PREVENIREA INDIVIDUALĂ A INFRACȚIUNII DE FRAUDĂ INFORMATICĂ DE INFRACTORII DIGITALI ÎN CALITATE DE MERCENARI

INDIVIDUAL PREVENTION OF COMPUTER FRAUD CRIME BY DIGITAL CRIMINALS AS MERCENARIES

Igor Soroceanu,
doctorand, magistru în drept,
Institutul de Administrație Publică al Universității de Stat din Moldova,
ORCID: 0000-0002-8719-0454

CZU: 343.72:004

Abstract

During the last decades, cyberspace has had a huge impact on all components of human society. The evolution of humanity and the activities of modern society, the defense of fundamental rights, economic and social interactions depend more and more on communication infrastructures and information technology. In recent years it has been observed that while the digital world brings enormous benefits, it is also vulnerable. Cyberspace incidents, whether intentional or accidental, are growing at an alarming rate and could disrupt the provision of essential services such as water, health, electricity or mobile phone services. Threats that may have different origins, including criminal, politically motivated, terrorist or state-sponsored attacks, as well as natural disasters or unintentional mistakes. The economy of the states is already affected, in different proportions, by cybercrime activities directed against individuals and public and private sectors. For these reasons, in the following order, we propose to carry out a research in the field of individual prevention of the crime of computer fraud by digital criminals as mercenaries.

Keywords: *online space, illegal acts, mercenaries, cyber attacks, criminal prevention.*

Introducere. Un loc important în sistemul prevenirii infracțiunilor de fraudă informatică îl ocupă prevenirea individuală, care constă în aplicarea unui complex de activități în privința unor anumite persoane cu scopul preîntâmpinării comiterii infracțiunii.

Prevenirea individuală se realizează, mai întâi de toate, prin influența asupra acestor persoane predispuse să comită infracțiuni, precum și asupra mediului social.

În calitate de obiecți ai unei asemenea preveniri apar indivizii, al căror comportament și mod de viață denotă posibilitatea lor reală de a comite fapte infracționale. Viziunile, motivele, sistemul orientărilor de valoare ale personalității pot deveni o bază pentru aplicarea asupra ei a influenței preventive doar în cazul când aceste elemente s-au manifestat în comportamentul antisocial.

Așadar, prevenirea individuală trebuie să fie îndreptată asupra personalității și a trăsăturilor ei negative, asupra mediului care determină formarea

personalității, precum și asupra împrejurărilor, condițiilor, situațiilor, care favorizează comiterea faptelor penal-condamnabile.

Materiale utilizate și metode aplicate. În procesul elaborării articolului științific ne-am ghidat de mai multe metode de cercetare științifică care au făcut posibilă investigarea corespunzătoare a subiectului, dintre care putem enumera: metoda analizei, metoda sintezei, metoda deducției, metoda sistemică, metoda istorică, precum și metoda comparativă.

Baza teoretico-juridică a demersului științific cuprinde literatura de specialitate atât autohtonă, cât și străină, care direct sau indirect, abordează esența și conținutul generic al tematicei supuse analizei.

Rezultatele obținute în baza analizelor științifice efectuate. În cazul prevenirii individuale a infracțiunilor de fraudă informatică, aceasta este orientată asupra delicvenților care se află la etapa personalității criminale deja formate. În orientarea lor socială predomină acel component negativ care determină alegerea unei căi infracționale de satisfacere a necesităților. La etapa dată are loc formarea motivației criminale, care se poate realiza prin pregătirea, tentativa sau prin fapta infracțională consumată. Din aceste considerente, prevenirea individuală a infracțiunilor constă, în primul rând, în preîntâmpinarea infracțiunilor concepute și pregătite.

O sarcină majoră în cazul prevenirii individuale a infracțiunilor de fraudă informatică o constituie stabilirea obiectivului care urmează a fi supus prevenirii. Deși nu există o opinie unică în acest domeniu, totuși majoritatea savanților consideră că prevenția individuală se realizează în privința persoanelor care:

- nu comit fapte ilicite, dar se află în condiții nefavorabile, sub influența cărora ar putea comite asemenea fapte;
- duc un mod de viață antisocial, comit delicte ce nu prezintă un pericol social sporit;
- se caracterizează prin formarea motivelor și scopurilor infracționale, pregătirea unei infracțiuni concrete;
- au început comiterea infracțiunii, dar n-au dus-o până la capăt;
- au săvârșit infracțiunea și pot admite recidivul;
- au fost eliberate de la răspundere și pedeapsă penală în modul prevăzut de lege;
- au ispășit pedeapsa sub forma privativă de libertate.

