**UNIVERSITATEA DE STAT DIN MOLDOVA**

Cu titlu de manuscris
C.Z.U.: 343.98:004(043.2)

**PURICI SVETLANA**

# METODICA CERCETĂRII INFRACȚIUNILOR DIN DOMENIUL INFORMATICII

**SPECIALITATEA: 554.04 – CRIMINALISTICĂ, EXPERTIZĂ JUDICIARĂ, INVESTIGAȚII OPERATIVE**

Autoreferatul tezei de doctor

**CHIȘINĂU, 2018**

Teza a fost elaborată în cadrul Departamentului Drept Procedural
al Facultății de Drept, Universitatea de Stat din Moldova

**Conducător științific:**

**GOLUBENCO Gheorghe**, doctor în drept, profesor universitar,
specialitatea 554.04 – Criminalistică, expertiză judiciară, investigații operative

**Referenți oficiali:**

1. ***CUȘNIR Valeriu***, dr. hab. în drept, prof. univ.;
2. ***RUSU Vitalie***, dr. în drept, conf. univ.

**Componența consiliului științific specializat:**

1. ***BRÎNZĂ Sergiu***, președinte al CȘS, dr. hab. în drept, prof. univ.;
2. ***VIZDOAGĂ Tatiana***, secretar științific al CȘS, dr. în drept, conf. univ.;
3. ***DOLEA Igor***, membru al CȘS, dr. hab. în drept, prof. univ.;
4. ***GHEORGHIȚĂ Mihai***, membru al CȘS, dr. hab. în drept, prof. univ.;
5. ***OSOIANU Tudor***, membru al CȘS, dr. în dept, prof. univ.;
6. ***EȘANU Adriana***, membru al CȘS, dr. în drept, conf. univ.

Susținerea va avea loc la **15.09.2018**, ora **10:00**,
în ședința Consiliului științific specializat **D 30.554.04-03**
din cadrul Universității de Stat din Moldova (MD-2009, Republica Moldova, mun. Chișinău, str. A. Mateevici, 60, bloc IV, aula 222)

Teza de doctor și autoreferatul pot fi consultate la biblioteca Universității de Stat din Moldova, Biblioteca Națională a Republicii Moldova și la pagina web a CNAA (www.cnaa.md).

Autoreferatul a fost expediat la „**10**” **08.2018**.

Secretar științific al
Consiliului Științific Specializat,
dr., conf. univ. VIZDOAGĂ TATIANA

Conducător științific, GOLUBENCO Gheorghe
dr., prof. univ.

Autor PURICI Svetlana

## REPERE CONCEPTUALE ALE CERCETĂRII

**Actualitatea temei.** Dezvoltarea tehnologiei informației și continua globalizare a rețelelor informatice au condus la un progres de necontestat al societății și la asigurarea transparenței în viața publică, dar au determinat și apariția unei noi forme de criminalitate – *criminalitatea informatică*.

Internetul, în acea formă în care îl cunoaștem la etapa actuală, a trecut printr-un proces complex de evoluție, în prezent reprezentând un instrument inevitabil pentru viața cotidiană, astfel prezentând o pistă ce permite desfășurarea diferitor acțiuni, printre care și a celor nepermise de lege. Apariția internetului a facilitat migrarea infracțiunilor tradiționale în spațiul virtual, astfel rezultând infracțiunile cibernetice.

Treptat, lumea virtuală a evoluat, prin prisma oportunităților pe care le oferă oamenilor, astfel devenind un izvor nesecat de informații și resurse incontestabil de valoroase, dar pe de altă parte și un spațiu nemărginit de victime și infractori. Progresul semnificativ de dezvoltare a tehnologiilor informaționale și mijloacelor, care formează spațiul cibernetic, a devenit nu doar un beneficiu, dar a generat și apariția urmărilor negative, pericolelor legate de posibilitatea utilizării acestor tehnologii și mijloace, în scopuri incompatibile cu sarcinile de asigurare a securității personale, naționale și internaționale.

