CZU 343.7:004
DOI https://doi.org/10.52388/1811-0770.2024.1(251).08

CADRUL LEGAL PRIVIND FRAUDELE ÎN DOMENIUL INFORMATICII ȘI PREVENIREA ACESTORA

Alexandru MARIȚ
Doctor în drept, profesor universitar, Academia de Studii Economice din Moldova,
Chișinău, Republica Moldova
e-mail: *alexmarit123@gmail.com*
https://orcid.org/0000-0002-3198-8398

Infracțiunile din domeniul informatic reprezintă un tip de infracțiuni relativ nou și specific, cercetarea lor necesită elaborarea unor metode noi, folosirea unor tactici criminalistice specifice acestui tip de infracțiuni. În literatura de specialitate întâlnim mai multe strategii elaborate de către doctrinari, mai multe recomandări tactico-metodice care urmează a fi îndeplinite de către ofițerii de urmărire penală, şi specificul probei digitale. La rândul său criminalitatea informatică reprezintă diverse activități infracționale care implică computere și sisteme informatice fie ca instrument principal, fie ca țintă principală. Aceste activități includ: infracțiuni clasice (cum ar fi frauda, falsul și furtul de identitate); infracțiuni legate de conținut (de exemplu, distribuirea de pornografie infantilă sau incitarea la ură rasială on-line); și infracțiuni specifice computerelor și sistemelor informatice (de exemplu, atacuri împotriva sistemelor informatice, atacuri de tip DDoS – de blocare a accesului și programe malware).

Cuvinte-cheie: *securitate informatică, protecția datelor, dovezi electronice, atac cibernetic, victime cibernetice, fraude în mediul informatic, prevenire infracționalitate on-line.*

LEGAL FRAMEWORK FOR COMBATING INFORMATION FRAUD AND PREVENTION STRATEGIES

Computers crimes are a relatively new and specific type of crime, their research requires the development of new methods, the use of forensic tactics specific to this type of crime. In the literature we find several strategies developed by doctrinaires, several tactical-methodical recommendations to be met by prosecuting officers, and the specifics of digital evidence. In turn, cybercrime represents various criminal activities that involve computers and computer systems either as a main tool or as a main target. These activities include: classic crimes (such as fraud, forgery and identity theft); content-related offenses (eg distribution of child pornography or incitement to racial hatred online); and computer and computer-specific offenses (for example, attacks on computer systems, DDoS attacks - blocking access, and malware).

Keywords: *computer security, data and information protection, electronic evidence, cyber attack, cyber victims, computer fraud, online crime prevention.*

CADRE JURIDIQUE SUR LA FRAUDE INFORMATIQUE ET SA PRÉVENTION

Les crimes informatiques sont un type de crime relativement nouveau et spécifique, leur recherche nécessite le développement de nouvelles méthodes, l'utilisation de tactiques médico-légales spécifiques pour ce type de crime. Dans la littérature, nous trouvons plusieurs stratégies développées par le doctrinaire, plusieurs recommandations tactiques et méthodiques à respecter par les officiers de police judiciaire et les spécificités de la preuve numérique. La cybercriminalité,

à son tour, représente diverses activités criminelles impliquant des ordinateurs et des systèmes d'information, soit comme outil principal, soit comme cible principale. Ces activités comprennent: les crimes classiques (tels que la fraude, la falsification et le vol d'identité); les crimes liés au contenu (par exemple, la distribution de pornographie juvénile ou l'incitation à la haine raciale en ligne); et les crimes spécifiques aux systèmes informatiques et d'information (par exemple, les attaques contre les systèmes d'information, les attaques de blocage DDoS et les logiciels malveillants).

Mots-clés: *sécurité informatique, protection des données, preuves électroniques, cyberattaque, cyber-victimes, fraude informatique, prévention de la criminalité en ligne.*

ЗАКОНОДАТЕЛЬНЫЕ РАМКИ ОТНОСИТЕЛЬНО МОШЕННИЧЕСТВА В СФЕРЕ ИНФОРМАТИКИ И ЕГО ПРЕДУПРЕЖДЕНИЯ

Преступления в компьютерной сфере представляют собой относительно новый и специфический вид преступлений, их исследование требует разработки новых методов, использования криминалистической тактики, специфичной для данного вида преступлений. В специальной литературе мы находим несколько стратегий, разработанных доктринерами, несколько тактико-методических рекомендаций, которые должны выполнять сотрудники уголовного преследования, а также специфику цифровых доказательств. В свою очередь, киберпреступность представляет собой различную преступную деятельность, в которой компьютеры и компьютерные системы используются либо в качестве основного инструмента, либо в качестве основной цели. Данная деятельность включает: классические преступления (такие как мошенничество, подделка документов и кража личных данных); преступления, связанные с контентом (например, распространение детской порнографии или разжигание расовой ненависти в Интернете); и преступления, характерные для компьютеров и информационных систем (например, атаки на компьютерные системы, DDoS-атаки и вредоносное ПО).

Ключевые слова: *компьютерная безопасность, защита данных и информации, электронные доказательства, кибератака, кибержертвы, мошенничества в ИТ-среде, предотвращение онлайн-преступлений.*

Introducere

Tehnologiile informaţionale, ca şi orişice alt produs al geniului uman, sunt vulnerabile şi, în cazul unei gestionări incorecte sau intenţionat greşite pot genera o reacţie în lanţ cu un deznodământ nefast şi imprevizibil.

Aspectele teoretice privind cercetarea acestei categorii de infracțiuni, cu rergret, sunt mai puțit reflectate în doctrina criminalistică, în ştiinţa dreptului procesual penal, rămânând, în permanenţă actuale. În acest context, cercetarea criminalistică a infracţiunilor din domeniul informaticii este actuală.

Astfel că, din cauza lipsei de date fiabile, este dificil să se estimeze impactul unei pregătiri necorespunzătoare pentru atacuri cibernetice. Impactul economic al criminalității informatice a crescut de cinci ori între 2013 și 2017, afectând atât guvernele, cât și întreprinderile, indiferent de dimensiunea lor. Creșterea prevăzută a primelor de asigurare cibernetică, și anume de la 3 miliarde de euro în 2018 la 8,9 miliarde de euro în 2020, reflectă această tendință.

Atacurile de anvergură mondială Wannacry *(ransomware)* și NotPetya (*malware de ștergere*) au afectat, în 2017, peste 320 000 de victime din aproximativ 150 de țări. Aceste incidente au condus la o oarecare „trezire” globală în fața amenințării reprezentate de atacurile cibernetice, apărând un nou elan de a integra securitatea cibernetică în reflecția convențională cu privire la politici. Pe lângă aceasta, 86 % dintre cetățenii UE consideră acum că riscul de a deveni victimă a criminalității informatice este în creștere.

