CRIMINALITATEA CIBERNETICĂ – CU UN PAS ÎNAINTE. METODICI DE INVESTIGARE

Mihai GHEORGHIŢĂ, Svetlana DUŞA

Catedra Drept Procesual Penal şi Criminalistică

Given that information has become very valuable, temptations to defraud the system containing it became increasingly higher. Given that the reason is financial or otherwise, or simply entertainment, cyber-crime found a good place in computer networks.

Infracţiunea cibernetică devine, pe zi ce trece, un pericol din ce în ce mai mare, iar calculatorul electronic este un factor criminogen de prim ordin în acest sens ce pune la dispoziţia conduitei criminale atât un nou obiect (informaţia conţinută şi procesată de sistemele informatice), cât şi un nou instrument. În contextul în care informaţia a devenit foarte valoroasă, tentaţiile de fraudare a sistemelor care o conţin au devenit din ce în ce mai mari. Având ca motiv fie interese financiare sau de alt gen, fie pur şi simplu distracţia, infracţionalitatea şi-a găsit un loc bun şi în reţelele de calculatoare.

În acest sens, prin natura sa eterogenă şi necontrolată de vreo autoritate, comunicarea în Internet, mai restrâns IRC [1], reprezintă un mediu excelent de a exprima liber opiniile şi identitatea proprie. Acest lucru implică însă şi posibilitatea formării unor comunităţi, ale căror preocupări nu sunt dintre cele mai paşnice. Astfel, persoanele interesate de piraterie software, audio/video-pornografie sau de accesul neautorizat la sistemele de calcul îşi pot uşor găsi parteneri cu preocupări similare între ceilalţi utilizatori.

Comunicarea lipsită de bariere le permite celor experimentaţi în activităţi ilegale să le transmită celorlalţi cunoştinţele lor. De multe ori, aceştia din urmă doresc să îşi demonstreze capacităţile nou-dobândite pentru a obţine recunoaştere şi a fi acceptaţi de comunităţile „experimentaţilor", astfel fiind o dată în plus motivaţi în a comite infracţiuni informatice [2].

În lumea reală există persoane care pătrund în case şi pot fura tot ce găsesc valoros. În lumea virtuală există indivizi care pătrund în sistemele informatice şi „fură" toate datele valoroase.

Sistemele de calcul sunt în general protejate de accesul persoanelor neautorizate. Există mai multe mecanisme de autentificare şi apoi autorizare a utilizatorilor, însă cel mai răspândit este cel bazat pe nume de utilizator şi parolă (username şi password). Un utilizator primeşte un nume şi o parolă pe care le foloseşte atunci când vrea să acceseze un serviciu sau un calculator [3].

Perechea nume de utilizator / parolă are pentru sistemele informatice rolul de încuietoare a uşii, ca şi în cazul protejării unei camere la intrarea străinilor. Încuietoarea este considerată drept un mijloc sigur de protecţie, însă în realitate există persoane capabile, pentru care aceasta nu constituie o problemă atunci când doresc accesul în încăpere. Acelaşi lucru este, spre regret, valabil şi pentru lumea virtuală, care ar trebui să rămână inviolabilă.

Drept urmare la cele expuse mai sus, infracţionalitatea cibernetică include următoarele categorii de autori [4]:

- ✓ ***hackeri*** – persoane, mai ales tineri, care pătrund în sistemele informatice din motive legate de provocare intelectuală sau de obţinerea şi menţinerea unui anumit statut în comunitatea prietenilor;
- ✓ ***spioni*** – persoane care pătrund în sistemele informatice pentru a obţine informaţii care să le permită câştiguri de natură politică;
- ✓ ***teroriştii*** – persoane care pătrund în sistemele informatice cu scopul de a provoca teamă, precum şi în scopuri politice;
- ✓ ***atacatori cu scop economic*** – pătrund în sistemele informatice ale concurenţilor comerciali, cu scopul de a obţine câştiguri financiare, în interesul altor persoane;
- ✓ ***criminali de profesie*** – pătrund în sistemele informatice ale întreprinderilor pentru a obţine câştig financiar, în interes personal;
- ✓ ***vandali*** – persoane care pătrund în sistemele informatice cu scopul de a cauza pagube.

Astfel, în lumea virtuală există anumite etape ale avansării de la un simplu utilizator la autorul unei fapte infracţionale [5]:

- În aceste situații *novicele* este de obicei un începător singuratic. Nu are experiență în calculatoare şi nici cum să pătrundă în sisteme din afară. Novicele lucrează singur şi nu are ajutor, fiind de cele mai dese ori un experimentator care nu comite ilegalități [6].
- *Ucenicul* este acel novice care progresează dincolo de fazele inițiale, în general cu ajutorul IRC, schimbând mesaje cu cei care i se aseamănă, astfel nu numai că îşi îmbunătățeşte considerabil cunoştințele, dar devine parte a unei rețele. El învață să îşi acopere mai bine urmele şi să intre sau să iasă din sisteme informatice fără să atragă atenția.
- *Vizitatorul* este, probabil, cel mai „inocent" dintre atacatori. Această persoană este un simplu trecător curios. Rareori se întâmplă ca el să compromită sistemele, în afara cazului în care întâlneşte o oportunitate serioasă [7].
- *Amatorul avansat* sau, altfel spus, *semi-profesionistul*, spre deosebire de vizitator, este greu de detectat şi de cele mai dese ori are o dorință specială de a face rău. Pentru mulți din această categorie scopul principal este să vadă cât de mult pot distruge [8].
- *Profesionistul* este diferit de toate celelalte categorii de intruşi: este o persoană bine antrenată, un spion profesionist al calculatoarelor. Aceste persoane se pricep foarte bine să intre într-un sistem de calcul şi să îl părăsească fără să fie observați în vreun fel [9].

