SCURTĂ INCURSIUNE ÎN CARACTERISTICA CRIMINALISTICĂ A INFRACȚIUNILOR INFORMATICE

SHORT INTRODUCTION TO THE FORENSIC CHARACTERISTICS OF CYBERCRIMES

Boris TALPĂ, doctorand,
Universitatea de Stat din Moldova

Summary: The development of the Internet has determined both the transformation of the society into an informational society, as well as the occurrence of the phenomenon of globalization. The informational society operates in a computer space called cyberspace. In this study, a brief forensic characteristic of the phenomenon of cybercrime was realized, the essence and the negative impact of these crimes on the society were explained. The author points out that these types of crimes are committed by malicious persons, regardless of age, without any territorial limit and with any type of computer systems in their diversity.

Keywords*: computer crimes, computer crime, computer system, computer viruses, botnet, cyberspace, criminal investigation body, forensic investigation, mode of operation, material means of evidence.*

Potrivit raportului cu privire la Indicele Global Cybersecurity (GCI v3) realizat și analizat de către Uniunea Internațională a Telecomunicațiilor, Republica Moldova s-a clasat pe locul 31 la nivel regional şi pe locul 53 la nivel global, aceasta fiind printre țările care au dezvoltat angajamente complexe și se angajează în securitatea informatică, programe și inițiative.

Acest indice este axat pe politicile guvernamentale și structurile legislative ale UE și reprezintă o referință de încredere ce măsoară angajamentul țărilor pentru securitatea cibernetică la nivel global cu scopul de a crește gradul de conștientizare cu privire la importanța și dimensiunile diferite ale problemelor existente [1].

Datorită finanțărilor externe, privatizării rețelelor de telefonie, una din condițiile Băncii Mondiale, care au dus la modernizarea acestora, inclusiv prin utilizarea fibrei optice, au avut ca efect clasarea Republicii Moldova pe locul trei din lume după viteza de acces la Internet, potrivit clasamentului Net Index, elaborat de compania Ookla, care administrează serviciul Speedtest, fiind depășită de așa țări dezvoltate ca Singapore și Coreea de Sud [2].

Totuși, evoluția tehnologiei informației și sistemelor informatice aflată în pronunțata accesiune, și-a pus amprenta asupra tuturor domeniilor vieții sociale, economice, civile etc., influențând decisiv progresul umanității. Acest adevărat *”cyberspațiu”* oferă pe lângă multiplele avantaje, posibilitatea săvârșirii de infracțiuni într-o altfel de modalitate decât cea tradițională.

Criminalitatea în mediul virtual, generic denumită *e-crime* sau *cybercrime* a cunoscut o evoluție dramatică, acestui fenomen putem distinge patru etape, și anume:

- **prima** *(specifică anilor* ***'80),*** *care a fost* ***caracterizată*** *de* **banalizarea informaticii, piratarea programelor, falsificarea cărţilor de credit** *etc.;*

- *a doua* (specifică sfârşitului anilor '80), a fost favorizată de apariţia reţelelor locale şi extinse, precum şi a punţilor de legătură, şi caracterizată de importante *deturnări de fonduri şi „isprăvile" hacker-ilor* care accesau calculatoarele NASA, CIA şi oricare altă ţintă care reprezenta un simbol politico-tehnologic sau un element al puternicului complex militaro-industrial american;

- *a treia* (specifică anilor '90), care a coincis cu proliferarea sistemelor informatice şi reţelelor de comunicaţii (Internet-ului, în special) şi a fost caracterizată de *specializarea infractorilor,* apariţia unor „veritabili" profesionişti ai pirateriei, deturnărilor de fonduri, sabotajelor informatice;

- *a patra* (în prezent), favorizată de faptul că sistemele informatice au pătruns în toate sectoarele vieţii sociale şi le controlează pe cele mai importante dintre ele (transporturi, apărare, etc.), şi care este caracterizată de conturarea de *noi şi grave ameninţări* ca *terorismul informatic, războiul informatic etc.* [3, p.53].