Materiale utilizate şi metode aplicate

Ca suport metodologic şi teoretico-ştiinţific al cercetării noastre la constituit teoria dreptului penal naţional şi internaţional, al criminologiei și criminalisticii, ale directivelor europene, precum şi altor materii socio-umane care au fost puse la baza studiului.

Scopul prezentului studiu în efectuarea, pe baza cercetărilor teoretice şi a materialelor în domeniu, a unor investigaţii ample în privinţa problemelor enunțate. Ca suport metodologic în contextul studiului efectuat au fost utilizate un şir de metode de cercetare, precum ar fi: metoda analizei, care a constat în examinarea critică a doctrinei penale și a celei criminologice referitoare la tematica fraudelor/escrocheriilor în domeniul informaticii. Baza informaţională este constituită din importanţa teoretică și aplicativă a studiului. Elementul aplicativ al studiului sau cercetării se manifestă printr-o expunere a formelor acestora și a informației utile de apărare împotriva lor.

Rezultate obţinute şi discuţii

Așadar, în mediul informatic, frauda poate avea mai multe forme și adesea se poate confunda cu înșelăciunea tradiţională, iar mijlocul de realizare fiind computerul [1, p. 227].

Dat fiind mediul informatic în care acestea sunt iniţiate, considerăm necesar să amintim următoarele tipuri de escrocherii și fraude, cum ar fi:

– „Bait and switch” (momește și schimbă);

– „Scrisorile nigeriene” sau „Prizonierul spaniol”);

– „Facturarea falsă”;

– „Frauda salam”;

– Înființarea de firme „fantomă” etc.

Așadar, printre tipurile sau formele amintite mai sus de escrocherii/fraude, modalitatea de ***„Momește și schimbă”*** (*Bait and Switch*) este o formă de fraudă informatică în care făptuitorul ademenește potenţiali clienţi făcând publicitate (preţ foarte mic, profitabilitatea afacerii etc.) unor produse, care fie nu există în realitate, fie sunt ulterior schimbate cu produse aparent similare, dar cu calităţi net inferioare.

În esenţă, clientului i se prezintă posibilitatea de a achiziţiona un anumit produs la un preţ foarte mic, însă în momentul onorării comenzii, acestuia i se comunică faptul că produsul „nu mai există în stoc” şi i se oferă o altă posibilitate, un alt produs (contrafăcut) ca o „consolare” pentru „inexistenţa” celui original prezentat în anunţ. Caracteristic pentru această escrocherie/fraudă este faptul că în nici un moment autorul nu are de gând (nu intenţionează) să vândă produsul-momeală.

Fapta se realizează cel mai adesea prin intermediul sistemelor informatice şi al reţelei Internet. Ademenirea clienţilor se poate face şi prin mesaje de poştă electronică (email) sau prin intermediul unei (bine alcătuite) pagini de Web [2, p. 264].

Tipul sau forma de ***„Trucuri bazate pe încredere - abuzul de încredere”*** (*Confidence Tricks*). Se bazează pe intenţia de a induce în eroare o persoană sau un grup de persoane (denumite „ţinte”) cu privire la posibilitatea de a câştiga importante sume de bani sau de a realiza ceva însemnat. De obicei, făptuitorul se bazează pe ajutorul unui complice, care, pe parcursul înşelăciunii, va acţiona psihologic asupra ţintei inducându-i artificial senzaţia că „Jocul”, „acţiunea” etc., sunt cât se poate de reale şi profitabile, ele însuşi „având încredere în autor”.

La origine, acest truc se baza pe exploatarea anumitor laturi ale personalităţii umane, cum ar fi lăcomia sau *necinstea.* Adesea, victimelor le sunt exploatate dorinţele de *„înavuţire rapidă”,* de *„câştiguri de bani fără efort”* sau de investiţii „prea bune ca să fie adevărate”. Astfel, spre exemplu, ţinta va fi convinsă de către făptuitor că va câștiga o importantă sumă de bani participând la înşelarea unei a treia persoane, care, de fapt, este în legătură cu infractorul şi participă în complicitate la realizarea acestei acţi-

uni. Bineînţeles, victima este cea care pierde „jocul”. Şi în acest caz, abordarea victimei de către infractor şi chiar desfăşurarea acţiunii se vor face prin intermediul mijloacelor electronice (email, pagină Web etc.).

O altă modalitate o constituie ***„Escrocherii /Fraude cu avans”*** (*Advance Fee Fraud*). Sunt adesea cunoscute sub denumirea de „transferuri nigeriene” sau „scrisori nigeriene” ori, pur şi simplu, „înşelătorii 419” (după numărul articolului din Codul Penal al Nigeriei care încriminează astfel de fapte). În acest caz, victimele sunt oameni bogaţi sau investitori din Europa, Asia Australă sau America de Nord.

Mijloacele de comitere variază de la scrisorile expediate prin poştă sau faxuri la email sau pagini web, în special după 1990. Schema de operare este relativ simplă. O persoană (investitor, om de afaceri etc.) este contactată după următorul şablon: „ ... oficial cu rang înalt din Nigeria, intenţionez să expediez importante fonduri şi vă solicit ajutorul de a folosi conturile dvs. pentru transferul bancar, în schimbul unui comision de 10-20% din suma transferată ...”. Presupusa afacere este în mod atent prezentată şi ca un “delict nesemnificativ” (gen white collar crime - infracţionalitatea gulerelor albe), care, însă, oferă posibilitatea unor „importante câştiguri”. Inducerea, aproape subliminal, a ideii de ,,mică ilegalitate” în legătură cu „operaţiunea” are rolul de a descuraja victima să raporteze cazul autorităţilor în momentul în care realizează că, dându-şi *detaliile de cont* unor necunoscuţi, a fost în realitate deposedată de toate lichidităţile sau economiile [2, p. 231].

Astfel de înşelăciuni îşi au originea în Nigeria şi, de regulă, sunt pregătite astfel încât adresele de email, site-urile Web, numerele de telefon sau fax etc. să pară a fi cele ale unor centre de afaceri, firme sau chiar instituţii guvernamentale locale.

Există şi cazuri în care, în corespondenţa prin email, autorii au solicitat în mod direct victimelor sume de bani în lichidităţi pentru aşa-zise, persoane sau ale altor oficiali ori ale personalului bancar care urma să asigure „transferul cel mare” etc.