Criminalitatea cibernetică constituie un pericol sporit atât pentru subiecți individuali, cât și pentru statele lumii, chiar și pentru întreaga comunitate internațională, prezentând un caracter transfrontalier. Lupta cu această categorie de infracțiuni trebuie să fie una dintre prioritățile de bază ale comunității internaționale, statele trebuie să elaboreze reglementări similare în combaterea lor.

În ultimii ani, creșterea numărului de Internet Service Provideri, accesul la abonamente gratuite și ușurința prin care poți cădea în capcana unui infractor cibernetic au amplificat complexitatea investigațiilor criminalistice în domeniu. Din perspectiva unei asemenea problematici, infracțiunile din mediul respectiv prezintă dificultăți la 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, existența insuficientă a instrumentelor internaționale de cooperare, reglementările neclare la nivel național, complexitatea procedurii de investigare a infracțiunilor cibernetice și necesitatea de pregătire a organelor de urmărire penală, precum și a specialiștilor în domeniu, resursele financiare limitate în vederea investigării acestor tipuri de infracțiuni, deznădăjduirea victimelor și ezitarea acestora de a apela la organele de drept, vulnerabilitatea internetului ca

platformă complexă, creează impedimente în activitatea de urmărire penală și într-un final atragerea infractorilor cibernetici 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. Inventarea calculatoarelor, a telefoanelor mobile, internetului, a tabletelor și altor gadget-uri, au fost întotdeauna însușite de către infractori cu pași rapizi, care au fost dintotdeauna interesați să le folosească ca instrumente pentru realizarea scopurilor infracționale.

Actualitatea și importanța prezentei teze de doctor este determinată și de faptul că autorul a identificat soluțiile pentru o serie de probleme tactico-organizatorice privind cercetarea infracțiunilor informatice, în prezent nefiind analizate sub aspect teoretic și practic în publicațiile autohtone. În particular, nu este elaborat un algoritm al aplicării tacticii și metodicii de cercetare a infracțiunilor informatice, nu și-a găsit soluționare în practica autohtonă a organelor competente problema audierii, cercetării la fața locului, percheziției, ridicării și conservării datelor informatice, expertizei și constatării tehnico-științifice; un loc aparte în această lucrare îl are aplicarea măsurilor speciale de investigații în cazul infracțiunilor supuse cercetării; nu sunt elaborate recomandări de cercetare a infracțiunilor cibernetice, de unde și necesitatea de a generaliza și interpreta teoretic și practic rezultatele acestor noi experiențe.

Deși există anumite lucrări dedicate cercetării diferitor aspecte ale infracțiunilor informatice, întrebările legate de tactica și metodica criminalistică, metodologia învingerii și neutralizării activităților de împiedicare a bunei desfășurări a procesului penal la investigarea acestor categorii de infracțiuni, anterior în literatura științifică autohtonă nu a fost studiată.

Totalitatea circumstanțelor indicate condiționează actualitatea prezentei lucrări.

Dată fiind această situație ne vedem îndreptățiți și motivați să inițiem o cercetare privind metodica cercetării infracțiunilor din domeniul informaticii, care este una din sarcinile prioritare ale criminalisticii contemporane.

**Descrierea situației în domeniul de cercetare și identificarea problemelor de cercetare.**

În vederea realizării scopului științific propus, au fost stabilite anumite obiective printre care, cercetarea materialelor științifice referitoare la descrierea fenomenului criminalității cibernetice, inclusiv în corelație cu alte categorii de infracțiuni, publicate în Republica Moldova, România, Federația Rusă, S.U.A. și în alte state, identificându-se, astfel, locul cercetării realizate în cadrul investigațiilor științifice întreprinse până la moment.

În literatura de specialitate autohtonă, spre deosebire de alte state, metodica investigării infracțiunilor în domeniul informaticii este tratată în linii mari, din care motiv, se constată o necesitate stringentă de a efectua studii aprofundate în domeniu.

Pentru studierea diferitor aspecte ale temei, s-a purces la o antrenare a unui contingent masiv de elaborări științifice, atacând subiecte directe, ce țin de fenomenul criminalității cibernetice.