Reglementarea infracțiunilor informatice în legislația națională a venit ca o adaptare firească a legislației la realități ce nu puteau fi ignorate. Astfel, în Codul penal al Republicii Moldova, adoptat prin Legea nr. 985 din 18.04.2002, în vigoare din 12.06.2003 în premieră a fost introdus capitolul "*Infracțiuni informatice și Infracțiuni în domeniul telecomunicațiilor*", care cuprindea inițial trei articole: art. 259 – Accesul ilegal la informația computerizată; art. 260 – Producerea, importul, comercializarea sau punerea ilegală la dispoziție a mijloacelor tehnice sau produselor program și art. 261 - Încălcarea regulilor de securitate a sistemului informatic.

După ratificarea Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23.11.2001, prin Legea nr. 6 din 02.02.2009, Codul penal al R.Moldova, fiind armonizat în conformitate cu prevederile Convenției prin Legea nr 278 din 18.12.2008, ambele publicate în MO la 20.02.2009, a fost suplinit cu articole noi 260^1-260^6, care prevedeau noi tipuri de infracțiuni cum ar fi interceptarea ilegală a unei transmisii de date, perturbarea funcționării sistemului informatic, falsul informatic, frauda informatică, etc. [4].

Convenţia încearcă, în principal, să armonizeze dispoziţiile de drept substanţial cu caracter penal în domeniul informatic, să implementeze dispoziţii procedurale necesare pentru investigarea şi urmărirea unor asemenea infracţiuni şi să pună la punct un sistem rapid şi eficient de cooperare internaţională.

Dacă în primul capitol al Convenţiei se dau înţelesul unor termeni şi expresii, apoi capitolul doi se referă atât la incriminarea unor fapte ca infracţiuni,

cât şi la alte aspecte de drept penal material, referitoare la răspunderea penală, participaţie şi sancţiuni.

Sunt definite nouă infracţiuni grupate în patru categorii diferite. Astfel, sunt considerate infracţiuni ce aduc atingere confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice: accesarea ilegală (art. 2), interceptarea ilegală (art. 3), alterarea integrităţii datelor (art. 4), alterarea integrităţii sistemului (art. 5) şi abuzurile asupra dispozitivelor (art. 6). Sunt prevăzute ca infracţiuni în legătură cu mediul informatic falsificarea informatică (art. 7) şi frauda informatică (art. 8). O altă categorie de infracţiuni se referă la pornografia infantilă (art. 9), iar ultima categorie face referire la infracţiuni care aduc atingere proprietăţii intelectuale şi drepturilor conexe (art. 10).

Secţiunea a II-a a Capitolului al II-lea se referă la dispoziţii procedurale în materie penală, aplicabile în cazul săvârşirii infracţiunilor indicate, în cazul săvârşirii oricărei infracţiuni de drept comun prin intermediul sistemelor informatice ori în situaţiile în care dovada săvârşirii oricărei infracţiuni se regăseşte stocată într-un sistem informatic. Totodată, se stabilesc condiţiile şi măsurile de protecţie. Astfel, se instituie măsuri privind conservarea rapidă a datelor informatice stocate (art. 16), privind conservarea şi dezvăluirea parţială rapidă a datelor referitoare la trafic (art. 17), privind ordinul de punere la dispoziţie a datelor (art. 18), privind percheziţia şi sechestrarea datelor informatice stocate (art. 19), privind colectarea în timp real a datelor referitoare la trafic (art. 20), precum şi privind interceptarea datelor referitoare la conţinut (art. 21). De asemenea, sunt prevăzute dispoziţii referitoare la competenţă.

Capitolul al III-lea conţine dispoziţii privind asistenţa judiciară internaţională în materie penală în privinţa infracţiunilor săvârşite prin mijloace informatice, incluzând şi dispoziţii referitoare la extrădare. De asemenea se pun bazele unei reţele de cooperare care să funcţioneze non-stop între statele semnatare, pentru a prelua şi rezolva cu promptitudine cererile de asistenţă judiciară [5, p.74].