În alte abordări, se preciza că „pentru a putea facilita transferul, trebuie ca dumneavoastră (ex. Investitorul) să aveţi deschis un cont la o bancă nigeriană, în valoare de cel puţin 100.000 USD”. În câteva situaţii, chiar, victimele au fost invitate în Nigeria să se întâlnească cu respectivii „oficiali guvernamentali” sau cu „alte persoane importante” - în fapt complici ai autorilor care susţineau scenariul ,,autenticităţii şi iminenţei expatrierii de fonduri”. în 1995, un cetăţean american care a întreprins o astfel de vizită în Nigeria a fost ucis, moment în care anchetele au fost preluate spre soluţionare de către US Secret Service.

Astfel de fapte se produc încă frecvent în Nigeria, dar fenomenul s-a şi internaţionalizat. Astfel că, cel mai răsunător succes al organelor de securitate a fost arestarea, în 2004, la Amsterdam, a 52 de persoane implicate în acţiuni similare.

Într-*o altă variantă a fraudei*, ***„Facturarea falsă”*** victima primeşte un mesaj de email de la un presupus avocat ori reprezentant al unei societăţi de administrare valori mobiliare sau imobiliare prin inteimediul căruia este anunţata cu privire la decesul unei „rude foarte îndepărtate”, de care, bineînţeles, victima nu avea cunoştinţă, şi care i-ar fi lăsat o moştenire însemnată. Autorul solicită într-un mesaj ulterior victimei detaliile conturilor bancare în vederea „transferului bancar al lichidităţilor moştenite” (sume exorbitante care au menirea să inhibe instinctul de apărare).

În cea mai nouă versiune a acestui tip de fraudă, autorul se oferă să cumpere unul dintre produsele scumpe postate spre vânzare de victimă pe o pagină de Web specializată în vânzări şi cumpărări online (ex. eBay**),** printr-un ordin de plată, filă check sau alt insttument oficial emis de a autoritate bancară în mod „accidental” check-ul va avea înscrisă o sumă

mai mare decât valoarea produsului „cumpărat", motiv pentru infractor să-i solicite (prin email) victimei să-i retumeze diferenţa de bani, telegrafic, la o terţă adresă, la confirmarea primirii coletului. De regulă, check-ul intră ca bun de plată după o zi sau două, însă contrafacerea lui iese la iveală abia după aproape o săptămână, timp în care victima a apucat să trimită şi produsul şi „restul de bani" infractorului.

„Depozitele false" (*Fake Escrow*) este o altă metodă de fraudare în sisteme informatice este aceea prin care, autorul, după ce câştigă o licitaţie de produse pe un site Internet specializat (gen eBay sau AltaVista), solicită victimei utilizarea unui site (sau serviciu) de escroc „sigur", „neutru" care să „depoziteze" bunurile (în general echipamente electonice) până la perfectarea aranjamentelor financiare. Bineînţeles, *site*-ul de escroc este creat şi controlat de infractor, iar la primirea bunurilor „gaj", respectiva pagină Web este închisă (dezactivată) iar contul șters.

„Escrocherie/ Frauda salam", este la rândul său o operaţiune destul de simplu de realizat, dar care necesită accesul în sistemul informatic al unei instituţii bancare. Autorul accesează aplicaţia informatică de gestionare de conturi clienţi sau pe cea de facturare şi modifică anumite linii din program în aşa fel încât produce o rotungjire în minus a sumelor rezultate din calculele bancare specifice, diferenţele fiind direcţionate către un anumit cont. Numele escrocheriei/ fraudei este sugestiv pentru operaţiunea de obţinere, sumare şi transfer a tuturor procentelor rezultate din rotungirile aritmetice impuse prin soft,

„Prizonierul Spaniol" este o metoda, pe cât de simplă, pe atât de jenantă pentru victime, îşi are originea într-o înşelăciune la modă în secolul 17. în esenţă, autorul contactează ţinta (om de afaceri, familia acestuia, persoane cu tendinţe caritabile etc.) printr-un mijloc electronic (email, mesagerie instanţă - IM etc.) şi îi „dezvăluie" faptul că este în legătură (telefonică, email etc.) cu un „foarte important" ori „binecunoscut" personaj din lumea politică economică- socială ori artistică, ce se află încarcerat sub un alt nume în Spania, fiind victima unei înscenări. Întrucât personajul ar dori să evite publicitatea de scandal, autorul înşelăciunii solicită „sprijinul financiară" al ţintei pentru a „plăti cauţiunea personafităţii arestate", turnând ca aceasta, la revenirea în ţară, să se „revanşeze considerabil". Adesea, frauda nu se opreşte după primul transfer bancar de acest gen, victima realizând mult mai târziu, în cursul corespondenţei electronice cu autorul, că sunt necesare şi alte „operaţiuni costisitoare" cărora a trebuit (trebuie) să le facă faţă „pentru eliberarea personajului", totul fiind, evident, construit artificial. Succesul fraudei rezidă de cele mai multe ori în măiestria jocului psihologic al autoului care îmbracă povestea „incredibilă" întro aură de mister şi confidenţialitate, reuşind să-i creeze victimei impresia că participă la o „acţiune de mare însemnătate'' în plan politic-economic-social ori artistic [3].

În acest context unii specialişti avertizează -, psihologii Bitdefender atenţionează oricine poate deveni victima escrocheriilor pe Facebook Qichepcate fi păcălit de esaixte ***"Ghici cine ți-a vizualizat pofilul Dvs?"*** dar şi multe altele, avertizează analiştii comportamentali şi psihologii din cadrul *Bitdefender.*

Un studiu realizat pe parcursul a doi ani de lumizorul de soluţii software arată că escrocii infectează milioane de utilizatori Facebook cu scheme cunoscute, prezentate sub altă formă. O echipă de analişti comportamentali şi psihologi a analizat cele cinci categorii de escrocherii şi a concluzionat că ***nu există un profil al victimei tipice.***

"Cele mai mari vulnerabilităţi" apar din cauza unor dispoziţii umane generale care îl pot influenţa pe orice utilizator la un moment dat. Este greu pentru noi, oamenii, să acceptăm comportamentul nostru iraţional, sau faptul că ne lăsăm pradă impulsurilor pe care le atribuim, în mod normal, celor mai puţin "educaţi", a spus psihologul Nansi Lungu, Behavior Analyst la Bitdefender.

Cu toate acestea, analiza psihologică a evidenţiat o legătură strânsă între *victime şi lipsa de informare,* în special în ceea ce priveşte modul de funcționare a reţelei sociale Facebook în timp ce aproape jumătate dintre ameninţările banetice mizează pe cunoaștarea utilizatorilor de a şti cine le-a vizualizat profilul, una din trei fraude atrag victimele cu functionalităţi pe care Facebook nu le-a implementat încă, precum butonul de "Dislike" sau dorința de a personaliza.