Cu scopul perfectării teoretice a fenomenului în cauză s-au studiat câteva grupuri de surse teoretice. A fost firesc să se înceapă cu selectarea unor studii de referință ce au o anumită atribuție la determinarea fenomenului în cauză. Ele reprezintă operele unor cunoscuți criminaliști și juriști, de obicei, teorii și concepții clasice care au fost utilizate la formularea unor postulate ce au condus la o coagulare a logicii evoluției infracțiunilor în domeniul informaticii, până la determinarea reperelor metodologice.

Dat fiind faptul că spațiul cibernetic reprezintă al cincilea spațiu comun, după cel terestru, naval, aerian și cosmic, criminalitatea informatică necesită coordonare, cooperare și măsuri normative specifice la nivel internațional (inclusiv referitoare la colaborarea operativă și prin crearea organelor regionale de combatere), nefiind suficientă în acest sens numai elaborarea unei legislații adecvate la nivel intern.

Printre cei mai de vază oameni de știință care au cercetat domeniul infracțiunilor informatice, viziunile și exegezele cărora au constituit baza științifico-teoretică a tezei, se numără: Golubenco Gh., Gheorghiță M., Doraș S., Vizdoagă T., Croitor E., Dolea Ig., Roman D., Brînză S., Stati V., Amza T., Amza C., Dobrinoiu M., Moise A. C., Lungu S., Tilea M., Voinea D., Vasiu I., Vasiu L., Olteanu G., Stancu E., Ioniță G., Ghervase D., Neamțu M., Trancă An., Trancă D., Lazareva N., Bîstreacov E.N., Ivanov A. N., Klimov V.A., Meșereakov V., Andreev B.V., Pak P.N., Horst V., Jmîhov A., Filipov A., Dobrovoliskii D.V., Iablokov N., Lopatina T.M., Vardanian A.V., Nikitina E.V., Menjega M., Hudeakov P.V., Ovseanikov D., Aleskerov V.I., Maximenko I., Sizonenko A.B., Șîșkin V., Voroșilova T., Kosînkin A., Davîdov V., Kovaleov C.A., Vehov V.B., Propastin S., Sussmann M., Reyes A., Wiles J., Kleiman D.

**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.

**Metodologia cercetării ştiinţifice.** În urma analizei spectrului doctrinar și normativ al temei investigate, s-a ajuns la concluzia că cercetarea oricărei probleme de drept poate pretinde la stabilirea adevărului doar atunci când se fundamentează pe o metodologie corespunzătoare. În procesul investigației au fost utilizate astfel de metode, precum: analitică, exegetică, sistemică, istorică, dialectică, prospectivă, comparativă, logico-juridică, demonstrației, deducției, analizei sintetice, etc. Aspectele teoretice ale studiului dat se bazează pe cercetarea nemijlocită a surselor bibliografice.

**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.** 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.

**Rezultatele științifice principale înaintate spre susținere:** 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.

**Implementarea rezultatelor științifice.** Rezultatele teoretice și practice ale cercetării au fost discutate în cadrul ședințelor Departamentului Drept Procedural, Facultatea de Drept, USM. Concluziile și recomandările, care formează rezultatele științifice ale cercetării realizate și-au găsit reflectare în publicarea articolelor în reviste științifice, inclusiv participări la conferințe științifico-practice internaționale și naționale, fapt ce a contribuit la îmbogățirea cadrului teoretic național privind metodica cercetării infracțiunilor din domeniul informaticii. Rezultatele cercetării pot fi aplicate în procesul de instruire a studenților, masteranzilor, doctoranzilor din cadrul facultăților de drept a instituțiilor de învățământ universitar, precum și în activitatea practică a organelor de drept.

**Aprobarea rezultatelor ştiinţifice.** Concluziile de bază şi recomandările formulate în teză sunt reflectate în cadrul a 12 publicaţii ştiinţifice, expuse în reviste de specialitate din ţară şi de peste hotare. Unele concepte şi idei au fost publicate în rapoarte şi comunicări la conferinţe ştiinţifice naţionale şi internaţionale.

Prezenta lucrare a fost elaborată în cadrul Universităţii de Stat din Moldova, unde a fost analizată şi prezentată spre susţinere conform procedurilor şi în baza actelor normative de rigoare.