Astfel, calitatea de persoană predispusă la comiterea infracțiunii de fraudă informatică prevede anumite particularități.

Vorbind de personalitatea potențialului făptuitor al infracțiunii de fraudă informatică, putem menționa faptul că infractorii care săvârșesc asemenea infracțiuni sunt, de regulă, cetățeni care prin statutul lor se află deasupra oricăror suspiciuni. Ei comit actele criminale în legătură cu afacerile, cultura și mediul lor profesional, sunt conștienți de caracterul legal ori ilegal al conduitei lor, dar nu se consideră infractori, fiind convinși că rațiunea și rentabilitatea primează în fața legii. Astfel se poate spune că ei consideră că au un drept personal, în virtutea poziției sociale pe care au dobândit-o, de a încălca legea. Un asemenea comportament este învățat în interacțiunea cu alte persoane în procesul comunicării, iar direcțiile specifice ale motivelor și impulsurilor sunt învățate din conținutul legilor, care sunt favorabile sau nefavorabile.

Atitudinea societății și reacția sa față de aceste infracțiuni deseori îi încurajează pe infractori. Astfel, scopul principal urmărit de infractori este reușita, succesul social sau financiar. În realizarea acestui scop, chiar dacă există și mijloace legale, mijloacele ilegale sau imorale nu sunt excluse, în măsura în care sunt eficace și eficiente, astfel, vechiul principiu machiavelic „scopul scuză mijloacele" este permanent în actualitate. Reacția societății față de criminalitatea dată este, de asemenea, reținută comparativ cu reacția față de criminalitatea clasică[1].

În acest context, putem menționa faptul că profilaxia individuală nu-și va atinge scopul fără o studiere profundă a particularităților fiecărei persoane în parte. O asemenea studiere poate fi efectuată numai în urma adunării informației cu caracter biografic despre o anumită persoană, informației obținute din diferite surse despre comportamentul la serviciu, în cercul de prieteni, rude, vecini. O asemenea studiere va permite de a prognoza comportamentul probabil, posibil al persoanei, de a alege cele mai raționale și adecvate măsuri de preîntâmpinare pe cazul dat.

Elementele principale ale profilaxiei individuale a infracțiunilor date sunt:

- relevarea persoanelor predispuse la comiterea infracțiunilor;
- studierea prin utilizarea forțelor, mijloacelor și măsurilor speciale de investigații a contingentului de persoane, aflat sub supraveghere profilactică;
- documentarea faptelor și împrejurărilor, a acțiunilor și comportamentului acestor persoane, care asigură succesul măsurilor profilactice individuale;
- înfăptuirea proactivă a măsurilor speciale cu scopul stabilirii semnalmentelor de pregătire de comitere a infracțiunilor, a intențiilor sau a activității criminale a

[1] Voicu C., Sandu F., Boroi A., Molnar I. *Drept penal al afacerilor*, București: Editura Rosetti, 2002, p. 8.

persoanelor, aflate sub supraveghere specială, complicitatea lor la comiterea infracțiunilor, rămase nedescoperite[2].

Persoanele predispuse de a comite infracțiuni se depistează în procesul activității cotidiene contravenționale, speciale de investigații, de urmărire penală și profilactice.

În scopul primirii oportune a informațiilor despre asemenea persoane, se stabilește o legătură permanentă cu alte instituții cu atribuții în domeniul combaterii criminalității.

Datele despre persoanele predispuse de a comite infracțiuni se conțin în:

- condițiile și registrele de evidență a evenimentelor, persoanelor reținute și aduse la poliție, de înregistrare a materialelor de urmărire penală;
- materialele despre refuzul pornirii urmăririi penale sau procedurii de supraveghere asupra dosarelor penale finisate sau clasate, materialele privind contravențiile administrative;
- comunicările, avizele și alte documente parvenite din subdiviziuni ale organelor afacerilor interne, instituțiile penitenciare, comenduirile speciale;
- petițiile cetățenilor și administrației întreprinderilor, instituțiilor, organizațiilor, materialele din presă, radio și televiziune;
- sentințe, decizii, hotărâri ale instanțelor judecătorești;
- comunicările colaboratorilor confidențiali;
- informațiile acumulate în timpul petrecerii operațiunilor tip, prin înfăptuirea măsurilor speciale de investigații, din sondaje.