Tombole false, cum ar fi cele cu bilete gratis la Disneyland sau puncte de joc, reprezintă 16.51% din numeroasele escrocherii din ultimii doi ani, în timp de materialele pornografice cu celebrităţi reprezintă 7.53%. Escrocheriile de pe Facebook fac bani prin chestionare frauduloase sau ***viruşi de tip Troian*** care ***fură parole bancare*** sau din browser.

Deşi sunt încă o categorie de nişă, materialele video ce promovează violenţa câştigă popularitate, avertizează experţii în securitate ai Bitdefender. Escrocheriile de tip "Like and Share" care se folosesc de imagini şocante, precum animale lovite, copii suferinzi şi femei torturate reprezintă 1% din totalitatea fraudelor, potrivit studiului. Cel mai recent exemplu este cel în care un material video cu o femeie ucisă de soţul ei pentru că a sărutat alt bărbat a infectat utilizatorii cu viruşi.

Cele mai populare categorii de escrocherii folosite de criminalii cibernetici pentru a păcăli utilizatorii de Facebook sunt:

1. Ghici cine ţi-a vizualizat profilul? - 45.50%
2. Noi funcţionalităţi ale Facebook - 29.53%
3. Escrocherii cu premii - 16.51%
4. Escrocherii cu celebrităţi - 7.53%
5. Materiale video cu atrocităţi - 0.93%

Bitdefender recomandă utilizatorilor să actualizeze sistemul de operare, soluţia antivirus şi alte aplicaţii software pentru a opri hackerii din exploatarea vulnerabilităţilor găsite în sistem. Utilizatorii trebuie să evite să completeze chestionare pe Facebook sau să apese Like sau Share pentru a vizualiza un video. Pentru a atrage atenţia în rândul utilizatorilor de Facebook, Bitdefender a lansat recent şi o lista anuală cu cele mai populare 10 scam-uri găsite pe reţeaua socială.

Studiul a analizat 850.000 de escrocherii răspândite în ţări precum România, Statele Unite, Marea Britanie, Australia, Germania, Spania, Franţa şi Arabia Saudită începând cu octombrie 2012. Pentru mai multe informaţii privind psihologia celor care devin victime ale păcălelilor pe Facebook, putem accesa studiul integral realizat de Bitdefender pe acest subiect [4].

Ca temei de pornire a urmăririi penale pe cazurile de comitere a escrocheriilor/fraudelor în domeniul tehnologiilor informaţionale pot fi:

- plângerile cetăţenilor, funcţionarilor, persoanelor cu funcţii de răspundere din diferite instituţii, organizaţii, întreprinderi utilizatori ai informaţiilor care au fost accesate ilegal;
- comunicările cu privire la fapta comisă sau în proces de pregătire parvenite din diferite surse.

Aşadar în contextul utilizării tot mai accentuate a Internetului în *activităţile comerciale, de business, de administraţie,* în aplicaţii din domeniul *sănătăţii* sau pentru *învăţământ la distanţă*, fapt ce a condus şi la apariţia şi extinderea unor noi concepte (*e-commerce, e-leaming, e-health, e-work, e-govemment*), apare ca esenţială stabilirea unui *cadru robust de încredere* pentru aplicaţiile informatice care implementează astfel de servicii. Internetul contribuie la accelerarea fluxului de activităţi în domenii din cele mai diverse.

Aplicaţiile din domeniul comercial, de exemplu, implică necesitatea unor schimburi de *documente sub formă digitală* între firme, organizaţii şi/sau persoane particulare. Câteva premise valabile pentru aplicaţii suport pentru e-servicii pot fi menţionate în acest context.

În primul rând, persoanele care *intră în legătură prin Internet pentru realizarea unor tranzacţii*

şi acţiuni specifice domeniului (comerţ electronic, aplicaţii de învăţământ distanţă, *tele-working, telemedicină* etc.) nu se cunosc în prealabil sau nu se află într-o întâlnire directă, fizică.

Este cazul, de exemplu, al unor *cumpărături on-line,* de pe *site-uri comerciale,* unde cumpărătorul conectat comandă produse/servicii şi plăteşte. *î*n acelaşi timp, anumite portaluri pe Internet destinate unor tranzacţii industriale oferă servicii on-line care cer o angajare contractuală imediată.

În al doilea rând, în Internet circulaţia informaţiilor se face liber, fără un control şi o cenzură restrictivă. De aici rezultă însă şi *pericolul interceptării* acestora, *modificării* sau *falsificării datelor transmise,* de exemplu din *contractele de natură confidenţială sau strategică dintre companii* (organizaţii). Dezvoltarea Internetului în ultimii ani a fost puternic stimulată de perspectiva realizării de *afaceri on-line,* de avantajele implementării unor aplicaţii practice în domenii din cele mai diverse, *de la administraţia publică centrală şi locală până la învăţământ, medicină, cercetarea ştiinţifică* etc. Până şi cele mai banale tranzacţii se pot desfăşura prin Internet. Acesta va face să cadă barierele fizice existente până acum în calea comunicării. În acest context extrem de dinamic, asigurarea securităţii tranzacţiilor prin Internet constituie cea mai importantă provocare ce stă în faţa acestor tipuri de aplicaţii (de e-commerce, e-health, e-government, e-learning, e-work). Pentru majoritatea organizaţiilor, interesul în ceea ce priveşte *securitatea informatică este proporţional cu modul în care sunt percepute ameninţările şi vulnerabilităţile sistemelor de calcul.*

În cele ce urmează vor fi prezentate o serie de concepte şi principii generale care trebuie luate în considerare pentru implementarea unor politici eficiente capabile să combată, dai-mai ales să prevină fraudele/escrocherie şi, mai general vorbind, incidentele de securitate care pot afecta ficţionarea sistemelor informatice şi de comunicaţii. Identificarea riscurilor şi răspunsul la fraude electronice la modul general, fraudele implică utilizarea unor metode incorecte sau neautorizate pentru a obţine anumite avantaje faţă de alţi parteneri, utilizatori, beneficiari ai anumitor servicii ş.a.m.d. Circumstanţele în care fraudele apar (şi, în context, fraudele electronice, în aplicaţii bazate pe Internet aşa cum sunt şi cele de e-commerce, e-health, e-government, e-learning şi e-work) pot fi foarte diverse. Unele dinte acestea includ: fraude în aplicaţii de format electronic, fraude în aplicaţiile de nivel guvernamental (în sisteme de e-government), fraude cu efecte asupra consumatorilor individuali, fraude care afectează drepturile de proprietate intelectuală, fraude care afectează companiile de asigurări, fraude în sistemele de sănătate (asociate cu atacuri la adresa sistemelor suport pentru aplicaţii de e-health, de exemplu), ***fraude cu cărţi de credit falsificate*** (legate până la uimă tot de aplicaţiile de comerţ electronic), ş.a.m.d. [4].