**Publicaţiile la tema tezei.** Rezultatele investigaţiilor au fost reflectate în 12 publicaţii ale autoarei, dintre care 7 cu un singur autor. Volumul total al publicaţiilor este de 7.2 coli de autor.

**Volumul şi structura tezei.** Având în vedere standardele stabilite, teza de doctorat are următoarea structură: text de bază 140 de pagini, adnotare în limbile română, rusă şi engleză, lista abrevierilor, introducere, trei capitole divizate în secţiuni, concluzii generale şi recomandări, bibliografia din 360 titluri, 25 anexe, declaraţia privind asumarea răspunderii, CV-ul autorului.

**Cuvintele-cheie**: criminalitate informatică, internet, sistem informatic, probe electronice, versiuni criminalistice, metodică, cercetarea infracţiunilor, măsuri speciale de investigaţii.

## CONŢINUTUL TEZEI

Lucrarea este precedată de o ***Introducere***, în care se argumentează actualitatea şi importanţa temei cercetate, sunt specificate scopul şi obiectivele tezei, este reflectată noutatea ştiinţifică a rezultatelor obţinute, precum şi problema ştiinţifică importantă în domeniul de cercetare. Tot în aceeaşi ordine de idei sunt determinate semnificaţia teoretică şi valoarea aplicativă a lucrării, fiind evidenţiată aprobarea rezultatelor şi descris sumarul capitolelor tezei.

În ***Capitolul I*** „***Analiza situaţiei în domeniul cercetării infracţiunilor informatice***”, alcătuit din patru subcapitole este expusă o examinare a materialelor ştiinţifice publicate în RM şi în străinătate, ce ţin de problematica cercetării infracţiunilor din domeniul informaticii, astfel, fiind scoasă în evidenţă contribuţia doctrinei în acest sens, iar conţinutului surselor bibliografice s-a realizat în ordine cronologică, fiind luate în calcul importanţa şi genul lucrărilor. Concluziile din acest capitol, în vederea realizării scopului ştiinţific propus, au întrunit anumite obiective printre care, cercetarea materialelor ştiinţifice referitoare la descrierea fenomenului criminalităţii cibernetice, inclusiv în corelaţie cu alte categorii de infracţiuni, publicate în RM, România, Federaţia Rusă, SUA şi în alte state, identificându-se, astfel, locul cercetării realizate în cadrul investigaţiilor ştiinţifice întreprinse până la moment. În literatura de specialitate autohtonă, spre deosebire de alte state, metodica investigării infracţiunilor în domeniul informaticii este tratată în linii mari, din care motiv, se constată o necesitate stringentă de a efectua studii aprofundate în

domeniu. Cu scopul perfectării teoretice a fenomenului în cauză s-au studiat câteva grupuri de surse teoretice. A fost firesc să se înceapă cu selectarea unor studii de referință ce au o anumită atribuție la determinarea fenomenului în cauză. Ele reprezintă operele unor cunoscuți criminaliști și juriști, de obicei, teorii și concepții clasice care au fost utilizate la formularea unor postulate ce au condus la o coagulare a logicii evoluției infracțiunilor în domeniul informaticii, până la determinarea reperelor metodologice. Analiza recomandărilor științei criminalistice și a specificului legislației regionale și naționale a contribuit la realizarea primului studiu științific aprofundat din acest domeniu în RM.

Astfel, 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).

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.

În acest sens, comunitatea internațională a elaborat acte la diferite nivele, care reglementează cooperarea statelor și organizațiilor în combaterea criminalității informatice.

***Capitolul II „Caracteristica criminalistică și organizarea cercetării infracțiunilor din domeniul informaticii”*** a fost alcătuit din subcapitolele: *Noțiunea de infracțiune informatică și criminalitate informatică. Clasificarea infracțiunilor informatice; Modelul și caracteristica criminalistică ale infracțiunilor informatice; Situațiile tipice de urmărire penală și versiunile criminalistice; Măsuri tactice și strategice de depășire a obstacolelor care împiedică buna desfășurare a investigării infracțiunilor informatice și concluzii la acestea*. În acest capitol s-a definit conceptul de criminalitate informatică, ce 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, îndreptate împotriva relațiilor sociale în domeniul informaticii și comunicațiilor electronice, securității statului, minorului, proprietății intelectuale și drepturilor conexe, vieții private, secretului corespondenței electronice,

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.