Săvârșirea faptelor descrise supra presupune, inclusiv sub raport informatic, moduri de operare specifice fiecărui delict cibernetic în parte. Cea mai mare provocare o constituie dificultatea stabilirii făptuitorului, întinderea și impactul actului infracțional. Deficiențele reglementărilor procesual-penale de acest domeniu și lipsa de cunoștințe privind tehnologiile informaționale moderne în rândul ofițerilor de urmărire penală, facilitează menținerea nivelului ridicat de latență.

În sensul legii privind prevenirea si combaterea criminalității informatice nr. 20 din 03.02.2009, prin sistem informatic se înțelege orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor [6]. Astfel, o infracțiune informatică, în zilele noastre, poate fi comisă nu numai prin intermediul computerului propriu zis, care

este utilizat în activitățile zilnice, ci și prin diversitatea dispozitivelor mobile (celulare) de comunicare și sisteme de comunicații.

Potrivit aceleiași surse prin date informatice se înțelege orice reprezentare de fapte, informații sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic.

În ceea ce privește definirea noțiunii de criminalitate informatică, consider că cea mai reușită și cuprinzătoare variantă este prezentată în ”Ghidul introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică”. De altfel, definiție, ce se regăsește și în documentele Organizației Națiunilor Unite [7, p.74].

Prin infracțiune informatică în sens larg se înțelege: „orice infracțiune în care un calculator sau o rețea de calculatoare este obiectul unei infracțiuni, sau în care un calculator sau o rețea de calculatoare este instrumentul sau mediul de înfăptuire a unei infracțiuni”.

Prin infracțiune informatică în sens restrâns se înțelege: „orice infracțiune în care făptuitorul interferează, fără autorizație, cu procesul de prelucrare automată a datelor”.

Și, dacă am tot menționat supra despre sisteme informatice, date informatice etc, consider că este momentul pentru a face o succintă incursiune în arhitectura sistemelor de calcul, mediilor de stocare, dispozitivelor periferice, rețelelor de calculatoare și elementelor de interconectare a acestora etc. Or, principalele probleme care trebuie clarificate în cadrul investigării infracțiunilor informatice se referă la identificarea mijloacelor și utilajelor tehnice de accesare care au fost folosite sau au fost destinate să servească la comiterea faptei, a informațiilor obținute în urma acțiunii ilegale, a hardware-ului ca rezultat al delictului ce face parte din categoria corpurilor delicte, respectiv identificarea făptuitorului și a eventualilor participanți.

Calculatorul electronic sau PC – principala sursă de informații pentru un investigator, constituie un echipament capabil de a procesa informații, de a efectua calcule complexe și a stoca informațiile pe unitățile de hard-disc. Cele mai des utilizate sunt calculatoarele PC și cele portabile cum ar fi: laptop, Poket PC, Palm, și altele. Toate calculatoarele au compartimentele Hard și Soft.

Compartimentul Soft constituie totalitate sau o parte a programelor, procedurilor, regulilor şi documentelor asociate ale unui sistem de prelucrare a informaţiei [8]. Acesta include sistemul de operare – cel mai important program, care în mod obligatoriu trebuie rulat pe un calculator (Microsoft Windows, Apple Macintosh, Linux, etc), alte produse program necesare utilizatorului pentru satisfacerea necesităților sale în lucru cu calculatorul.

Compartimentul Hard constituie echipamente, mijloace tehnice destinate sistemelor de calculatoare [8]. În calitate de unități hard pot fi: placa de bază,

microprocesorul, controllerul, *HARD-discul* (ROM – Read Only Memory), memoria internă a calculatorului; *memoria RAM* (Random Access Memory) sau memoria operativă, ea reprezintă un spațiu temporar de lucru, iar programele și datele se vor pierde odată cu deconectarea calculatorului; *memoria Cache* – care este mai apropiată de microprocesor decât de memoria internă, blocul de alimentare ș.a. [8].

Medii de stocare externe stick-uri de memorie în toată diversitatea lor, CD-ROM, DVD-ROM, discuri SDD portabile sau detașabile ș.a. destinate pentru stocarea, păstrarea și transportarea informației computerizate.