În contextul expansiunii tehnologiilor informatice şi de comunicaţii, beneficiile acestora nu ar trebui să ascundă şi potenţialul pentru realizarea de *fraude electronice* la scară mare, fraude care să afecteze sistemele suport pentru aplicaţii de e-commerce, e-health, e-government, e-leaming şi e-work. Beneficiile enorme aduse de aceste tehnologii utilizatorilor furnizează şi pentru *infractorii cibernetici* oportunităţi multiple.

Astfel, aceştia devin capabili:

- să comunice unul cu altul în secret;
- să îşi ascundă adevăratele identităţi pentru a evita detecţia şi pentru a penetra sisteme informatice la distanţă;
- să falsifice şi să altereze documente cu regim privat; să manipuleze sistemele de plată elecfronică pentru a obţine ilegal fonduri.

Astfel, câteva mecanisme ale fraudelor electronice, adică fraudele care implică sisteme de plăţi bazate pe hârtie:

• atunci când bunuri şi servicii sunt obţinute efectiv on-line, dar totuşi sunt plătite utilizând instrumente de plată bazate pe hârtie (cum ar fi ordine de plată, cecuri ş.a.), fraudele se pot realiza la fel ca în trecut;

• vulnerabilităţile sunt legate în principal de utilizatorii individuali ce folosesc conturi deschise *folosind detalii de identificare false*, de situaţii de depăşire a balanţei creditului sau chiar de falsificarea sau alterarea unor instrumente de plată ca atare.

• în condiţiile în care este o presiune pentru efectuarea cât mai rapidă *a tranzacţiilor electronice,* vânzătorii ar putea dori *să nu mai aştepte ca informările introduse să fie şterse* sau să se *efectueze verificări de autenticitate* înainte de autorizarea distribuirii de bunuri sau furnizării de servicii, prin urmare *deschizând calea unor potenţiale fraude*. La rândul lor, clienţii ar putea trimite informaţii specifice unui cec unui vânzător despre care *nu deţin informaţii independente, care poate fi localizat într-o ţară străină.*

Fraude implicând ***sisteme de debit direct***:

• Plăţile on-line se pot efectua prin debit direct, caz în care sumele de bani sunt transferate direct din contul plătitorului la banca destinaţie, sau prin intermediul unui instrument de transfer în care un client poate solicita băncii sale să debiteze din contul său o sumă care este electronic creditată pentru alt cont.

• Pentru ca astfel de tranzacţii să aibă loc, *anumiţi paşi preliminări* trebuie efectuaţi de către părţile implicate, incluzând schimbul de detalii despre conturi şi realizarea a diverse verificări de identificare. Din punctul de vedere al cumpărătorului, un element de risc apare dacă fondurile sunt transferate înainte ca bunurile să sosească sau ca serviciul să fie efectiv furnizat.

• Din punctul de vedere al vânzătorului, este necesar ca fondurile să sosească înainte ca bunurile să fie livrate sau ca serviciul să fie furnizat. Principalul mijloc de protecţie împotriva unor astfel de fraude solicită comercianţilor să adopte paşi adecvaţi pentru autentificarea detaliilor de cont furnizate de către cumpărător şi să se asigure că fondurile corespunzătoare sunt ţinute în cont pentru a acoperi operaţia de cumpărare.

Obţinerea autorizaţiei de la o instituţie financiară este primul pas în prevenirea fraudelor.

Fraude implicând ***sisteme electronice de transfer de fonduri****:*

- Au fost dezvoltate *diverse sisteme* pentru a permite *clienţilor, băncilor şi comercianţilor să comunice în mod securizat unul cu celălalt.*

- Respectivele sisteme electronice de transfer de fonduri au devenit deja operaţionale ca substitute pentru tranzacţiile prin cecuri bazate pe hârtie, şi aceste sisteme pot fi adaptate pentru utilizarea în tranzacţii realizate prin Internet. Totuşi, aceste sisteme creează un serios risc de securitate dacă nu se implementează *proceduri adecvate pentru verificarea disponibilităţii fondurilor* care ar trebui transferate sau pentru *un control riguros al accesului la conturi***.**

- În plus, există posibilitatea manipulării şi interceptării informaţiilor transmise prin reţea „în clar" (în fonnă necriptată). De aceea, pentru a *securiza operaţiunile de transferuri electronice de fonduri***,** *datele sunt de regulă criptate folosind algoritmi* care cedează mesajele transmise. La destinaţia legitimă ele vor fi decodate folosind *chei* cunoscute doar de către *transmiţător* şi *receptor*. Riscul major asociat cu un astfel de sistem constă în posibilitatea ca respectivele chei de criptare să fie interceptate, îh care caz datele din cadrul sistemului ar putea fi dezvăluite sau manipulate.

- Majoritatea fraudelor/escrocheriilor pe scară largă la transferurile electronice de fonduri au implicat interceptarea sau alterarea mesajelor electronice transmise de la calculatoarele instituţiilor financiare. Pentru a îmbunătăţi securitatea tranzacţiilor bazate pe cărţi de credit şi realizate prin Internet, diferite companii au proiectat sisteme căi care să asigure că *identitatea părţilor contractante* poate fi *autentifica-*

tă şi că vânzătorii sunt capabili să determine dacă un client deţine în mod real fondurile necesare pentru a putea realiza tranzacţia.

- Fraude implicând *sisteme bazate pe cârduri***:** în prezent, plăţile efectuate folosind *smart carduri* pot lua o varietate de forme. Însă există şi riscuri aferente acestora. Principalul risc de securitate asociat cu smart cardurile este determinat de *modul în care datele sunt criptate***.** Mecanismul de criptare utilizat poate fi spart dacă anumite tipuri de *erori* au apărut *la nivelul cârdului*. Unele defecte de proiectare sau din fabricaţie pot spori riscurile de spargere a mecanismelor de protecţie prin criptare.

Fraude implicând ***„cash" electronic*** (şi tanzacţiile bazate pe *portofel electionic*):

Sunt în curs de dezvoltare variate sisteme care vor permite efectuarea de tranzacţii în mod securizat prin Internet folosind „cash" electronic, sau elemente de valoare care sunt înregistrate digital pe calculatoare. Ele trebuie să folosească *mecanisme de criptare eficiente*, şi de regulă se bazează pe *criptarea cu chei publice* [4].