La rândul său, criminalitatea informatică în *sens larg* reprezintă ansamblul infracțiunilor săvârșite pe un anumit teritoriu într-o anumită perioadă, îndreptate împotriva relațiilor sociale în domeniul informaticii și comunicațiilor electronice, securității statului, minorului și proprietății intelectuale și drepturilor conexe, 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.

Clasificarea infracțiunilor informatice trebuie să reiasă din specificul legislației naționale, acordurile internaționale în domeniu la care RM este Parte și din definiția noțiunii de criminalitate informatică în sens larg.

De exemplu, în cazul fraudelor informatice, săvârșite la procurarea online a bunurilor sau a serviciilor 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, 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 [1, p. 219].

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 datelor și sistemelor informatice [2, p. 388].

Modelul criminalistic al infracțiunilor devine, după cum menționează mai mulți criminaliști, un „*etalon*”, „*clișeu*” care se suprapune pe caracteristica criminalistică a cauzei cercetate.

Astfel, modelul criminalistic al infracțiunilor informatice reprezintă un ansamblu de

informații sistematizate, cu privire la specificul probelor digitale, particularitățile infracțiunilor și infractorilor cibernetici, care se reflectă în cadrul pregătirii, săvârșirii și tăinuirii infracțiunilor informatice și ce permit algoritmizarea procesului de cercetare și descoperire a acestor categorii de infracțiuni.

Infractorii folosesc un număr redus de instrumente destinate pentru mascarea datelor sistemului informatic utilizat (spre exemplu aplicații de ascundere a adresei IP), deoarece nu s-a trecut la executarea nemijlocită a infracțiunii și pentru a nu îngreuna procesul de căutare a produselor sau a serviciilor prin utilizarea acestor instrumente.

Oricum nu s-ar ascunde infractorul acesta urmează să ofere și informație veridică. Astfel, la cea de-a doua etapă, la completarea formularelor online, comercianții solicită diverse date despre cumpărător [3, p. 223].

Una din cele mai frecvent întâlnite 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 că infracțiunea a fost săvârșită, fie de către un terț 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 astfel de program care executa automat un set predefinit de instrucțiuni, în ambele situații, fără știrea utilizatorului sau deținătorul legitim al sistemului informatic [4, p. 167, 5, p. 162].

Printre cele mai relevante semne caracteristice ale infracțiunilor cibernetice sunt [6, p. 248]: legătura cu alte genuri de infracțiuni (în deosebi cu criminalitatea organizată și cea economică), caracterul tehnologic avansat, nivelul înalt de latență, caracterul bine organizat, profesional, transfrontalier și transnațional, fiind cele mai dinamice în dezvoltare, având costuri reduse pentru săvârșire, conturându-se trăsături politice, extremiste și teroriste.

Până în prezent CSJ nu s-a expus referitor la aplicarea legislației în cazul infracțiunilor informatice în vederea asigurării unei practici judiciare unice. În vederea îmbunătățirii situației existente în domeniu, este necesară o activitatea concentrată a organelor statului, în particular, este necesară elaborarea unei hotărâri explicative cu privire la examinarea cazurilor de criminalitate informatică și de administrare a probelor electronice.

Infractorii informatici sunt persoane cu 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 alterată diminuată asupra ilegalității comportamentului său, daunei provocate, riscurilor de a fi denunțat, descoperit și sancționat, cu sau fără cunoștințe tehnice în domeniul tehnologiilor informaționale, 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 cu motivație infracțională diversificată (fie materială, sexuală, ideologică, politică, obsedată de statut sau de investigație). În majoritatea covârșitoare a cazurilor ei sunt de gen masculin, cu vârsta cuprinsă între 16-55 de ani, care acționează în grup, neavând în majoritatea cazurilor antecedente penale.

