice în domeniul de cercetare*** realizate rezidă în elaborarea metodicii de cercetare criminalistică a infracțiunilor din domeniul informaticii, ceea ce a contribuit la identificarea procedeelor tactice, metodice și tehnice adecvate, în vederea aplicării lor la investigarea acestor infracțiuni, precum și la realizarea primei lucrări științifice aprofundate în domeniu din Republica Moldova.

2. În vederea realizării scopului științific propus, s-a recurs la o analiză multiaspectuală a unui număr reprezentativ de elaborări științifice, în care sunt abordate subiecte directe, referitoare la metodica de cercetare a infracțiunilor din domeniul informaticii (inclusiv cu privire la noțiunea și clasificarea infracțiunilor date, la modelul și caracteristica criminalistică, la situațiile tipice și versiunile criminalistice, la particularitățile tactice de efectuare a acțiunilor de urmărire penală și a măsurilor speciale de investigații îndreptate în vederea descoperirii acestui gen de infracțiuni), inclusiv și analiza corespunderii la standardele de combatere a criminalității informatice a Legii comunicațiilor electronice.

3. În rezultatul studiului, am constatat că printre cele mai relevante semne caracteristice ale infracțiunilor informatice sunt: legătura cu alte genuri de infracțiuni, caracterul tehnologic avansat, nivelul înalt de latență, caracterul bine organizat, profesional, transfrontalier și transnațional, aceste infracțiuni fiind cele mai dinamice în evoluție, având costuri reduse pentru săvârșire și manifestând trăsături politice, extremiste și teroriste [162, p. 248].

4. În opinia noastră, infractorii digitali sunt persoane cu o flexibilitate înaltă de trecere operativă de la dimensiunea reală la cea virtuală, de la o relație mediată de un spațiu emotiv-fizic la o relație mediată de un spațiu emotiv-artificial, având o percepție diminuată asupra ilegalității comportamentului lor, daunei provocate, a riscurilor de a fi descoperit și sancționat [360, p. 56].

5. Probele electronice reprezintă informații cu valoare doveditoare, care sunt stocate, prelucrate sau transmise prin intermediul unui sistem informatic. Ele se produc în mediul informatic și constituie rezultatul transformării informației computerizate în urma ștergerii, copierii, blocării, modificării sau a oricărei alte intervenții în funcționarea mijloacelor de stocare, prelucrare sau transmitere a datelor informatice sau a rețelei de comunicații [360, p. 74].

6. Prezenta cercetare permite identificarea anumitor cauze care generează o descoperire insuficientă a infracțiunilor informatice, și anume [360, p. 149]:

a) lipsa unor recomandări metodice, în RM, privind acest tip de infracțiuni, iar propunerile metodice înaintate generalizează neîntemeiat toate categoriile de infracțiuni, săvârșite cu utilizarea sistemelor și rețelelor informatice, dat fiind faptul că practica solicită existența unor recomandări mult mai concrete, deseori recomandările existente fiind departe de posibilitățile reale ale persoanelor care trebuie să le implementeze în practică, prevăzând sarcini tehnice neadecvate;

b) nu sunt efectuate măsuri speciale de investigații și acțiuni de urmărire penală suficiente;

c) având în vedere neasigurarea tehnico-materială suficientă a organelor de urmărire penală, nu sunt utilizate la nivelul necesar mijloacele tehnice și produsele program criminalistice;

d) nivelul redus de pregătire a reprezentanților organelor de drept în acest domeniu la efectuarea acțiunilor de urmărire penală;

e) implicarea insuficientă a specialiștilor din domeniul IT;

f) necunoașterea posibilităților anumitor acțiuni de urmărire penală (spre exemplu, ale expertizei informaționale), din care cauză numeroase circumstanțe care ar fi putut obține un statut probatoriu rămân în afara materialelor cauzei penale.

Reieșind din concluziile formulate, se impun următoarele **recomandări**:

1. Legiuitorul urmează să instituie reguli procesuale general-valabile cu privire la examinarea sistemelor informatice și a suporturilor de stocare a datelor informatice, efectuată în cadrul acțiunii de urmărire penală, la orice etapă procesuală – fie în cadrul urmăririi penale, fie la etapa judiciară. Din aceste considerente, este oportună introducerea unui articol nou în CPP privind reglementarea acțiunilor de urmărire penală efectuate asupra datelor informatice, în redacția: „***Articolul 130[1]***. *Percheziția informatică*” [360, pp. 124,150].

2. Este necesară transpunerea în CPP al RM, dar și în Legea cu privire la asistența juridică internațională în materie penală, a instituției conservării datelor informatice, prevăzută în Legea privind prevenirea și combaterea criminalității informatice, în vederea asigurării protejării probelor electronice volatile. Astfel, este necesară completarea CPP cu art.130^2 având următorul conținut: „***Articolul 130[2]***. *Conservarea imediată a datelor informatice*” [360, p. 151].

În acest context, urmează a fi completată și Legea cu privire la asistența juridică internațională în materie penală, după cum urmează: - la art. 1 alin. (3) cu lit. a^1) având următorul cuprins: „*a^1) conservarea imediată a datelor informatice;*”; - cu articolul 13^1 în următoarea redacție: „***Articolul 13[1]***. *Conservarea imediată a datelor informatice*”.

3. Dat fiind faptul că, la ratificarea Convenției CE cu privire la criminalitatea informatică, RM s-a obligat să prevadă în legislația sa internă măsuri specifice cercetării infracțiunilor informatice, cum ar fi identificarea abonatului (art.18), percheziția (cercetarea) datelor informatice (art.19), colectarea în timp real a datelor referitoare la trafic (art.20) și interceptarea datelor

referitoare la conținut (art.21), la cercetarea infracțiunilor informatice pe care le enumeră la art.2-11, a altor infracțiuni săvârșite prin intermediul sistemelor informatice, precum și la colectarea probelor electronice, indiferent de categoria infracțiunii, se impune modificarea CPP, prin realizarea posibilității efectuării acestor măsuri la cercetarea infracțiunilor respective [360, p. 153].

4. Conținutul art.134[1] CPP („*Monitorizarea conexiunilor comunicațiilor telegrafice și electronice*”) urmează a fi racordat la denumirea acestuia, așa încât să reglementeze doar ridicarea datelor referitoare la traficul informatic. Totodată, colectarea informațiilor cu privire la conținutul comunicării informatice urmează să fie expusă într-un articol nou (*„Interceptarea informatică”*) [360, p. 133].

5. Este necesară eliminarea lacunei legislative de la art.133 CPP („*Reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale*”) și art.134[1] CPP („*Monitorizarea conexiunilor comunicațiilor telegrafice și electronice*”) , prin care ambele reglementează modul de ridicare a comunicărilor electronice: „comunicări prin poșta electronică”, „comunicații electronice”, „corespondență electronică”. Astfel, propunem modificarea alin.(2) al art.133 CPP, prin excluderea cuvintelor „și prin poșta electronică”, iar după îmbinarea „scrisori de orice gen,” să fie introduse cuvintele „cu excepția celor electronice,” [360, p. 134].

6. În vederea identificării conexiunilor dintre infracțiunile săvârșite în diferite locuri, a stabilirii legăturilor dintre diferite persoane, fapte și circumstanțe, a punerii în aplicare a tuturor activităților criminalistice la un nivel tehnologic avansat, se impune crearea unei baze de date centralizate pentru organele de drept, cu informație operativă pe cauzele de criminalitate informatică, care să conțină date cu privire la [360, p. 154]:

- toate operațiunile de plată electronică frauduloase (reușite și nereușite);
- conturile (bancare, telefonice, electronice) care au avut legătură directă cu infracțiunile informatice, inclusiv ale victimelor, de buffer și pentru lichefierea mijloacelor bănești;
- persoanele care au fost implicate direct în aceste infracțiuni;
- adresele IP prin intermediul cărora au fost efectuate conexiunile în procesul de pregătire, săvârșire și ascundere a infracțiunii (și anume, ale serverelor și sistemelor informatice utilizate la: gestionarea centrelor de control al botnetului, răspândirea virușilor, accesarea neautorizată a informației computerizate și altele);
- numele de domeniu ale site-urilor utilizate în pregătirea și comiterea infracțiunii;
- numerele de telefon, adresele poștelor electronice, conturile din softurile de comunicare rapidă, adresele MAC ale dispozitivelor ș.a., având legătură directă; viruși, botneturi etc.;
- subdiviziunile organelor de drept care au efectuat investigațiile, instituțiile de expertiză care au examinat sistemele și rețelele informatice.

Pe lângă datele textuale formalizate, baza de date ar trebui să prevadă și posibilitatea de a salva date-media indexate: texte, imagini, înregistrări video și audio, documente electronice.

7. Este imperios necesară elaborarea unei metodologii noi cu privire la metodica și tactica criminalistică în cercetarea infracțiunilor informatice, care să prevadă [360, p. 154]:

- acțiunile preparatorii de bază, specifice investigării infracțiunilor informatice, pe care urmează să le întreprindă ofițerul de urmărire penală atât în procesul de pregătire pentru efectuarea acțiunii de urmărire penală, cât și la efectuarea nemijlocită a acestora;

- regulile generale și speciale referitoare la administrarea probatoriului în aceste cauze;

- recomandări fundamentale, valabile pentru acțiunile de urmărire penală, efectuate în cadrul cercetării infracțiunilor respective, privind conservarea probelor, participanții la acțiunea procesuală, instructajul membrilor grupului, participarea specialistului, instrumentele și mijloacele necesare, asigurarea securității locului și a probelor, examinarea și ridicarea probelor tradiționale și a celor electronice, realizarea copiilor probelor digitale, etichetarea, împachetarea, transportarea și păstrarea probelor electronice, limitele implicării suspectului la examinarea și ridicarea probelor electronice, depășirea capcanelor de distrugere a informațiilor digitale, specificul examinării produselor program și a documentelor electronice, stabilirea și examinarea fișierelor criptate, conținutul procesului-verbal al acțiunii de urmărire penală;

- regulile specifice situațiilor de ridicare a informației electronice, împreună sau fără suportul de stocare a datelor informatice;

- procedeele și consecutivitatea examinării sistemului informatic, în dependență de starea acestuia (aflat sau nu în funcțiune, conectat sau nu la sursa de alimentare cu energie electrică);

- particularitățile ridicării notebook-urilor, tabletelor și a echipamentelor mobile, ale cercetării suporturilor de stocare a datelor informatice și ale documentelor electronice;

- întrebările-tip aplicate la audierea persoanelor, specifice cercetării acestei categorii de infracțiuni, care vor asigura ca persoana care efectuează audierea să nu scape din vedere anumite împrejurări sau situații, să cerceteze concomitent toate versiunile posibile;

- particularitățile, regulile metodologice și recomandările practice privind investigarea paginilor web și a site-urilor, specifice pentru fiecare etapă și obiectiv trasat, inclusiv cele legate de examinarea materialului publicat (proprietățile, metadatele, obiectul infracțiunii, împrejurările în care a fost efectuat materialul, paginile web și site-urile modificate sau șterse, identificarea victimei), stabilirea datelor privind numele de domeniu, identificarea datelor serverului-gazdă;

- sarcinile de bază ale expertizelor tehnice ale calculatoarelor: asupra componentelor hardware ale sistemului informatic (expertiza tehnică a dispozitivelor); asupra produselor

program; ale celei informaționale (privind datele informatice stocate în sistemul informatic) – asupra rețelei informatice și componentelor acesteia.

8. În vederea ameliorării situației existente în domeniu, este necesară aplicarea în practică a recomandărilor metodice cu privire la cercetarea infracțiunilor informatice, a altor infracțiuni săvârșite prin intermediul sistemelor informatice, precum și la colectarea probelor electronice, indiferent de categoria infracțiunii [360, p. 156].

Avantajele acestor recomandări se relevă în următoarele domenii:

Domeniul legislativ: prin implementarea recomandărilor propuse, se va asigura uniformizarea sistemului juridic, precum și consecvența normelor procesual-penale, prin finalitatea lor reprezentând și o contribuție esențială la realizarea obligației pozitive a statului nostru de a aduce legislația internă în corespundere cu normele dreptului internațional, și anume, cu prevederile Convenției CE privind criminalitatea informatică și altor acte ce derivă din aceasta.

Domeniul jurisprudențial: se va asigura aplicarea corectă și unitară de către organele de urmărire penală și instanțele de judecată a normelor cu privire la cercetarea infracțiunilor informatice; se va pune la dispoziția organelor de urmărire penală diferite acțiuni tactice, măsuri strategice și metodici cu privire la cercetarea infracțiunilor din domeniul informaticii.

Domeniul economic: se va realiza prevenirea prejudiciilor materiale considerabile, cauzate de această categorie de infracțiuni; va fi posibilă inițierea procedurilor de recuperare a daunelor deja cauzate, în urma descoperirii infracțiunilor, a identificării și atragerii la răspundere penală a făptuitorilor; organul de urmărire penală va avea posibilitatea de a opta pentru cea mai eficientă și mai proporțională cale de administrare a probatoriului și de dovedire a vinovăției, fără a apela, de fiecare dată, la metode și procedee complexe, costisitoare și disproporționale; se vor reduce cheltuielile generate de eventuale condamnări ale Republicii Moldova la Curtea Europeană a Drepturilor Omului în legătură cu încălcarea Convenției Europene a Drepturilor Omului.

Planul cercetărilor de perspectivă în investigarea temei este orientat spre:

- Desfășurarea cercetărilor referitoare la erorile judiciare, admise la investigarea infracțiunilor din domeniul informaticii.
- Elaborarea unui proiect de Hotărâre Explicativă a Plenului Curții Supreme de Justiție a Republicii Moldova cu privire la examinarea cazurilor de criminalitate informatică și de administrare a probelor electronice.
- Evaluarea impactului amendamentelor propuse în legislația procesual-penală asupra calității aplicării legii în domeniul metodicii cercetării infracțiunilor informatice.
- Dezvoltarea particularităților cercetării infracțiunilor din domeniul informaticii.

BIBLIOGRAFIE

[1] Potorac E., Andonii V. Criminalitatea în domeniul informaticii. În: Probleme ale dezvoltării economiei de piață și dreptului în condițiile actuale. Tezele conf. practico-științifice internaționale. Bălți: Institutul Nistrean de Economie și Drept, 2006, p.442-448.

[2] Вехов В. Б. Компьютерные преступления. Способы совершения, методики расследования. Москва: Право и Закон, 1996. 182 с.

[3] Legea pentru aprobarea Concepţiei securităţii naţionale a Republicii Moldova. Nr. 112 din 22.05.2008. În: Monitorul Oficial al Republicii Moldova, 03.06.2008, nr. 97-98.

[4] Hotărârea Parlamentului pentru aprobarea Strategiei securităţii naţionale a Republicii Moldova. Nr.153 din 15.07.2011. În: Monitorul Oficial al Republicii Moldova, 14.10.2011, nr. 170-175.

[5] Dușa S., Gheorghiță M. Criminalitatea cibernetică – cu un pas înainte. Metodici de investigare. În: Studia Universitatis, Seria Ştiinţe Sociale, CEP USM, Chişinău, 2011, vol. V, nr. 3 (43), p.187.

[6] Ciuvaga D. Infracțiunile digitale. https://goo.gl/jR1Evq (vizitat 09.08.2017).

[7] Golubenco Gh. Criminalistică: obiect, sistem, istorie. Chişinău: Tipografia Centrală, 2008. 216 p.

[8] Doraș S. Criminalistica. Chișinău: Tipografia Centrală, 2011. 632 p.

[9] Gheorghiță M. Tratat de metodică criminalistică. Chișinău: CEP USM, 2015. 532 p.

[10] Gheorghiță M. Tratat de criminalistică. Chișinău: Tipografia Centrală, 2017. 872 p.

[11] Amza T., Amza C. P. Criminalitatea Informatică. București: Lumina Lex, 2003. 509 p.

[12] Lungu S. ș.a. Cercetarea la fața locului în cazul infracțiunilor săvârșite prin mijloace electronice. În: Investigarea criminalistică a locului faptei. București: Luceafărul, 2004, p.406-411.

[13] Gheorghiță M. ș.a. Ghid de expertize judiciare. Chișinău: Elena V.I., 2005. 104 p.

[14] Георгицэ М. Возможности судебных экспертиз: криминалистическое обеспечение (научно-практическое пособие). Кишинэу: Tipografia Centrală, 2008. 200 с.

[15] Dobrinoiu M. Infracţiuni în domeniul informatic. Bucureşti: CH Beck, 2006. 401 p.

[16] Vasiu I., Vasiu L. Prevenirea criminalității informatice. București: Hamangiu, 2006. 216 p.

[17] Olteanu G. I. Metodologie criminalistică. Cercetarea structurilor infracţionale şi a unora dintre activităţile ilicite desfăşurate de acestea. București: AIT Laboratories, 2007. 423 p.

[18] Лазарева Н. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: Studia Universitatis, nr. 6. CEP USM, 2007, p. 133-141.

[19] Cârjan L., Chiper M. Criminalistică. Tradiție și modernism. București: Carte Veche, 2009. 544 p.

[20] Ioniță Gh. Iu. O scurtă analiză a infracțiunilor din sfera criminalității informatice incriminate în Legea nr. 161/2003 și în noul Cod penal al României. În: Revista Română de Criminalistică, 2011, vol. XI, nr. 2(74), p. 673-681.

[21] Croitor E. Categoriile „purtător tehnico-electronic de informație" și „înregistrări" în probatoriul penal. În: Revista Institutului Național al Justiției, 2010, nr.3-4 (15), p.116-117.

[22] Stancu E., Moise A. C. Considerații privind fenomenul de criminalitate informatică. În: Analele Universității din București: C.H. BECK, 2010, p.41-59.

[23] Moise A. C., Stancu Em. Criminalistica. Elemente metodologice de investigare a infracțiunilor. București: Universul Juridic, 2017. 356 p.

[24] Ioniță Gh. Iu. Criminalitatea informatică și investigarea criminalistică digitală. În: Revista Română de Criminalistică, 2010, vol. XI, nr. 3 (69), p.395-398.

[25] Moise A. C. Pregătirea cercetării la fața locului în cazul infracțiunilor informatice. În: Revista Română de Criminalistică, 2010, vol. XI, nr. 1(67), p.327-330.

[26] Moise A. C. Metodologia investigării criminalistice a infracțiunilor informatice. București: Universul Juridic, 2011. 438 p.

[27] Ghervase D. G. Securitatea informațiilor și internetul. Craiova: Universitaria, 2013. 124 p.

[28] Neamțu I. Vulnerabilități ale sistemelor informatice. Sibiu: Univ. „Lucian Blaga", 2013. 100 p.

[29] Ruiu M. Criminalistică. București: Universul Juridic, 2013. 352 p.

[30] Ruiu M. Metodologia investigării criminalistice a unor genuri de infracțiuni. București: Universul Juridic, 2014. 192 p.

[31] Cristescu D. I., Enescu V. C. Prolegomene privind administrarea și expertizarea probelor multimedia. Timișoara: Solness, 2013. 224 p.

[32] Stancu E., Manea T. Tactică criminalisctică. București: Universul Juridic, 2017. 224 p.

[33] Trancă A., Trancă D.C. Infracțiunile informatice în noul CP. București:Univ.Juridic, 2014.243 p.

[34] Brînză S., Stati V. Tratat de drept penal. P.Specială. Chișinău: Tipografia Centrală, 2015. 1298 p.

[35] Dolea Ig. Codul de procedură penală al RM. Chișinău: Cartea Juridică, 2016. 1172 p.

[36] Brânză S., Ulianovschi X., Stati V. Drept penal. Partea specială. Chișinău: Cartier, 2005. 804 p.

[37] Dobrinoiu V., Pascu, I., Hotca M. A. Noul Cod Penal comentat. Partea Specială. Ediția a II-a, revăzută și adăugită. București: Universul Juridic, 2014. 1154 p.

[38] Dobrinoiu M. Analiza juridică a infracțiunii de fals informatic. https://e-crime.ro/ecrime/site/files/19791236022059articol-ADPI-4.pdf (vizitat 02.06.2017).

[39] Vasiu I., Vasiu L. Frauda informatică. În: Revista de Drept Penal, București, 2005, nr.1, p. 45.

[40] Drăgan A. T. Frauda informatică în sistemul infracțiunilor contra patrimoniului în noul Cod penal român. În: Revista Naţională de Drept, Chișinău, 2016, nr. 6, p.63-67.

[41] Alecu Gh. Subiecții activi și pasivi ai infracțiunilor comise prin sisteme informatice, în viziunea noului Cod Penal. În: Reformele cadrului legal și instituțional din RM prin prisma practicilor europene. Tezele conf. științifice internaționale, Chișinău: USEM, ICEȘD, IISD al AȘM, 2010.

[42] Spiridon I. C. Reflecții cu privire la legislația română în domeniul criminalității informatice. În: Revista Dreptul, 2008, nr.6.

[43] Dobrinoiu M. Consideraţii privind încadrarea juridică a accesului ilegal la poşta electronică a unei persoane. În: Revista de Drept Penal, 2008, nr.3. https://e-crime.ro/ (vizitat 22.12.2017).

[44] Electronic evidence - a basic guide for First Responders. https://goo.gl/SNQrCh (20.05.2017).

[45] Dobrinoiu M. Infracțiunea de alterare a integrității datelor informatice. În: Revista Română de Dreptul Proprietății Intelectuale, 2006, nr.3, p.57.

[46] Hotca M., Dobrinoiu M. Infracțiuni prevăzute în legi speciale. București: C.H.Beck, 2008. 832 p.

[47] Sussmann M. The critical challenges from international high-tech and computer-related crime at the millennium. În: Duke Journal of Comparative & International Law, 1999, vol. IX, p.451-489.

[48] Быстряков Е. Н., Иванов А. Н., Климов В. А. Расследование компьютерных преступлений: учебное пособие. Саратов: СГАП, 2000. 232 с.

[49] Electronic Crime Scene Investigation, 2001. https://goo.gl/wQ4AQb (vizitat 18.05.2017).

[50] Moore R. To view or not to view: Examining the plain view doctrine and digital evidence. În: American Journal of Criminal Justice, 2004, vol. 29, nr.1, p.57-73.

[51] Мещеряков В. А. Основы методики расследованя преступлений в сфере компьютерной информации. Автореф. дис. канд. юрид. наук. Воронеж, 2001.

[52] Андреев Б. В., Пак П. Н., Хорст В. П. Расследование преступлений в сфере компьютерной информации. Москва: Юрлитинформ, 2001. 150 с.

[53] Smith S. The Concept of Security in a Globalized World. În: The Otago University Conference. Tezele conf. internaţionale. Otago, 2002.

[54] Головин А. Ю. Криминалистическая систематика. Москва: ЛексЭст, 2002. 335 с.

[55] Жмыхов А. А. Компьютерная преступность за рубежом и ее предупреждение. Дис. канд. юрид. наук. Москва, 2003. 178 с.

[56] Филиппов А. Г. Криминалистика: Учебник для высших юридических учебных заведений. Москва: Спарк, 2004. 750 с.

[57] Шурухнов Н. Г. Криминалистика: Учебное пособие. Москва: Юристь, 2005. 639 с.

[58] Baylis J. International and global security in the post-cold war era in The Globalization of World Politics, New York: Oxford University Press, 2005. p. 299-324.

[59] Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью. Дис. канд. юрид. наук. Москва, 2005. 218 с.

[60] Яблоков Н. П. Криминалистика: Учебник. 3-е изд. Москва: Юристь, 2007. 781 с.

[61] Reyes A., Wiles J. The Best Damn Cybercrime and Digital Forensics Book Period. Burlington: Syngress Publishing, 2007. 738 p.

[62] Егоров Н. Н. Вещественные доказательства: уголовно-процессуальный и криминалистический аспект. Москва: Юрлитинформ, 2007. 300 с.

[63] Kleiman D. The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensics Investigators. Burlington: Syngress Publishing Inc., 2007. 960 p.

[64] Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности. Дис. канд. юрид. наук. Москва, 2007, 418 с.

[65] Варданян А. В., Никитина Е. В. Расследование преступлений в сфере высоких технологий и компьютерной информации. Москва: Юрлитинформ, 2007. 309 с.

[66] Cross M. Scene of the Cybercrime. Rockland: Syngress Publishing Inc., a II-a ред., 2008. 744 p.

[67] Кузнецов А. П., Гарипова Н. В. Проблемы определения непосредственного объекта в преступлениях в сфере компьютерной информиции. În: Следователь, 2008, Т.7, с.5-7.