Investigarea criminalistică a sistemelor informatice

Întâi de toate, trebuie să specificăm faptul că organele abilitate să efectueze controlul de stat în domeniul informatic sunt obligate, în procesul activităților de control, să ofere explicații cu privire la aplicarea cerințelor legislației în domeniul securității tehnologiilor informaționale şi să respecte procedura stabilită pentru protecția informației în funcție de gradul de criticitate şi importanță al acesteia [10]. Odată ce este respectată procedura stabilită pentru realizarea activităților de control de stat şi perfectarea rezultatelor acestor activități, se întreprind măsuri de lichidare a consecințelor încălcării cerințelor de securitate şi a regulilor de evaluare a conformității cu standardele solicitate. Controlul de stat presupune şi controlul existenței contractelor de licență şi al clarității în materia dreptului de proprietate asupra software-urilor şi respectării drepturilor de proprietate intelectuală [11].

Este bine cunoscut că doar o mică parte din faptele penale legate de utilizarea sistemelor informatice ajung la cunoştința organelor de drept, astfel încât e foarte greu de realizat o statistică a evoluției acestui fenomen şi a numărului real de infracțiuni comise.

S-a estimat că doar 5% din faptele comise ajung la cunoştința organelor de urmărire penală. Cifra neagră este motivată de mai multe cauze, dintre care menționăm:

- tehnologia sofisticată utilizată de făptuitori [12];
- lipsa instruirii specifice a colaboratorilor organelor de drept [13];
- lipsa unui plan de reacție în caz de atacuri, din partea victimelor acestor fapte penale, ceea ce poate duce la neidentificarea pierderilor provocate;
- temere, incertitudine şi neîncredere la sesizarea organelor de drept despre săvârşirea infracțiunilor.

În acest context, autoritățile şi instituțiile publice competente în domeniul prevenirii şi combaterii criminalității informatice în Republica Moldova sunt [14]:

1. Ministerul Afacerilor Interne, Serviciul de Informații şi Securitate şi Centrul pentru Combaterea Crimelor Economice şi Corupției – formează şi actualizează în permanență bazele de date privind criminalitatea informatică;
2. Ministerul Afacerilor Interne – desfăşoară activități operative de investigație, de urmărire penală, de cooperare internațională, de identificare a persoanelor care comit infracțiuni informatice;
3. Serviciul de Informații şi Securitate – desfăşoară activități de prevenire şi combatere a criminalității informatice ce prezintă amenințări la adresa securității naționale, activități operative de investigații, de depistare a legăturilor organizațiilor criminale internaționale;
4. Procuratura Generală:
   a) coordonează, conduce şi exercită urmărirea penală;
   b) dispune, în cadrul desfăşurării urmăririi penale, la solicitarea organului de urmărire penală sau din oficiu, conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, față de care există pericolul distrugerii ori alterării, în condițiile legislației de procedură penală;
   c) reprezintă învinuirea, în numele statului, în instanța de judecată.

Investigarea criminalistică a sistemelor informatice trebuie să prezinte o serie de caracteristici specifice, necesare asigurării unui grad înalt de corectitudine a concluziilor rezultate. Aceste caracteristici sunt [15]:

- ✓ *autenticitate* (dovada sursei de proveniență a probelor);
- ✓ *credibilitate* (lipsa oricăror dubii asupra credibilității şi soliditătii probelor);
- ✓ *completitudine* (prelevarea tuturor probelor existente şi integritatea acestora);
- ✓ *lipsa interferențelor şi contaminării probelor* ca rezultat al investigației sau al manipulării probelor după ridicarea acestora.

De asemenea, investigația criminalistică în domeniul tehnologiilor informaționale mai presupune [16]:

1) existența unor proceduri pre-definite pentru situațiile întâlnite în practică;
2) anticiparea posibilelor critici ale metodelor folosite, pe temeiul autenticității, credibilității, completitudinii şi afectării probelor oferite;
3) posibilitatea repetării testărilor realizate, cu obținerea unor rezultate identice;
4) anticiparea problemelor legate de admisibilitatea probelor;
5) acceptarea faptului că metodele de cercetare utilizate la un moment dat pot deveni subiectul unor modificări pentru viitor.

Pregătirea membrilor echipei ce participă la investigație. Natura infracțiunilor informatice cere ca urmărirea penală să se realizeze în cadrul unei echipe de investigatori. Atât datorită caracteristicilor speciale ale echipamentelor ce fac obiectul investigației, cât şi metodelor întrebuințate în investigarea criminalistică a sistemelor informatice, membrii echipei de investigatori trebuie să posede cunoştințe şi aptitudini adecvate specificului investigației. Astfel, e de menționat faptul că oponenții organelor de urmărire penală şi de constatare a infracțiunilor săvârşite prin Internet, de regulă, sunt persoane cu capacități intelectuale excepționale, posedă vaste cunoştințe profesionale atât în materie tehnică, cât şi juridică, iar posibilitățile de ordin material sunt sporite.