Locul comiterii infracțiunilor informatice este legat direct de caracterul predominant transfrontalier al acestei categorii de infracțiuni, în majoritatea cazurilor fiind diferit de locul survenirii consecințelor faptei. Pe de o parte, 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.

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 orice altă intervenție în funcționarea mijloacelor de stocare, prelucrare sau transmitere a datelor informatice sau a rețelei de comunicații. Printre particularitățile acestor categorii de probe este că aparent ele nu sunt evidente, sunt volatile, fiind conținute în echipamente informatice, nu sunt obiecte tangibile, de regulă, prezintă o anumită valoare materială.

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.

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.

***Capitolul III „Particularitățile tactice de efectuare ale unor acțiuni de urmărire penală și măsuri speciale de investigații la cercetarea infracțiunilor informatice”*** cuprinde subcapitolele: *Aspecte generale privind efectuarea unor acțiuni inițiale și ulterioare de urmărire penală Audierea persoanelor în cadrul cercetării infracțiunilor informatice Cercetarea la fața locului Percheziția, ridicarea de obiecte și documente. Conservarea imediată a datelor cu privire la traficul informatic Efectuarea expertizei și constatărilor tehnico-științifice Măsuri speciale de investigații pertinente cercetării infracțiunilor informatice și concluziile de rigoare*.

Încă de la etapa urmăririi penale apar probleme cu privire la pregătirea organului de drept la administrarea probelor electronice. Acest fapt se datorează nivelului insuficient de pregătire a organului de urmărire penală, implicarea redusă a specialiștilor în domeniul IT, 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.

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 fiind ridicate probele aflate nemijlocit în zona de activitate a făptuitorului, în cazul infracțiunilor informatice regula respectivă parțial decade, datorită specificului volatil al probelor electronice.

Cercetarea infracțiunilor cibernetice 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 actorilor implicați la combaterea fenomenului în cauză.

Este imperios elaborarea unei metodologii noi cu privire la metoda și tactica criminalistică la cercetarea infracțiunilor cibernetice.

La efectuarea cercetării la fața locului, percheziției, ridicării de obiecte și documente etc., ofițerul de urmărire penală urmează să întreprindă diverse acțiuni preparatorii de bază specifice investigării infracțiunilor cibernetice, atât în procesul de pregătire de efectuare a acțiunii de urmărire penală, cât și la efectuarea nemijlocită a acestora.

Organul de urmărire penală trebuie să respecte diverse reguli generale și speciale referitoare la administrarea probatoriului în cauzele de criminalitate informatică, să ia în considerație anumite recomandări fundamentale, valabile pentru acțiunile de urmărire penală efectuate în cadrul investigării infracțiunilor respective, legate de conservarea probelor, participanții la acțiunea procesuală, participarea specialistului, instrumentele și mijloacele necesare, asigurarea securității locului și a probelor, fotografierea și înregistrarea video a

acțiunii, examinarea și ridicarea probelor tradiționale și 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.

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 acestor situații. Mai mult decât atât, examinarea sistemelor informatice se efectuează după anumite procedee și într-o anumită consecutivitate, în dependență de starea acestuia (aflat sau nu în funcțiune, conectat sau nu la sursa de alimentare cu energie electrică). Ridicarea notebook-urilor, tabletelor și a echipamentelor mobile, cercetarea suporturilor de stocare a datelor informatice și a documentelor electronice, de asemenea posedă anumite reguli și particularități specifice.

În cadrul audierii persoanelor implicate în cauzele de infracțiune informatică organul de urmărire penală trebuie să țină cont de calitățile profesionale ale intervievatului, calitatea lui procesuală, precum și de cunoștințele lui despre cazul investigat. Ofițerul de urmărire penală urmează să facă uz de întrebările-tip specifice investigării acestei categorii de infracțiuni, care sunt extrem de relevante în vederea stabilirii tuturor circumstanțelor cauzei penale. Ele vor asigura ca persoana care efectuează audierea să nu scape din vedere anumite împrejurări sau situații, să cerceteze concomitent toate versiunile posibile. Totuși, ofițerul de urmărire penală va lua în calcul și specificul fiecărui caz concret, suplimentând întrebările-tip care urmează a fi adresate persoanei audiate cu anumite chestiuni particulare cazului.