[68] Дуленко В. А., Мамлеев Р. Р., Пестриков В. А. Уголовно-правовые, криминологические и криминалистические проблемы расследования преступлений в сфере высоких технологий и компьютерной информации, Уфа: УГАТУ, 2009. 224 с.

[69] Holt T. J., Bossler A. M. Cybercrime in progress. New York: Routledge, 2016. 236 p.

[70] Литвинов Д. В., Скрыль С. В., Тямкин А. В. Исследование механизмов противодействия компьютерным преступлениям. Воронеж: Воронежский институт МВД, 2009. 218 с.

[71] Осипенко А. Л. О характеристике способов совершения сетевых компьютерных преступлений. В: Вестник криминалистики, 2009, н.4, с. 149-155.

[72] Ворошилова Т. В. Социальная и психологическая характеристика личности компьютерного преступника. Москва, 2009. 46 с.

[73] Менжега М. М. Методика расследования создания и использования вредоносных программ для ЭВМ. Москва: Юрлитинформ, 2010. 168 с.

[74] Худяков П. В., Овсянников Д. В. Особенности производства следственных действий при расследовании преступлении в сфере компьютерной информации. Челябинск: Челябинский юридический институт МВД России, 2010. 68 с.

[75] Алескеров В. И., Максименко И. А. Уголовно-правовая и криминалистическая характеристика современных видов преступлений в сфере компьютерной информации. Лекция. Домодедово: ВИПК МВД России, 2011. 27 с.

[76] Сизоненко А. Б., Шишкин В. Н. Особенности раскрытия преступлений в сфере компьютерной информации. Краснодар: КУ МВД России, 2011. 196 с.

[77] Good Practice Guide for Digital Evidence. ACPO. https://goo.gl/9WCiL1 (vizitat 20.05.2017).

[78] Смолькова И. В. Великие и выдающиеся, знаменитые и известные личности об уголовном судопроизводстве. Москва: Юрлитинформ, 2012. 688 с.

[79] Клементьев А. С., Бойко О. С. Организация взаимодействия МВД стран СНГ по предупреждению преступлений в сфере информационно-коммуникационных технологий. Домодедово: ВИПК МВД России, 2012. 37 с.

[80] Косынкин А. А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации: монография. Москва: Юрлитинформ, 2013. 216 с.

[81] Нарижный А., Пихов А. Использование специальных познаний при раскрытии и расследований преступлений в сфере высоких технологий. Краснодар:КУ МВД, 2014.62 с.

[82] Алескеров В. И., Куц Ф. А. Преступления, совершаемые в телекоммуникационых сетяхб как разновидность преступлений в сфере компьютерной информации. Домодедово: ВИПК МВД России, 2014. 38 с.

[83] Давыдов В. О. Методика расследования экстремистских преступлений, совершенных в компьютерных сетях. Москва: Юрлитинформ, 2014. 184 с.

[84] Мусиенко О. Особенности криминалистической характеристики преступлений, совершаемых в сфере компьютерной информации и сотовой связи. În: Зж, 2014, p.44-49.

[85] Ковалев С. А., Вехов В. Б. Особенности компьютерного моделирования при расследовании преступлений в сфере компьютерной информации. Москва: Буки-Веди, 2015. 182 с.

[86] Пименов В. А., Горошко И. В. Организационные и правовые проблемы борьбы с хищениями денежных средств с использованием вредоносных компьютерных программ. Москва: Академия управления МВД России, 2015. 168 с.

[87] Зеленский В. Д., Меретуков Г. М. Криминалистика. С.-Петербург: Юр.центр, 2015. 704 с.

[88] Bowles S. și Hernandez-Castro J. The first 10 years of the Trojan Horsedefence. În: Computer Fraud & Security, 2015. http://goo.gl/KGR4iD (vizitat 30.11.2016).

[89] Алескеров В. И., Колокольчикова О. Н. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации. Домодедово: ВИПК МВД, 2016. 106 с.

[90] Смирнова И. Г. и др. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ. М: Юрлитинформ, 2016. 312 с.

[91] Пропастин С. В., Тактика допроса по делам о неправомерном доступе к компьютерной информации. Омск: Образование Информ, 2016. 48 с.

[92] Аверьянова Т., Белкин Р., Корухов Ю. Криминалистика. М: Норма-инфра, 2017. 928 р.

[93] Савельева М. В., Смушкин А. Б. Криминалистика. Москва: Юстиция, 2017. 236 с.

[94] Кадникова Н. Г. Комментарий к УК РФ. Москва: Книжный мир, 2005. 911 с.

[95] Лебедева В. М. Комментарий к Уголовному кодексу РФ. Москва: Норма, 2006. 760 с.

[96] Овчинникова Н. А. Комментарий к УК РФ: расширенний уголовно-правовой анализ с материалами судебно-следственной практике. Москва: Экзамен, 2007. 976 с.

[97] Улезько С. И. Комментарий к УК РФ. Ростов-на-Дону: МарТ, 2002. 864 с.

[98] Витвицкий А. А. Уголовное право. Особенная часть: учебник. Москва: Приор, 1999. 608 с.

[99] Чучаева А. И. Новое в Уголовном кодексе. Москва: КонсультантПлюс, 2012. 94 с.

[100] Ваулина Т. И. Уголовное право. Особенная часть. Москва: Норма, 1998. 768 с.

[101] Звечаровского И. Э. Уголовное право России. Особенная часть. Москва, 2010. 976 с.

[102] Грачева Ю. В., Ермакова Л. Д. Комментарий к УК РФ. Москва: Проспект, 2006. 661 с.

[103] Коршунова О. Н. Курс криминалистики. Том 1. Санкт-Петербург: Юр. центр, 2016. 717 с.

[104] Наумов А. В. Комментарий к Уголовному кодексу РФ. Москва: Юристъ, 1997. 824 с.

[105] Скуратова Ю. И., Лебедева В. М. Комментарий к УК РФ. НОРМА-Инфра, 2001. 896 с.

[106] Мазуров В. А. Компьютерные преступления. Москва, 2002. 148 с.

[107] Богомолов М. В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации. Красноярск, 2002. 58 с.

[108] Сивицкая Н. Признаки объективной стороны несанкционированного доступа к компьютерной нформации. În: Судовы веснік, 2007, nr. 3, с.69-72.

[109] Коженевский С. Методы гарантированного уничтожения данных на жестких магнитных дисках. Публикации ЕПОС, 2003. с.36-52.

[110] Лосев В. Преступления против информационной безопасности. În: Судовы веснік, 2002, nr. 1, с.40-43.

[111] Рарога А. И. Уголовное Право РФ. Особенная Часть. Москва: МО РФ МГЮА 2004. 519 с.

[112] Козаченко И., Незнамова З., Новоселов Г. Уголовное право. М: Норма-Инфра, 1998. 768 с.

[113] Гульбин Ю. Преступления в сфере компьютерной информации. В: Российская юстиция, 1997, № 10, с.24-25.

[114] Гадельшин Р. И., Кузнецов В. К. Криминалистика. Москва: КНОРУС, 2016. 220 с.

[115] Смирнова И. Г., Коломинов В. В., Егерева О. А. Киберпреступность в ряде стран Азиатско-Тихоокеанского региона. În: Евразийская парадигма России и трансформация политико-правовых институтов. Tezele conf. internaţionale. Улан-Уд: 2012, с.173-178.

[116] Schjolberg S. A cyberspace treaty - A United Nations Convention or Protocol on cybersecurity and cibercrime. 2010. https://goo.gl/TJwWPC (vizitat 20.03.2017).

[117] Zainea M., Simion R. Infracţiuni în domeniul informatic. Bucureşti: C.H.Bech, 2009. 271 p.

[118] European Cybercrime Centre - EC3. EUROPOL. https://goo.gl/qzCdwc (vizitat 22.04.2017).

[119] About ENISA. https://www.enisa.europa.eu/about-enisa (vizitat 22.04.2017).

[120] INTERPOL Global Complex for Innovation. https://goo.gl/d7E4XG (vizitat 22.04.2017).

[121] Берд К. Война со многими неизвестными. În: Компьютерра, 2009, nr. 20, с.26-31.

[122] Electronic Evidence Guide. A basic guide for police officers, prosecutors and judges. Version

2.0. Strasbourg, 2014. https://rm.coe.int/1680465f73 (vizitat 11.05.2017).

[123] Internet Crime Complaint Center (IC3). https://www.ic3.gov/default.aspx (vizitat 15.05.2017).

[124] Ioniță Gh. Iu. Considerații generale cu privire la metodologia cercetării infracțiunilor din sfera criminalității informatice. În: Revista Română de Criminalistică, 2010, v.XI, nr.5(71), p.525-529.

[125] Ordin nr. 4682/C/2016 pentru aprobarea Regulamentului de organizare şi funcţionare al DIICOT. 2016, https://goo.gl/hp6wS9 (vizitat 23.04.2017).

[126] Serviciul de combatere a criminalităţii informatice. https://goo.gl/erBdq6 (vizitat 23.04.2017).

[127] Organigrama DCCO. https://goo.gl/RkTCkc (vizitat 23.04.2017).

[128] Registrul de stat al experților judiciari atestați. https://goo.gl/x5rdjJ (vizitat 23.04.2017).

[129] Dușa S., Purici D. Problematica competenţei organului de urmărire penală în cazul infracţiunilor informatice şi al infracţiunilor în domeniul telecomunicaţiilor. În: Studia Universitatis, Seria Ştiinţe Sociale, CEP USM, Chişinău, 2011, vol. V, nr. 3(43), p.197-202.

[130] Convenția Consiliului Europei cu privire la criminalitatea informatică, adoptată la 23.11.2001 în Budapesta. https://goo.gl/uuJpqb (vizitat 21.03.2017).

[131] Legea pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică. Nr.6 din 02.02.2009. În: Monitorul Oficial al Republicii Moldova, 20.02.2009, nr.37-40.

[132] Dascălu I., Ștefan C., Țupulan M. C. Percheziția judiciară. Craiova: Sitech, 2008.

[133] Proiectul legii pentru modificarea și completarea unor acte legislative nr. 161 (HG.434 2016-04-11), https://goo.gl/7Vh35j (vizitat 11.01.2018).

[134] Joint opinion on the draft Law nr.161 amending and completing moldovan legislation in the field of cybercrime. Venice Commission 2016, https://goo.gl/2DbiFx (vizitat 11.01.2018).

[135] Convenția Națiunilor Unite împotriva criminalității transnaționale organizate, adoptată la 15.11.2000. https://www.unodc.org/unodc/treaties/CTOC/#Fulltext (vizitat 21.03.2017).

[136] Legea pentru ratificarea Convenției Națiunilor Unite împotriva criminalității transnaționale organizate. Nr.15 din 17.02.2005. În: Monitorul Oficial al RM, 04.03.2005, nr.36-38.

[137] Convenția europeană de asistență juridică în materie penală. În: Tratatele internaționale, 1999, vol.14, p.71.

[138] Hotărârea Parlamentului pentru ratificarea Convenţiei europene de asistenţă judiciară în materie penală. Nr.1332 din 26.09.1997. În: Monitorul Oficial al RM, 30.10.1997, nr. 71/604.

[139] Модельный уголовный кодекс: постановление Межпарламентской ассамблеи государств-участников СНГ. Информ. бюл. Межпарламентской ассамблеи СНГ, 1996, nr. 10.

[140] Acord privind colaborarea statelor-membre ale CSI în lupta cu infracţiunile în domeniul informaţiei computerizate. Minsk, 2001. https://goo.gl/G94NAX (vizitat 06.06.2017).

[141] О Межгосударственной программе совместных мер борьбы с преступностью в 2011-2013 годы. Решение Совета глав государств СНГ. În: СПС Консультант +, Москва: 2010.

[142] Recomandări pentru cooperarea dintre autoritățile de aplicare a legii și furnizorii de servicii de internet împotriva criminalității informatice. https://rm.coe.int/16802fe14e (vizitat 12.05.2017).

[143] Legea telecomunicațiilor. Nr.520 din 07.07.1995. Abrogată prin Legea nr.241 din 15.11.2007. În: Monitorul Oficial al Republicii Moldova, 14.03.2008, nr.51-54.

[144] Гаджиев М. С. Криминологический анализ преступности в сфере компьютерной информации. Автореф. дис. канд. юрид. наук. Махачкала, 2004. 19 с.

[145] Legea cu privire la informatizare şi la resursele informaţionale de stat. Nr.467 din 21.11.2003. În:

Monitorul Oficial al Republicii Moldova, 01.01.2004, nr. 6-12/44.

[146] Hotărârea Guvernului cu privire la Pagina oficială a Guvernului RM în rețeaua Internet. Nr.1464 din 24.12.2007. În: Monitorul Oficial al Republicii Moldova, 28.12.2007, nr.203-206/1499.

[147] Згадзай О. Э., Казанцев С. Я. Киберпреступность: факторы риска и проблемы борьбы. În: Вестник НЦ БЖД, 2013, nr. 4 (18), с.80-86.

[148] Vasiu I. Criminalitatea Informatică. A II-a editie, București: Nemira, 2001. 240 p.

[149] Ghidul introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitata informatică. IN, RITI dot-GOV, MCTI, București, 2004. http://riti-internews.ro/ro/ghid.htm (vizitat 22.04.2017).

[150] Recommendation No. R (89) 9 on computer-related crime and final report of the European Committie on crime Problems. Council of Europe, Computer-related Crime, Strasbourg, 1990.

[151] Legea cu privire la informatică. Nr.1069 din 22.06.2000. În: Monitorul Oficial al Republicii Moldova, 05.07.2001, nr. 73-74/547.

[152] Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности. Дис. канд. юрид. наук. Москва, 2013, 30 с.

[153] International review of criminal policy. United National Manual on the prevention and control of computer-related crime. 1994. https://goo.gl/kZgF1Y (vizitat 22.04.2017).

[154] Directiva Consiliului Europei 91/250/EEC din 14.05.1991 cu privire la protecția programelor pentru calculator. https://goo.gl/6kDHDT (vizitat 26.10.2017).

[155] Legea privind prevenirea şi combaterea criminalităţii informatice. Nr.20 din 03.02.2009. În: Monitorul Oficial al Republicii Moldova, 26.01.2010, nr. 11-12/17.

[156] Protocol adițional la Convenția CE privind criminalitatea informatică. 2003. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 (vizitat 21.03.2017).

[157] Estorcare prin apeluri cu suprataxă. IGP, 2017. https://goo.gl/4TsdsU (vizitat 27.12.2017).

[158] Bădărău El., Șoimu Il. Securitatea în internet, problemele juridice în dreptul informațional. În: Anuar Științific, Institutul de Relații Internaționale din Moldova, 2012, p.230-235.

[159] A Road Map for Digital Forensic Research, DFRWS tehnical report. Digital Forensic Research Workshop (DFRWS), Utica, 2001.

[160] Dicționarul explicativ al limbii române. http://www.dex.ro/ (vizitat 20.10.2017).

[161] Гаврилин Ю. В. Преступления в сфере компьютерной информации: квалификация и доказывание. Москва: Книжный мир, 2003. 245 с.

[162] Purici S. Modelul şi cararcteristica criminalistică ale infracțiunilor informatice şi din domeniul telecomunicațiilor., În: Integrare prin cercetare și inovare. Tezele conf. Științifice naționale cu participare internațională, Chișinău, Științe Juridice, CEP USM, 2017, p.248-252.

[163] Trei persoane suspectate de șantaj. IGP, 2016. https://goo.gl/y2hoaE (vizitat 27.12.2017).

[164] Prima operațiune desfășurată la nivel european pentru combaterea activităților de spălare de bani. IGP, Chișinău, 2016. https://goo.gl/fqphto (vizitat 27.12.2017).

[165] Angheloiu I., Gyorfi Eu., Patriciu V. Securitatea și protecția informației în sistemele electronice de calcul. București: Editura Militară, 1986. 310 p.

[166] Cetăţeni ai Republicii Moldova implicaţi în comercializarea şi utilizarea softului maliţios „CITADEL". PG, 2014. http://procuratura.md/md/newslst/1211/1/5916/ (vizitat 22.12.2017).

[167] Евдокимов К. Н. Политические факторы компьютерной преступности в России. с. 41-47.

[168] Ciobanu Ig. Criminologie. Chișinău: Tipografia Centrală, 2013.

[169] Ciobanu Ig. Criminalitatea organizată la nivel transnațional. În: Analele științifice ale Universității de Stat din Moldova, Chișinău, 2000, vol. I, p.91-95.

[170] Jaishankar K. Establishing a Theory of Cyber Crimes. În: International Journal of Cyber Criminology. 2007. http://www.cybercrimejournal.com/Editoriaijccjuly.pdf (vizitat 15.12.2017).

[171] Dobrinoiu M. Infractori digitali. În: Revista Intelligence, București, 2008, nr. 4, p.13.

[172] Крылов В. Информационные компьютерные преступления, М: Норма-инфра, 1997. 276 с.

[173] Ищенко Е. П. Криминалистика: Учебник. Москва: Юристь, 2000. 751 с.

[174] Косенков А. Н., Черный Г. А. Общая характеристика психологии киберпреступника, 2012, nr. 3, с. 87-94.

[175] Аверьянова Т., Белкин Р., Корухов Ю. Криминалистика. Москва: Норма, 2007. 944 р.

[176] Polițiștii din Republica Moldova apreciați în cadrul atelierului de lucru la Eurojust din Haga. IGP, Chișinău, 2017. https://goo.gl/9jz8YH (vizitat 27.12.2017).

[177] MediaRing cu Eduard Harunjen, Procurorul General al RM, rubrică realizată de portalul Media Azi. PG, 2017. http://www.procuratura.md/md/newslst/1211/1/7029/ (vizitat 22.12.2017).

[178] Buță V., Ion E. Religie și securitate în Europa secolului XXI - glosar de termeni. București: Universitatea de Apărare „Carol I", 2007. 468 p.

[179] Bădălan E., Zaharescu L., Bogdan V. Sisteme globale de securitate, București:Ctea, 2009. 150 p.

[180] Administrator de site trimis în judecată pentru coruperea alegătorilor. PG, Chișinău, 2015. http://www.procuratura.md/md/newslst/1211/1/6521/?attempt=1 (vizitat 22.12.2017).

[181] Мешеряков В. А. Преступления в сфере компьютерной информации: правовой и криминалестический анализ. Воронеж: Воронежский гос. университет, 2001. 176 с.

[182] Ofițerii de investigații au reținut un hacker, suspectat de spargerea site-urilor oficiale. IGP, 2016. https://goo.gl/a2ed8x (vizitat 27.12.2017).

[183] Cioclei V., Ilie A. Impactul dreptului penal european asupra noului CP român. În: Analele Universității din București. Seria Drept., C.H. BECK, 2012, p.330-342.

[184] Шурухнов Н. Г. Расследование неправомерного доступа к компьютерной информации. Москва: Щит-М, 1999. 254 с.

[185] Croitor E. Purtătorii tehnico-electronici de informație în calitate de înregistrări în probatoriul penal. Probleme de administrare și admisibilitate. Teză de dr. în drept. Chișinău, 2012. 169 p.

[186] Internet Wi-Fi gratuit în troleibuzele din Chişinău. Direcţia Relaţii Publice, Primăria mun. Chișinău, 2016. http://chisinau.md/libview.php?l=ro&idc=403&id=14293 (vizitat 03.04.2017).

[187] Научно-практический комментарий к УК РФ. Н. Новгород: НОМОС, 1996. 608 с.

[188] Уголовный кодекс РФ. Постатейный комментарий. Москва: ЗЕРЦАЛО, 1997. 791 с.

[189] Уничтожение информации на винчестере: eRazer. În: журнал "Хакер", 2007. https://xakep.ru/2007/11/13/41093/ (vizitat 07.04.2017).

[190] Баранов И. Уничтожение информации. În: Бизнес и безопасность, 2003, nr. 3.

[191] Давыдов С. Компьютер для мачо. Самоучитель. Санкт-Петербург: Питер, 2005. 207 с.

[192] Специалисты нашли еще один троян для MacOS. https://goo.gl/2oDGXL (vizitat 07.04.2017).

[193] Крылов В. Информационные преступления - новый криминалистический объект. În: Российская юстиция, 1997, nr. 4, с.22-23.

[194] Vasiu I. Informatica juridică şi drept informatic. Cluj Napoca: Albastră, 2007. 224 p.

[195] Коршунова О. Н. Курс криминалистики. Санкт-Петербург: Юрид. центр, 2016. 747 с.

[196] Groza B. Introducere în Sistemele Criptografice cu Cheii Publice. Timişoara: UPT, 2007.

[197] Legea comunicaţiilor electronice. Nr.241 din 15.11.2007. În: Monitorul Oficial al Republicii Moldova, 14.03.2008, nr. 51-54/155.

[198] Безмалый В., Безмалая Е. Взлом операционных систем (на примере Windows NT/2000/9x). 2008. http://xaker.name/threads/8960/ (vizitat 07.04.2017).

[199] Социнженерия как оружие массового поражения. Крис Касперски, 2008. http://arhiv.xaker.name/threads/11714/ (vizitat 07.04.2017).

[200] Социальная инженерия как способ совершения преступлений в сфере компьютерной информации. 2008. https://www.hackzone.ru/articles/view/id/3253/ (vizitat 07.04.2017).

[201] Hotărîrea Plenului CSJ a RM cu privire la practica judiciară în cauzele penale privind minorii. Nr. 39 din 22.11.2004. În: Buletinul CSJ a Republicii Moldova, 2005, nr.7/6.

[202] Хилюта В. Банковская карточка как средство совершения преступления. În: Банкаускі веснік, 2009, nr. 22(459), с. 50-54.

[203] Беркинбаев Т. Б. Особенности выявления и расследования преступлений, совершаемых в сфере банковской деятельности. Автореф. дис. канд. юрид. наук. Челябинск, 2006, с.22-29.

[204] Stancu Em., Dragomir C. Aspecte de ordin tehnic şi legislativ privind fraudele de carduri. În: Revista Dreptul, 2009, nr. 7, p.180-192.

[205] Encescu Fl. Consideraţii asupra disputei dintre teorecticienii şi practicienii dreptului privind încadrarea juridică penală a skimming-ului. În: Justiţie şi Criminalitate Informatică. Tezele seminarului ştiinţific cu participare internaţională. Târgu-Jiu, 2009.

[206] Stancu E., Dragomir C. Aspecte în legătură cu atacurile informatice îndreptate împotriva instituţiilor de credit. În: Revista Dreptul, 2009, nr.10.

[207] Бабенко И. Расследование компьютерных преступлений в сфере электронной коммерции и электроных платежных средств. În: Securitatea informaţională, Tezele conf. internaţionale (ediţia a VII-a). Chişinău: ASEM. Laboratorul de securitate informaţională, 2010, c.88-91.

[208] Purici S., Golubenco Gh. Etapa alegerii produsului sau serviciului în cadrul investigaţiilor preliminare în cazul operaţiunilor frauduloase de plată electronică. În: Integrare prin cercetare şi inovare. Rezumatele conf. ştiinţifice naţionale. Chişinău: Ştiinţe Juridice, USM, 2016, p.219-223.

[209] A fost deferit justiţiei tînărul, care îşi cumpăra bilete de avion, prin utilizarea datelor cardurilor bancare străine. PG, Chişinău, 2015. https://goo.gl/HESHkM (vizitat 22.12.2017).

[210] Purici S., Analiza criminalistică preliminară în cadrul efectuării operaţiunilor frauduloase de plată on-line. În: Integrare prin cercetare şi inovare. Rezum. conf. şt. Chişinău: 2016, p. 223-227.

[211] A fost reţinut complicele tînărului, care îşi cumpăra bilete de avion, prin utilizarea datelor cardurilor bancare străine. PG, Chişinău, 2014. https://goo.gl/N3JSgd (vizitat 22.12.2017).

[212] Purici S., Driga C., Purici D. Particularităţile investigaţiilor preliminare online în cazul infracţiunilor cibernetice. În: Наука в современном мире (Science in the modern world). Tezele conf. internaţionale, Chişinău, „Liceul" şi „Мир науки", 2015, 244-261 p.

[213] Stancu Em., Dragomir C. Fraudele comise prin mijloace electronice de plată în Noul Cod penal. În: Analele Universităţii din Bucureşti. Seria Drept, C.H. BECK, 2010, p.31-40.

[214] Chelnerul şi barmanul unui local din capitală sustrăgeau bani de pe cardurile clienţilor. PG, 2015.

http://www.procuratura.md/md/newslst/1211/1/6034/?attempt=2 (vizitat 22.12.2017).