Un bun investigator trebuie să posede următoarele cunoştințe şi aptitudini [17]:

- cunoştințe suficiente asupra tehnicilor informatice, care să-i permită să înțeleagă funcționarea unui sistem informatic, să analizeze documentația tehnică şi să apeleze, dacă este nevoie, la tehnici informatice evoluate care să-l ajute în atingerea scopului urmărit;
- cunoştințe suficiente asupra tehnicilor utilizate de companii, în special asupra sistemelor contabile, pentru a putea înțelege caracteristicile sistemelor care ar putea face obiectul unor fraude, astfel încât să poată stabili atât modul de operare, cât şi să dirijeze investigația până acolo unde ar putea găsi probe relevante;
- cunoştințe suficiente asupra tehnicilor de securitate internă, astfel încât investigația să poată fi efectuată cu rapiditate şi fiabilitate şi să fie îndreptată în direcția corectă;
- înclinare spre detaliu [18];
- obiectivitate.

O primă decizie ce urmează a fi luată este cea de a analiza sistemul informatic la fața locului, sau ridicarea acestuia şi analiza în laborator. La luarea acestei decizii, trebuie luate în considerație următoarele aspecte:

- obținerea calității superioare în urma unei analize efectuate în condiții de laborator;
- măsura în care ridicarea sistemului informatic afectează activitatea bănuitului [19].

Utilitatea următoarelor criterii presupune aprecierea oportunității ridicării sistemelor informatice:

- criteriul volumului probelor [20];
- criteriul dificultăților de natură tehnică.

Înainte de a trece la examinarea sistemelor informatice, nu trebuie neglijate procedurile criminalistice tradiționale de analiză a spațiului percheziționat, cum ar fi prelevarea probelor fizice (amprente, alte urme materiale).

Recomandările generale, pe care ofițerul de urmărire penală, procurorul şi expertul/specialistul urmează să le îndeplinească la examinarea computerului la locul infracțiunii, sunt [21]:

- înainte de a deconecta computerul, este necesar, după posibilitate, de a închide toate programele utilizate de către acesta. Remarcăm faptul că ieşirea incorectă din careva programe poate duce la defectarea programului sau, şi mai grav, la lichidarea informației;
- a acorda importanță sporită şi a lua măsuri privind instalarea parolei de acces la programele securizate;

- la implicarea activă a colaboratorilor întreprinderii, care încearcă să împiedice grupul de urmărire penală, este necesar a deconecta sursa de energie a tuturor computerelor, a le sigila şi ridica împreună cu suportul magnetic pentru examinarea informației în condiții de laborator; în caz de necesitate, personalul poate fi trecut în altă încăpere;
- la apariția necesității, urmează să fie consultat personalul întreprinderii. În acest caz, se efectuează audierea separată a persoanelor. O astfel de metodă oferă posibilitatea de a obține o cantitate semnificativă de informație corectă şi de a evita survenirea daunelor intenționate;
- a stabili lista lucrătorilor temporari care activează în cadrul companiei în scopul identificării informaticienilor şi altor specialişti în sfera tehnologiilor informaționale. Prezența accesului la calculator sau la rețeaua de calculatoare reduce esențial cercul de persoane bănuite;
- înregistrarea datelor tuturor persoanelor care se află în instituție la momentul apariției grupului de urmărire penală, indiferent de explicațiile lor vis-à-vis de aflarea în instituția dată;
- a stabili lista colaboratorilor întreprinderii care au acces nemijlocit la tehnica computerizată.

Principalele acțiuni de urmărire penală pe astfel de cauze penale sunt: *percheziția* şi *expertiza tehnico-computerizată*.

Pentru efectuarea percheziției ofițerul de urmărire penală sau procurorul stabileşte în primul rând tactica efectuării acesteia, determină timpul începerii percheziției şi măsurile care asigură efectuarea ei pe neaşteptate (inopinat), precum şi confidențialitatea acesteia. Percheziția trebuie efectuată atunci când posibilitatea de a lucra la calculatorul în cauză este redusă la minimum [22], pentru a preveni ştergerea sau modificarea în alt mod a informației relevante procesului penal.

În literatura de specialitate găsim următoarele etape de relevare a probelor [23]:

1) *examinarea probelor* – examinarea detaliată a probelor, în vederea căutării elementelor care sunt în legătură cu fapta penală investigată [24];
2) *analiza probelor* – determinarea semnificației probelor şi relevarea concluziilor cu privire la fapta investigată;
3) *prezentarea probelor* – sintetizarea concluziilor şi prezentarea lor într-un mod clar pentru nespecialişti. Această sinteză trebuie susținută de o documentație tehnică detaliată;
4) *restituirea probelor* – dacă e cazul, returnarea către proprietarii de drept a obiectelor ridicate în timpul investigației.

Probele digitale (specifice infracțiunilor cibernetice) [25]**.** Probele digitale cuprind probele informatice, probele audio digitale, video digitale, cele produse sau transmise prin telefoane mobile, faxuri digitale etc.

Una dintre particularitățile acestui tip de probe este că ele aparent nu sunt evidente, fiind amplasate în echipamentele informatice ce le stochează. În acest sens, este nevoie de echipamente de investigație şi de software-uri specifice pentru a face ca aceste probe să fie disponibile, tangibile şi utilizabile.