Dispozitive periferice – asigură introducerea în calculator a informațiilor de pe suporturi externe și extragerea informațiilor din calculator și depunerea lor pe suporturi externe. În calitatea de dispozitive periferice de intrare pot fi tastatura, mouse-ul, microfonul, creionul optic, touchpad, joystick. Dispozitivele periferice de ieșire sunt monitorul, imprimantele de diferite modele și construcții, scanerul, plotter-ul etc.

Rețea de calculatoare constituie ansamblu de noduri de prelucrare a datelor interconectate în scopul transportului de date. [8] O altă noțiune utilizată este lucrul în rețea, care reprezintă conceptul de conectare a unor calculatoare, care partajează resurse. Calculatoarele dintr-o rețea se împart în servere. Rețelele sunt clasificate după mai multe criterii dar în primul rând după întinderea geografică care poate fi de la câțiva metri până la câteva mii de kilometri. Astfel după tehnologia de transmisie sunt rețele cu difuzare și rețele punct-la-punct; după scara la care operează (distanța) se cunosc rețele locale LAN (Local Area Network), rețele metropolitane MAN (Metrou Area Network), rețele de arie întinsă WAN (Wide Area Network) și Internetul; după topologie rețelele se clasifică în 4 tipuri: magistrală, stea, inel și combinate; după tipul sistemului de operare utilizat se cunosc rețele *peer-to-peer* și rețele bazate pe server.

Infracțiunile informatice, se clasifică în dependență de rolul pe care l-au avut sistemele informatice:

1. infracțiuni săvârşite cu ajutorul sistemelor informatice, în care respectivele constituie un instrument de facilitate a comiterii unor infracțiuni.

Este vorba de infracțiuni „tradiționale” desăvârșite prin utilizarea sistemelor informatice și în care ”*modus operandi*” nu este îndreptat împotriva funcționării corespunzătoare a unui sistem informatic sau asupra informațiilor cuprinse în el, ci rezultatul procesării datelor este utilizat pentru înfăptuirea infracțiunilor clasice. Făptuitorii astfel fac apel la mijloace netradiționale pentru înfăptuirea unor infracțiuni cu caracter ”tradițional”. Din acestea fac parte infracțiunile de spălarea banilor, fabricarea sau punerea în circulaţie a semnelor băneşti false sau a titlurilor de valoare false, confecţionarea, deţinerea, vânzarea sau folosirea documentelor oficiale, a imprimatelor, ştampilelor sau sigiliilor false, ș.a.

2. infracțiuni săvârşite prin intermediul sistemelor informatice, în care acestea, incluzând și datele stocate în acestea, constituie ținta infracțiunii.

Din acestea fac parte infracțiunile de acces ilegal la informaţia computerizată, interceptarea ilegală a unei transmisii de date informatice, perturbarea funcţionării sistemului informatic, falsul informatic, frauda informatică, ș.a. [9].

Aria infracțiunilor informatice este extrem de întinsă, ea variind de la catastrofe până la sustrageri neînsemnate. Ele sunt comise, de regulă, pentru a provoca daune, iar modurile de operare întâlnite în criminalitatea informatică se realizează prin intermediul unor atacuri asupra sistemelor şi reţelelor informatice.

Un atac asupra unui sistem informatic se realizează, prin următorii paşi:

1. *Cercetarea sistemului informatic în vederea obţinerii de informaţii.*

Primul pas în cadrul unui atac informatic, îl reprezintă cercetarea sistemului informatic pentru a obţine informaţii importante care pot fi utilizate în atac. Așadar, este important să se obţină informaţii, cum ar fi de exemplu tipul hardware-ului utilizat, versiunea software, informaţii personale ale utilizatorilor, care pot fi utilizate în următorul pas. Acţiuni utile în obţinerea informaţiilor includ: „*ping sweeps*" (metodă de a scana reţeaua) pentru a determina dacă sistemul informatic ţintă răspunde; scanarea porturilor pentru a observa care porturi pot fi deschise; întrebări care trimit mesaje de avariere înapoi la sistem, când o problemă de transmitere a fost detectată; ghicirea parolelor.