[215] The history of banking Trojans. https://goo.gl/uK3Vj5 (vizitat 20.07.2016).

[216] Эволюция Zeus. Part I. 2012. https://habrahabr.ru/post/161707/ (vizitat 12.08.2016).

[217] Иванов Н. А. Применение специальных познаний при проверке "цифрового алиби". În: Информационное право, 2006, с.31-33.

[218] Easttom C., Taylor J. Computer Crime, Investigation, And the Law, Boston: Course Technology, Cengage Learning, 2010. 499 p.

[219] Ciampa M. Security. Guide To Network Security Fundamentals. Boston: Course Technology, Cengage Learning, 2009. 24 p.

[220] Shinder D. L., Tittel E. Scene of the cybercrime. Computer Forensics Handbook. Rockland: Syngress Publishing Inc, 2002. 716 p.

[221] Wannacry Ransomware: recent cyber-attack. 2017. https://goo.gl/AC2aZW (vizitat 15.05.2017).

[222] WannaCry: o nouă amenințare de tip ransomware cu victime la scară globală. 2017. https://cert.ro/citeste/wannacry-ransomware-alerta (vizitat 15.05.2017).

[223] DEEP WEB LINKS. 2013. http://deepweblinks.org/ (vizitat 12.05.2017).

[224] Walsh D. A Beginner's Guide to Exploring the Darknet. https://goo.gl/427YyQ (12.05.2017).

[225] Investigating the Dark Web, 2014. https://goo.gl/fP1MTM (vizitat 12.05.2017).

[226] Deep Web Directories and Search Engines. 2013. https://goo.gl/3c65TR (vizitat 12.05.2017).

[227] Barbosa L., Freire, J. An Adaptive Crawler for Locating Hidden-Web Entry Points. http://www.cs.utah.edu/~juliana/pub/ache-www2007.pdf (vizitat 12.05.2017).

[228] Ntoulas Al. ș.a. Downloading Hidden Web Content. https://goo.gl/Sc8ndt (vizitat 12.05.2017).

[229] Guide to Tor hidden services and elements of the Tor. https://goo.gl/cg8qLs (vizitat 12.05.2017).

[230] Hotărârea Guvernului cu privire la Agenţia de Stat pentru Protecţia Moralităţii pe lângă Ministerul Culturii. Nr.1400 din 17.12.2001. În: Monitorul Oficial al RM, 27.12.2001, nr.158/1455.

[231] Гаврилин Ю. В., Шипилов В. В., Особенности следообразования при совершении мошенничества в сфере компьютерной информации. В: Рос.следователь, 2013, № 23, с.2-6.

[232] Яблокова Н., Александрова И. Криминалистика. Москва: Норма ИНФРА-М, 2017. 752 с.

[233] Golubenco Gh. Criminalistică: cercetarea urmelor materiale ale infracțiunii, Chișinău: Tipografia Centrală, 2015. 116 p.

[234] Leu C. Cercetarea la fața locului în cazul infracțiunilor săvârșite prin mijloace electronice. Investigarea criminalistică a locului faptei, București: Luceafărul, 2004.

[235] Golubenco Gh. Tehnica criminalistică: exegeză istorico-filosofică în contextul evoluției tehnicii generale. În: Legea și Viața, Chișinău, 2001, nr. 10, p. 4.

[236] Протасевич А., Зверянская Л. Проблемы собирания и оценки компьютерной информации как доказательства. În: Современная криминалистика. Москва: АУ МВД, 2012, с.274-275.

[237] Moise A. C. Considerații privind probele digitale. În: Revista Română de Criminalistică, 2011, nr. 2, p.683-687.

[238] Hosmer C. Proving the Integrity of Digital Evidence with Time. În: International Journal of Digital Evidence, 2002, vol.I, nr. 1. https://goo.gl/WJcN7m (vizitat 23.04.2017).

[239] Крылов В. Расследование преступлений в сфере информации. М: Городец, 1998. 264 с.

[240] Gheorghiță M. Criminalistica. Chișinău: Museum, 1995. 114 p.

[241] Георгицэ М., Дмитриев Г. Электронно-вычислительную технику – на службу следствию. În: Следствие и Дознание, 1987, nr.121, с. 85.

[242] Георгицэ М. ЭВМ – эффективное средство решения задач следователей, Теория криминалистики и методика расследования преступлений. Москва, 1990. 132 с.

[243] Legea privind protecția datelor cu caracter personal. Nr. 133 din 08.07.2011. În: Monitorul Oficial al Republicii Moldova, 14.10.2011, nr. 170-175.

[244] Legea cu privire la registre. Nr.71 din 22.03.2007. În: Monitorul Oficial al Republicii Moldova, 25.05.2007, nr. 70-73.

[245] Gheorghiță M. Noi abordări științifice în tactica criminalistică. În: Legea și Viața, Chișinău, 2012, nr. 2, p.4.

[246] Dolea Ig. Drepturile persoanei în probatoriul penal. Chișinău: Cartea Juridică, 2009. 416 p.

[247] Руденко А. В. Понятие криминалистической версии. În: "Чёрные дыры" в Российском Законодательстве, 2010, с.119-121.

[248] Яблоков Н. П. Криминалистика: Учебник. 2-е изд. Москва: Юристь, 2001. 718 с.

[249] Procuratura acordă atenţie sporită combaterii criminalităţii cibernetice. PG, Chişinău, 2018. http://procuratura.md/md/newslst/1211/1/7410/ (vizitat 09.03.2018).

[250] Белкин Р. С. Криминалестическое обеспечение деятельности криминальной милиции и органов предварительного расследования. Москва: Новый Юрист, 1997. 400 с.

[251] Golubenco Gh. Obiectul și sistemul criminalisticii: probleme actuale. În: Legea și viața, Chișinău, 2005, nr. 10, p. 4-8.

[252] Purici S. In dubio pro reo: Apărarea Cal Troian în cauzele de criminalitate informatică. În: Revista Penalmente/Relevant, Universitatea „Nicolae Titulescu", 2016, nr. 2/2016, p. 166-172. https://goo.gl/wihmW6 (vizitat 23.04.2017).

[253] Purici S. Bune practici internaționale cu privire la investigarea infracțiunilor informatice. Studia Universitatis Moldaviae, Seria Ştiinţe Sociale, CEP USM, Chişinău, 2015, nr. 3(83), p.162.

[254] Галкин А. И. Компьютерная информация как обьект уголовно-правовой защиты. În: Следователь. Федеральное издание, 2009, nr.4, с.2-6.

[255] Purici S., Gheorghiță M. Măsuri tactice și strategice de depășire a obstacolelor care împiedică buna desfășurare a investigării infracțiunilor informatice. În: Studia Universitatis Moldaviae, Seria Științe Sociale, CEP USM, Chișinău, 2017, nr. 8(108), p.146.

[256] United States v. Dodd, 598 F.3d 449, 451-53 (8th Cir. 2010).

[257] United States v. Creel, 783 F.3d 1357 (11th Cir. 2015).

[258] Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. Москва: НОРМА-ИНФРА, 2001. 240 с.

[259] Крупные атаки хакеров в 2001-2016 годах, 2016. http://tass.ru/info (vizitat 17.04.2017).

[260] Сидоренко Е. В. Взаимодействие государственного обвинителя и оперативных работников в нейтрализаций преступного пртиводействия осушествлению судебного рассмотрения уголовного дела. În: Криминалистический вестник, С.-Петербург, 2005, nr.4, с.75-77.

[261] Тепуков А. В. Преодоление противодействия доказыванию по уголовным делам в отношении прокуроров, руководителей следственных органов и следователей. În: Закон и право, Юнити-Дана, 2009, nr. 6, с.77-79.

[262] Бабаева Э. У. Проблемы теории и практики преодоления противодействия уголовному преследованию. Москва: Юрлитинформ, 2006. 312 с.

[263] Кривенко А. И. Теория и практика взаимодействия следователя с органами, осушествляющими оперативно-розыскную деятельность. М: Юрлитинформ, 2008. 240 с.

[264] Ратинов А. Р. Судебная психология для следователей. Москва: Юрлитинформ, 2001. 352 с.

[265] Журавлёв А. Следователь как субъект процессуального руководства расследованием. В: Актуальные проблемы современного процесса РФ. Самара, 2008, nr.3, с.216-221.

[266] Старичков М. В. Тактика проведения обыска, связонного с изъятием носителей компьютерной информации. În: Криминалистика: актуальные вопросы теории и практики. Ростов-на-Дону: ФГОУ ВПО "РЮИ МВД России", 2010, с.167-169.

[267] Мерецкий Н. Е. Опыт использования тактических комбинации при расследование преступлений. În: Актуальные вопросы криминалистического обеспечения судопроизводства. Иркутск: БГУЭП, 2010.

[268] Краснова Л. Б. Компьютерные объекты в уголовном процессе и криминалистике. Воронеж, 2005. 152 с.

[269] Понамарев И. П. Цифровое алиби. Воронеж: Воронежского гос. университета, 2010. 275 с.

[270] Alibiul. Wikipedia. https://ro.wikipedia.org/wiki/Alibi (vizitat 25.07.2017).

[271] Purici S. Particularităţile problemelor care urmează a fi soluţionate în cadrul investigării criminalistice a infracţiunilor informatice. În: Studia Universitatis Moldaviae, Seria Ştiinţe Sociale, CEP USM, Chişinău, 2015, nr. 8(88), p.144.

[272] Шурухнов Н. Г. Расследование неправомерного доступа к компьютерной информации: учебное пособие. Москва: Московский университет МВД России, 2004. 352 с.

[273] Purici S. Aspecte procesuale şi criminalistice privind investigarea crimelor cibernetice la etapa actuală. În: Analele Ştiinţifice ale USM, Ştiinţe socioumanistice, Chişinău, 2012, vol.II, p.3.

[274] Chirilă M. Tactica pregătirii percheziţiei la cercetarea infracţiunilor informatice. În: Правовые реформы в постсоветских странах. Tezele conf. ştiinţifico-practice. Chişinău: 2014, p.286-287.

[275] Шатшюович П. Проблемные вопросы преступлений в сфере компьтерной информации. În: Научные исследования высщей школы. Tezele conf. ştiinţifice. Тюмень: 1998, с. 8-12.

[276] Филиппов А. Г. Криминалистика: Учебник для высших юридических учебных заведений. 2-е издание. Москва: Спарк, 2000. 687 с.

[277] Forensic Examination of Digital Evidence: A Guide. https://goo.gl/21eJ59 (vizitat 20.05.2017).

[278] Driga C., Purici S. Fighting the classical crime-scene assumptions. Critical aspects în establishing the crime-scene perimeter. În: Revista Challenges of the Knowledge Society. Criminal Law, Bucureşti, 2016, p. 1006. https://goo.gl/4JuHh7 (vizitat 01.10.2017).

[279] Brenner S. W., Carrier B., Henninger, J. The Trojan Horse Defense în Cybercrime Cases. 21 Santa Clara High Tech.L.J. 1, 2004. 54 p.

[280] Haagman D., Ghavalas B. Trojan defense. În: Digital Investigation, 2005, nr. 2, p.22-30.

[281] Moise A. C. Probele în criminalitatea informatică. În: Revista Doctrinară, 2009, nr. 4, p.1-5.

[282] Усова А. И. Судебно-экспертное исследование компьютерных средств и систем. Москва: Право и закон, 2003. 368 с.

[283] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. Москва: Горячая линия-Телеком, 2002. 336 с.

[284] Пропастин С. В. Осмотр или судебное экспертиза: выбор в пограничных ситуацыях. În: Современное право, 2013, с.129-132.

[285] Constantin Al. Recomandări în investigarea criminalistică informatică. În: Revista Română de Criminalistică, 2006, nr. 6.

[286] United States Computer Emergency Readiness Team, 2008. https://goo.gl/szxGng (23.04.2017).

[287] Shipley T. G., Reeve H. R. Collecting evidence from a running computer. În: The National Consortium For Justice, 2006. https://goo.gl/ECXMc2 (vizitat 23.04.2017).

[288] Navigator web. Wikipedia. https://ro.wikipedia.org/wiki/Navigator_web (vizitat 02.01.2018).

[289] Motor de căutare. Wikipedia. https://goo.gl/QWsM8r (vizitat 02.01.2018).

[290] Brown C. L.T. Computer Evidence. Hingham: Charles River Media Inc, 2006. 394 p.

[291] Android: using puk code to reset pin. 2013. https://goo.gl/e3ZckJ (vizitat 13.04.2017).

[292] GSMARENA. http://www.gsmarena.com/ (02.05.2017).

[293] Legea pentru completarea articolului 118 din Codul de procedură penală al RM nr. 122-XV din 14 martie 2003. Nr. 294 din 22.12.2016. În: Monitorul Oficial al RM, 03.02.2017, nr. 30-39.

[294] Zlati G. Percheziţia sistemelor informatice şi a mijloacelor de stocare a datelor informatice (II). În: Caiete de drept penal, 2014, nr. 4, p.77.

[295] Drăghici C., Ştefan C.E. Tactica efectuării percheziţiei şi a ridicării de obiecte şi înscrisuri. Craiova: Sitech, 2006. 251 p.

[296] Gheorghiță M. Tactica cercetării la fața locului. Chișinău: Angela Levința, 2004. 72 p.

[297] Victim identification. ICPO. https://goo.gl/ca1tDf (vizitat 16.10.2015).

[298] International Association of Internet Hotlines. https://goo.gl/19wd4A (vizitat 15.05.2017).

[299] McLean J. J. Homicide and Child Pornography. Handbook of Computer Cime Investigation. Forensic Tools and Technology, Londra: Academic Press, 2002, p.361-373.

[300] Fighting malware and cyber criminality. http://www.malwareurl.com/ (vizitat 15.05.2017).

[301] Hotărârea Guvernului cu privire la aprobarea Concepţiei sistemului informaţional automatizat „Registrul resurselor şi sistemelor informaţionale de stat”. Nr. 1032 din 06.09.2006. În: Monitorul Oficial al RM, 22.09.2006, nr.150-152.

[302] Croitor E. Administrarea probei electronice prin percheziția calculatorului în probatoriul procesual-penal. În: Revista de Științe Penale, 2008-2009, p.137-145.

[303] Croitor E. Argumentarea admisibilității înregistrărilor audio/video în procedura penală, din perspectiva drepturilor omului. În: Revista Națională de Drept, 2006, nr.6, p.73-78.

[304] Alecu Gh., Barbăneagră Al. Reglementarea penală și investigarea criminalistică a infracțiunilor în domeniul informatic. București: Pinguin Book, 2006. 271 p.

[305] Аверьянова Т. В., Белкин Р. С., Корухов Ю. Криминалистика. Москва: Норма, 2008. 944 с.

[306] Udroiu M., Slăvoiu R., Predescu O. Tehnici speciale de investigare în justiția penală. București: C.H.Beck, 2009. 240 p.

[307] Hotărârea Curții Europene de Justiție în cauzele conexate C-293/12 și C-594/12 din 08.04.2014., https://goo.gl/cMJLps (vizitat 15.05.2017).

[308] Legea cu privire la asistenţa juridică internaţională în materie penală. Nr. 371-XVI din 01.12.2006. În: Monitorul Oficial al Republicii Moldova, 2007, nr. 14-17.

[309] Россинская Е., Усов А. Судебная компьютерно-техническая экспертиза. Москва: Право и

Закон, 2001. 416 с.

[310] Россинская Е. Р. Судебная экспертиза в гражданском, административном и уголовном процессе. Москва: Норма, 2005. 655 p.

[311] Dascălu I. ș.a. Frauda în domeniul cardurilor. Târgoviște: Sfinx 2000, 2003. 140 p.

[312] Рубцов И. И. Комплексная методика производства автороведческих экспертиз: методические рекомендации. Москва: ЭКЦ МВД России, 2007. 188 с.

[313] Горобченко С. В. Методика расследования мошенничества в сфере оборота недвижимости. Дис. канд. юрид. наук. Нижневартовск, 2007, 210 с.

[314] Golubenco Gh., Neicuțescu O. Expertiza judiciară: noțiune, conținut, specific. În: Legea și Viața, Chișinău, 2009, nr. 4, p. 50.

[315] Маклаков Г. Ю., Рыжков Э. В. Особенности оперативно-розыскной деятельности при расследование преступлений в сфере высоких технологий. http://www.crime-research.org/ (vizitat 25.03.2017).

[316] Cybercrime training for judges and prosecutors: a concept. Council of Europe. Directorate General of Human Rights and Legal Affairs, 2009. https://goo.gl/RYkEMb (vizitat 23.04.2017).

[317] Bădărău El. Reglementarea răspunderii penale pentru infracțiunile în domeniul informatic în legislația Republicii Moldova. În: Revistă științifico-practică. IRIM, 2012, nr.1/2012, p. 120-128.

[318] Amza T., Moraru D. I. Internetul şi criminalitatea informatică. În: Criminalistica. Revistă de informare, documentare şi opinii, 2006, nr. 5, p.42-44.

[319] Purici S. Specificul activității speciale de investigații și acțiunii de urmărire penală întreprinse pentru administrarea probelor la cercetarea crimelor cibernetice, În: Studia Universitatis Moldaviae, Seria Ştiinţe Sociale, CEP USM, Chişinău, 2015, nr. 11, p.120-125.

[320] Explanatory Report to the Convention on Cybercrime. https://goo.gl/SdgLJe (vizitat 25.04.2017).

[321] T-CY Guidance Note #10. Production orders for subscriber information (Article 18 Budapest Convention). Strasbourg, 2017. https://goo.gl/fDWzeu (vizitat 05.05.2017).

[322] Constituția Republicii Moldova din 29.07.1994. În: Monitorul Oficial al RM, 29.03.2016, nr.78.

[323] Reguli de prestare a serviciilor poștale, aprobate prin Hotărârea Guvernului. Nr. 1457 din 30.12.2016. Monitorul Oficial al Republicii Moldova, 27.01.2017, nr. 24-29.

[324] Legea comunicațiilor poștale. Nr. 36 din 17.03.2016. În: Monitorul Oficial Republicii Moldova, 29.04.2016, nr. 114-122.

[325] Legea poștei. Nr. 463 din 18.05.1995. Abrogată prin Legea nr. 36 din 17.03.2016. În: Monitorul Oficial al Republicii Moldova, 29.04.2016, nr. 114-122.

[326] Bejanu A. Aplicarea mijloacelor tehnice de control la depistarea contrabandei comisă prin trimiterile poștale internaționale. În: Revista Națională de Drept, 2016, nr.5, p.63.

[327] Registrul public al Furnizorilor de servicii poștale. Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației. https://goo.gl/jSfYrn (vizitat 03.01.2018).

[328] Udroiu M. Tehnici speciale de investigare în justiția penală. București: C.H. Beck, 2009. 225 p.

[329] Hotărârea CtEDO, Campbell v. Regatul Unit (25.03.1992, nr. 13590/88, Par.48).

[330] Tudoran M. V. Teoria și practica interceptărilor și înregistrărilor audio sau video judiciare. București: Universul Juridic,, 2012. 407 p.

[331] Hotărârea CtEDO Klass și alții v. Germania, A28, 06.09.1978.

[332] Hotărârea CtEDO Kruslin v. Franța, 176-A, 24.04.1990.

[333] Hotărârea CtEDO Huvig v. Franța, 176-B, 24.04.1990.

[334] Hotărârea CtEDO Malone v. Marea Britanie, A82, 02.08.1984.

[335] Hotărârea CtEDO Halford v. Marea Britanie, Reports 1997 – III, 25.06.1997.

[336] Hotărârea CtEDO Lambert v. Franța, Reports 1998 – V, 24.08.1998.

[337] Pantea M. ș.a. Investigarea fraudelor informatice. Craiova: Sitech, 2008. 188 p.

[338] Грибков А. Спецслужбы будут прослушивать разговоры в Skype. 2012. https://goo.gl/ieN6Bu (vizitat 04.04.2017).

[339] Gărăiman D. Dreptul și informatica. București: All Beck, 2003. 341 p.

[340] Lucaci I., Marin R. Criminalitatea informatică. București: Fed Print S.A., 2003.

[341] How to Get Email Headers. https://goo.gl/bSc7Si (vizitat 17.05.2017).

[342] Mail Header Analysis for Spoof Protection. https://goo.gl/vNvnKX (vizitat 16.05.2017).

[343] Email Header Analysis. https://goo.gl/YZMdKw (vizitat 17.05.2017).

[344] Email Header Analyzer. https://goo.gl/tXMbm9 (vizitat 17.05.2017).

[345] G Suite Toolbox. Messageheader. https://goo.gl/F3Mxox (vizitat 17.05.2017).

[346] Purici S., Purici D. Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic., În: Integrare prin cercetare și inovare. Chișinău: Științe Juridice, CEP USM, 2017. Tezele conf. științifice, p.233.

[347] Registrul public al furnizorilor de reţele şi servicii de comunicaţii electronice. ANRCETI, 2017. http://anrceti.md/lista_furnizori_servicii_retele_ce (vizitat 03.01.2018).

[348] The Voluntary Cooperation Model and Production Orders for Subscriber Information. Service provider/law enforcement cooperation. https://rm.coe.int/16806bdafd (vizitat 05.05.2017).

[349] Law Enforcement Information Request for EMEIA Geographical Region. https://www.apple.com/legal/privacy/emeia-le-inforequest.pdf (vizitat 05.05.2017).

[350] Adresă IP. Wikipedia. https://ro.wikipedia.org/wiki/Adres%C4%83_IP (vizitat 26.04.2017).

[351] AFRNIC. The Internet Number Registry for Africa. http://www.afrinic.net/ (vizitat 05.05.2017).

[352] APNIC. The Regional Internet Registry IP addresses for the Asia Pacific. https://www.apnic.net/ (vizitat 05.05.2017).

[353] ARIN. American Registry for Internet Numbers. https://www.arin.net/ (vizitat 05.05.2017).

[354] LACNIC. Latin American and Caribbean Internet. http://www.lacnic.net/ (vizitat 05.05.2017).

[355] RIPE NCC. RIPE Network Coordination Centre. https://www.ripe.net/ (vizitat 05.05.2017).

[356] Regional Internet registry. https://goo.gl/BAFMcv (vizitat 16.10.2015).

[357] Titularii de licențe pentru utilizarea resurselor de numerotare. ANRCETI, 2017. http://anrceti.md/titulari_lic_resurse_numerotare (vizitat 05.05.2017).

[358] Hotărârea nr. 38/1 privind desemnarea administratorului bazei de date centralizate pentru implementarea şi realizarea portabilităţii numerelor în Republica Moldova. ANRCETI, Chișinău, 2012. http://www.anrceti.md/files/filefield/HCA%20admin.pdf (vizitat 05.05.2017).

[359] Portabilitatea numerelor în Republica Moldova. Î.C.S. „NP BASE" SRL. http://portare.md/ (vizitat 05.05.2017).

[360] Purici S., Metodica cercetării infracțiunilor din domeniul informaticii. Monografie. Chișinău: CEP USM. 2018, 221 p.