Datorită perfecționării permanente a tehnicii de calcul, modul de realizare a investigațiilor informatice nu poate fi consemnat în acte normative, cu toate că ar prezenta o oportunitate în plus pentru reprezentanții organelor de drept la studierea materiei în cauză. Din acest considerent, organizațiile responsabile de aplicarea legii dezvoltă în mod continuu practici şi proceduri de natură să ghideze modul în care se realizează investigațiile, la un anumit nivel de avansare a tehnicii.

Procedura ridicării sistemelor informatice poate fi divizată în următoarele etape [26]**:**

Etapa I. ***Închiderea sistemului*** [27]**.** ***Fotografierea şi marcarea elementelor sistemului computerizat – un prim pas important.*** Întâi de toate, trebuie să fotografiem sistemul informatic în plan mare (fotografia de nod), din față şi din spate, fie prin filmare. Fotografierea şi marcarea elementelor sistemului computerizat, care urmează a fi ridicat, dă posibilitatea de a restabili cu exactitate starea tehnicii computerizate la examinarea ulterioară în condiții de laborator. Consemnarea, în variantă foto sau video, are relevanță şi pentru a arăta starea în care se găsea echipamentul în momentul ridicării, prevenind astfel plângerile legate de o eventuală deteriorare a acestuia în decursul cercetării.

După executarea măsurilor enumerate este necesar a efectua examinarea preliminară a tehnicii de calcul în scopul determinării programelor care lucrează la moment. În caz dacă se stabileşte că rulează un program de nimicire a informației, lucrul acestuia urmează a fi întrerupt şi examinarea, din acest moment, va începe anume de la respectivul calculator, iar toate aceste acțiuni, precum şi schimbările care au loc pe ecranul monitorului, se vor consemna în procesul-verbal. Dacă calculatoarele care se află în încăpere sunt conectate într-o

reţea locală, examinarea lor ar fi raţional să fie începută de la „server" [28], după care se va trece şi la restul calculatoarelor care funcţionează, precum şi la cealaltă tehnică de calcul şi la sursele de alimentare cu curent electric.

Dacă sistemul a fost găsit închis în momentul pătrunderii investigatorilor, sub nici un motiv acesta nu trebuie pornit. Se va proceda în continuare trecând la celelalte etape. Dacă însă sistemul a fost găsit deschis, el trebuie închis pentru a se putea proceda la ridicarea lui [29].

Expertul / specialistul. Dacă pentru examinare au fost incluşi un expert sau specialist, atunci acţiunile acestora obligatoriu se vor fixa procesual. Nu este exclus că o informaţie importantă (care ulterior poate fi folosită ca probă) să fie transmisă prin reţea în altă parte. Nu este exclus la fel şi cazul în care acest loc va fi un alt stat decât Republica Moldova, iar uneori informaţia necesară procesului penal poate să se afle în mai multe ţări concomitent. În acest caz, un specialist competent neapărat va sesiza aceste aspecte pentru a stabili locul celorlalte sisteme computerizate, unde a fost transmisă informaţia.

Verificarea de semne ale programelor virulente. Pentru aceasta, computerul nu trebuie încărcat din sistemul operaţional, procedeu inadmisibil, deoarece, ulterior, în şedinţa de judecată, există riscul să apară posibilităţi de a învinui organele de urmărire penală de introducere forţată şi intenţionată în calculator a programelor cu caracter virulent. Astfel de învinuiri pot pune la îndoială acţiunile expertului/specialistului şi concluziile acestuia.

Etapa a II-a. ***Etichetarea şi identificarea componentelor***. În cazul în care se impune dezasamblarea, fiecare component al sistemului trebuie etichetat înainte de modificarea configuraţiei în vederea ridicării probelor. În cazul cablurilor, se etichetează atât cablul, cât şi suporturile de unde a fost debranşat. În cazul existenţei unor suporturi care nu au conectate cabluri, este recomandabil să fie etichetate cu inscripţia „*neocupat*". Ar fi util să se realizeze şi o schiţă a componentelor, cu precizarea simbolurilor folosite pentru etichetare.

Etapa a III-a. ***Protejarea la modificare***. Toate suporturile magnetice de stocare a datelor trebuie protejate împotriva modificării conţinutului lor.

Accesul proprietarului la computerul confiscat şi copia de rezervă a informaţiei. În diferite surse de specialitate sunt descrise cazurile când bănuiţilor în săvârşirea infracţiunilor li s-a permis accesul la computerul confiscat. Mai târziu aceştia povesteau cunoscuţilor cum codificau file-urile „sub nasul poliţiştilor", iar aceştia din urmă nici nu bănuiau nimic. Pentru a evita astfel de cazuri, este necesar a limita la maximum accesul şi a împiedica orice apropiere a proprietarului de sistemul informatic [30]. Dacă totuşi colaboratorul organelor de drept ia decizia de a cerceta computerul, primul lucru ce urmează a fi efectuat este de a face copii de pe hard-disc şi dischete, care vor fi ridicate drept corpuri delicte [31].

Căutarea şi copierea file-urilor temporare. Multe software-uri pentru procesarea textelor şi programelor de administrare a bazelor de date creează file-uri temporare drept produs colateral al funcţionării normale a programului de asigurare. Majoritatea utilizatorilor computerului nu realizează importanţa creării acestor file-uri, de aceea ele sunt de obicei lichidate la sfârşitul lucrului. Însă, datele care se conţin pe aceste file-uri lichidate pot fi cele mai importante. Îndeosebi, dacă file-ul iniţial a fost cifrat sau documentul de pregătire a textelor a fost cules, dar niciodată nu s-a păstrat pe disc, astfel de file-uri pot fi restabilite.