2. *Pătrunderea în sistemul informatic*

Imediat ce sistemul informatic ţintă a fost identificat, iar informaţiile despre el au fost adunate, următorul pas este de a lansa atacul în scopul pătrunderii în sistem.

3. *Modificarea setărilor sistemului informatic*

Modificarea setărilor sistemului informatic reprezintă următorul pas după ce s-a pătruns în sistemul informatic. Acest pas permite atacatorului să reintre în sistemul informatic compromis mult mai uşor.

4. *Comunicarea cu alte sisteme*

Odată ce reţeaua sau sistemul informatic au fost compromise, atunci atacatorul le utilizează în scopul de a ataca alte reţele şi computere. Aceleași instrumente care sunt utilizate în pasul nr. 1, sunt acum îndreptate spre alte sisteme.

5. *Afectarea reţelelor şi a dispozitivelor*

Acest pas include ştergerea sau modificarea fișierelor, furtul datelor valoroase, distrugerea computerelor, sau atacurile DOS (*Denial of service attacks*) [10, p.142].

Un alt mod de atac informatic ar fi utilizarea virușilor informatici, care la rândul său nu sunt alt ceva decât un software creat de un specialist în domeniul IT și, care pătrunde într-un sistem informatic fără știrea sau cunoștința deținătorului acestuia. De obicei un virus se ataşează la un fişier astfel încât virusul rulează în

memorie sau în sistemul de operare de fiecare dată când sistemul execută fişierul infectat. Efectele virușilor pot fi benigne, ca exemplu afișarea periodică a unui mesaj glumeț, dar se poate ajunge și la efecte foarte grave cum ar fi pierderea definitivă a informațiilor din computer sau distrugerea unității de stocare a memoriei. Orice program care se multiplică fără acordul utilizatorului este un virus.

Virușii rău intenționați (malware) se clasifică în viruși *hardware*, care afectează discul dur și memoria, și viruși *software* ce afectează fișierele și programele aflate în memorie sau pe disc, inclusiv sistemul de operare sau componentele acestuia.

Un vierme la rândul său, este un program destinat pentru a obţine avantajul faţă de o vulnerabilitate într-o aplicaţie sau într-un sistem de operare în scopul de a penetra un sistem. Spre deosebire de virus, viermele este un program de sine stătător şi el există independent de alte programe, iar pentru a rula nu are nevoie de alte programe. Acţiunile pe care viermii le realizează includ ştergerea fişierelor unui sistem informatic, sau controlul de la distanţă al computerului de către atacator.

Un **Cal Troian** est un tip de program spion, care apare că ar realiza ceva util, dar care în realitate permite ștergerea sau modificarea fișierelor, transmiterea fişierelor prin reţea la atacator sau instalarea în sistemul informatic de alte programe şi viruşi.

Botnets face parte din categoria programelor malițioase care aduc profit prin intermediul acțiunilor pe care le efectuiază. Astfel, Calul Troian, Viermele şi Virusul reprezintă programe care permit computerului infectat să fie plasat sub controlul de la distanţă al unui atacator.

Computerul infectat este cunoscut sub denumirea de „*zombie*.” Când sute, mii sau chiar zeci de mii de computere *zombie* se află sub controlul unui atacator, acesta creează un botnet.

Modul de investigare a unei fraude informatice nu diferă mult de modul de cercetare a infracțiunilor clasice, însă poate uneori să devină mult mai complexă.

Obiectivul activităţii desfăşurate de organele de urmărire penală, ca fază a procesului penal, constă în **strângerea probelor necesare cu privire la existenţa infracţiunii, identificarea făptuitorilor şi a victimelor şi la stabilirea răspunderii făptuitorilor.**

Din perspectiva prezentului studiu, am identifica următoarele cerințe:

a. Necesitatea formării echipelor de investigaţie;

b. Prezenţa specialiştilor ce pot înţelege detaliile tehnice ale infracţiunii;

c. Investigarea incidentelor prin verificarea dosarelor;

d. Studierea locului infracţiunii.