Fraude legate de identitate: Progresele în comerţul electronic au creat premise pentru noi forme de acţiuni ilegale şi frauduloase, puţin probabil să fie întâlnite în sistemele tranzacţionale tradiţionale. Spre exemplu, mulţi consumatori întâmpină mari dificultăţi în a-şi identifica partenerii de afaceri (sau de tranzacţii realizate prin Internet). Unii comercianţi recurg în mod intenţionat la mascarea (ascunderea) identităţilor lor reale tocmai pentru a preveni posibilele fraude în tranzacţiile electronice. în practică, tehnologiile Internet asigură utilizatorilor instrumente relativ simple pentru mascarea (ascunderea) identităţilor reale ale acestora. Adresele de Internet, de poştă electionică, spre exemplu, pot fi uşor manipulate pentru a include detalii care nu sunt reale, sau sursa mesajului poate fi făcută anonimă sau modificată astfel încât mesajul să apară ca provenind de la un alt utilizator.

Există mai ***multe tipuri de escrocherii/fraude electronice,*** dintre care sunt 3 tipuri de escrocherii/ fraude mai des întâlnite în aplicaţiile bazate pe trazactii electronice:

– Primul tip este acela în care o anumită entitate *pretinde că vinde ceva ce nu deţine cu adevărat,* dar pentru care *solicită plata în avans.*

– Un al doilea tip conduce la *livrarea de bunuri* sau *servicii* care sunt în realitate de *o calitate inferioară celei pentru care s-a plătit***.**

– Un al treilea tip de escrocherie/fraudă se manifestă prin acţiuni *de convingere a clienţilor să achiziţioneze ceva ce ei nu doresc cu adevărat*, prin intermediul unor *tehnici de marketing şi de promovare foarte agresive.*

În acest fel, trebuie să ştim care ar trebui să fie răspunsul la escrocheriile/fraudele electronice, aşadar, în ceea ce priveşte răspunsul la fraudele electronice vom face careva abordări general recunoscute care sunt sau trebuie avute în vedere.

Prima abordare se bazează pe *constiuirea unui cadru legal adecvat***,** deci pe *reglementarea legislativă* a răspunsului la acţiuni frauduloase realizate pe cale electronică. Problema este însă încă pe larg dezbătută, fiindcă se pune probleme de existență a unei transparenţă, dar totodată şi de o protecţie a confidenţialităţii utilizatorilor.

A doua abordare urmăreşte elaborarea unor cunoscute *moduri clare de practică pentru aplicaţiile bazate pe tranzacţii electronice.* Sunt vizate aspecte cum ar fi cele referitoare la *conţinutul de date* ce poate fi transmis în cursul tranzacţiilor, la *serviciile de certificare* pentru *protejarea acestor date* şi *garantarea autenticităţii* lor.

A treia abordare urmăreşte *adoptarea unor strategii preventive***.** Acestea au în vedere elaborarea unor recomandări şi politici de control al tentativelor de escrocherie/fraudă electronică în special prin utilizarea unor tehnologii eficiente de securitate informatică. în acest context, *adoptarea unor politici cla-*

re de control al *tentativelor de fraudă în interiorul organizaţilor* reprezintă un principiu esenţial pentru prevenirea şi limitarea efectelor fraudelor în aplicaţii care implică *transferul de date sensibile*, a căror dezvăluire poate avea consecinţe serioase pe scară mai largă, aşa cum sunt şi aplicaţiile de "e-commerț", "e-health", "e-government", "e-leaming" şi "e-work". Stabilirea unor principii referitoare, de exemplu, la utilizarea etică a tehnologiilor informatice şi la modul de reacţie la anumite tipuri de fraude sunt, de asemenea, esenţiale pentru succesul unor aplicaţii cum sunt cele menţionate anterior. De o importanţă particulară este necesitatea de a dezvolta *politici specifice de securitate informatică* împreună cu recomandări adecvate pentru raportarea utilizării în scopuri rău intenţionate a tehnologiilor informatice şi de comunicaţii. Astfel de politici trebuie să aibă în vedere comportamentul on-line specific al angajaţilor instituțiilor sau organizaţiilor implicate în aceste aplicaţii, vizând de exemplu aspecte practice cum ar fi *nivelul de securitate* pe care îl asigură *sistemele de autentificare a utilizatorilor* (prin parole, ş.a), accesul la şi utilizarea sistemelor de calcul organizaţionale în scopuri private, utilizarea serviciilor de poştă electronică îh scopuri personale, descărcarea de software de pe fntemet, sau utilizarea unor materiale care implică probleme de drepturi de autor.

Prin urmare, elaborarea unor *strategii eficiente de management* al escrocheriilor/fraudelor, de prevenire şi limitare a efectelor acestora, este o prioritate pentru oiganizaPe implicate îh realizarea de tranzacţii electronice pentru aplicaţii de e-commerce. Politici adecvate de control şi management al esaocheriilor/fiaudelor trebuie adoptate pe scară largă atât în sectorul public, cât şi îh cel privat. Din perspectivă tehnologică, o gamă largă de soluţii au fost proiectate şi introduse în scopul reducerii riscurilor de escrocherii/fiaude electronice pentru tranzacţiile comerciale realizate prin Internet (îh aplicaţii de comerţ electonic). în ceea ce priveşte securitatea echipamentelor (hardware), acestea trebuie protejate astfel încât să se restricționeze accesul la resursele informaționale stocate, eventual prin firewall sau alte dispozitive, în scopul prevenirii unor intiuziuni capabile să conducă la fraude electronice cu consecinţe serioase pentru instituții financiare sau firmele implicate.

Escrocheriile/fraudele în *aplicaţiile de comerţ electronic* trebuie prevenite sau, dacă tot au apărut, trebuie să fie detectate rapid pentru a li se limita pe cât posibil consecinţele. Dacă nu este posibil să se prevină 100% acţiunile frauduloase on-line, cel putin poate fi posibil ca prin intermediul **unor soluţii software de detecţie** să se identifice prezenţa unor acţiuni tranzacţionale frauduloase, şi aceasta tocmai pentru a reduce potenţialele pierderi cauzate de astfel de escrocherii/fraude. Diferite firme dezvoltă soluţii software dedicate utilizate în prevenirea escrocheriilor/fraudelor electronice. O altă modalitate îh care escrocheriile/fraudele pot fi detectate se bazează pe monitorizarea activităţii pe Internet a angajaţilor companiilor. Utilizarea sistemelor de calcul de către angajaţi, şi mai ales activităţile on-line ale acestora, pot fi monitorizate prin soluţii software care, ţin evidenţa pentru respectivele activităţi. De asemenea, filtrarea accesului către exterior (prin politici adecvate la nivel de *firewall,* de exemplu) poate preveni sau limita tentativele de fraudă prin Internei [4].