Informaţiile ce nu pot fi imprimate de asemenea reprezintă surse importante pentru investigatori. Astfel de informaţii sunt: data şi timpul, ataşate fiecărui fişier, informaţiile despre crearea, accesarea şi modificarea unor fişiere (furnizate, de exemplu, de editoarele de text), comentariile şi notele ce nu sunt destinate imprimării etc.

Etapa a IV-a. ***Ridicarea propriu-zisă***. Ridicarea probelor trebuie făcută cu multă grijă, evitându-se orice avariere a componentelor. Este recomandabilă împachetarea componentelor în ambalajul original, dacă acesta poate fi găsit, sau în ambalaj special ce asigură protecţia electrostatică a acestora. De asemenea, toate suporturile magnetice de stocare a datelor vor fi ambalate şi sigilate în aşa fel, încât accesul la ele să nu fie permis până la despachetarea în laborator.

Fixarea rezultatelor cercetării. Metodica efectuării acţiunilor procesuale menţionate mai sus şi cerinţele faţă de actele procedurale ale acestor acţiuni sunt reglementate în articolele Codului de procedură penală al Republicii Moldova [32]. Veridicitatea procesului-verbal constă în corespunderea conţinutului acestuia cu ceea ce s-a depistat în timpul examinării, cu enumerarea tuturor obiectelor ridicate. Veridicitatea sporeşte şi atunci când, pe parcursul cercetării, au fost utilizate: tehnica criminalistică; mijloace speciale de depistare şi relevare a urmelor infracţiunii; scheme; înregistrări video; precum şi cunoştinţele specialiştilor care au

participat la cercetare [33]. În procesul examinării este necesar a reflecta în procesul-verbal şi în schema anexată la acesta locul aflării calculatorului şi a instalațiilor lui periferice (imprimantă, modem, tastieră, monitor şi alte componente), destinația fiecăreia, denumirea, numărul, seria, prezența conexiunii la rețeaua locală de calculatoare sau la rețelele de telecomunicații, starea instalațiilor.

Transportarea probelor în laborator [34]**.** Transportarea echipamentelor trebuie făcută cu multă grijă, având în vedere fragilitatea lor. Este necesar să fie luate precauțiuni legate de protejarea față de şocuri fizice, umiditate, căldură şi, mai ales, de influența undelor electromagnetice. În legătură cu acest din urmă aspect trebuie evitată plasarea echipamentelor în apropierea surselor de radiații electromagnetice, cum ar fi aparate de fax, copiatoare, stații radio, telefoane mobile. Este recomandabilă măsurarea cu instrumente speciale a câmpului electromagnetic în spațiile unde sunt depozitate echipamentele ridicate.

Analiza probelor. Echipamente necesare investigației [35]**.** Odată aduse în laborator, componentele trebuie asamblate pentru a reconstitui sistemul original. Pentru aceasta se vor folosi fotografiile sau casetele video cu înregistrările efectuate anterior ridicării probelor, respectându-se conexiunile originale, precum şi informațiile obținute de la martori în legătură cu practicile de utilizare a sistemului informatic respectiv.

Se recomandă ca analiza criminalistică a conținutului discului să se facă pe o copie fidelă a discului original, realizată în laborator cu ajutorul unor instrumente (programe şi dispozitive) speciale [36], acestea fiind numite măsuri de securitate [37]. Procedeul nu presupune doar copierea tuturor fişierelor aflate pe disc, ci a întregului conținut al discului, sector cu sector, inclusiv a fişierelor temporare, a fişierelor de schimb, a fişierelor şterse, chiar informația aflată pe porțiunile avariate ale discului etc. Se recomandă realizarea a două copii, pe una dintre ele realizându-se analiza propriu-zisă, cealaltă fiind o copie de rezervă [38].

Expertiza

Expertiza de bază şi cea mai importantă este cea a tehnicii de calcul şi a informației stocate în ea sau, cum mai este numită în literatura de specialitate [39], tehnico-programistă sau tehnico-computerizată.

Efectuarea unei astfel de expertize la noi în țară este posibilă în laboratorul de expertize judiciare inginero-tehnice de la Centrul Național de Expertize Judiciare sau cu atragerea specialiştilor cu calificarea respectivă din alte instituții, chiar şi din alte state.

Pentru soluționare, expertizei tehnico-programiste i se pot înainta următoarele întrebări [40]:

1. Ce fel de informații conțin blocurile de sistem şi purtătorii magnetici? Care este destinația lor şi care sunt posibilitățile de utilizare?
2. Se conțin pe blocurile de sistem şi suporți magnetici fişiere textuale? Dacă da, care este conținutul şi posibilitățile de utilizare a acestora?
3. Se află informație distrusă pe suporții magnetici prezentați? Este posibilă restabilirea ei? Dacă da, care este conținutul şi posibilitățile de utilizare?
4. Ce fel de produse de programă se conțin pe suporții magnetici? Care este conținutul lor, destinația şi posibilitatea de utilizare?
5. Putea oare blocul de sistem, prezentat spre cercetare, să fie scos intenționat din funcțiune de către posesorul lui? Dacă da, prin ce metodă? [41]
6. Se află pe suporți magnetici programe specializate, utilizate pentru selectarea parolei sau a altui procedeu de pătrundere ilegală în rețeaua de calculatoare? Dacă da, care este denumirea şi particularitățile lor, posibilitățile utilizării acestora pentru pătrundere în rețeaua computerizată concretă?
7. Care este cauza lipsei accesibilității către purtătorul magnetic de informație, prezentat spre cercetare? [42]
8. Sunt careva semne ce confirmă utilizarea programei concrete pentru pătrunderea ilegală în rețeaua computerizată menționată? Dacă da, atunci care este structura cronologică a acțiunilor necesare pentru pornirea programei concrete sau pentru efectuarea unei operațiuni concrete?
9. Este posibil, lucrând în rețeaua computerizată concretă, de a efectua în produsele de program careva modificări ale fişierelor? Dacă da, atunci care, în ce mod şi de la care calculator pot fi făcute schimbări analogice?
10. Există posibilitatea de a primi acces la informația confidențială care se află în rețeaua indicată? În ce mod se efectuează un astfel de acces?
11. În ce mod are loc accesul ilegal în rețeaua computerizată locală? Care sunt semnele ce confirmă o astfel de pătrundere?

12. Dacă accesul ilegal la sistemul de operare a avut loc din afară, atunci care sunt posibilităţile de identificare a calculatorului de la care a avut loc accesul?

13. Dacă lipsesc semnele pătrunderii în reţeaua de calculatoare de la un utilizator exterior, atunci se poate constata de la care calculator este posibil a efectua operaţiuni asemănătoare?

Pot fi înaintate spre soluţionare şi întrebări privind compatibilitatea unor sau altor programe, posibilitatea utilizării programei concrete la un calculator concret şi la altele de acest gen.

În afară de acestea, putem pune întrebări despre destinaţia unui sau altui obiect utilizat în tehnica de calcul, precum: care este destinaţia obiectului, posibilităţile utilizării şi ce fel de particularităţi constructive el are; din ce părţi constă acesta; a fost elaborat în condiţii industriale sau în condiţii artizanale; dacă obiectul a fost confecţionat în condiţii artizanale, atunci în care sfere ale ştiinţei, tehnicii şi meşteşugăritului posedă cunoştinţe persoana care a creat acest obiect, care este nivelul de pregătire a persoanei indicate; poate fi compatibil obiectul menţionat cu alte obiecte, care sunt acestea? [43].

Asistenţa juridică internaţională în materie penală şi criminalitatea informatică

Conştientizarea pericolului social al faptelor penale de natură informatică a atras încriminarea acestora în numeroase state ale lumii. A luat astfel fiinţă conceptul de „drept penal cu specific informatic", ca o reflectare a numeroaselor elemente de noutate introduse în materia dreptului penal, de noile forme de criminalitate bazate pe tehnologia modernă. Legiferarea în domeniul criminalităţii informatice datează cu anii '70.

În acest sens, la nivel internaţional, Consiliul Europei a iniţiat o serie de reglementări cu privire la criminalitatea informatică. Astfel, dacă în 1995 a fost adoptată Recomandarea nr. R (95) 13 cu privire la problemele de procedură penală legate de tehnologiile informaţionale, atunci în 23 noiembrie 2001 a fost semnată, la Budapesta, Convenţia privind criminalitatea informatică [44]. Convenţia îşi propune să prevină actele îndreptate împotriva confidenţialităţii, integrităţii şi disponibilităţii sistemelor informatice, a reţelelor şi a datelor, precum şi a utilizării frauduloase a unor asemenea sisteme, reţele şi date, prin asigurarea incriminării unor asemenea conduite şi prin încurajarea adoptării unor măsuri de natură să permită combaterea eficace a acestor tipuri de infracţiuni, menite să faciliteze descoperirea, investigarea şi urmărirea penală a acestora. Drept puncte de pornire, pentru elaborarea Convenţiei, au servit un şir de alte acte normative internaţionale, anume:

- ✓ Convenţia Consiliului Europei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal (1981);
- ✓ Convenţia Naţiunilor Unite privind drepturile copilului (1989);
- ✓ Convenţia Organizaţiei Internaţionale a Muncii privind interzicerea celor mai grave forme ale muncii copiilor (1999);
- ✓ Recomandările Comitetului de Miniştri al Consiliului Europei:
  - nr. R (85) 10 privind aplicarea în practică a Convenţiei Europene de asistenţă judiciară în materie penală, referitoare la comisiile rogatorii pentru supravegherea telecomunicaţiilor;
  - nr. R (88) 2 privind măsurile vizând combaterea pirateriei în domeniul drepturilor de autor şi al drepturilor conexe;
  - nr. R (87) 15 vizând reglementarea utilizării datelor cu caracter personal în sectorul poliţiei;
  - nr. R (95) 4 privind protecţia datelor cu caracter personal în domeniul serviciilor de telecomunicaţii, cu referire specială la serviciile de telefonie;
  - nr. R (89) 9 referitoare la criminalitatea în legătură cu utilizarea calculatorului, care indică structurilor legiuitoare naţionale principiile directoare pentru definirea anumitor infracţiuni;
  - nr. R (95) 13 privind problemele de procedură penală în legătură cu tehnologia informaţiei.