Din punct de vedere **tactic**, trebuie **clarificate** următoarele aspecte (regula celor 7 întrebări):

- „***ce***”?, – ce faptă a fost comisă? –, respectiv natura faptei;

- „***unde***”?, – unde a fost comisă fapta? – respectiv locul comiterii faptei;

- „***când***”?, – când a fost comisă fapta? – respectiv timpul comiterii faptei;

- „***cum***”?, – cum a fost comisă fapta? – respectiv modalitatea comiterii faptei;

- „***cine***”?, – cine a comis fapta? – respectiv autorul faptei;

- „***cu cine***”?, – cu cine a fost comisă fapta? – respectiv cine a participat la comiterea faptei;

- „***de ce***”? – de ce a fost comisă fapta? – respectiv mobilul şi/sau scopul comiterii faptei.

Aceste aspecte privesc, în realitate **conţinutul constitutiv al infracţiunii** care trebuie probat, şi anume:

- ***obiectul*** infracţiunii – valoarea socială ocrotită atât sub aspect juridic cât şi material, respectiv întrebarea **„ce”**;

- ***subiectul activ*** al infracţiunii – persoanele implicate în comiterea infracţiunii, respectiv întrebările **„cine”** şi **„cu cine”**;

- ***latura obiectivă*** a infracţiunii – conduita interzisă şi, mai ales, locul, timpul şi modalitatea comiterii faptei – respectiv întrebările **„unde”, „când”, „cum”**;

- ***latura subiectivă*** a infracţiunii – vinovăţia şi, mai ales, mobilul şi/sau scopul comiterii faptei – respectiv întrebarea **„de ce”**, **„pentru ce”**.

Internetul este alcătuit din computere, în acest context probele trebuie căutate ținând cont de funcţia pe care o îndeplineşte computerul investigat în reţea şi de modul cum acesta este configurat. În toate situaţiile însă comportamentul utilizatorului este înregistrat în fişiere care mai sunt numite şi „log” adică jurnal. Aceste fişiere constituie şi principala sursă pentru identificare indiciilor şi probelor în investigaţiile on-line.

Atunci când este identificat un indiciu într-un fişier jurnal, acesta ne poate conduce către alt computer.

Un aspect de asemenea important în desfăşurarea investigaţiilor informatice este cooperarea ofițerului de urmărire penală, a procurorului cu furnizorii de servicii Internet, cu operatorii de telecomunicaţii şi cu alte organe private din acest domeniu.

Încadrarea juridică unei astfel de fapte, este de regulă mai complicată de cât incriminarea a altor tipuri de activităţi criminale.

În acest sens este important să ne amintim despre mijloacele de probă prevăzute de art.93 CPP și anume: declaraţiile bănuitului şi ale învinuitului, declaraţia părţii vătămate, părţii civile şi civilmente responsabile, declaraţiile martorilor, înscrisurilor, înregistrărilor, fotografiile, mijloacele materiale de probă, constatările tehnico–ştiinţifice, constatările medico–legale, rapoartele de expertiză [11].

Pentru investigarea respectivelor categorii de fapte, o importanță aparte prezintă mijloacele materiale de probă care pot furniza date despre activitatea infracţională prin informaţiile stocate în conţinutul lor. De multe ori prin simpla

lor vizualizare, obținem probe directe ale săvârșirii unei infracţiuni sau indirecte, acestea constituind indicii ale săvârșirii unei infracţiuni ce trebuie coroborate cu probe directe.

Culegerea datelor în mediul informatic şi transformarea acestora în probe se face în funcţie de indiciile existente în cazul investigat, caracteristicile determinând procedura ce trebuie urmată.

Dacă informaţia cu privire la comiterea unei fraude informatice face referire la un nume (*nickname*) sau canal de IRC este recomandabil folosirea motoarelor de căutare pe bază de cuvinte cheie.

La urmărirea penală a infracţiunilor informatice vom avea în vedere şi cracteristica criminologică a infracţiunilor ca fapte antisociale individuale, prin care se urmăreşte cunoaşterea din punct de vedere ştiinţific a condiţiilor şi a cauzelor care generează faptele penale.