ANEXE
ANEXA 1

Cauzele penale examinate în perioada anilor 2003-2017 pe teritoriul RM

	Numărul cauzelor penale intentate															
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total
177	2	2	3	2	2	2	4	4	7	11	12	9	10	26	22	**118**
178	0	0	1	1	2	0	3	10	8	10	8	4	9	9	13	**78**
185[1]	0	1	25	58	38	20	41	16	7	2	14	21	14	5	7	**269**
185[2]	0	0	0	0	0	0	2	3	6	4	7	11	4	13	7	**57**
185[3]	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	**1**
208[1]	0	0	0	0	0	1	1	0	4	7	15	11	18	29	38	**124**
237	7	10	6	10	8	165	19	44	32	44	19	10	9	3	3	**389**
259	0	0	0	2	2	4	2	1	0	1	4	6	2	5	0	**29**
260	0	1	1	1	0	0	0	1	3	0	1	1	4	4	0	**17**
260[1]	0	0	2	0	0	0	0	0	2	0	0	0	2	1	0	**7**
260[2]	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	**2**
260[3]	0	0	0	0	0	0	0	3	2	2	0	0	1	3	1	**12**
260[4]	0	0	0	0	0	0	0	1	0	0	0	1	0	2	0	**4**
260[5]	0	0	0	0	0	0	1	1	0	2	3	0	8	1	6	**22**
260[6]	0	0	0	0	0	0	1	1	3	5	13	13	10	8	10	**64**
261	0	1	3	0	2	2	1	1	1	0	0	1	1	0	0	**13**
261[1]	0	1	1	1	1	0	1	3	4	2	8	7	5	3	6	**43**
Total	**9**	**16**	**43**	**75**	**55**	**194**	**76**	**89**	**79**	**90**	**104**	**96**	**97**	**113**	**113**	**1249**

Fig.A1.1. (Evoluția cauzelor penale înregistrate în perioada anilor 2003-2017)

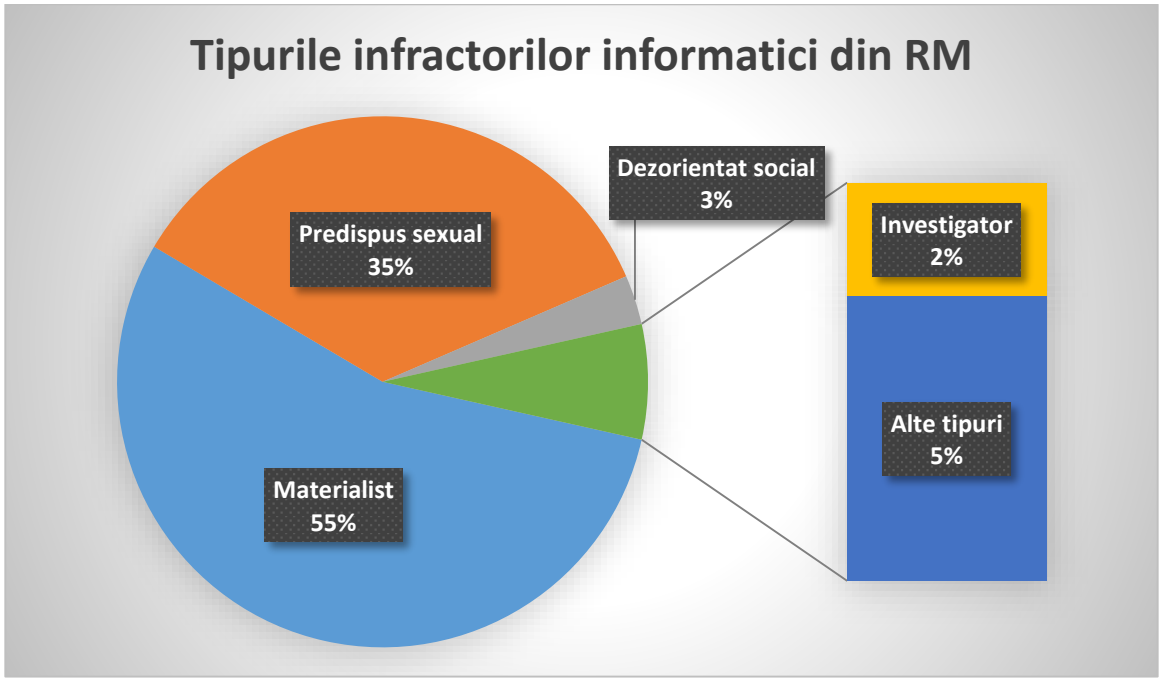


Fig.A1.2. Tipurile infractorilor informatici din RM în baza motivației infracționale, reieșind din sentințele de condamnare

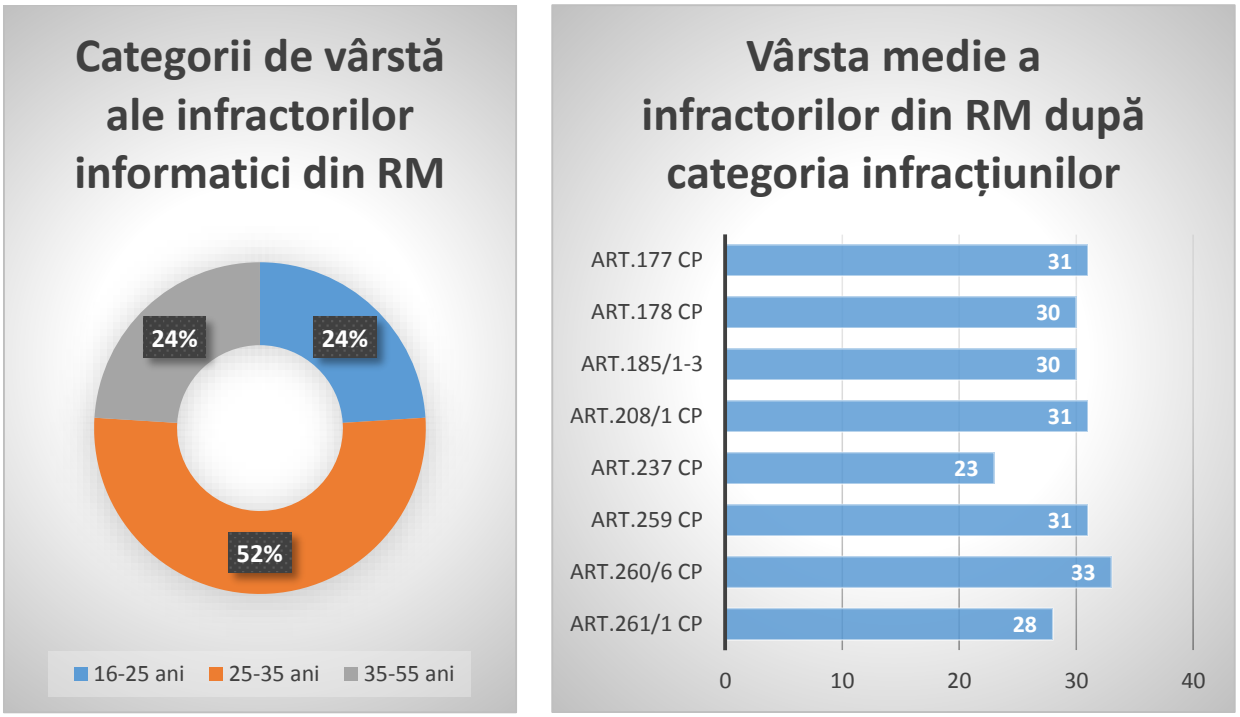


Fig.A1.3. Vârsta infractorilor informatici din RM potrivit datelor din sentințele de condamnare

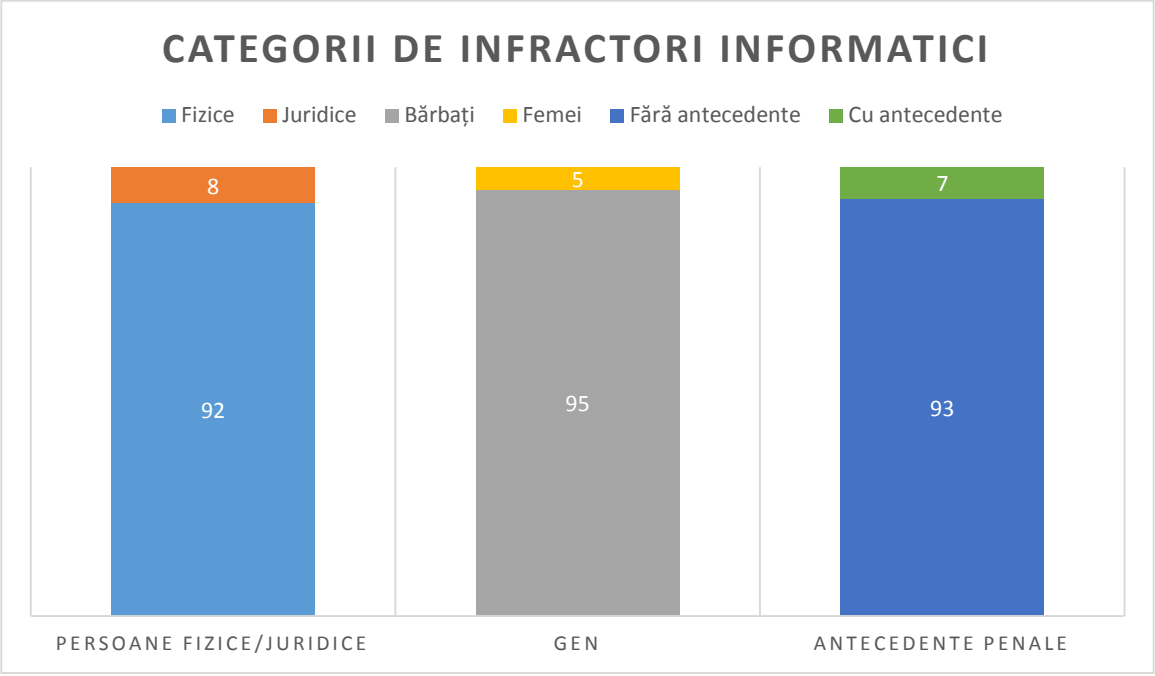


Fig.A1.4. Categoriile infractorilor informatici din RM potrivit sentințelor de condamnare

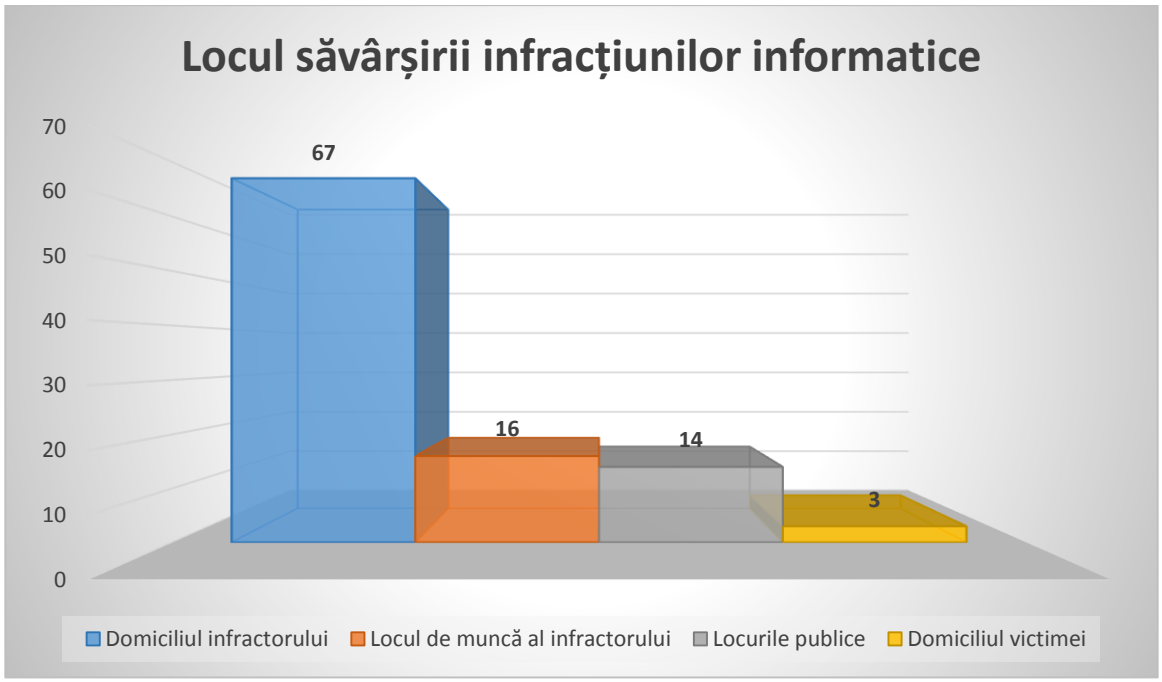
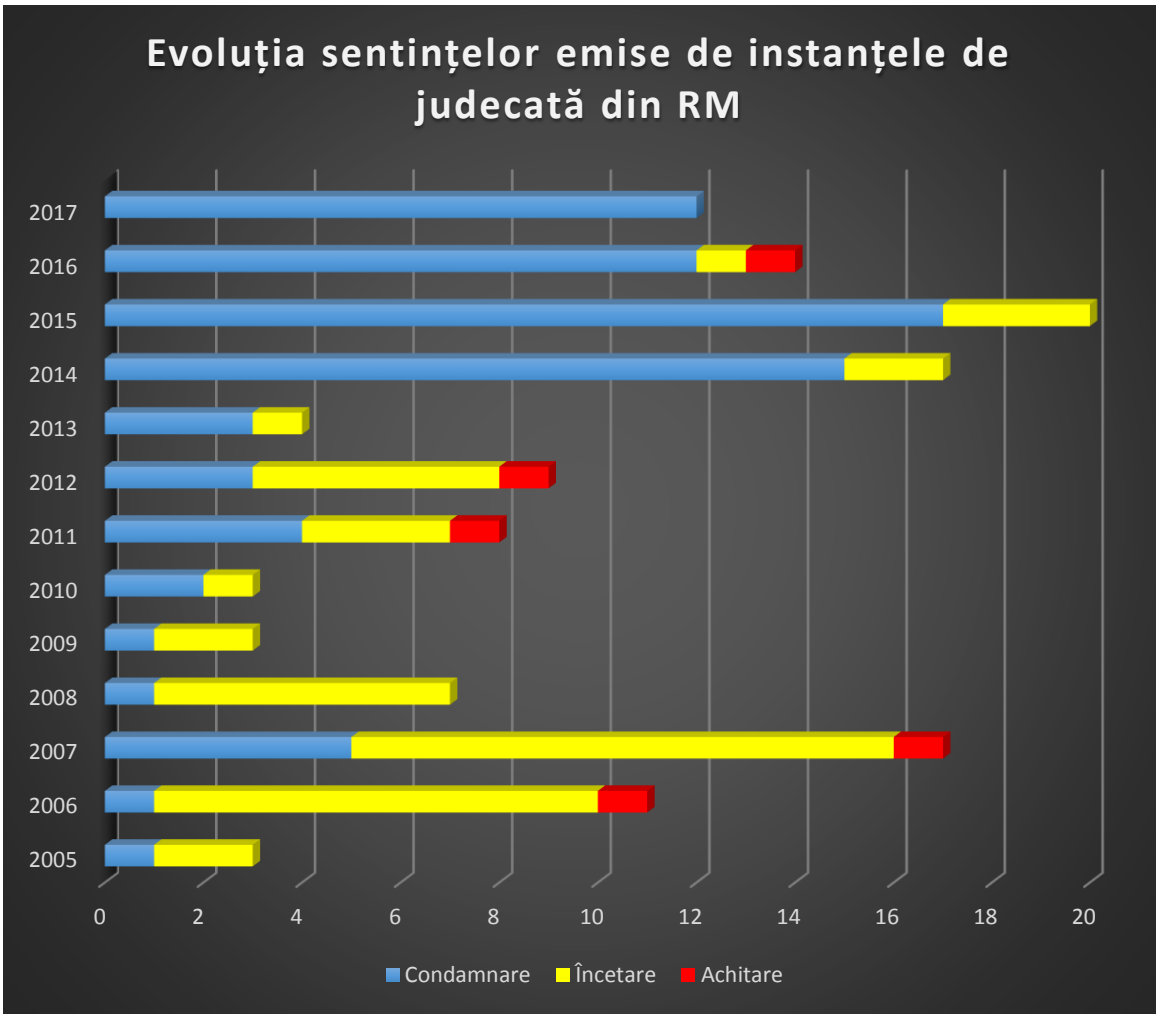


Fig.A1.5. Locul săvârșirii infracțiunilor informatice în RM, potrivit sentințelor de condamnare



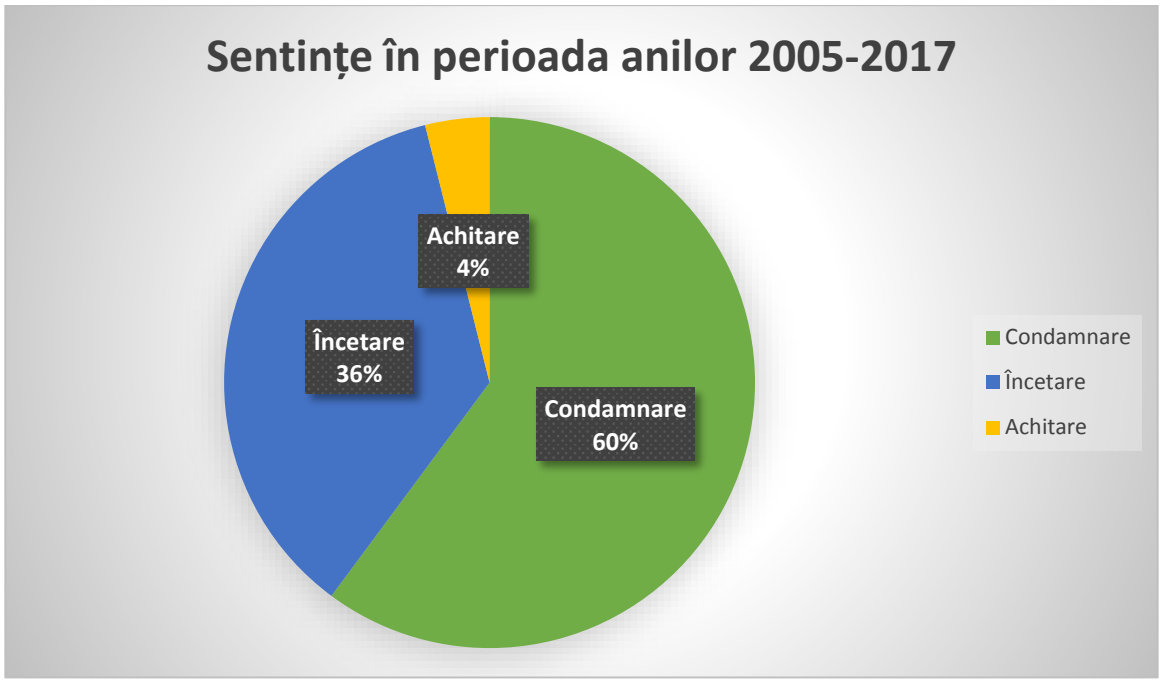


Fig.A1.6. Categoriile sentințelor emise de către instanțele de judecată din RM în cazurile de criminalitate informatică

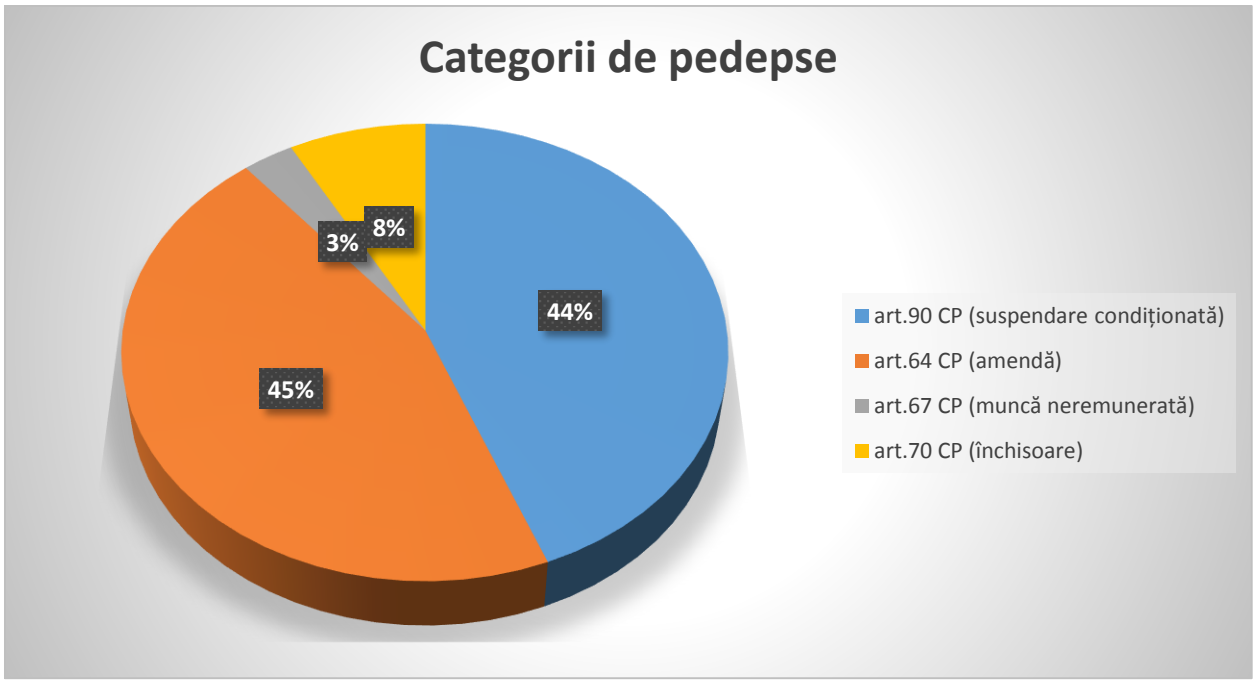
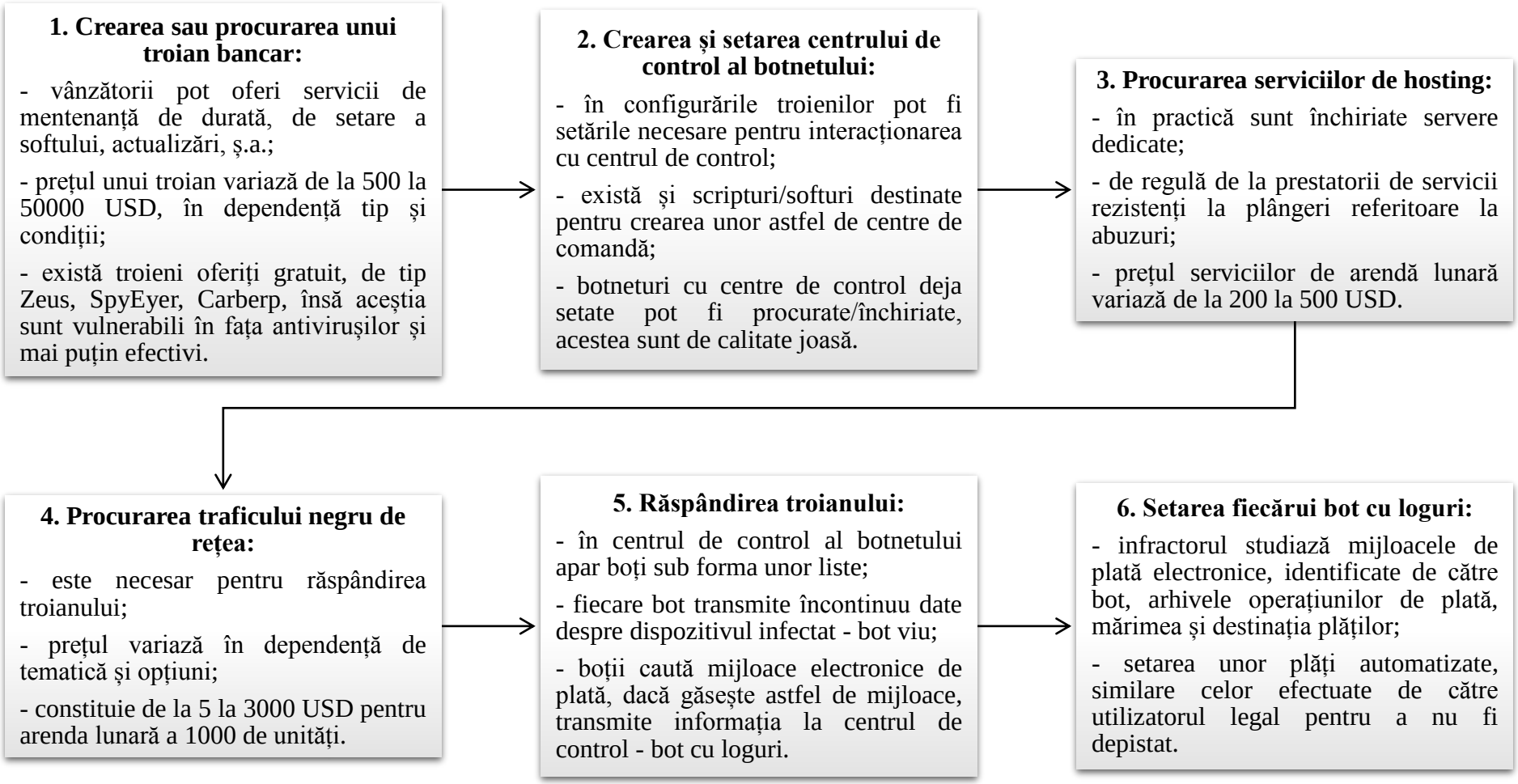
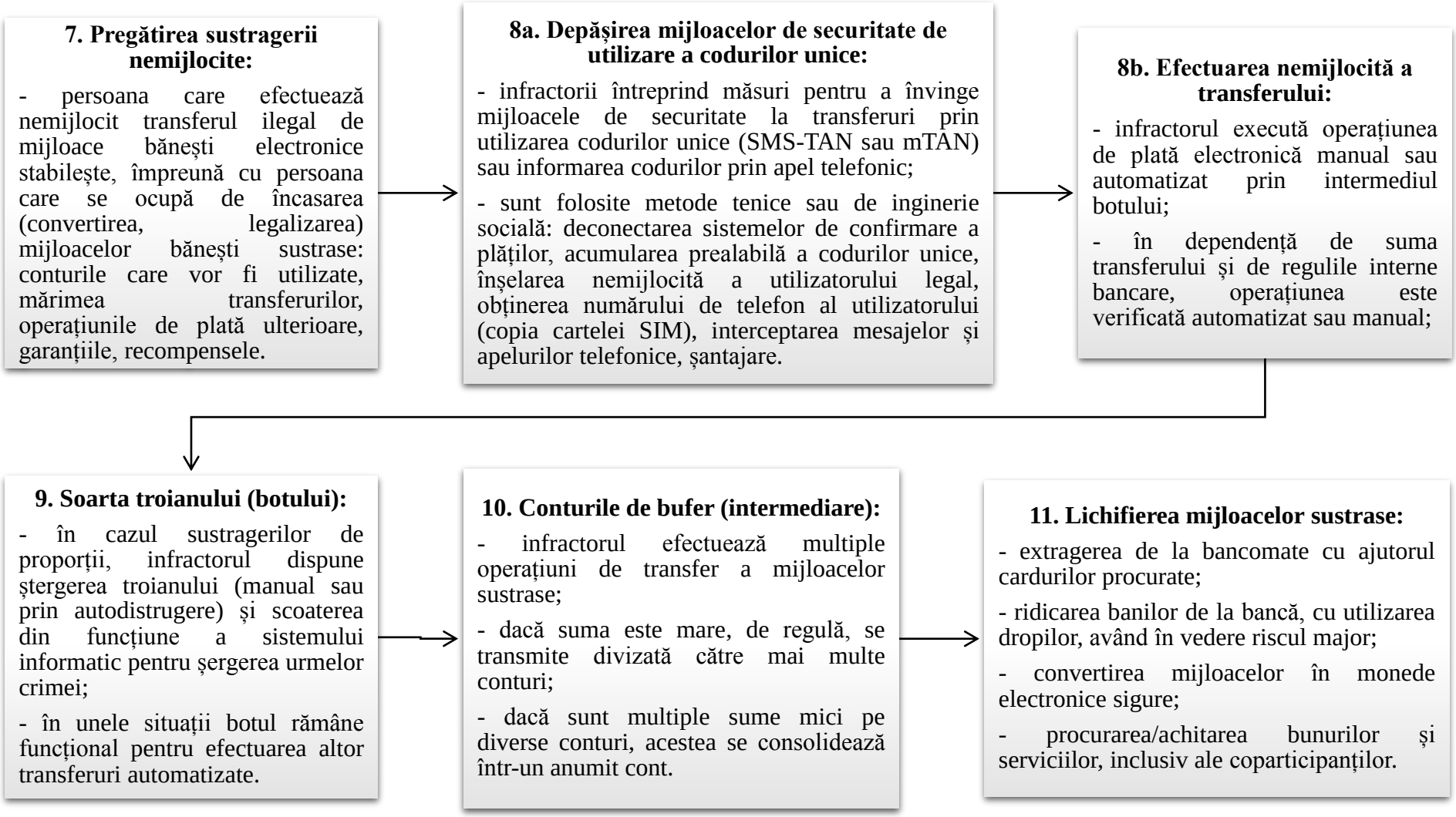