Relativ recent s-a extins categoria tinerilor competenți în calculatoare, care, de acasă, pot accesa sistemele mari, considerând acțiunile lor ca un test de isteține, devenit din ce în ce mai periculos.

Noua categorie de infractori care acționează în spațiul cibernetic nu este compusă din persoane speciale. Criminalii electronici nu reprezintă doar o schimbare de nume în ceea ce privește abordarea infracțiunilor tradiționale într-o formă nouă. Infractorii digitali, ca de altfel și faptele comise de aceștia, reprezintă o transformare fundamentală în felul nostru de a aborda problema crimei și criminalității[3].

Categorii de infracțiuni, care formează acum un nou tip de criminalitate, sunt comise tot de oameni, tot cu vinovăție, și au în vedere, de regulă, realizarea unor beneficii patrimoniale.

---

[2] Горяинова К.К., Овчинскова В.С., Шумилова А.Ю. *Оперативно-розыскная деятельность*: Учебник. Москва, ИНФРА-М, 2002, стр. 573.

[3] Amza Tudor, Amza Cosmin. *Criminalitatea informatică*. București: Ed. Lumina Lex, 2003, p. 58.

Experții occidentali în analiza criminalității informatice propun luarea în considerare a patru categorii de bază în care pot fi împărțiți acești indivizi: Hackeri; Phreaks și crackeri; Traficanții de informații și mercenarii; Teroriștii și devianții.

Ce este un hacker? La prima vedere pare o întrebare foarte ușoară, cu un răspuns simplu și clar, de genul: „indivizi diabolici, pe care-i vezi la TV sau despre care citești în ziare, acuzați că au spart sistemul informatic al unei bănci, au reprogramat sateliți militari, au lansat viruși informatici etc.”[4].

În mass-media, aproape fără excepție, cuvântul hacker este sinonim cu cel de criminal informatic. Filmele făcute la Hollywood ajută din plin la încetățenirea acestei imagini, deoarece îi distribuie pe hackeri în rolurile celor mai sofisticați criminali. În altele, hackerii apar ca genii informatice, care pot salva omenirea de la distrugere. În consecință, confuzia publicului este maximă: pe de o parte, hackerii sunt niște cybercriminali care pot duce la distrugerea civilizației, pe de altă parte, sunt niște genii care conduc societatea spre progrese nemaiîntâlnite.

Problema este și mai mult complicată de faptul că nici măcar hackerii „adevărați” nu sunt de acord cu o definiție precisă. Peter Sommer, coautor al cărții Hackers Handbook, definește hackerul în evoluție: în primii ani ai deceniului șapte era „nonconformistul, neconvenționalul și programatorul foarte inteligent”, dar în timp a început să fie „aventurierul rețelei”, iar de pe la mijlocul anilor 80, a început să fie sinonim cu „criminalul informatic”.

Alți autori utilizează termenul în sens și mai larg pentru a-i descrie pe cei care utilizează mijloace ascunse și malițioase împotriva autorităților. Chiar și protestatarii împotriva armelor nucleare care au dat jos gardurile de sârmă ghimpată au fost considerați hackeri.

Cercetările în domeniu au dus la perceperea unei caracteristici pe care o au în comun hackerii: ei nu sunt nici mai mult nici mai puțin decât exploratori – echivalentul actual al botaniștilor – care investighează lumea digitală, și nu pe cea naturală.

A fi hacker nu este neapărat diabolic (ilegal, criminal) și hackerii preferă să utilizeze cuvinte ca phreaker sau cracker pentru a-i descrie pe cei care se abat de la calea legală. Dacă ținem seama de motivația și amenințările prezentate de acțiunile lor, categoriile de hackeri ar putea fi mai multe[5]. Cea mai numeroasă categorie a lor este cea constituită pe rațiuni sociale. Grupul are o mentalitate de „bandă” și este puternic mânat de ideea de a face/ a fi ceva special, prin care să-și asigure faima și/sau celebritatea.

[4] Vasiu Ioana. *Totul despre Hackeri*. București: Ed. Nemira, 2000, p. 5.
[5] *Ibidem*, p. 12.