Astfel, există mai multe diferenţe între criminalitatea care se săvârşeşte în mediul informatic şi criminalitatea tradiţională, atât în comiterea infracţiunilor, cât şi referitor la investigarea acestora.

De multe ori infractorul informatic este departe de locul unde se săvârşeşte fapta ilicită. Infractorii pot alege locul unde ei se vor afla în momentul săvârşirii infracţiunii, întrucât criminalitatea din spaţiul informatic nu necesită prezenţa fizică a infractorului la locul săvârşirii faptei ilicite.

Este dificil a răspunde la întrebarea care sunt categoriile de infractori în cyberspaţiu, aceasta depinde atât de o combinaţie de factori sociali, tehnologici şi legali, cât şi de modul în care aceste categorii de infractori sunt definite.

O clasificare succintă a infractorilor din cyberspaţiu ar fi următoarea:

Utilizatorii neglijenţi care violează politicile de securitate sau nu respectă practicile de securitate, şi prin urmare, datele care se află în reţea pot fi afectate;

Infractorii tradiţionali care comit infracţiuni convenţionale, aceştia folosind computere sau alte tipuri de dispozitive electronice pentru comunicaţii şi care păstrează înregistrările în sprijinul activităţilor lor infracţionale;

Şarlatanii şi hoţii incluzând pe cei care practică activităţi de *phishing, spoofing, spimming* (mesaje comerciale nesolicitate trimise printr-un sistem de mesagerie instantanee), sau „*înşală*” oamenii în alte moduri în vederea obţinerii de câştiguri financiare;

Hacker-ii, computer trespassers (intruşii informatici) şi password crackers (spărgătorii de parole) cunoscuţi şi sub numele de hacker-i *white hat* sau *gray hat,* care urmând tradiţia eticii originale a *hacker-ilor*, folosesc computerele pentru a explora ilegal, pentru a învăţa şi pentru a prelua controlul asupra sistemelor ca să facă pozne, şi care ar putea să găsească, să exploateze, sau să expună vulnerabilităţile de securitate ș.a.

Această categorie de infractori pot fi experţi în domeniul noilor tehnologii, cum sunt, de exemplu, hackerii, experţii în securitatea sistemelor informatice,

programatorii şi alţi specialişti în domeniul Internetului. De asemenea, infractorii din cyberspaţiu pot acţiona ca un grup organizat prin schimbul de informaţii fără a dezvălui identitatea lor pe Internet, îngreunând activităţile de investigare ale organelor de urmărire penală.

Unul din cele mai întâlnite motive pentru săvârşirea infracţiunilor din spaţiul informatic este **amuzamentul,** iar făptuitorii în marea sa parte reprezintă hackerii tinerii, care au această motivaţie infracţională. Din categoria hackerilor tineri fac parte *pionierii,* care sunt fascinaţi de noile tehnologii şi învaţă cum funcţionează sistemele informatice; *derbedeii* reprezintă nişte hackeri jucăuşi care nu intenţionează să facă rău nici unei persoane, putând oricând accesa neautorizat un site web şi lăsa un mesaj inofensiv; *exploratorii* care sunt caracterizaţi de curiozitatea de a pătrunde neautorizat în sistemele informatice şi în reţelele informatice doar în scopul de a cunoaşte ce se află în acestea; *jucătorii* care accesează neautorizat sistemele informatice în tocmai ca pe un joc prin testarea măsurilor de securitate, fiind motivaţi de dorinţa de a le accesa.

Alte motive pentru săvârşirea infracţiunilor informatice este **profitul financiar** deoarece majoritatea persoanelor rău intenționate au ca motivaţie infracţională obţinerea de câştiguri financiare, iar altele din **motive emoţionale** cum sunt supărarea, furia, sau chiar răzbunarea pentru greşelile reale sau imaginare îi determină să săvârşească anumite fapte, pe care în mod normal nu le-ar săvârşi. O persoană foarte supărată este temporar cel puţin o persoană tulburată emoţional.

Infractorii cibernetici care acţionează din furie ar putea fi, de exemplu, soţi dispreţuiţi, angajaţi concediaţi, parteneri de afaceri care se simt că au fost înşelaţi sau furaţi etc. [12, p.223].