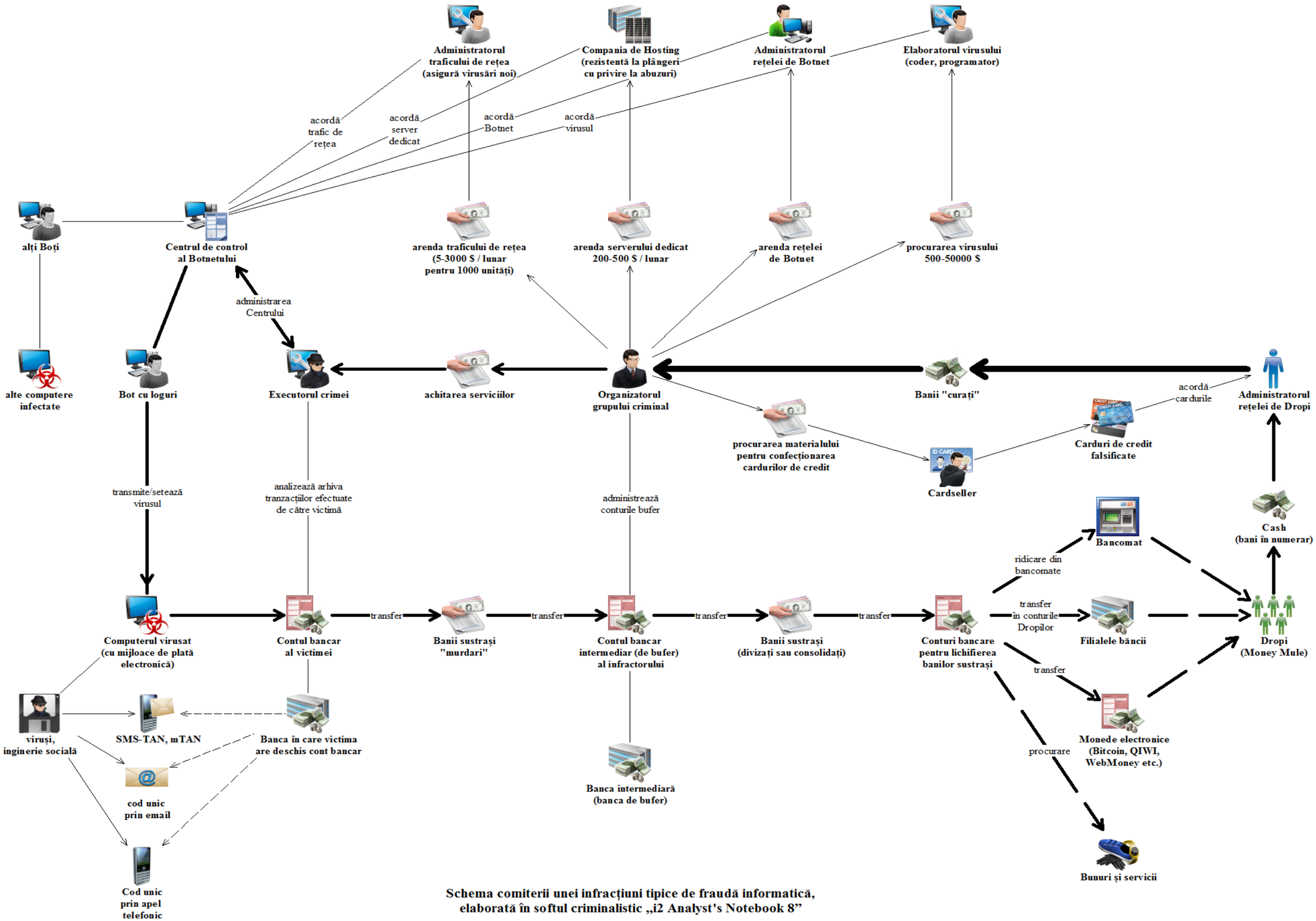
Fig.A1.7. Categoriile pedepselor aplicate de către instanțele de fond din RM în cazurile de criminalitate informatică

ANEXA 2

Model tipic de săvârșire a unei fraude informatice cu utilizarea produselor program




7. Pregătirea sustragerii nemijlocite:
- persoana care efectuează nemijlocit transferul ilegal de mijloace bănești electronice stabilește, împreună cu persoana care se ocupă de încasarea (convertirea, legalizarea) mijloacelor bănești sustrase: conturile care vor fi utilizate, mărimea transferurilor, operațiunile de plată ulterioare, garanțiile, recompensele.
8a. Depășirea mijloacelor de securitate de utilizare a codurilor unice:
- infractorii întreprind măsuri pentru a învinge mijloacele de securitate la transferuri prin utilizarea codurilor unice (SMS-TAN sau mTAN) sau informarea codurilor prin apel telefonic;
- sunt folosite metode tenice sau de inginerie socială: deconectarea sistemelor de confirmare a plăților, acumularea prealabilă a codurilor unice, înșelarea nemijlocită a utilizatorului legal, obținerea numărului de telefon al utilizatorului (copia cartelei SIM), interceptarea mesajelor și apelurilor telefonice, șantajare.
8b. Efectuarea nemijlocită a transferului:
- infractorul execută operațiunea de plată electronică manual sau automatizat prin intermediul botului;
- în dependență de suma transferului și de regulile interne bancare, operațiunea este verificată automatizat sau manual;
9. Soarta troianului (botului):
- în cazul sustragerilor de proporții, infractorul dispune ștergerea troianului (manual sau prin autodistrugere) și scoaterea din funcțiune a sistemului informatic pentru șergerea urmelor crimei;
- în unele situații botul rămâne funcțional pentru efectuarea altor transferuri automatizate.
10. Conturile de bufer (intermediare):
- infractorul efectuează multiple operațiuni de transfer a mijloacelor sustrase;
- dacă suma este mare, de regulă, se transmite divizată către mai multe conturi;
- dacă sunt multiple sume mici pe diverse conturi, acestea se consolidează într-un anumit cont.
11. Lichifierea mijloacelor sustrase:
- extragerea de la bancomate cu ajutorul cardurilor procurate;
- ridicarea banilor de la bancă, cu utilizarea dropilor, având în vedere riscul major;
- convertirea mijloacelor în monede electronice sigure;
- procurarea/achitarea bunurilor și serviciilor, inclusiv ale coparticipanților.



Schema comiterii unei infracțiuni tipice de fraudă informatică, elaborată în softul criminalistic „i2 Analyst's Notebook 8”

ANEXA 3

Clasificarea infractorilor informatici în cazul fraudelor informatice

ANEXA 4

Exemplu de extras din jurnale stocate pe un server ce găzduiește un site destinat pentru comercializarea biletelor pentru avion

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Q	R
1	id	ip	codefro	codeto	datefrom	dateto	oneway	srccount	adtcount	ythcount	chdcount	infcount	prefclass	aver	date	browser	isloadtime
2	1483760	89.	J	PAR	2014-05-18	2014-05-20	N	0	1	0	0	0	Y	ro	2014-05-13 16:53:55	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/53	2014-05-13 16:54:12
3	1483761	89.	0	PAR	2014-05-17	2014-05-20	N	0	1	0	0	0	Y	ro	2014-05-13 16:54:26	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/53	2014-05-13 16:54:54
4	1483764	89.	0	KIV	PAR	2014-05-16	2014-05-20	N	0	1	0	0	0	Y	ro	2014-05-13 16:55:02	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/53	2014-05-13 16:55:24
5	1483766	89.	0	KIV	PAR	2014-05-15	2014-05-20	N	0	1	0	0	0	Y	ro	2014-05-13 16:55:33	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/53	2014-05-13 16:55:58
6	1483768	89.	0	KIV	PAR	2014-05-20	2014-05-25	N	0	1	0	0	0	Y	ro	2014-05-13 16:56:16	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/53	2014-05-13 16:56:37
7	1483772	89.	0	KIV	PAR	2014-05-21	2014-05-25	N	0	1	0	0	0	Y	ro	2014-05-13 16:56:58	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/53	2014-05-13 16:57:19
8	1483782	89.	0	BUH	PAR	2014-05-21	2014-05-25	N	0	1	0	0	0	Y	ro	2014-05-13 16:59:18	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/53	2014-05-13 16:59:43
9	1483784	89.	0	BUH	PAR	2014-05-22	2014-05-25	N	0	1	0	0	0	Y	ro	2014-05-13 17:00:04	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/53	2014-05-13 17:00:28
10	1493894	89.	0	KIV	PAR	2014-05-18	2014-05-23	Y	0	1	0	0	0	Y	ro	2014-05-16 13:39:53	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/53	2014-05-16 13:40:13
11	1559543	89.	0	KIV	BCN	2014-06-04	2014-06-10	Y	0	1	0	0	0	Y	ro	2014-06-03 18:09:39	Mozilla/5.0 (Linux; U; en-us; KFSOWI Build/JDQ39)	2014-06-03 18:09:53
12	1559546	89.	0	KIV	BCN	2014-06-05	2014-06-10	Y	0	1	0	0	0	Y	ro	2014-06-03 18:10:17	Mozilla/5.0 (Linux; U; en-us; KFSOWI Build/JDQ39)	2014-06-03 18:10:27
13	1559548	89.	0	KIV	BCN	2014-06-06	2014-06-13	Y	0	1	0	0	0	Y	ro	2014-06-03 18:10:49	Mozilla/5.0 (Linux; U; en-us; KFSOWI Build/JDQ39)	2014-06-03 18:11:07
14	1559581	89.	0	PAR	CMB	2014-06-04	2014-06-10	Y	0	1	0	0	0	Y	ro	2014-06-03 18:20:29	Mozilla/5.0 (Linux; U; en-us; KFSOWI Build/JDQ39)	2014-06-03 18:20:41
15	1559622	89.	0	PAR	CMB	2014-06-04	2014-06-10	Y	0	1	0	0	0	C	ro	2014-06-03 18:39:00	Mozilla/5.0 (Linux; U; en-us; KFSOWI Build/JDQ39)	2014-06-03 18:39:26
16	1559623	89.	0	PAR	CMB	2014-06-05	2014-06-10	Y	0	1	0	0	0	C	ro	2014-06-03 18:40:02	Mozilla/5.0 (Linux; U; en-us; KFSOWI Build/JDQ39)	2014-06-03 18:40:12
17	1559692	89.	0	PAR	JTR	2014-06-04	2014-06-10	Y	0	1	0	0	0	Y	ro	2014-06-03 18:57:04	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/53	2014-06-03 18:57:19
18	1560076	89.	0	KIV	BCN	2014-06-10	2014-06-10	N	0	1	0	0	0	Y	ro	2014-06-03 20:50:33	Mozilla/5.0 (Linux; U; en-us; KFSOWI Build/JDQ39)	2014-06-03 20:50:45
19	1560080	89.	0	KIV	BCN	2014-06-09	2014-06-10	N	0	1	0	0	0	Y	ro	2014-06-03 20:51:06	Mozilla/5.0 (Linux; U; en-us; KFSOWI Build/JDQ39)	\N
20	1560089	89.	1	KIV	BCN	2014-06-10	2014-06-10	Y	0	1	0	0	0	Y	ro	2014-06-03 20:52:53	Mozilla/5.0 (Linux; U; en-us; KFSOWI Build/JDQ39)	2014-06-03 20:53:02

Fig.A4.1. Exemplu de loguri de pe un server

ANEXA 5

Modele de date solicitate la procurarea online a bunurilor și serviciilor

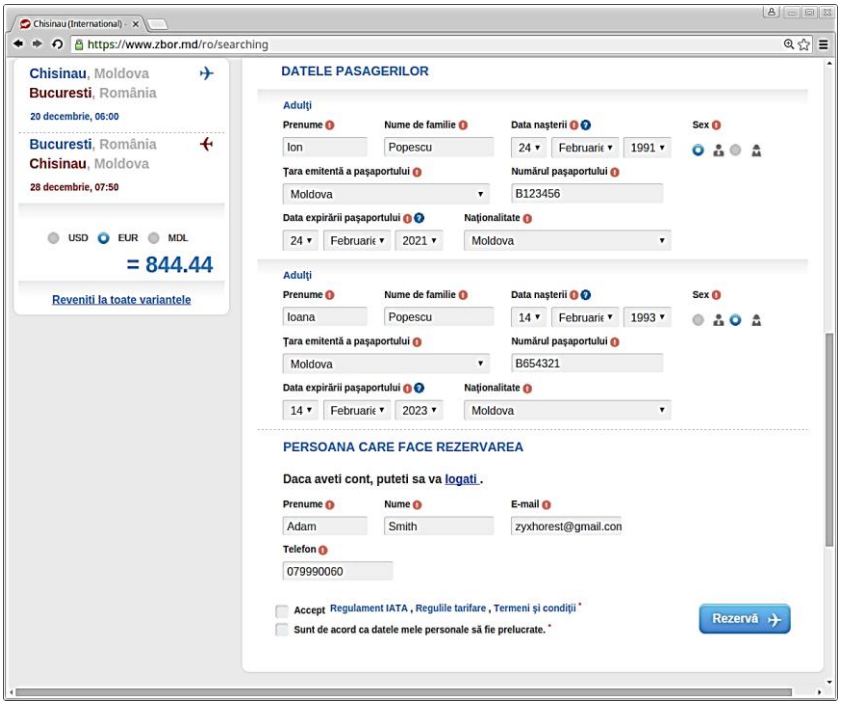


Fig.A5.1. Exemplu de formular electronic la procurarea online a serviciilor de transport aerian

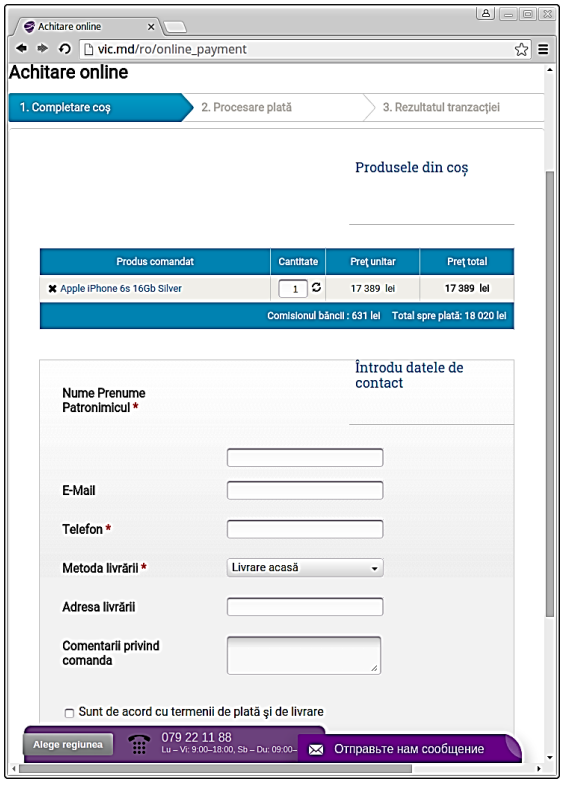


Fig.A5.2. Exemplu de formular electronic la procurarea online a bunurilor

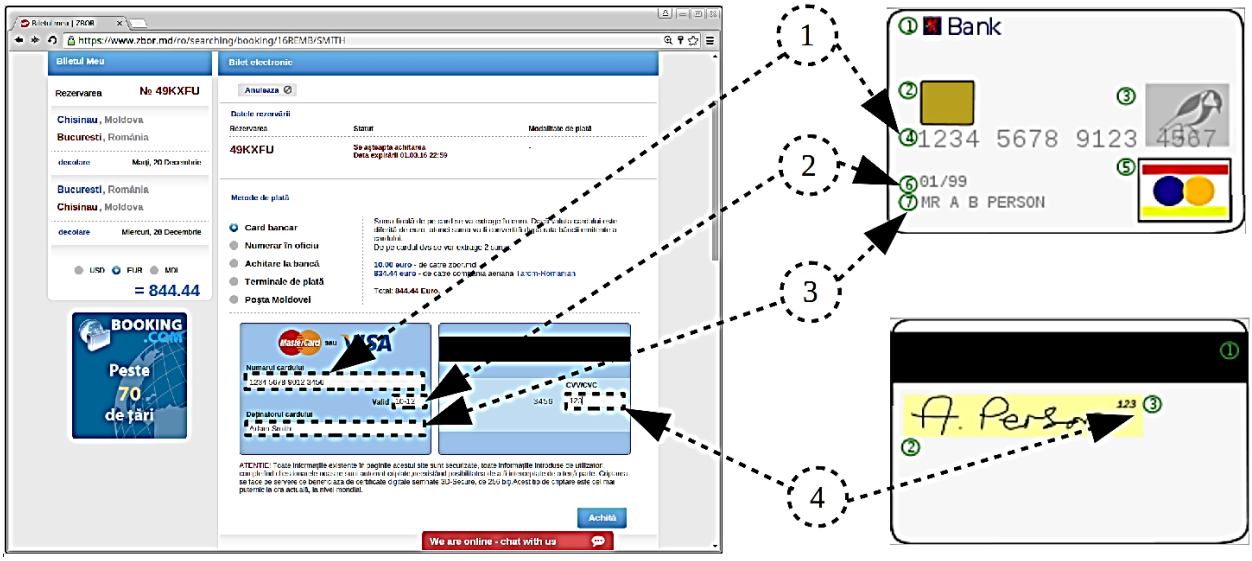
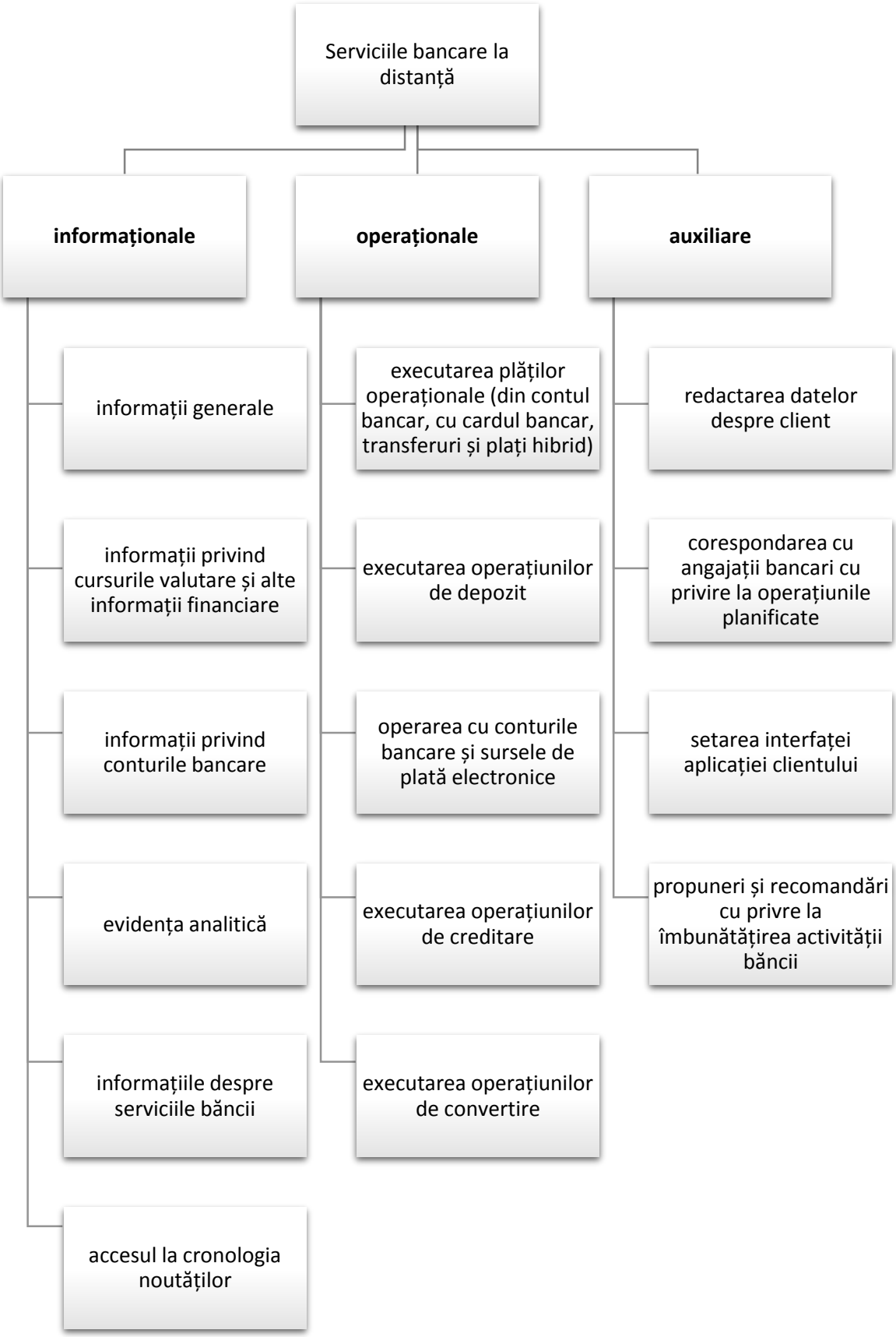