Un alt grup este cel format din cei care acționează din rațiuni tehnice. Mulți din primul grup ar dori să facă parte și din acesta, dar, în realitate, puțini se ridică la nivelul cerut. Din acest grup fac parte hackeri care vor să ajute la evoluția tehnologiei, să fie un element al progresului. Ei consideră că, penetrând sisteme informatice și arătând slăbiciunile acestora, sunt capabili să forțeze rezolvarea problemelor de către firmele implicate.

Un al treilea grup important de hackeri este constituit în jurul motivațiilor politice. Și în acest caz întâlnim o dorință arzătoare a unei părți din primul grup de a fi considerată parte a categoriei „politice" hackerilor. Persoanele din acest grup au puternice simțăminte, atașamente politice sau fac față unor regimuri politice dure. Aceștia penetrează sisteme informatice alese în funcție de credințele lor politice, pentru a-și face cunoscute opiniile. Este foarte greu de spus care sunt cu adevărat implicați politic și care nu. La fel de greu de distins, în anii 1960, erau cei care au devenit hippies din cauza războiului – ca un fel de revoltă și protest politic – de cei care au făcut-o din cu totul alte motive, ori din simplă imitație.

O subcategorie importantă din cadrul acestui grup este cea a teroriștilor informatici (o demarcație fină între activiștii politici și teroriști).

Grupul patru este rezervat hackerilor care urmăresc câștiguri personale. Spionajul corporatist, instituții financiare, chiar persoane care se ocupă cu distribuirea programelor piratate pentru calculator. Hackerii din acest grup fac tot ce este posibil pentru a-și ascunde preocupările.

A cincea categorie, având motivații guvernamentale, împinge categoria a treia la un nivel mai înalt. Aici sunt incluse acte comise de un guvern contra altuia. Războiul informațional și spionajul guvernamental intră în această categorie.

Phreaker – este un hacker care se concentrează pe sistemele de telefonie, intrând neautorizat pe convorbirile de interior dintr-o companie sau folosind generatoare de ton pentru a efectua convorbiri internaționale pe gratis.

Etimologic, cuvântul a apărut din combinația Phone Breaker. Phreaking este termenul desemnat pentru următoarele acțiuni:

- arta și știința de a pătrunde (neautorizat) în rețeaua de telefonie (pentru a face ilegal și gratuit apeluri internaționale);
- spargerea sistemelor de securitate în orice alt context (în special, dar nu exclusiv, în rețelele de telecomunicații).

Crackerii reprezintă categoria de infractori care reușesc să pătrundă în sistemele informatice ale unei organizații, instituții sau companii, prin violarea sistemelor de securitate[6].

[6] Amza Tudor, Amza Cosmin. *Criminalitatea informatică*. București: Ed. Lumina Lex, 2003, p. 60.

Aceștia realizează conectarea de la distanță prin intermediul unui computer și a unui modem. Pentru a-și atinge scopurile, crackerii fac adesea apel la rețeaua publică de telecomunicații, prin intermediul căreia realizează conexiunea cu sistemul informatic vizat.

Ca o caracteristică, crackerii folosesc sistemele de comunicații și calculatoarele până la ultimele limite, iar dacă au reușit să pătrundă în pragul computerului nu se dau înapoi de la comiterea unor fapte grave, cu repercusiuni deosebite asupra acestuia, ca de exemplu: introducerea de viruși și cai troieni în sistem, furtul de date confidențiale, etc.

Dacă la începuturi rețeaua Internet era atacată, de regulă, din incinta universităților, fiindcă doar acestea aveau acces la ea, acum situația este cu totul alta, crackerii putând sparge o rețea de aproape oriunde: de acasă, din mașină sau de la serviciu.

Traficanții de informații și mercenarii sunt o altă categorie. Spre deosebire de hackeri, traficanții de informații și mercenarii comit infracțiuni de pe urma cărora realizează profituri financiare sau alte avantaje patrimoniale mari. Ei se ocupă cu spionajul economic și vând concurenței secretele firmelor ale căror rețele reușesc să le penetreze.

Deși folosesc aceleași metode de pătrundere în rețelele informatice și aceleași instrumente, traficanții de informații și mercenarii comit faptele lor cu intenție criminală de la bun început, urmărind realizarea unor profituri considerabile. Deseori, cei care comit aceste fapte sunt angajați de firmele concurente sau sunt chiar salariați ai companiilor ale căror informații le sustrag.

În rândul acestor infractori intră și acele categorii de persoane care folosesc un sistem de comunicații prin cablu în scopuri ilegale și pentru a obține profit.