Investigării paginilor web și a site-urilor le sunt aplicabile anumite particularități, reguli metodologice și recomandări practice specifice pentru fiecare etapă și obiectiv trasat, inclusiv 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), stabilirea datelor cu privire la numele de domeniu, precum și identificarea datelor serverului gazdă.

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.

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 (susceptibile alterării sau pierderii), securizării rapide a integrității datelor informatice pentru a putea permite organului de urmărire penală ridicarea ulterioară a acestora, 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.

Un rol deosebit la investigarea și descoperirea infracțiunilor în domeniu îl au expertizele tehnice ale calculatoarelor: asupra componentelor hardware ale sistemului informatic (expertiza tehnică a dispozitivelor); asupra produselor program; informațională (a datelor informatice stocate în sistemul informatic); asupra rețelei informatice și componentelor acesteia. La dispunerea acestora ofițerul de urmărire penală trebuie să țină cont de sarcinile de bază ale fiecăreia.

Odată cu ratificarea Convenției Consiliului Europei 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). Deși Convenția se referă la criminalitatea informatică, ea prevede posibilitatea aplicării acestor măsuri atât la investigarea 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 infracțiuni. Cu toate acestea, specific procesului penal cu privire la cercetarea infracțiunilor cibernetice, organul de urmărire penală poate dispune efectuarea măsurilor speciale de investigații doar într-un număr restrâns de cazuri, având în vedere faptul că majoritatea infracțiunilor din această categorie sunt infracțiuni ușoare și mai puțin grave. Ceea ce este paradoxal, simpla identificare a abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice ori al unui punct de acces la un sistem informatic, monitorizarea conexiunilor comunicațiilor telegrafice și electronice măsuri vitale la investigarea unei infracțiuni cibernetice, de regulă, nu pot fi efectuate. Din aceste motive se impune modificarea CPP, prin deschiderea posibilității realizării acestor măsuri la investigarea infracțiunilor respective (infracțiunilor informatice, a altor infracțiuni săvârșite prin intermediul sistemelor informatice, cât și la colectarea probelor electronice indiferent de categoria infracțiunii).

Conținutul art.$134^1$ CPP urmează a fi racordat la denumirea acestuia, astfel 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, ținând cont de specificul comunicațiilor electronice.

Constatăm o lacună legislativa și la capitolul concurenței dintre normele procesuale de la art.133 CPP („Reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale") și 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 tehnologiilor informaționale: poștă electronică (fie prin intermediul browser-ului sau aplicațiilor), programe pentru schimb de mesaje (WhatsApp, Viber, ICQ, Skype). Această situație provoacă confuzia normelor care trebuie aplicate în cazul necesității ridicării conținutului corespondenței electronice, iar diferența majoră constă în instituția care urmează a fi implicată în acest proces: instituția poștală sau cea care prestează servicii de livrare a corespondenței electronice.

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 [7]. Astfel, conform datelor din 03.01.2018 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. [8, p. 233].

Atunci când există suspiciuni cu privire la implicarea unei persoane la săvârșirea infracțiunii informatice, organul de urmărire penală și organul care realizează activitatea specială de investigații, au sarcina preliminară să stabilească 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) coraportul dintre făptuitor, faptă și urmări [9, p. 144].

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 [10, p. 50].

Specific procesului penal cu privire la cercetarea infracțiunilor cibernetice, organul de urmărire penală poate dispune efectuarea măsurilor speciale de investigații doar într-un număr restrâns de cazuri, având în vedere faptul că majoritatea infracțiunilor din această categorie sunt infracțiuni ușoare și mai puțin grave. Ceea ce este paradoxal, simpla identificare a abonatului, proprietarului sau utilizatorului unui sistem de comunicații electronice, monitorizarea conexiunilor comunicațiilor telegrafice și electronice măsuri vitale la investigarea unei infracțiuni cibernetice, de regulă, nu pot fi efectuate [11, p. 220].