Înţelegerea motivaţiei infractorilor din cyberspaţiu este utilă în cadrul desfăşurării unei investigări pentru stabilirea profilului infractorului din cyberspaţiu în scopul identificării corecte a suspectului.

Generalizând cele menționate supra, susținem că fenomenul criminalității informatice este unul aflat în continuă dezvoltare, se diversifică ca urmare a dezvoltării continue a tehnologiilor ce generează la rândul lor apariția de noi aplicații și dispozitive, permițând infractorilor să-și remodeleze tehnicile de operare și să creeze noi oportunități de săvârșire a infracțiunilor informatice.

Dezvoltarea și răspândirea programelor de *ransomware*, *botnet* și de interferență neautorizată în sistemele informatice se repercutează asupra securității persoanelor, a disponibilității și integrității datelor personale, precum și asupra protecției confidențialității și a libertăților fundamentale ale acestora. Cu toate că lupta cu criminalitatea în general și, în special, împotriva criminalității informatice reprezintă o prioritate a Agendei europene privind securitatea informatică.

Un număr considerabil de atacuri informatice împotriva persoanelor fizice sau juridice rămân deseori nedeclarate, nedetectate sau nedescoperite, astfel, făp-

tuitorii fiind încurajați să continue activitatea infracțională, inclusiv și datorită nesancționării la timp a ilegalităților săvârșite.

Pentru a fi asigurate scopurile procesului penal este important ca organul de urmărire penală să aplice și să manipuleze procedeele probatorii reglementate în Codul de procedură penală, pentru asigurarea cerințelor de calitate a probelor administrate, sarcină care poate fi realizată doar dacă ofițerii de urmărire penală și ofițerii de investigații vor stăpâni abilități, inclusiv de ordin tactic criminalistic, necesare identificării și cercetării infracțiunilor informatice. În acest sens ar fi binevenită crearea unui centru de formare continuă în acest domeniu.

Referințe bibliografice:

1. https://stisc.gov.md/ro/content/republica-moldova-clasata-pe-locul-53-raportul-indicele-global-cybersecurity-2018 (vizitat la 15.09.2019).
2. https://www.speedtest.net/global-index (vizitat la 18.09.2019).
3. Gheorghe-Iulian Ioniță, Infracțiuni din sfera criminalității informatice, Ed.Pro Universitaria, București, 2013.
4. Codul penal al Republicii Moldova, nr. 985-XV din 18.04.2002. În: Monitorul Oficial l Republicii Moldova nr.128-129/1012 din 13.09.2002. Republicat în: Monitorul Oficial al Republicii Moldova nr.72-74/195 din 14.04.2009.
5. Maxim Dobrinoiu, Infracțiuni în domeniul informatic, editura C.H.Beck, București 2006.
6. Lege privind prevenirea şi combaterea criminalităţii informatice, nr. 20-XVI din 03.02.2009. În: Monitorul Oficial nr.11-12/17 din 26.01.2010.
7. Romanian Information Technology Initiative și Guvernul României, *Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică*, București, 2004.
8. Lege cu privire la informatică, nr. 1069-XIV din 22.06.2000. În: Monitorul Oficial al Republicii Moldova nr.73-74/547 din 05.07.2001.
9. Nicolae Sfetcu, *Manualul investigatorului în criminalitatea cibernetică*, https://www.academia.edu/24276353/Manualul_investigatorului_%C3%AEn_criminalitatea_informatic%C4%83 (vizitat la 15.09.2019).
10. Adrian Cristian Moise, *Metodologia investigării criminalistice a infracțiunilor informatice*, Editura Universul Juridic, București 2011.
11. Codul de procedură penală al Republicii Moldova, nr. 122-XV din 14.03.2003. În: Monitorul Oficial al Republicii Moldova, nr.104-110/447 din 2003. Republicat în: Monitorul Oficial al Republicii Moldova nr. 248-251/699 din 05.11.2013.
12. Adrian-Cristian Moise, Dimensiunea criminologică a criminalității din cyberspațiu, Editura C.H.Beck, București 2015.