Profitul sau avantajul patrimonial urmărit în cursul acestei activități infracționale este indicatorul de bază care face deosebirea de ceilalți atacatori cibernetici. Indivizii care fac parte din această categorie de cybercriminali își desfășoară activitatea prin pătrunderea ilegală în sistemele de computere de unde extrag informații sau de unde realizează transferuri ilegale de fonduri financiare, dar, frecvent, ei realizează și furturi de identitate pentru a-și acoperi urmele în cursul operațiunilor. Furtul de identitate este folosit, totodată, și pentru efectuarea unor operațiuni frauduloase în sistemele financiar-bancare, pentru a achiziționa bunuri sau servicii în sistem online ori chiar pentru trecerea frauduloasă a frontierelor, pentru a se sustrage de la unele servicii publice sau de la unele interdicții dictate în urma unor hotărâri judecătorești. Alți autori relevă următoarele tipuri de infractori digitali.

Delapidatorii au devenit „hoți informatici” printr-o explicație foarte simplă: înregistrările la care trebuie să ajungă și modalitățile de acoperire a faptelor sunt realizabile cu ajutorul calculatorului[7].

De regulă, delapidatorii sunt de vârstă mijlocie, cu destulă credibilitate în cadrul organizației în care își desfășoară activitatea, câștigată îndeosebi printr-o prezentă îndelungată în aceeași unitate. Sunt buni cunoscători ai măsurilor antifurt și de control al fraudelor, iar locul lor de muncă le permite să aibă acces legal în sistemele informatice sau la valorile patrimoniale publice ori private. De cele mai multe ori, ei se cred neglijați, mai ales că nu ocupă o funcție mai bună în sistem.

Totul începe de la existența unor probleme personale de natură financiară, prin îmbolnăvirea unor membri ai familiei sau datorită unor mofturi pe care nu și le permit să și le satisfacă, dorinței de a trăi „pe picior mare”. Totuși, pe ultima sută de metri, operează bunul-simț. După ce provoacă o pagubă mai însemnată, ei se opresc din activitatea infracțională pentru o foarte bună bucată de timp.

Detractorul este un adevărat „hoț informatizat” și lucrează adesea în domeniul prelucrării automate a datelor. În majoritatea cazurilor, detractorul este un bărbat în jurul vârstei de 35 de ani. Salariul său se situează, ca mărime, în prima jumătate a salariilor din firmă. Vechimea sa în organizație nu este mai mare de trei ani. Locuiește într-un cartier respectabil, este căsătorit și, eventual, are 1-2 copii. S-a ocupat de „șterpeliri” timp de aproximativ 18 luni și a obținut venituri din această activitate ce reprezintă aproximativ 120 de procente din venitul său anual. Este capabil să conducă un centru de calcul sau să fie șeful echipei de programare sau de exploatare a sistemului informatic. Motivația faptelor sale poate fi una de natură egocentrică sau, în virtutea poziției pe care o ocupă, consideră că este normal să execute lucrări personale în sistem, să vândă software sau orice altceva.

Trișorul, de regulă, este femeie. De cele mai multe ori, este singurul părinte al unuia sau a doi copii și poate să aparțină, în mod vizibil, unor grupuri minoritare. Vârsta este între 25 și 35 de ani. Profesia este cea de responsabil introducere date și, prin prisma acesteia, are posibilitatea să-și adauge drepturi bănești suplimentare, pe care de multe ori le împarte unor societăți caritabile. Pare să aibă și o motivație ideologică sau să acționeze sub un sindrom invers „Robin Hood”.

În cele mai multe dintre cazurile înregistrate, trișorul a operat pe un anumit scenariu timp de doi ani, apoi a abandonat activitatea infracțională.

O altă categorie sunt teroriștii și extremiștii. Așa cum practica a dovedit-o, mulți criminali care acționează în spațiul cibernetic folosesc sistemul de

[7] Oprea D. *Protecția și securitatea informațiilor*. Iași: Ed. Polirom, 2003, p. 162.

comunicare prin cablu în scopuri politice sau pentru realizarea unor activități care sunt scoase în afara legii [8].

Caracteristica acestui grup de infractori este aceea că, spre deosebire de primele două, folosesc sistemele informatice pentru a promova acțiunile teroriste, inclusiv prin mijloace electronice, cât și pentru a propaga idei care să promoveze ura de rasă sau ura între anumite organizații, pentru a instiga mase de oameni la un comportament social ilegal, așa cum ar fi transmisiile de imagini cu pornografie infantilă sau încurajarea pornografiei online.