Astfel, fiecare stat, parte contractantă a Convenţiei, adoptă măsuri legislative şi alte măsuri care se dovedesc a fi necesare pentru a obliga un furnizor de servicii în domeniul informaticii să păstreze confidenţialitatea oricărei informaţii în legătură cu acest subiect.

De asemenea, Convenţia prevede, în caz de urgenţă, că fiecare parte poate formula o cerere de asistenţă mutuală prin mijloace rapide de comunicare, precum faxul sau poşta electronică, cu condiţia ca aceste mijloace să ofere condiţii suficiente de securitate şi de autentificare (inclusiv folosirea codării, atunci când este necesar), cu o confirmare oficială ulterioară, dacă partea solicitată va revendica acest lucru. Partea solicitată va accepta cererea şi va răspunde prin oricare dintre mijloacele sale rapide de comunicare.

O altă poziție interesantă, pe care o oferă Convenția, se remarcă prin faptul că o parte poate, în limitele dreptului său intern şi în absența unei cereri prealabile, să comunice unei alte părți informații obținute în cadrul propriilor anchete (investigații), în cazul în care consideră că acest lucru ar putea ajuta partea destinatară la începerea sau finalizarea cu succes a procedurilor având ca obiect infracțiuni stabilite în domeniul tehnologiilor informaționale. În acest sens, un punct şi mai interesant este că orice cerere sau comunicare formulată în baza celor expuse mai sus poate fi avansată prin intermediul Organizației Internaționale de Poliție Criminală (Interpol), ceea ce sporeşte considerabil operativitatea investigării.

Din punctul nostru de vedere, conservarea rapidă a datelor informatice stocate în rezultatul efectuării acțiunilor de urmărire penală reprezintă o lecție bine însuşită de părțile contractante la Convenția privind criminalitatea informatică. Astfel, o cerere de conservare va trebui să precizeze:

a) autoritatea care solicită conservarea;
b) infracțiunea care va face obiectul urmăririi penale, precum şi o scurtă expunere a faptelor care au legătură cu aceasta;
c) datele informatice stocate care vor trebui conservate şi natura legăturii lor cu infracțiunea;
d) toate informațiile disponibile care vor permite identificarea posesorului datelor informatice stocate sau locația sistemului informatic;
e) necesitatea măsurii conservării;
f) faptul că partea are intenția de a formula o cerere de asistență mutuală în vederea percheziției ori accesării printr-un mijloc similar, sechestrului sau obținerii printr-un mijloc similar, ori divulgării datelor informatice în cauză.

Un aspect plauzibil este faptul că Convenția prevede ca fiecare parte contractantă să desemneze un punct de contact disponibil 24 de ore din 24, 7 zile din 7, în scopul asigurării unei asistențe imediate pentru investigațiile referitoare la infracțiunile privind sisteme sau date informatice, sau pentru a strânge dovezile unei infracțiuni în format electronic.

Concluzii şi recomandări

Suntem conştienți de profundele schimbări determinate de digitalizarea, convergența şi globalizarea continuă a rețelelor de calculatoare. Astfel, în acest scop, în Republica Moldova s-a făcut un pas important, prin crearea unei Secții specializate în cadrul Procuraturii Generale [45], apoi prin elaborarea şi semnarea unui plan comun de acțiuni [46] în a căror realizare vor fi implicate diferite instituții statale [47].

Prin urmare, există necesitatea perfecționării procesului de investigare a infracțiunilor informatice prin:

1) elaborarea instrumentelor metodice şi dezvoltarea unui sistem terminologic unic, general valabil;
2) inițierea creării laboratorului de prevenire şi investigare a infracțiunilor cibernetice;
3) reglementarea în Codul de procedură penală a procedeului probatoriu de conservare a datelor informatice ori a datelor referitoare la traficul informatic [48];
4) organizarea seminarelor şi cursurilor specializate în domeniu pentru reprezentanții organelor de drept, mai cu seamă pentru procurori şi ofițerii de urmărire penală, dar şi pentru judecători (ghiduri, metodici general accesibile [49]);
5) elaborarea unor mecanisme de colaborare între instituțiile statale, private, mass-media, societatea civilă, în scopul prevenirii şi combaterii infracțiunilor săvârşite prin intermediul tehnologiilor informaționale.

Referințe:

1. IRC – este abrevierea Internet Relay Chat, un serviciu care permite comunicarea în timp real folosind mesaje text – chat-ul.
2. www.riti-internews.ro.
3. Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică elaborat de „Internews Network, RITI dot-GOV" şi „USAID". - Bucureşti, 2004, p.73.
4. Dobrinoiu M. Infracțiuni în domeniul informatic. - Bucureşti, 2006, p.246.
5. www.mcti.ro.
6. Este destul de uşor a depista, deoarece nu este capabil să îşi „şteargă urmele". Rezultatele „muncii" acestuia pot fi găsite, de regulă, în câteva locații: 1) fişiere cu parole; 2) fişiere de configurare pentru utilizatori; 3) fişiere de configurare a sistemului. Cea mai bună metodă de a combate novicii este educarea utilizatorilor, deoarece novicii profită de lipsurile în administrarea parolelor.