Fig.A5.3. Exemplu de formular electronic pentru efectuarea unei plăți online

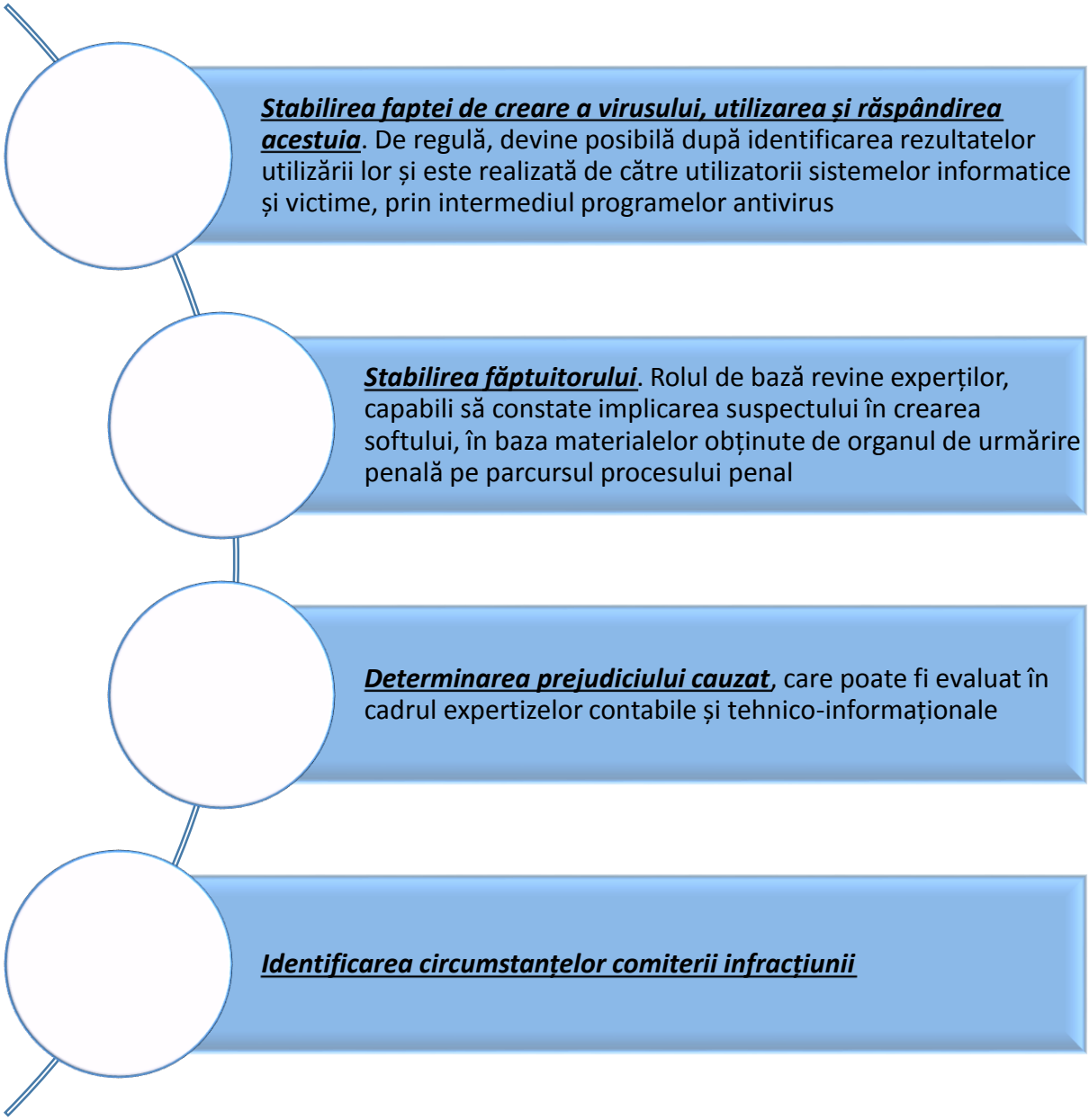
ANEXA 6

Serviciile la distanță prestate de către instituțiile financiar-bancare



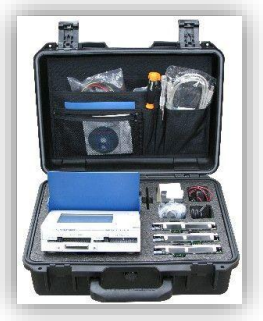
ANEXA 7

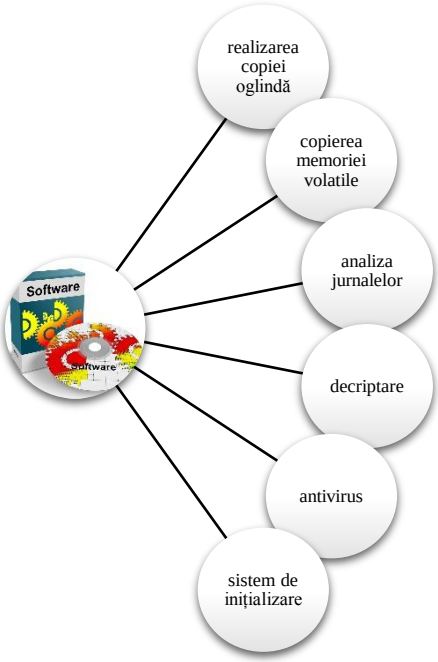
Sarcinile de bază la cercetarea unei infracțiuni informatice, săvârșite cu utilizarea virușilor

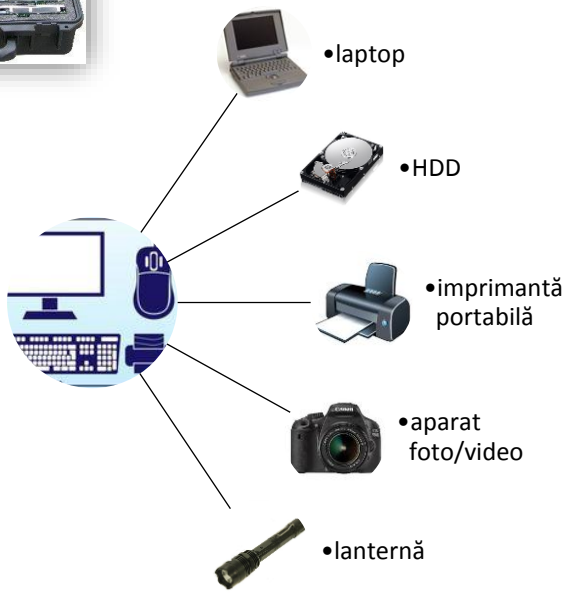


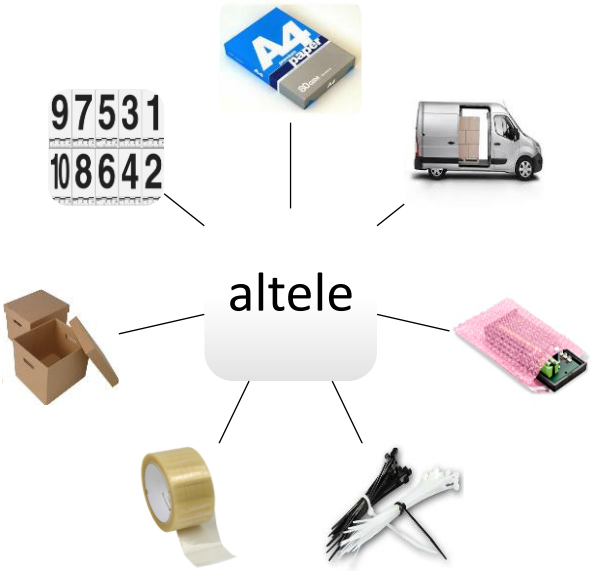
ANEXA 8

Model de trusă criminalistică, necesară specialistului criminalist la cercetarea unei infracțiuni informatice



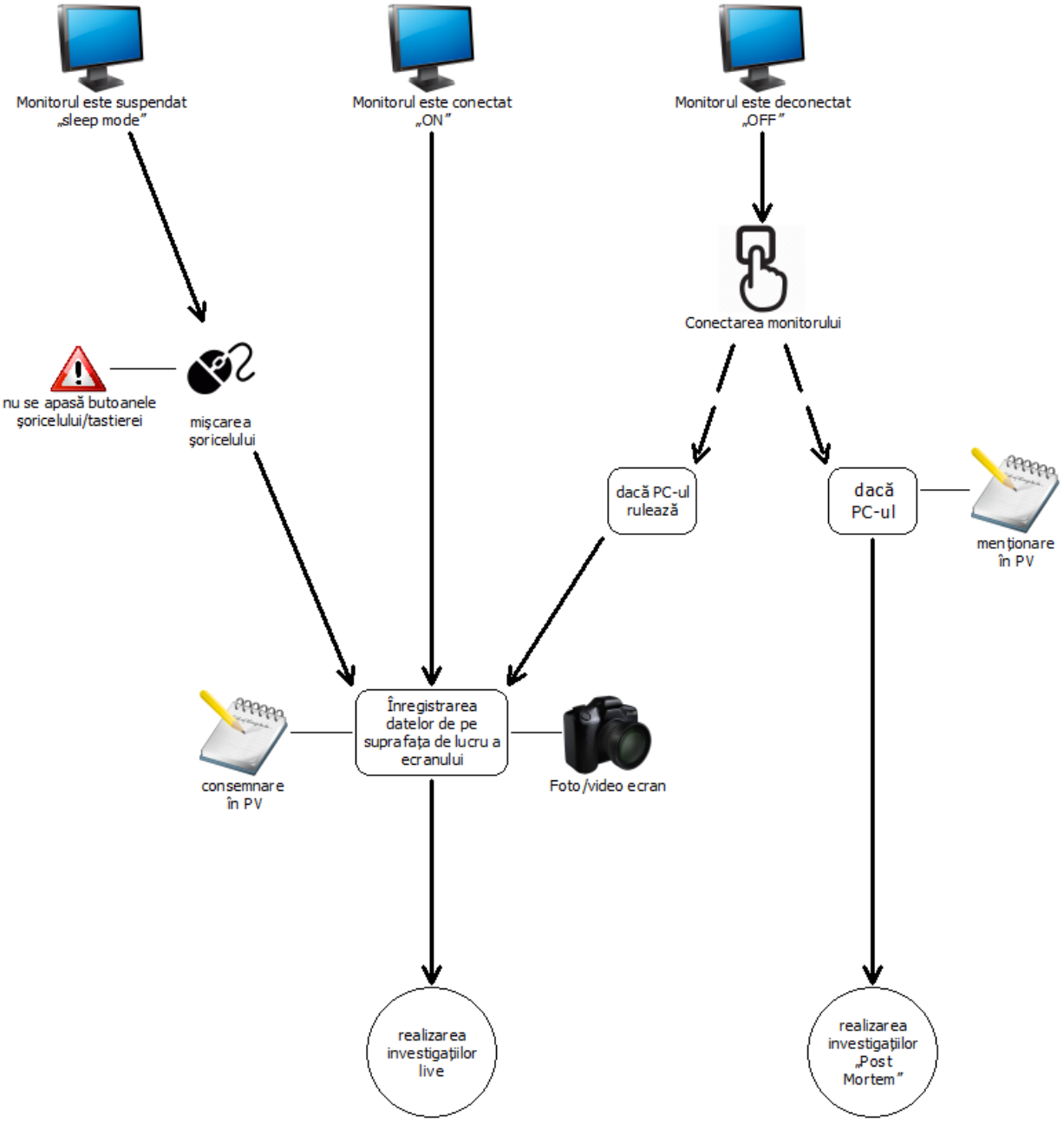






ANEXA 9

Verificarea stării monitorului



ANEXA 10

Utilitare program pentru salvarea informației computerizate temporare (memoriei volatile)

Nr. ord.	Categoria informației temporare	Utilitare program pentru salvare	
		Windows	Linux
1.	Informația privind configurația curentă a rețelei	netstat –a	netstat –a, ifconfig
2.	Programele și serviciile care utilizează conexiunile de rețea	sc queryex, netstat -ab	netstat -tunp
3.	Date privind sesiunile curente ale utilizatorilor	Psloggedon, whoami, ntlast, netusers /l	w, who -T, last
4.	Conținutul dispozitivului de memorie operativă	Dumpit, Winen, Mdd	dd, fmem
5.	Lista proceselor pornite	PsList, ListDLLs, CurrProcess, tasklist	ps –ef, lsof
6.	Fișierele deschise	Handle, PsFile, Openfiles, net file	lsof, fuser
7.	Fișiere publice în rețea	Net share, Dumpsec	showmount –e, showmount –a, smbclient –L
8.	Porturile deschise	OpenPorts, ports, netstat –an	netstat –an, lsof
9.	Parolele și cheile introduse	kldstat	lsmod, kldstat
10.	Configurația rețelei	Systeminfo, msinfo32, ipconfig /all	ifconfig –a netstat –in
11.	Timpul curent	time /T, date /T, uptime	time, date, uptime
12.	Routing-Tables, ARP caches, Kernel statistics	Route PRINT, arp –a, netstat	netstat –r –n, route, arp –a
13.	DNS Cache	Ipconfig /displaydns	rndc dumpdb (dacă este instalat)
14.	Sistemele de fișiere criptate montate	Manage-bde (Bitlocker), efsinfo (EFS)	mount -v, ls /media
15.	Sistemele de fișiere conectate temporar	Fsinfo, reg (Mounted Devices)	mount -v, ls /media
16.	Remote logging- and monitoring data	psloglist	/etc/syslog.conf Port UDP 514
17.	Mediile de stocare	reg (Mounted Devices), Net share, netstat –a	mount -v, ls /media
18.	Environment variables	cmd /c set	env, set
19.	Clipboard	Pclip	
20.	Conținutul discurilor	FTK Imager, EnCase, Tableau Imager	Dc3dd, ewfacquire, Guymager

ANEXA 11

Exemplu de obținere a informației din memoria operativă (memoria Dump) în sistemul de operare Windows 8

1. Apăsăm Click dreapta pe „Acest PC” (Figura A11.1.).

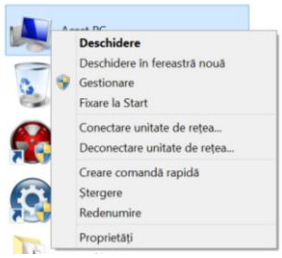


Fig.A11.1. Meniul de la elementul „Acest PC”

2. Apăsăm Click stânga la „Proprietăți” din meniu. Va apărea fereastra „Sistem”, în care vom alege „Setări complexe de sistem”. Va apărea o fereastră „Proprietăți sistem”, în care vom trece la compartimentul „Complex”, iar la „Pornire și recuperare” alegem „Setări” (Figura A11.2.).

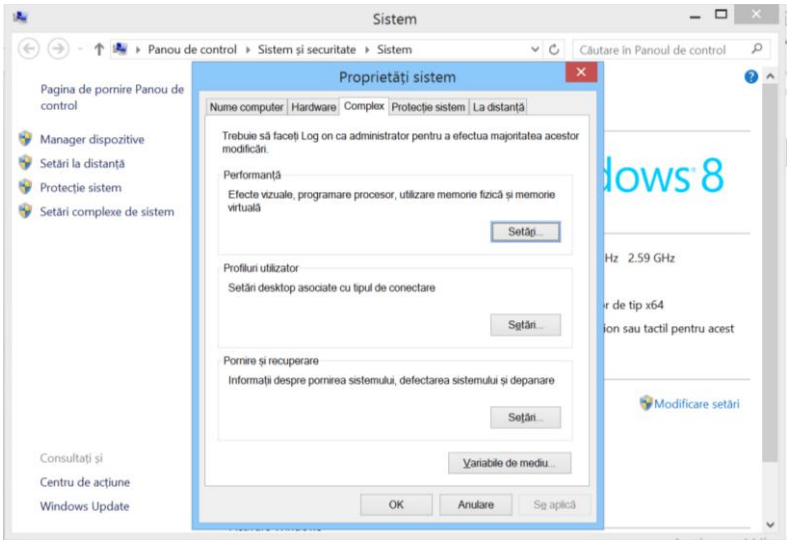


Fig.A11.2. Proprietăți sistem

3. În rubrica „Defecțiuni de sistem” debifăm la „Repornire automată”, iar la „Fișier Dump” indicăm calea unde dorim să fi creat Dump-ul (Figura A11.3.).

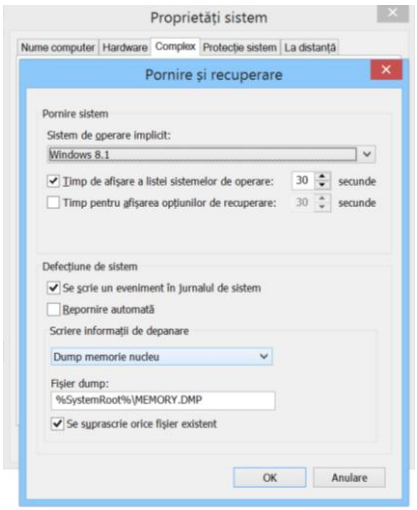


Fig.A11.3. Pornire și recuperare

4. În rubrica „Scriem informații de depanare” alegem din listă „Dump memorie nucleu” (Figura A11.4.).

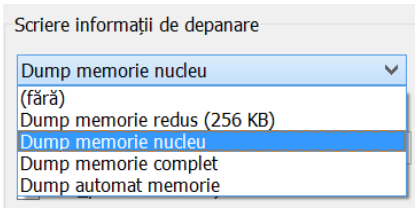


Fig.A11.4. Scriem informații de depanare

5. Apăsăm butonul „OK”. Memoria Dump va fi înscrisă în fișierul calea către care a fost aleasă mai sus.

ANEXA 12

Proprietățile fotografiilor în format electronic

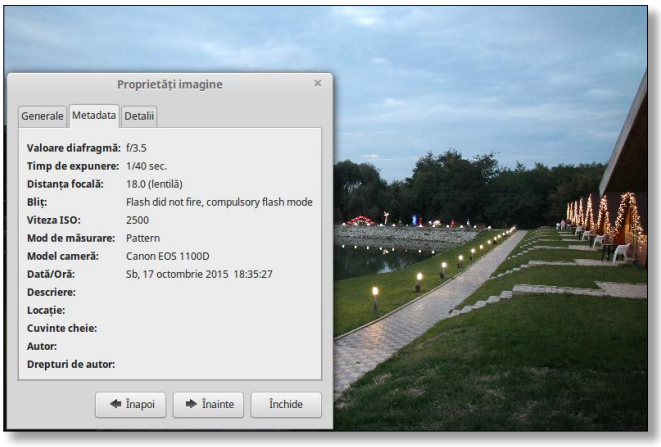


Fig.A12.1. Metadatele fotografiei realizate cu un aparat foto digital

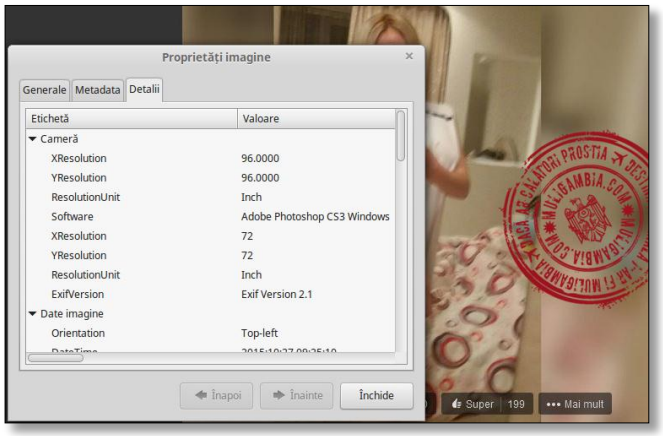


Fig.A12.2. Detaliile produsului program în care a fost prelucrată fotografia digitală

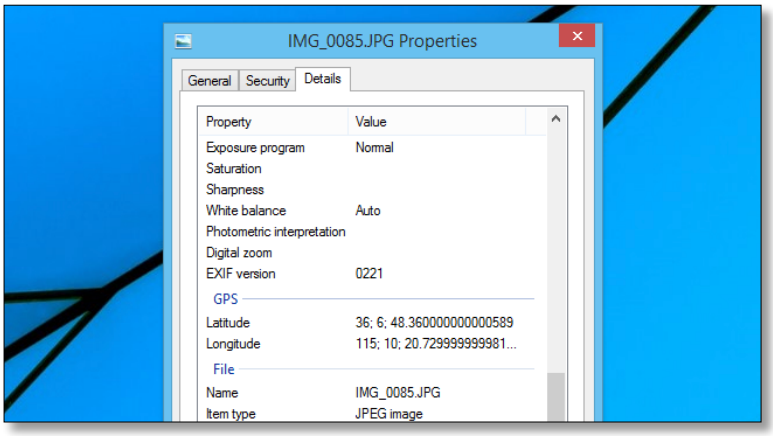


Fig.12.3. Metadatele cu privire datele GPS ale locului unde a fost realizată fotografia

ANEXA 13

Cercetarea paginilor web șterse/modificate

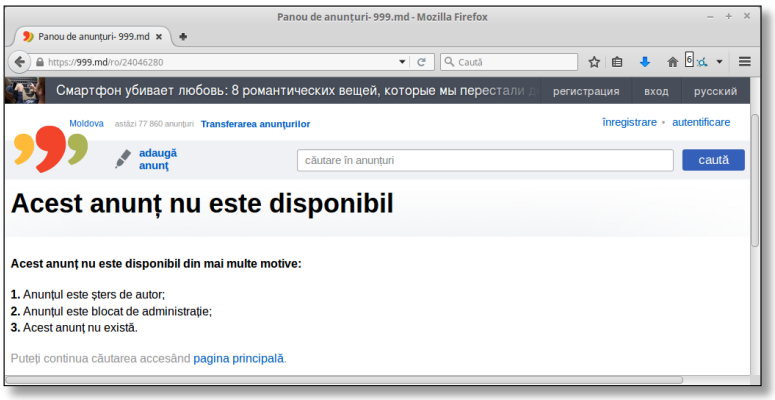


Fig.A13.1. Exemplul unei pagini web inaccesibile

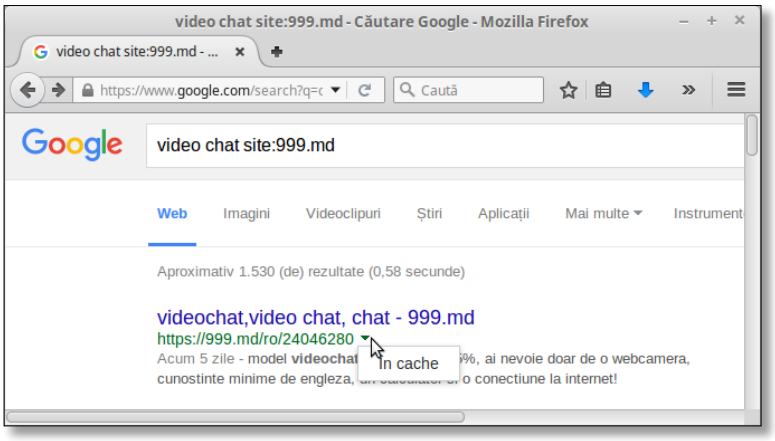


Fig.A13.2. Instrumentul „În cache” al motorului de căutare Google

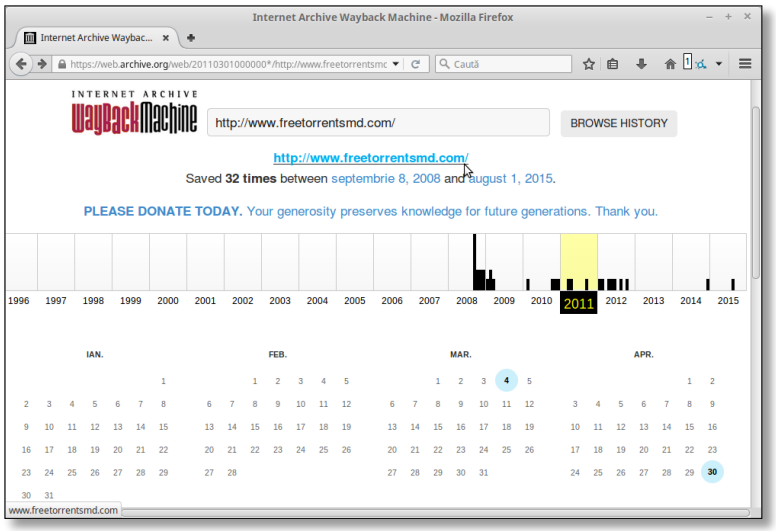


Fig.A13.3. Internet Archive Wayback Machine

ANEXA 14

Exemplu de identificare a adreselor IP implicate în descărcarea/încărcarea fișierelor torrent