Deseori, activitatea lor încalcă granița dintre libertatea de expresie și faptele ilicite.

Măsurile profilactice individuale se desfășoară conform planului, eficient și hotărât, cu folosirea tuturor forțelor și mijloacelor, pentru a exclude formarea intențiilor criminale la persoana supusă profilaxiei.

În cadrul profilaxiei individuale ofițerii de investigații fac următoarele activități cu caracter individual profilactic:

- supravegherea comportamentului și modului de viață în familie, la locul de trai și de muncă;
- influența de ordin educativ, prin petrecerea convorbirilor, formarea încrederii că delictele antisociale și purtarea analogică se condamnă de societate și vor rămâne nepedepsite;
- folosirea posibilităților administrațiilor, întreprinderilor, organizațiilor, cât și a societății la locul de trai și de serviciu a persoanei supuse profilacticii, pentru influență educațională;
- stabilirea rudelor și cunoștințelor care ar putea să influențeze pozitiv asupra persoanelor supuse profilacticii și atragerea lor la asemenea convorbiri;
- folosirea confidenților și persoanelor de încredere, care cunosc persoanele supuse profilacticii pentru verificarea modului de viață și comportării la locul de trai și serviciu, pentru realizarea influenței educaționale, cât și pentru identificarea indivizilor care influențează negativ asupra lor;
- reacționarea la contravenții și alte acțiuni ilicite;
- efectuarea măsurilor profilactice în privința persoanelor din cercul apropiat care-i instigă la comiterea contravențiilor și alte acțiuni ilicite, încetarea influenței negative din partea acestor persoane;
- încetarea influenței demoralizatoare a persoanelor supuse profilacticii asupra altor persoane care-l înconjoară[9].

[8] Amza Tudor, Amza Cosmin. *Criminalitatea informatică*. București: Ed. Lumina Lex, 2003, p. 6

[9] Лукашов В.А. *Оперативно-розыскное предупреждение преступлений.* Москва, 1991, стр.

În concluzie, considerăm că succesul creării unei societăți informatice depinde, în mare parte, de soluționarea unui spectru de probleme juridice, economice și organizaționale, cum ar fi:

1) elaborarea și definirea unei terminologii unice în domeniul securității informatice și a dreptului informatic;
2) analiza practicilor moderne și armonizarea actelor normative în vigoare cu practicile internaționale, și anume armonizarea în materie de documentare a dovezilor și de reproducere a înregistrărilor informatice – societatea informațională are nevoie de un drept specific evoluat;
3) reglementarea tranzacțiilor electronice. Elaborarea unui cadru legal adecvat pentru afaceri, care să reglementeze nu numai comerțul electronic și semnătura electronică, ci și aspectele referitoare la banii electronici, fiscalitatea și modul de încheiere a contractelor în Internet;
4) elaborarea tehnicilor și metodologiilor de investigare a infracțiunilor informatice. Datorită caracterului transfrontalier al criminalității informatice, armonizarea legislației cu cea internațională trebuie să vizeze, în principal, dreptul de autor, confidențialitatea datelor, prevenirea și combaterea criminalității informatice, precum și promovarea standardelor tehnice care să asigure intercomunicarea noilor rețele de comunicații.
5) crearea programelor de studiu și pregătirea specialiștilor în domeniul securității informatice;
6) crearea în structurile de stat a funcțiilor responsabile pentru implementarea și administrarea mecanismelor de securitate informațională;
7) organizarea seminarelor de aprofundare a cunoștințelor și de schimb de experiență cu specialiștii în domeniu din alte țări.

Bibliografie

1. Amza Tudor, Amza Cosmin. *Criminalitatea informatică*. București: Ed. Lumina Lex, 2003.
2. Oprea D. *Protecția și securitatea informațiilor*. Iași: Ed. Polirom, 2003.
3. Voicu C., Sandu F., Boroi A., Molnar I. *Drept penal al afacerilor*. București: Editura Rosetti, 2002.
4. Vasiu Ioana. *Totul despre Hackeri*. București: Ed. Nemira, 2000.
5. Горяинова К.К., Овчинскова В.С., Шумилова А. Ю. *Оперативно-розыскная деятельность: Учебник.* Москва: ИНФРА-М, 2002.
6. Лукашов В.А. *Оперативно-розыскное предупреждение преступлений,* Москва, 1991.