Dacă ar fi să vorbim despre **recomandări pentru prevenirea escrocheriilor/fraudelor informatice prin e-mail;** este necesar să evităm efectuarea de transferuri bancare către parteneri străini de afaceri, fără *a verifica telefonic veridicitatea schimbării unor practici comerciale stabilite anterior.*

Este necesară o anumită precauţie și atunci *când se solicită prin e-mail schimbarea adresei de corespondenţă electionică, a contiirilor bancare* ori *a valutelor în care se fac plăţile* sau este necesar de observat cu precauție atunci că s-a schimbat *ţara în care sunt deschise conturile* în care trebuie să faceţi plăţile. Business E-mail Compromise Fraud „BEC

Fraud" presupune accesarea de către infractori în mod neautorizat a conturilor de e-mail ale unor societăți comerciale din străinătate, monitorizarea corespondenţei purtate de către angajaţii respectivei societăţi şi simularea corespondenţei reale pe care aceştia o poartă cu societatea parteneră de afaceri, prin *intermediul unei adrese de e-mail asemănătoare sau identice*. Această activitate are de regulă ca finalitate *deturnarea transferului de bani către un cont bancar diferit* faţă de cel al beneficiarului legitim, *contul bancar fiind controlat de alţi membri ai grupării infracționale*.

Frauda ţinteşte societăţile comerciale ce lucrează cu furnizori sau clienţi străini (activităţi de comerţ exterior) şi efectuează cu regularitate plăti prin transfer bancar. Din analiza cazurilor investigate, s-a constatat că societăţile comerciale ce desfăşoară activităţi comerciale din R.Moldova (cu personalitate juridică română) au avut calitatea de victimă, în majoritatea cazurilor, în sensul ca au trimis bani în alte conturi decât cele legitime ale furnizorului extern Din aceeași analiză a rezultat că, în aproape toate cazurile semnalate, compromiterea sistemelor informatice, respectiv a adresei de poştă electronică, a avut loc la societăţile comerciale străine care erau în relaţii comerciale cu cele locale.

Astfel că, printre ***strategiile de protecţie împotriva EA C/BEC,*** se enumeră***:***

• Evitarea utilizării conturilor de e-mail: web-based (yahoo, hotmail, gmail etc) pentru activitatea societăţii comerciale.

• Recomandabilă este utilizarea unor conturi de e-mail dintr-un domeniu propriu și se cere să fim *suspicioşi* cu privire la *mesajele în care se solicită efectuarea unor operaţiuni în secret* sau a unor *operaţiuni rapide* către *destinatari incerţi* sau *neverificaţi***.**

• Trebuie să avem în vedere crearea unor *proceduri minimale de audit IT* şi de *securitate referitoare la plăţi,* în sensul implementării unei *verificări în minim doi paşi*.

În acest sens, ca ***exemple,*** pot servi:

• 1. Stabilire de *o comunicare alternativă,* cum ar fi *cea telefonică* cu furnizorul sau clientul străin *pentru a valida orice schimbare a practicii comerciale statuate*, pentru *a elimina posibilitatea hakenilui* și de a intercepta o eventuală comunicaţie.

• 2. Utilizarea de *semnături digitale* sau a *criptării mesajelor* între părţile implicate în activitatea comercială.

• 3. Raportarea şi *nedeschiderea mesajelor nesolicitate sau de tip SPAM*, acestea putând conţine ***malware.***

• 4. De a nu utiliza funcţia „Reply" pentru a răspunde în corespondenţa de serviciu. În acest sens se recomandă folosirea funcţiei „Forward" şi scrierea în mod manual sau de selectat doar din agendă adresa de e-mail unde se dorește să tansmită mesajul.

Este necesar să fim *precauți la schimbarea subită a unor practici comerciale stabilite anterior***,** *în special a conturilor de e-mail* sau *conturilor bancare* şi a *valutelor în care se fac plăţile,* precum şi a ţării în care sunt deschise conturile. Este așadar necesar de verificat telefonic la funizor sau client, la un număr sau numere de telefon deţinut anterior şi de verificat în mod suplimentar dacă modificările solicitate prin e-mail sunt reale.

Respectiv, ***escrocheria/frauda are trei componente principale:***

1. Componenta de Social Engineering **-** prin care se strâng date istorice ordine, referitoare la societăţile ţintite (sediu social, persoane din management, contul bancar, adrese de poştă electronică, portofoliul de clienţi, eventuale documente accesibile ordine ce prezintă elemente de identificare ale societăţii comerciale ce pot fi utilizate pentru a crea aparenţa de legitimitate).

2. Componenta de intruziune/compromiterea adresei de poştă electonrcă (EAC - Email Account Compromise.) *Deschiderea unui cont cu acte false*

în străinătate, pe numele furnizorului sau clientului străin.

3. Schema infracțională presupune *accesarea în mod neautorizată* a conturilor de e-mail ale unor societăţi comerciale din străinătate, monitorizarea corespondenţei purtate de către angajaţii respectivei societăţi şi simularea corespondenţei reale cu societatea parteneră din RM, prin *intermediul unei adrese de e-mail asemănătoare sau identice***.** Această activitate are de regulă ca finalitate deturnarea transfeiului de bani către un cont bancar diferit faţă de cel al beneficiarului legitim, acest cont bancar *fiind controlat de către alţi membri ai grupării infracţionale.*

Aşadar, vorbind despre ***elemente generale de protecţie din zona guvernantei corporative relatăm:***

1. Societăţile comerciale care conştientizează şi înţeleg existenţa acestui tip de fraudă prezintă un risc mult mai scăzut de a cădea victimă şi pot recunoaşte mai uşor tentativele de acest gen, astfel *probabilitatea efectu, ării unor transferuri eronate scăzând substanţial***.**

2. Se cere, în *primul rând, instruirea personalului referitor la tipologia de escrocherie/ fraudă.*

3. Societăţile comerciale care beneficiază de un sistem de securitate ordine solid (mai ales pentru sistemele informatice utilizate de peisonalul "joint line") prezintă un risc mult mai scăzut de a cădea victimă incidentelor de tip EAC.