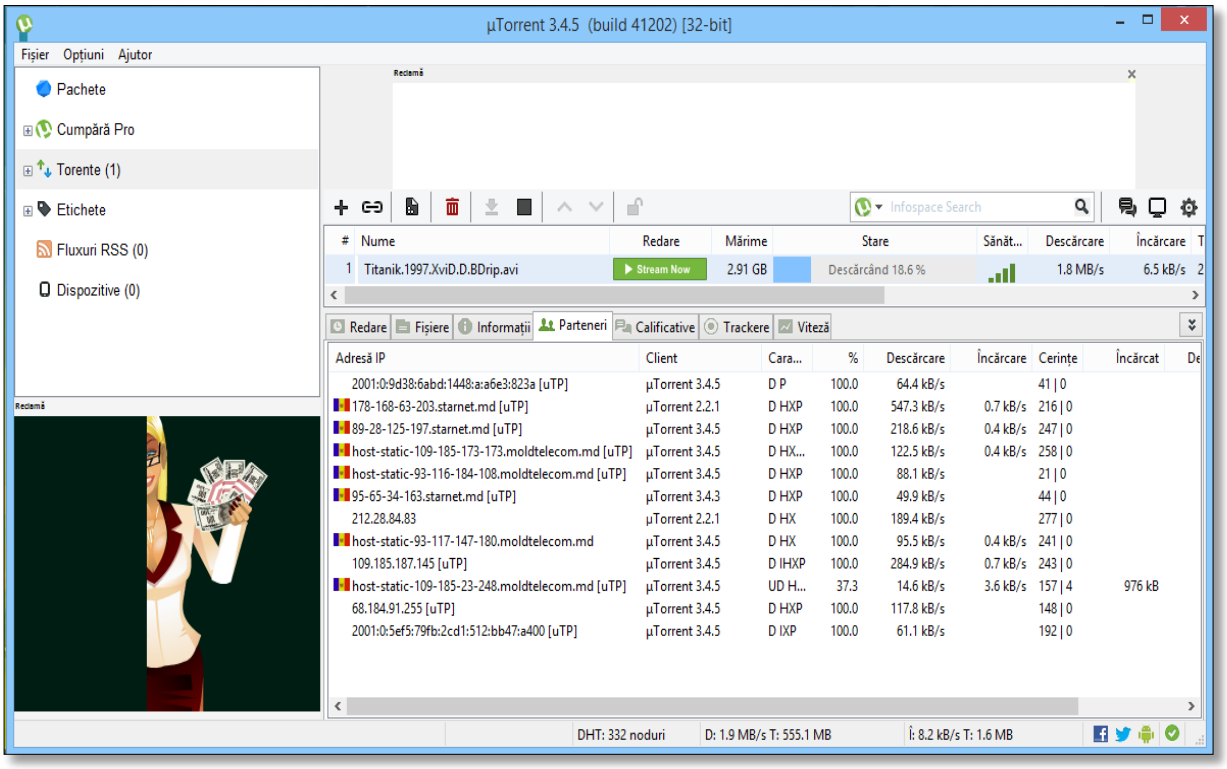


Fig.A14.1. Exemplu de informații dintr-o aplicație de tip P2P

ANEXA 15

Exemplu de informații obținute prin investigarea denumirii de email cu utilizarea rețelei de socializare „Facebook” (în trei pași)

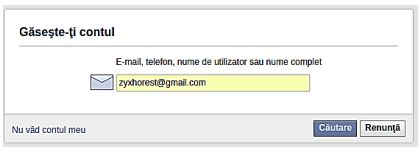
I-ul pas	Al II-lea pas	Al III-lea pas
- să acceseze pagina de start https://www.facebook.com/ - să facă click pe opțiunea „***Ai uitat parola?***”	- în fereastra apărută să introducă denumirea e-mailului, numărul de telefon sau numele de utilizator - să facă click pe butonul „***Căutare***”	- obținem denumirea contului din rețeaua de socializare „Facebook”, denumirea parțială a altor e-mailuri înregistrate, precum și datele parțiale cu privire la numere de telefon
		

Fig.A15.1. Extrase de pe site-ul www.facebook.com

ANEXA 16

Stabilirea informațiilor despre site-urile cu domeniile .md

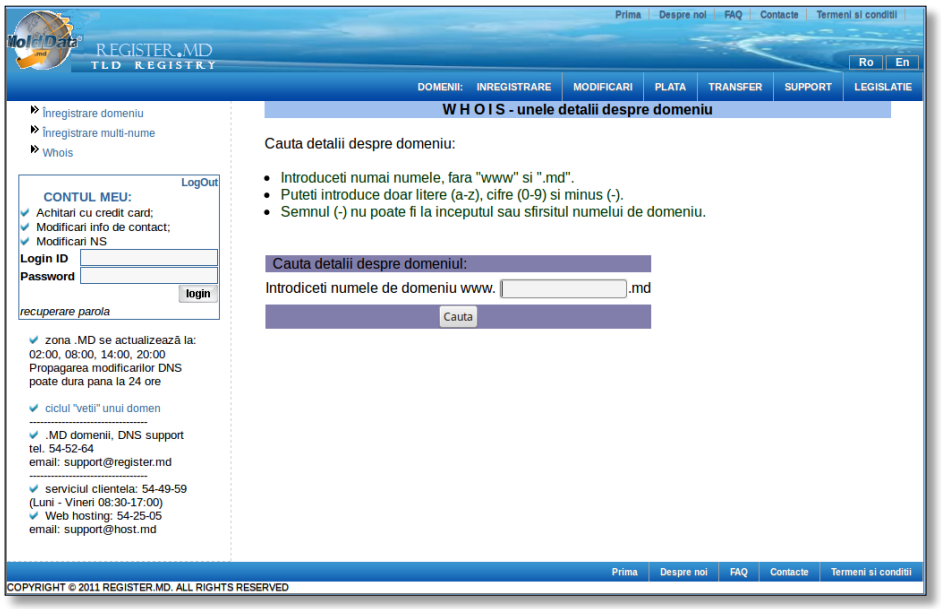


Fig.A16.1. Pagina web http://nic.md/RO/wh1.php

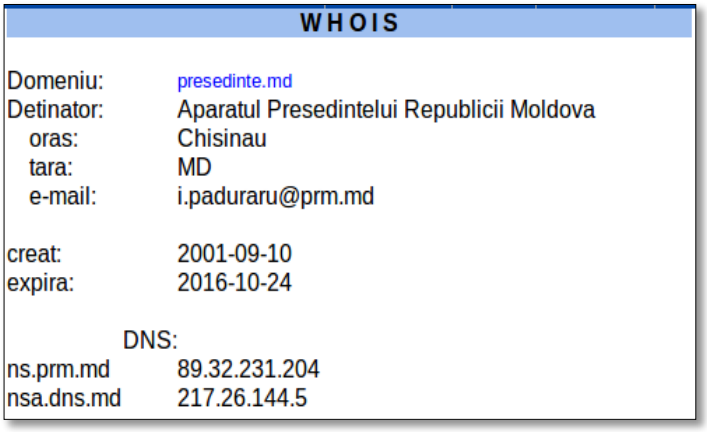


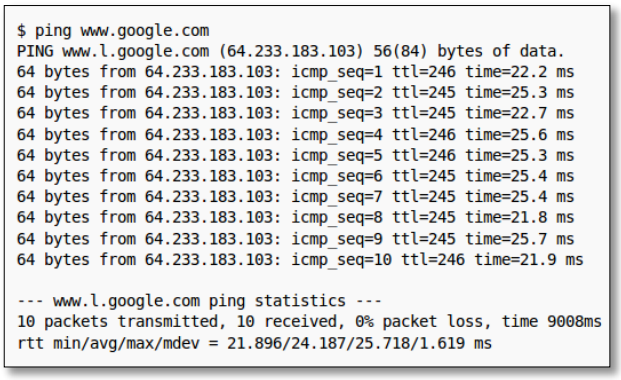
Fig.A16.2. Exemplu de detalii oferite de site-ul www.nic.md despre domeniile înregistrate .md

Astfel, pe pagina web http://nic.md/RO/wh1.php putem stabili informații cu privire la:

- deținătorul numelui de domeniu (persoana fizică/juridică, entitatea după care a fost înregistrat numele de domeniu) – numele și prenumele/denumirea;
- localitatea și țara de origine;
- e-mailul de contact;
- dată creării (înregistrării) și expirării numelui de domeniu;
- datele DNS.

ANEXA 17

Comanda PING în sistemul de operare Linux



```
$ ping www.google.com
PING www.l.google.com (64.233.183.103) 56(84) bytes of data.
64 bytes from 64.233.183.103: icmp_seq=1 ttl=246 time=22.2 ms
64 bytes from 64.233.183.103: icmp_seq=2 ttl=245 time=25.3 ms
64 bytes from 64.233.183.103: icmp_seq=3 ttl=245 time=22.7 ms
64 bytes from 64.233.183.103: icmp_seq=4 ttl=246 time=25.6 ms
64 bytes from 64.233.183.103: icmp_seq=5 ttl=246 time=25.3 ms
64 bytes from 64.233.183.103: icmp_seq=6 ttl=245 time=25.4 ms
64 bytes from 64.233.183.103: icmp_seq=7 ttl=245 time=25.4 ms
64 bytes from 64.233.183.103: icmp_seq=8 ttl=245 time=21.8 ms
64 bytes from 64.233.183.103: icmp_seq=9 ttl=245 time=25.7 ms
64 bytes from 64.233.183.103: icmp_seq=10 ttl=246 time=21.9 ms

--- www.l.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9008ms
rtt min/avg/max/mdev = 21.896/24.187/25.718/1.619 ms
```

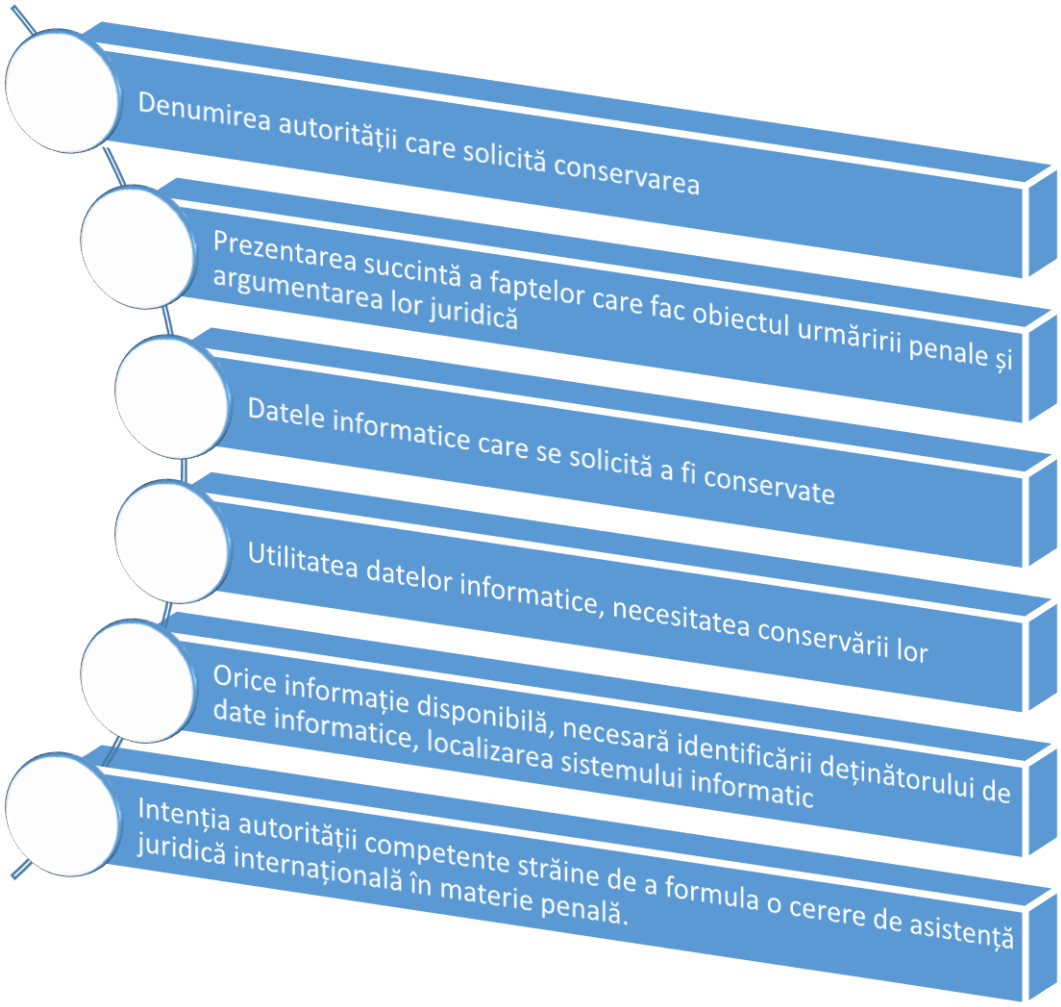
Fig.A17.1. Rezultatul comenzii ping către www.google.com dintr-un sistem de operare Linux

Listarea arată că www.google.com are o înregistrare CNAME DNS pentru www.l.google.com care este rezolvată sub forma adresei 64.233.183.103. Listarea arată mai apoi rezultatele a trimiterii de 10 pinguri către 64.233.183.103 cu răspunsuri sumarizate la final.

- timpul minim de ping a fost de 21.896 milisecunde
- timpul mediu de ping a fost de 24.187 milisecunde
- timpul maxim de ping a fost de 25.718 milisecunde.

ANEXA 18

Cererea de conservare imediată a datelor informatice



ANEXA 19

Întrebările înaintate la dispunerea expertizei tehnice a dispozitivelor informatice	
1.	tipul, marca, modelul, seria, numărul și proprietățile tehnice;
2.	caracteristicile și sarcinile funcționale;
3.	starea și configurația inițială;
4.	stare de fapt și configurația curentă;
5.	funcționalitatea (funcțional sau nefuncțional);
6.	abaterile de la parametrii tipici (normali), defectele fizice și cauzele producerii acestora;
7.	măsurile de protecție și posibilitățile de încălcare a acestora;
8.	cantitatea, marca, modelul, tipul, seria purtătorilor de informație instalați;
9.	accesibilitatea pentru citire a purtătorului de informație;
10.	structura și rezultatele utilizării dispozitivului;
11.	legătura de cauzalitate dintre folosirea dispozitivului și consecințele survenite;
12.	condițiile și locul în care a fost folosit;
13.	cronologia restabilită a consecutivității folosirii dispozitivului;
14.	produsele program instalate;
15.	existența produselor program destinate pentru conectare la distanță;
16.	setările conexiunii la internet, ISP-ul, loginul și parola;
17.	produsul program utilizat pentru conectare la internet.

Întrebările înaintate la dispunerea expertizei tehnice asupra produselor program	
1.	caracteristicile generale: denumirea, tipul, versiunea, felul de prezentare;
2.	destinația, sarcinile funcționale, setările și componentele produsului program;
3.	sistemele de operare cu care este compatibil;
4.	timpul creării, instalării, configurării, modificării, ștergerii;
5.	fișierele pe care le conține, parametrii lor (volumul, data creării, alte proprietăți), modul de introducere și extragere a informației, existența sau lipsa devierilor de la parametrii tipici;
6.	diagnosticul algoritmului produsului program, instrumentele utilizate la elaborarea acestuia, precum și platformele compatibile;
7.	particularitățile/rechizitele care permit identificarea autorului (elaboratorului);

8.	instrumentele utilizate la elaborare (limbajul de programare, bibliotecile standarde);
9.	starea inițială;
10.	starea de fapt curentă, modificările operate (atunci când există softul pentru instalare);
11.	scopul și condițiile modificării proprietăților și stării produsului program (intenționat, configurarea pentru anumite dispozitive, etc.), stabilirea modului de realizare a modificărilor în program (de exemplu: cu utilizarea unui virus, erorilor program);
12.	măsurile de protecție împotriva accesului nesancționat;
13.	structura mecanismului evenimentelor în rezultatul activității produsului program;
14.	legătura de cauzalitate dintre acțiunile utilizatorilor softului și consecințe;
15.	existența softurilor destinate copierii, blocării, modificării, distrugerii datelor informatice, virușilor, fiind necesară verificarea rulării acestuia la un moment dat în timp și eventuala corelare cu datele de creare și accesare de la documentele și fișierele incriminate precum și cu alte urme ale activității acestuia [294];
16.	existența produselor program pentru funcționalitatea dispozitivelor periferice.

Întrebările înaintate la dispunerea expertizei tehnice informaționale	
1.	caracteristicile amplasării (repartizării) logice a datelor informatice;
2.	proprietățile, caracteristicile, atributele și parametrii datelor informatice (dimensiunea, timpul creării, modificării, copierii, ștergerii, locația imaginii etc.);
3.	categoria informației (deschis, închis, șters, arhivat);
4.	tipul datelor informatice (text, grafic, bază de date, tabel electronic, multimedia etc.);
5.	accesibilitatea la datele informatice (liber, limitat ș.a.);
6.	proprietățile și caracteristicile mijloacelor de protecție și căile de violare a acestora;
7.	conținutul datelor protejate;
8.	necorespunderi ale prezentării tipice a datelor informatice (încălcarea integrității, necorespunderea formatului ș.a.);
9.	existența datelor despre faptele X și împrejurările Y;
10.	date despre proprietar (utilizator) al sistemului informatic (login, parolă, acces ș.a.);
11.	prezența datelor despre documentele (mostrele) prezentate, starea (întreg, fragmentar);
12.	starea inițială a datelor informatice înainte de ștergerea sau modificarea lor;
13.	modul și împrejurările de executare a operațiunilor de modificare, copiere, ștergere a

	datelor informatice;
14.	verificarea CRC și HASH codurilor
15.	adresele electronice către au fost expediate sau de la care au fost recepționate mesaje;
16.	conținutul corespondenței;
17.	urmele accesului neautorizat la informația din memoria calculatoarelor;
18.	posibilitatea restabilirii fișierelor pentru perioada X;
19.	site-urile accesate de pe sistemul informatic în perioada X;
20.	lista contactelor și conținutul mesajelor din aplicațiile de schimb rapid de mesaje;
21.	data rescrierii informației pe banda magnetică a cardului;
22.	informațiile inscripționate pe banda magnetică a cardului la moment, precum și cele anterioare, precum și autenticitatea acestora;
23.	modalitatea și dispozitivele utilizate la inscripționarea datelor pe banda magnetică a cardului;
24.	corespunderea cifrelor inscripționate ograf pe card cu codul PIN al cardului.

Întrebările înaintate la dispunerea expertizei tehnice asupra rețelelor informatice	
1.	proprietățile și caracteristicile mijloacelor tehnice și produselor program ale rețelei;
2.	locul, rolul și destinația funcțională a componentelor rețelei;
3.	arhitectura, configurația și componentele rețelei, accesul la datele informatice;
4.	apartenența rețelei unei anumite categorii în baza caracteristicilor acesteia;
5.	apartenența la un server sau aplicație client;
6.	starea de fapt și funcționalitatea rețelei, starea registrelor sistemului, componentei de dirijare a accesului. Stabilirea succesiunii de evenimente ce au avut loc în cadrul sistemului informatic se efectuează, de regulă, prin coroborarea înregistrărilor din jurnalele sistemului de operare (computer logs) privitoare la activitățile programelor informatice instalate, dacă aceste jurnale există, cu datele de creare, accesare, deschidere a documentelor identificate în sistem, sporind gradul de certitudine cu privire la stabilirea succesiunii de evenimente în situația în care sunt identificate astfel de jurnale de activitate a unui anumit program din sistem [252, p. 169];
7.	starea inițială a rețelei, atât în ansamblu, cât și a fiecărei componente în parte, locul procurării, concretizarea modificărilor operate (spre exemplu, instalarea unor componente suplimentare);

8.	cauzele modificării rețelei informatice (cum ar fi: modificarea nivelului de dirijare a accesului în rețea);
9.	legătura cauzală dintre utilizarea anumitor mijloace tehnice ale rețelei informatice și rezultatele aplicării lor.

ANEXA 20

Elementele obligatorii ale unor ordonanțe de dispunere a unor măsuri speciale de investigații

Reținerea, cercetarea, predarea, percheziționarea, ridicarea trimiterilor poștale

- Elementele prevăzute la art. 255 din CPP
- Motivele dispunerii reținerii, cercetării, predării, percheziționării sau ridicării trimiterilor poștale
- Denumirea instituției poștale asupra căreia se pune obligația de a reține trimiterile poștale
- Numele și prenumele persoanei sau persoanelor ale căror trimiteri poștale trebuie să fie reținute, adresa exactă a acestor persoane
- Genul de trimiteri poștale care se rețin, se cercetează, se predau, se percheziționează sau se ridică
- Durata măsurii.

Identificarea abonatului unui sistem de comunicații electronice

- Elementele prevăzute la art.255 din CPP
- Datele de identificare ale furnizorului de servicii care dispune de informațiile respective sau le ține la control
- Datele de identificare ale abonatului, proprietarului sau utilizatorului, dacă sunt cunoscute
- Mențiunea cu privire la obligația persoanei sau a furnizorului de servicii de a comunica imediat, în condiții de confidențialitate, informațiile solicitate
- Motivarea îndeplinirii condițiilor de dispunere a măsurii speciale de investigații

ANEXA 21

Elementele unui e-mail

Corpul mesajului	**Antetul mesajului**	**Anexa** (opțional)
• mesajul efectiv transmis	• informația privind numele și adresa expeditorului/ destinatarului, • data de expediere, • precum și, după caz, subiectul mesajului, • numele serverelor intermediare, • data și ora sosirii și expedierii din server	• fișiere care conțin poze, documente, sunete și imagini

ANEXA 22

Pașii care urmează a fi parcurși pentru citirea antetului unui e-mail

în dependență de programul utilizat pentru poșta electronic

A. Clienții de webmail

Gmail

- logare în Gmail
- deschiderea mesajului al cărui antet urmează a fi vizualizat
- în partea de sus a panoului de mesaje, clic pe săgeata de lângă **Reply**
- selectare **Show Original**

AOL

- logare în AOL
- deschiderea mesajului al cărui antet urmează a fi vizualizat
- selectare **View Message Source** de la rubrica **Action** din meniu

HOTMAIL

- logare în Hotmail
- selectare **Inbox** din meniu
- clic-dreapta pe mesajul al cărui antet urmează a fi vizualizat și selectarea **View Message Source**

YAHOO! Mail

- logare în Yahoo! Mail
- selectarea mesajului al cărui antet urmează a fi vizualizat
- clic pe **Actions** și selectarea **View Full Header**

B. Clienții de e-mail

Apple Mail

- deschiderea Apple Mail
- clic pe mesajul al cărui antet urmează a fi vizualizat
- selectare **View** din meniu, apoi **Message** și **All Headers**

Mozilla

- deschidere Mozilla
- clic pe mesajul al cărui antet urmează a fi vizualizat
- selectare **View** din meniu şi selectarea **Message Source**

Outlook

- deschidere Outlook
- deschiderea mesajului al cărui antet urmează a fi vizualizat
- clic pe **File**, apoi pe **Properties** și selectarea **Internet headers**

Outlook Express

- deschidere Outlook Express
- clic-dreapta pe mesajul al cărui antet urmează a fi vizualizat
- selectarea **Properties** și deschiderea **Details**

ANEXA 23

Formular al ordonanței de dispunere a identificării abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic

ORDONANȚĂ

mun. Chișinău [*data întocmirii*]

Procuror [*procuratura teritorială, specializată sau subdiviziunea Procuraturii Generale în care activează, numele și prenumele procurorului care întocmește ordonanța*], examinând materialele cauzei penale nr. [*numărul cauzei penale*],

CONSTAT:

În fapt, urmărirea penală în prezenta cauză a fost pornită la [*data începerii urmăririi penale*], în temeiul prevederilor art. [*norma materială în baza căreia a fost pornită urmărirea penală*] din Codul penal, de către [*organul de urmărire penală care a dispus pornirea urmăririi penale*].

În cadrul urmăririi penale s-a stabilit [*fabula succintă a cazului cercetat, modul de obținere a informației care urmează a fi verificată sau stabilită. De asemenea, trebuie indicate datele și sursele potrivit cărora informația necesară se află la furnizorul de servicii vizat (spre exemplu: datele de contact indicate pe site-ul furnizorului de servicii; datele obținute prin intermediul site-ului registratorului internațional, în dependență de regiunea unde ISP prestează serviciile internet, cum ar fi www.ripe.net; din bazele de date publice, cum ar fi www.portare.md, precum și din alte surse)*].