Convenția Consiliului Europei 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 faptul că aplicarea unor astfel de tehnici (cum ar fi colectarea datelor cu privire la trafic, interceptarea datelor referitoare la conținut) sunt adesea cruciale pentru investigația 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 pentru investigarea acestor infracțiuni informatice și a infracțiunilor săvârșite cu ajutorul sistemelor informatice [12], fapt despre care nu s-a ținut cont în legislația procesual penală a RM.

## CONCLUZII GENERALE ŞI RECOMANDĂRI

**Rezultatele obținute** în urma analizei și generalizării materiei expuse în teză constau în 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 [6, 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 [13, 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 [13, p 74].

6. Prezenta cercetare permite identificarea anumitor cauze care generează o descoperire insuficientă a infracțiunilor informatice, și anume [13, 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*” [13, 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*” [13, 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 [13, 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"*) [13, 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," [13, 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 [13, 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 [13, 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 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 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, luând în calcul și specificul fiecărui caz concret;

- 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 [13, 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.
- 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. Purici S., Golubenco Gh. Etapa alegerii produsului sau serviciului în cadrul investigațiilor preliminare în cazul operațiunilor frauduloase de plată electronică., т. 1, În: Integrare prin cercetare și inovare. Rezumatele conf. științifice naționale cu participare internațională. Chișinău: Științe Juridice, CEP USM, 2016, p.219-223.
2. Olteanu G. I. Metodologie criminalistică. Cercetarea structurilor infracţionale şi a unora dintre activităţile ilicite desfăşurate de acestea. Bucureşti: AIT Laboratories, 2007., 423 p
3. Purici S. Analiza criminalistică preliminară în cadrul efectuării operațiunilor frauduloase de plată on-line. În: Integrare prin cercetare și inovare. Rezumatele conf. științifice naționale cu participare internațională. Chișinău: CEP USM, 2016, p. 223-227.
4. 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. http://www.revista.penalmente.ro/wp-content/uploads/2016/12/@Svetlana-Purici-In-dubio-pro-reo-ap%C4%83rarea-de-tip-cal-troian.pdf (vizitat 03.01.2018).
5. Purici S. Bune practici internaționale cu privire la investigarea infracțiunilor informatice. Studia Universitatis Moldaviae, CEP USM, Chişinău, 2015, nr. 3(83), p.162.

6. Purici S. Modelul și cararcteristica criminalistică ale infracțiunilor informatice și 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.
7. Registrul public al furnizorilor de rețele şi servicii de comunicaţii electronice. Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei, 2017., http://anrceti.md/lista_furnizori_servicii_retele_ce (vizitat 03.01.2018)
8. 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 naționale cu participare internațională, pag. 233-237.
9. Purici S. Particularitățile problemelor care urmează a fi soluționate în cadrul investigării criminalistice a infracțiunilor informatice. În: Studia Universitatis Moldaviae, Seria Ştiinţe Sociale, CEP USM, Chişinău, 2015, nr. 8(88), p.144.
10. 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, Universitatea „Nicolae Titulescu", București, 2016, p. 1006. http://cks.univnt.ro/download/156_cks_2016_online_journal.pdf (vizitat 03.01.2018).
11. 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, pag. 120-125.
12. Council of Europe Treaty Series No. 185 - Explanatory Report to the Convention on Cybercrime https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b (vizitat 03.01.2018).
13. Purici S., Metodica cercetării infracțiunilor din domeniul informaticii. Monografie. Chișinău: CEP USM. 2018, 221 p.

## 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, 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.

**PURICI SVETLANA**

# METODICA CERCETĂRII INFRACȚIUNILOR DIN DOMENIUL INFORMATICII

**SPECIALITATEA: 554.04 – CRIMINALISTICĂ, EXPERTIZĂ JUDICIARĂ, INVESTIGAȚII OPERATIVE**

Autoreferatul tezei de doctor


| | |
|---|---|
| Aprobat spre tipar: data | Formatul hârtiei 60x84 1/16 |
| Hârtie ofset. Tipar ofset. | Tiraj … ex… |
| Coli de tipar.: … | Comanda nr. …. |

Centrul Editorial – Poligrafic al USM