Menționăm unele recomăndării pentru ***prevenirea fraudelor de card,*** pentru utilizarea acestora în mod sigur şi fără riscuri:

- este necesar de semnat cardul pe verso în chenarul rezervat în acest scop, în momentul primirii acestuia, folosind un pix cu pastă;

- este necesar de a distruge plicul ce conţine codul PIN primit de la banca, după ce acesta a fost transcris sau după ce l-am memorat;

- nu este indicat să se scrie niciodată Codul PIN pe spatele cardului;

- nu se introduce Codul PIN pe site-uri de Internet şi nu-1 divulgă telefonic;

- este necesar să se păstreze cu grijă cardul şi nu se dezvăluie informaţiile specifice de identificare (număr card, data expirării, nume, etc) altor persoane, chiar dacă acestea sunt sau se prezintă drept angajaţi ai băncii;

- este necesar de a ne asigurăm că în timpul tranzacţiilor efectuate cu folosirea Codului PIN, acesta nu este dezvăluit în mod voluntar sau involuntar altor persoane;

- nu este indicat și recomandabil de a se răspunde niciodată mesajelor primite prin SMS/e- mail prin care ni se solicită date personale (numărul de card, data expirării cardului, Codul PIN);

- nu se recomanda de a se împrumuta cardul personal bancar altor persoane;

- trebuie să asigurăm că în cursul tranzacţiilor comerciale cardul va rămâne tot timpul sub o atentă supraveghere;

- este necesar de a solicită tot timpil comercianţilor chitanţele aferente tranzacţiilor efectuate de noi şi de a se verifică cu atenţie informaţiile înscrise pe acestea;

- este recomandabil de a se păstra tot timpul toate chitanţele aferente tranzacţiilor şi este necesar de le verifica cu extrasul de cont sau rulajul bancar lunar;

- este necesar de a anunţa imediat furtul sau pierderea cardului la unul din numerele de telefon indicate de banca emitentă;

- ar fi recomandabil de a a proteja de fiecare dată cu mana introducerea codului PIN în ATM sau la când se va efectua o anume tranzacţie;

- nu trebuie să acceptăm ajutorul "binevoitor" al persoanelor care se oferă a te ajuta la retragerea de numerar de la ATM;

- este recomandabil să telefonăm la numărul prezent pe spatele cârdului pentru orice suspiciune pe care o avem la utilizarea cardului la ATM;

- în cazul în care suspectezi un caz de fraudă contactează imediat banca la numerele de telefon sau valabile 24 de ore din 24;

- banca va proceda la blocarea accesului cârdului la cont imediat după primirea telefonului de anunţ al pierderii/furtului cardului/tranzacţii suspecte;

- pentru lămurirea oricăror probleme legate de utilizarea cardului trebuie să ne adresăm doar la banca emitentă a cardului şi nu la comerciantului sau al băncii comerciantului/ATM-ului la care s-a utilizat cardul;

Pentru asigurarea securităţii tranzacţiilor efecuate prin inteimediul Internetului, vă sfătuim a vă înrola în serviciul 3D Secure. Inrolarea în acest serviciu vă oferi serviciului efectuat de noi o siguranţă sporită în efectuarea tranzacţiilor prin Internet [7].

Totodată, printre *măsurile de prevenire și de combatere a criminalității informatice și pentru protejarea datelor cu caracter bancar,* ar fi utile următoarele recomandări**:**

1. Întotdeauna încercați să operați cu terminalele din incinta băncilor sau încercați să folosiți, ATM-urile din marele centre comerciale;

2. Încercați să priviți terminalul înainte de a introduce cardul pentru a observa dacă nu a fost modificat terminalul;

3. *Asigură-te că nimeni nu vede pin-codul. Nimeni nu trebuie să afle pin-codul. (acoperă tastatura cu mâna cu care operezi)*

4. Se recomandă activarea notificării, sms pentru orice plată.

5. După dispariții din regimul obișnuit de trai, și la întoarcerea din călătorii se recomandă verificarea conturilor bancare;

6. Nu scăpați niciodată din vedere cardul;

7. Nu păstrați pin/codul împreună cu cardul, în celulare, agendă;

8. Este necesară protejarea calculatorului prin activarea unui sistem autorizat antivirus;

9. Trebuie de manifestat o atenție maximă la oferte speciale, mai ales oferte SHOCK;

10. Este nevoie de atenție la site-urile accesate, și mai ales la copierea design-ului site-urilor cunoscute;

11. Se cere o mare atenție la datele cu caracter personal;

12. Este nevoie de atenție sporită la procurarea on-line, numai de pe pagini criptate (HTTPS);

13. Pentru cumpărături se cere să fie utilizat doar un card special;

14. Este recomandabil de utilizat parole complicate.

Concluzii

Considerăm că succesul creării unei societăţi informatice depinde, în mare parte, de soluţionarea unui spectru de probleme juridice, economice şi organizaţionale. Este nevoie în acest sens de crearea programelor de studiu şi pregătirea specialiştilor în domeniul securităţii informatice; a funcţiilor responsabile pentru implementarea şi administrarea mecanismelor de securitate informaţională, organizarea seminarelor de aprofundare a cunoştinţelor şi de schimb de experienţă cu specialiştii în domeniu și din alte țări.

În contextul celor menționate *propunem* ca în cadrul facultăţilor de drept şi a facultăţilor tehnice să se creeze premize de instituire a specialităţilor cu profil de cercetare a acestui fenomen, a metodelor de investigare, combatere şi prevenire a infracţiunelor cibernetice. Ritmul rapid de evoluție a infracţiunilor informatice, infracțiuni periculoase pentru întreaga societate impune acțiuni urgente de combatere a actelor de terorizm informatic.

Cercetărilor în domeniul infracţionalităţii informatice sunt, prin natura lor, complexe şi implică utilizarea de echipamente sofisticate, cu costuri ridicate.

Astfel că, asigurarea unui nivel adecvat de protecție a sistemelor informatice ar trebui să facă parte dintr-un cadru cuprinzător și eficace de măsuri de prevenție care să completeze măsurile prevăzute de dreptul penal ca răspuns la criminalitatea informatică. Mai mult, creşterea nivelului de pregătire şi informare în domeniu al reprezentanţilor autorităţilor, sectorului privat şi al cetăţenilor, pot face posibilă implementarea corespunzătoare a recentelor strategii pentru securitatea informatică.

În ceea ce privește cooperarea internațională și public-privată în domeniul criminalității cibernetice este una benefică şi de perspectivă.

Securitatea cibernetică are nevoie de un fundament legislativ care trebuie dezvoltat.

Referințe bibliografice

1. DOBRINOIU, I. *Infracţiuni în domeniul informaticii.* Bucureşti, 2006.
2. STANCU, E. *Criminalistica - investigarea ştiinţifică a infracţiunilor*. Bucureşti: Edit. Actami, 1999.
3. STANCU, E. *Ciminalistica*. Vol. III. Bucureşti, 2004.
4. SOVIANY, Sorin. *Principii de tratare a fraudelor în aplicaţii informatice şi de comunicaţii electronice* http://www.agir.ro/buletine/689.pdfsursa http://www.agir.ro/buletine/689.pdf (accesat la 23.04.2024).
5. ВЕХОВ, В. Б. *Компюерные преступления. Способы совершения и методики расследования*. Москва, 1996. 182 с.
6. *Legile securităţii cibernetice.* https://intelligence.sri.ro/legile-securitatii-cibernetice/ (accesat la 07.01.2024).