În vederea stabilirii existenței sau inexistenței infracțiunii, a identificării făptuitorului, a constatării vinovăției, [*alte date concrete care urmează a fi stabilite prin realizarea acestei măsuri speciale de investigații*], precum și a stabilirii altor împrejurări importante pentru justa soluționare a cauzei, urmează a fi solicitată de la furnizorul de servicii [*datele de identificare ale furnizorului de servicii care dispune de informațiile necesare sau le ține la control*], informația cu privire la identificarea abonaților, proprietarilor sau utilizatorilor [*se indică: sistemul sau mijlocul de comunicații electronice utilizat ori punctul de acces la un sistem informatic, precum și datele de identificare ale abonatului, proprietarului sau utilizatorului, dacă sunt cunoscute*].

În drept, pentru efectuarea identificării abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic sunt îndeplinite:

1. Condițiile generale cu privire la efectuarea acțiunii de urmărire penală:

- imixtiunea organului de stat este prevăzută de lege, și anume de prevederile Convenției Consiliului Europei privind criminalitatea informatică, ratificate prin Legea nr. 6 din 02.02.2009, art.52 alin.(1) pct.14) și 17), art.57 alin.(2) pct.9), art.93 alin.(4), art.134^5 din Codul de procedură penală;

- reglementările sus-menționate sunt clare, accesibile și previzibile, legile enumerate mai sus fiind publicate în Monitorul Oficial al Republicii Moldova;

- imixtiunea organului de stat este necesară într-o societate democratică, fiind fondată pe o necesitate socială imperioasă și, mai ales, proporțională scopului legitim scontat de a descoperi o infracțiune îndreptată împotriva [*relațiile sociale contra cărora este îndreptată infracțiunea*];

- imixtiunea este proporțională în coraport cu interesul public de a descoperi infracțiunea și făptuitorul și de a nu-i permite să comită astfel de infracțiuni în continuare;

- imixtiunea are un scop legitim, și anume: apărarea ordinii, prevenirea faptelor ilegale, protejarea moralei, drepturilor și libertăților persoanei, îndeosebi a minorilor.

2. Condițiile generale cu privire la efectuarea măsurilor speciale de investigații:

- cu privire la organul competent de a efectua activitatea specială de investigații, fiind dispusă în sarcina ofițerilor de investigații din cadrul [*organul care va executa efectuarea activității speciale de investigații*];

- doar după pornirea urmăririi penale, urmărirea penală fiind pornită la [*data pornirii urmăririi penale*];

- pe altă cale este imposibilă realizarea scopului procesului penal și poate fi prejudiciată considerabil activitatea de administrare a probelor, or informația cu privire la abonații, proprietarii și utilizatorii sistemelor de comunicații electronice, ai mijloacelor de comunicații electronice sau ai punctelor de acces la sisteme informatice prin intermediul cărora [*faptele care au fost comise cu utilizarea acestor instrumente sau mijloace*] se păstrează doar la furnizorul de servicii, și anume la [*datele de identificare ale furnizorului de servicii care dispune de informațiile necesare sau le ține la control*];

- există o bănuială rezonabilă cu privire la săvârșirea unei infracțiuni [*categoria infracțiunii conform clasificării de la art.16 din Codul penal*], legea penală prevăzând pedeapsa maximă cu închisoare pe un termen de până la [*conform articolului din Partea Specială a Codului penal în temeiul căruia a fost pornită urmărirea penală*];

- acțiunea este necesară și proporțională cu restrângerea drepturilor și libertăților fundamentale ale omului.

3. Condițiile speciale cu privire la identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic:

- cu privire la organul competent să autorizeze efectuarea respectivei măsuri speciale de investigații, și anume procurorul, în corespundere cu prevederile art.132^2 alin.(1) pct.2) lit.a) din Codul de procedură penală;

- referitor la termenul efectuării măsurii speciale de investigații [*spre exemplu: potrivit art.20 alin.(3) lit.c) din Legea nr.241 din 15 noiembrie 2007 cu privire la comunicațiile electronice, furnizorii de rețele și/sau servicii de comunicații electronice, indiferent de tipul de proprietate, sunt obligați să păstreze toate informațiile disponibile, generate sau procesate în procesul furnizării propriilor servicii de comunicații electronice, necesare pentru identificarea și urmărirea sursei de comunicații electronice, identificarea destinației, tipului, datei, orei și duratei comunicației, identificarea echipamentului de comunicații al utilizatorului sau al altui dispozitiv utilizat pentru comunicație, identificarea coordonatelor echipamentului terminal de comunicații mobile și asigurarea prezentării acestor informații organelor împuternicite în condițiile legii. Informațiile ce țin de serviciile de telefonie mobilă sau fixă vor fi păstrate o perioadă de cel puțin un an, iar cele ce țin de rețeaua Internet – de cel puțin 6 luni. Obligația de păstrare se referă inclusiv la tentativele de apel eșuate.*]

Din considerentele menționate mai sus,

DISPUN:

1. A autoriza identificarea, prin intermediul furnizorului de servicii [*datele de identificare ale furnizorului de servicii care dispune de informațiile necesare sau le ține la control, inclusiv adresa fizică sau juridică*], a abonaților, proprietarilor și utilizatorilor sistemelor de comunicații electronice, mijloacelor de comunicații electronice sau ale punctelor de acces la sisteme informatice cărora [*adresa IP / numărul de telefon / contul electronic / etc.; data utilizării, după caz, timpul, fusul orar; datele de identificare ale abonatului, proprietarului sau utilizatorului, dacă sunt cunoscute*], inclusiv cu prezentarea următoarelor date [*se indică care anume date îi sunt necesare organului de urmărire penală: tipului de serviciu de comunicații utilizat (de*

exemplu: telefonie mobilă, redirecționare de apeluri, mesaje voce etc.), dispozițiilor tehnice luate în această privință (toate măsurile întreprinse pentru a-i permite unui abonat să beneficieze de serviciile de comunicații oferite) și perioadei serviciului; identității (denumirea sau numele și prenumele, data înregistrării sau nașterii, IDNO sau IDNP ș.a.), adresei poștale sau geografice, numărului de telefon al abonatului și oricărui alt număr de contact (inclusiv numărul de telefon, adresa web a site-ului sau numele de domeniu, adresa de e-mail, etc.), precum și a datelor referitoare la facturare și plată, disponibile în baza unui contract sau a unui aranjament de servicii; oricărei alte informații referitoare la locul în care se găsesc echipamentele de comunicație (cum ar fi aparatele de telefon, rețele locale și alele), disponibile în baza unui contract sau a unui aranjament de servicii].

2. A efectua măsura specială de investigații într-un termen de [*numărul de zile, la discreția procurorului*] de la data autorizării prezentei activități speciale de investigații.

3. A pune în sarcina ofițerilor de investigații din cadrul [*organul care va executa efectuarea activității speciale de investigații*] efectuarea măsurii speciale de investigații.

4. A obliga ofițerii de investigații, implicați în efectuarea măsurii speciale de investigații, să păstreze confidențialitatea informațiilor obținute în urma realizării activității speciale.

5. A informa furnizorul de servicii despre obligația sa de a comunica imediat, în condiții de confidențialitate, informațiile solicitate.

6. A informa persoanele care au fost supuse măsurii speciale de investigații, odată cu constatarea legalității efectuării măsurii speciale de investigații, despre dreptul de a lua cunoștință de procesul-verbal privind efectuarea măsurii speciale de investigații.

7. A informa procurorul care a autorizat măsura specială de investigații, la finisarea efectuării acesteia sau la momentul când vor dispărea temeiurile și motivele care au justificat autorizarea ingerinței, despre rezultatele obținute în efectuarea măsurii speciale de investigații, cu transmiterea procesului-verbal cu privire la efectuarea măsurii speciale de investigații, la care vor fi anexate materialele acumulate la efectuarea măsurii.

Procuror [*procuratura teritorială, specializată sau subdiviziunea Procuraturii Generale în care activează, numele și prenumele procurorului care întocmește ordonanța, precum și semnătura acestuia*]

ANEXA 24

Registratorii de internet internaționali

- African Network Information Centre – AfriNIC (www.afrinic.net), pentru Africa și regiunea Oceanului Indian;

- Asia-Pacific Network Information Centre – APNIC (www.apnic.net), pentru Asia și regiunea Oceanului Pacific;

- American Registry for Internet Numbers – ARIN (www.arin.net), pentru America de Nord;

- Latin American and Caribbean Internet Addresses Registry – LACNIC (www.lacnic.net), pentru America Latină și regiunea Caraibelor;

- RIPE Network Coordination Centre – RIPE NCC (www.ripe.net), pentru Europa, Orientul Apropiat și Asia Centrală.

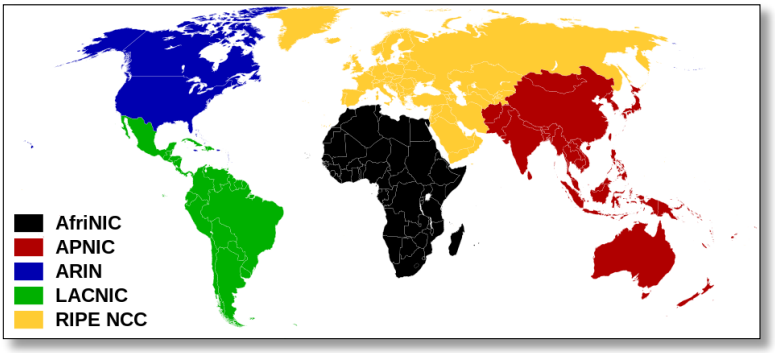


Fig.A24.1. Harta registratorilor de internet internaționali

ANEXA 25

Model de chestionar adresat experților judiciari în domeniul tehnologiilor informaționale

Stimate expert,

Universitatea de Stat din Moldova elaborează o cercetare în domeniul metodicii cercetării infracțiunilor informatice. Pentru asigurarea caracterului complet, real și obiectiv al studiului, USM roagă acordarea ajutorului Dumneavoastră, prin completarea chestionarului ce urmează:

Notă: Întrebările de mai jos se referă la acțiunile de urmărire penală (cum ar fi cercetarea la fața locului, reconstituirea faptei, experimentul, percheziția, ridicarea de obiecte și documente etc.), realizate în cadrul cercetării infracțiunilor informatice

1. La etapa pregătirii efectuării unei acțiuni de urmărire penală, inclusiv la instructajul membrilor grupului de urmărire penală, care vor participa la efectuarea acțiunii de urmărire penală, invitarea expertului/specialistului în domeniul tehnologiilor informaționale este necesară: ___ (*indicați cifra*)

1	2	3	4	5
Întotdeauna	De obicei	De la caz la caz	Uneori	Niciodată

2. La etapa efectuării nemijlocite a unei acțiuni de urmărire penală, participarea expertului/specialistului în domeniul tehnologiilor informaționale este necesară: ___ (*indicați cifra*)

1	2	3	4	5
Întotdeauna	De obicei	De la caz la caz	Uneori	Niciodată

3. Printre sarcinile de bază ale expertului/specialistului în domeniul tehnologiilor informaționale la etapa efectuării nemijlocite acțiunilor de urmărire penală sunt: (*bifați una sau mai multe opțiuni*)
□ stabilirea tipului și destinației sistemului informatic
□ examinarea dispozitivelor și conexiunilor cu alte sisteme informatice
□ stabilirea stării la moment a sistemului informatic
□ stabilirea tipului sistemului de operare
□ identificarea activităților realizate la moment în sistemul de operare
□ luarea deciziilor cu privire la acțiunile următoare asupra sistemului informatic
□ luarea măsurilor pentru obținerea accesului la informația computerizată
□ pregătirea sistemului informatic pentru transportare
□ conservarea probelor volatile
□ închiderea computerului pentru transportare
□ etichetarea, înregistrarea, împachetarea, transportul și prelucrarea probelor

4. Experții/specialiștii în domeniul tehnologiilor informaționale trebuie să utilizeze doar produse program și mijloace tehnice certificate, înregistrate din punct de vedere al protecției drepturilor de autor, adică să dispună de licență: ___ (*indicați cifra*)

1	2	3	4	5
Întotdeauna	De obicei	De la caz la caz	Uneori	Niciodată

5. Expertul/specialistul în domeniul tehnologiilor informaționale trebuie să NU admită „tratarea" fișierelor infectate. Faptul stabilirii prezenței virușilor doar se fixează. Fișierele infectate vor fi prezentate intacte expertului, pentru a stabili categoria virușilor, modul de răspândire, consecințele utilizării acestora, timpul instalării și nivelul de calificare al persoanei care l-a elaborat și/sau l-a instalat, structura, funcționalitatea, posibilitățile, setările, adresele centrelor de dirijare ale produsului program malițios. Fraza respectivă este valabilă: ___ (*indicați cifra*)

1	2	3	4	5
Întotdeauna	De obicei	De la caz la caz	Uneori	Niciodată

6. De regulă, verificarea prezenței produselor program malițioase (viruși) într-un sistem informatic se efectuează cu utilizarea a: ___ (*indicați cifra*)

1	2	3	4	5
Mai mult de trei antiviruși	Trei antiviruși	Doi antiviruși	Un antivirus	Fără nici un antivirus

7. Accesul și apropierea suspectului de sistemul informatic original (cu excepția clonei), mai ales dacă persoana are pregătire superioară în domeniul informatic, trebuie interzis: ___ (*indicați cifra*)

1	2	3	4	5
Întotdeauna	De obicei	De la caz la caz	Uneori	Niciodată

8. Se recomandă realizarea de pe dispozitivele de stocare a datelor informatice a: ___ (*indicați cifra*)

1	2	3	4	5
Mai mult de trei clone (copii criminalistice)	Trei clone	Două clone	O clonă	Nici o clonă

9. La audierea suspectului care are cunoștințe vaste la întrebările speciale și deține o experiență bogată în domeniu este necesară: ___ (*indicați cifra*)

1	Invitarea specialistului în domeniul tehnologiilor informaționale să participe la audiere

2	Consultarea prealabilă a organului de urmărire penală cu specialistul, în vederea pregătirii de audiere, fără participarea nemijlocită a specialistului
3	Implicarea specialistului este inoportună

10. Ce tipuri de expertize judiciare ați efectuat Dumneavoastră:

1	***Asupra componentelor hardware ale sistemului informatic:*** - computerele personale, precum și documentele tehnice ale acestora; - dispozitive periferice; - dispozitive de rețea (servere, cabluri de rețea. ș.a.); - sisteme integrate (telefoane mobile, ș.a.); - sisteme incorporate în baza controlerului cu microprocesor (dispozitiv de imobilizare, transponder, controler de croazieră); - orice componente ale obiectelor menționate mai sus.
2	***Asupra produselor program:*** - sistemul de operare, aplicațiile, programele incorporate în hardware, mijlocul de elaborare și rulare a softului; - aplicația de utilizare generală (redactori de text și grafici, sisteme de gestionare a bazelor de date, tabele electronice, prezentări și altele); - aplicația de utilizare specială într-un domeniu al științei tehnice, economiei.
3	***Informațională***: - fișiere text sau grafice, elaborate cu ajutorul mijloacelor informatice; - date în format multimedia; - baze de date electronice; - carduri bancare.
4	***Asupra rețelei informatice și componentelor acesteia***

Alte expertize în domeniu:_____
_____
_____
_____

Vă mulțumim!

DECLARAȚIA PRIVIND ASUMAREA RĂSPUNDERII

Subsemnata Purici Svetlana, declar pe răspundere personală că materialele prezentate în teza de doctorat sunt rezultatul propriilor cercetări și realizări științifice. Conștientizez că, în caz contrar, urmează să suport consecințele în conformitate cu legislația în vigoare.

Purici Svetlana

29 ianuarie 2018

CV AL AUTORULUI

Numele: Svetlana Purici

Data și locul nașterii: 19 octombrie 1986, Chișinău, Moldova

Cetățenia: Republica Moldova

Domiciliu: str. Grenoble 130/3, ap.20, Chișinău, Moldova

Telefon: 022 760 183, 078131211

Email: purici.svetlana@gmail.com

Aptitudini și competențe personale:

Limba maternă (de stat) – româna;

Limba engleză – bine;

Limba rusă – bine.

Studii:

2006-2010 – Universitatea de Stat din Moldova, Facultatea de Drept, specialitatea – drept penal;

2010-2012 – Învățământ postuniversitar specializat prin masterat în cadrul Universității de Stat din Moldova, Facultatea de Drept;

2012-2013 – Cursul de formare Modulul Psihopedagogic, în cadrul Universității de Stat din Moldova;

2014-2017 – Studii postuniversitare specializate prin doctorat, în cadrul Universității de Stat din Moldova, Facultatea de Drept.

Domeniile de interes științific:

Criminalistica, Metodica cercetării infracțiunilor informatice

Participări la foruri științifice (naționale și internaționale):

- 09-10 noiembrie 2017 – participantă la Conferința Științifică națională cu participare internațională „*Integrare prin cercetare și inovare*", Chișinău 2017, desfășurată în campusul Universității de Stat din Moldova, Facultatea de Drept, temele comunicărilor: *„Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic"* și *„Modelul și caracteristica criminalistică ale infracțiunilor informatice și din domeniul telecomunicațiilor"*.

- 30 martie 2017 – participantă la „*Moldova ICT Summit 2017*", desfășurat în mun. Chișinău.

- 28-29 septembrie 2016 – participantă la Conferința Științifică națională cu participare internațională „*Integrare prin cercetare și inovare*", Chișinău 2016, desfășurată în campusul Universității de Stat

din Moldova, Facultatea de Drept, temele comunicărilor: *„Analiza criminalistică preliminară în cadrul efectuării operațiunilor frauduloase de plată on-line”* și *„Etapa alegerii produsului sau serviciului în cadrul investigațiilor preliminare în cazul operațiunilor frauduloase de plată electronică”*.

- 20-21 mai 2016 – participantă la a 10-a Conferință Științifică Internațională „Provocările Societății Cunoașterii”/„CKS-Challenges of the Knowledge Society 2016”, organizată de Universitatea „Nicolae Titulescu” din București, desfășurată în campusul Universității „Nicolae Titulescu” din București, tema comunicării *„Fighting the classical crime-scene assumptions. Critical aspects în estamblishing the crime-scene perimeter în computer-based evidence cases”*.

- 28 aprilie 2016 – participantă la „*Moldova ICT Summit 2016*”, modulul ICT4 Internet Human Rights, desfășurat la Chișinău, Radisson Blu Leogrand Hotel, Raut Room.

- 10 noiembrie 2015 – participantă la Conferința Internațională științifico – practică „*Наука в современном мире (Science in the modern world)*”, desfășurată la Chișinău, 10 noiembrie 2015, cu tema comunicării „*Particularitățile investigațiilor preliminare online în cazul infracțiunilor cibernetice*”, Diploma de gradul II.

- 29 aprilie 2015 – participantă la „*Moldova ICT Summit 2015*”, modulul ICT4Development, desfășurat la Chișinău, Palatul Republicii, Big Hall.

- 25 – 27 iunie 2014 – participantă la ediția a 6-a a Conferinței Internaționale „*Justiție și criminalitate cibernetică*” desfășurată la Tg Jiu, România, organizat de către Tribunalul Gorj, Curtea de Apel Craiova și alții;

Activitate profesională:

2012 – prezent – lector universitar în cadrul Departamentului Drept Procedural, Facultatea de Drept, Universitatea de Stat din Moldova.

Lucrări științifice publicate:

1) Purici S., *Metodica cercetării infracțiunilor din domeniul informaticii. Monografie*, Chișinău: CEP USM. 2018, 221 p.
2) Purici S., *Modelul și caracteristica criminalistică ale infracțiunilor informatice și din domeniul telecomunicațiilor*, Conferința Științifică națională cu participare internațională „*Integrare prin cercetare și inovare*”, 09-10 noiembrie, 2017, Rezumate ale comunicărilor, Științe Juridice, CEP USM, Chișinău 2017, pag. 248.
3) Purici S., Purici D., *Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic*, Conferința Științifică

națională cu participare internațională „*Integrare prin cercetare și inovare*”, 09-10 noiembrie, 2017, Rezumate ale comunicărilor, Științe Juridice, CEP USM, Chișinău 2017, pag. 233.

4) Purici S., Gheorghiță M., *Măsuri tactice și strategice de depășire a obstacolelor care împiedică buna desfășurare a investigării infracțiunilor informatice*, Studia Universitatis Moldaviae, Seria Științe Sociale, Nr. 8(108), CEP USM, Chișinău, 2017, p. 146.
5) Purici S., *In dubio pro reo: Apărarea Cal Troian în cauzele de criminalitate informatică*, Revista Penalmente/Relevant, Universitatea „Nicolae Titulescu”, București, decembrie 2016, nr. 2/2016, pag.166-172 http://www.revista.penalmente.ro/wp-content/uploads/2016/12/@Svetlana-Purici-In-dubio-pro-reo-ap%C4%83rarea-de-tip-cal-troian.pdf http://www.revista.penalmente.ro/category/nr2-2016
6) Purici S., *Analiza criminalistică preliminară în cadrul efectuării operațiunilor frauduloase de plată on-line*, Conferința Științifică națională cu participare internațională „*Integrare prin cercetare și inovare*”, 28-29 septembrie, 2016, Rezumate ale comunicărilor, Științe Juridice, Volumul I, CEP USM, Chișinău 2016, pag. 223-227.
7) Purici S., Golubenco Gh., *Etapa alegerii produsului sau serviciului în cadrul investigațiilor preliminare în cazul operațiunilor frauduloase de plată electronică*, Conferința Științifică națională cu participare internațională „*Integrare prin cercetare și inovare*”, 28-29 septembrie, 2016, Rezumate ale comunicărilor, Științe Juridice, Volumul I, CEP USM, Chișinău 2016, pag. 219-223.
8) Purici S., Driga C., *Fighting the classical crime-scene assumptions. Critical aspects în establishing the crime-scene perimeter în computer-based evidence cases*, A 10-a Conferință Științifică Internațională „*Provocările Societății Cunoașterii/CKS-Challenges of the Knowledge Society*”, 20-21 mai, 2016, organizată de Universitatea „Nicolae Titulescu” din București, Revista Challenges of the Knowledge Society. Criminal Law, Universitatea „Nicolae Titulescu”, București, pag. 50-54, http://cks.univnt.ro/cks_2016_archive/cks_2016_articles.html
9) Purici S., Purici D., Driga C., *Particularitățile investigațiilor preliminare online în cazul infracțiunilor cibernetice*, Материалы Международной (заочной) молодежной научно-практической конференции под общей редакцией А.И. Вострецова, НАУКА В СОВРЕМЕННОМ МИРЕ (SCIENCE IN THE MODERN WORLD), november, 10, 2015, Chișinău, Diploma de gradul II, научное (непериодическое) электронное издание, Editura „Liceul”, Издательство „Мир науки”, 2015, УДК 001, ББК 72, pag. 244-261.
10) Purici S., *Specificul activității speciale de investigații și acțiunii de urmărire penală întreprinse pentru administrarea probelor la cercetarea crimelor cibernetice*, Studia Universitatis Moldaviae, Seria Științe Sociale, Nr. 11, CEP USM, Chișinău, ISSN 1814-3199, 2015, p.120.

11) Purici S., *Particularitățile problemelor care urmează a fi soluționate în cadrul investigării criminalistice a infracțiunilor informatice*, Studia Universitatis Moldaviae, Seria Științe Sociale, Nr. 8(88), CEP USM, Chișinău, ISSN 1814-319, 2015, p.144.

12) Purici S., *Bune practici internaționale cu privire la investigarea infracțiunilor informatice*, Studia Universitatis Moldaviae, Seria Științe Sociale, Nr. 3(83), CEP USM, Chișinău, 2015, p.162.

Premii:

Bursa de excelență a Guvernului, pentru anul 2017, în cadrul Concursului Republican „*Cu privire la acordarea Bursei de excelență a Guvernului și a Bursei nominale pentru doctoranzi, pe anul 2017*", în baza Hotărârii Guvernului nr. 89 din 21.02.2017, fiind doctorandă anul III la Facultatea de Drept, USM (2017);

Diplomă de gradul II, Conferința Internațională științifico-practică „***Наука в современном мире (Science in the modern world)***", desfășurată la Chișinău, 10 noiembrie 2015, cu tema comunicării „*Particularitățile investigațiilor preliminare online în cazul infracțiunilor cibernetice*".

Apartenența la societăți/asociații științifice naționale:

Membru al Senatului Universității de Stat din Moldova, noiembrie 2014 – prezent.