7. Dacă un vizitator va găsi un obstacol, de cele mai multe ori se va retrage, căutând alt sistem unde accesul este mai uşor. O excepţie de la această regulă, foarte rară, este situaţia în care vizitatorul observă un lucru interesant şi este dispus să îşi mai petreacă ceva timp pentru a-l putea studia.
8. În general, ei folosesc greşeli de programare a sistemului de operare pentru a ocoli mecanismele de autentificare şi a primi acces neautorizat la sistem.
9. Ei alterează sau ocolesc aplicaţiile de jurnalizare a activităţilor la fel de uşor cum pot compromite orice parte a sistemului. Cea mai bună apărare faţă de aceşti atacatori este evitarea conexiunii în reţea a sistemelor care conţin informaţii importante şi controlul strict al accesului fizic la acestea.
10. Дремлюга Р.И. Интернет-Преступность: Монография. - Владивосток: Издательство Дальневосточного Университета, 2008.
11. Asigurarea securităţii informaţionale la prestarea serviciilor publice electronice. Cerinţe tehnice, 2009, aprobat prin ordin al Procurorului General (nepublicat).
12. Ei alterează sau ocolesc aplicaţiile de jurnalizare a activităţilor la fel de uşor cum pot compromite orice parte a sistemului. Cea mai bună apărare faţă de aceşti atacatori este evitarea conexiunii în reţea a sistemelor care conţin informaţii importante şi controlul strict al accesului fizic la acestea.
13. Pregătirea personalului de specialitate este un proces de durată şi implică costuri considerabile. Asemenea investigaţii sunt consumatoare de timp. Un investigator în domeniul criminalităţii informatice poate lucra maximum asupra 3-4 cazuri pe lună, în timp ce un investigator tradiţional poate soluţiona între 40 şi 50 de cazuri în aceeaşi perioadă de timp.
14. Legea Republicii Moldova privind prevenirea şi combaterea criminalităţii informatice, nr.20 din 03.02.2009 // Monitorul Oficial al Republicii Moldova 2010, nr.11-12/17.
15. Богомолов М.В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации. - Красноярск, 2002, с.69.
16. Alecu Gh. Particularităţi ale investigaţiei penale şi criminalistice a unor infracţiuni din domeniul informatic // Avocatul poporului (Chişinău), 2005, nr.8, p.2; nr.9, p.7.
17. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. - Москва: Норма, 2004.
18. Foarte importantă, mai ales având în vedere specificul probelor electronice: abundenţa informaţiilor aflate pe un spaţiu de stocare de dimensiuni fizice reduse.
19. Lucaci I., Marin R. Investigarea infracţiunilor informatice. - Bucureşti: M.I., 2002, p.72.
20. Particularitatea sistemelor informatice de a permite stocarea unui volum foarte mare de informaţie într-un spaţiu de dimensiuni fizice reduse face ca investigaţia să necesite un volum mare de timp pentru obţinerea probelor relevante. Astfel de cercetări pot fi conduse mult mai eficient în laborator.
21. Вехов В.Б. Компьютерные преступления. Способы совершения методики расследования. - Москва, 1996.
22. Leu C. Cercetarea la faţa locului în cazul infracţiunilor informatice (Criminalitatea informatică), Volum: Investigarea criminalistică a locului faptei. - Bucureşti: Luceafărul, 2004, p.159.
23. Olteanu I.O. Metodologie Criminalistică – Cercetarea structurilor infracţionale şi a unora dintre activităţile ilicite desfăşurate de acestea. - Bucureşti: AIT Laboratories, 2005, p.405.
24. Acest lucru presupune localizarea şi identificarea probelor, precum şi documentarea fiecărui pas, în scopul facilitării analizei.
25. www.internews.org.
26. Vasiu L., Vasiu I. Informatică juridică şi drept informatic. - Cluj-Napoca: Albastră, 1997, p.81-83.
27. Dacă este posibil accesul nemijlocit la computer, se începe examinarea.
28. *Server* – un dispozitiv (combinaţie de hardware şi software) care oferă servicii şi / sau informaţii utilizatorilor (clienţilor).
29. Pentru închiderea sistemului se pot folosi următoarele procedee: • deconectarea de la alimentarea cu energie electrică; • închiderea conform procedurii obişnuite.
30. Mai ales dacă bănuitul are pregătire superioară în domeniul informatic, acesta poate altera voit datele aflate pe calculatorul său, fără ca investigatorii să poată sesiza acest lucru. Calculatorul bănuitului poate conţine unele comenzi ce pot produce pierderea datelor, comenzi ce pot fi mascate sub numele unor comenzi uzuale ale sistemului de operare folosit. Dacă bănuitul insistă să ajute investigatorii în procesul de închidere a calculatorului sau a procesului de ridicare a componentelor sistemului, aceştia pot cere bănuitului să le descrie operaţiunile pe care acesta doreşte să le execute, şi chiar să le scrie pe hârtie. Investigatorii nu vor urma indicaţiile bănuitului, ci le vor remite experţilor care efectuează analiza probelor. Aceştia vor putea fi avertizaţi în acest mod de eventualele capcane introduse de bănuit.
31. De obicei, probele computerizate se adună pe calea creării copiei exacte a originalului (probelor primare) până a purcede la analiza acestora. Dar, crearea copiilor file-urilor, utilizând doar programe–standard ale copierii de rezervă, nu este suficient. Corpurile delicte pot fi păstrate în formă de file-uri (lichidate sau ascunse (camuflate)), iar datele legate de aceste file-uri pot fi păstrate doar cu ajutorul unor programe de securitate speciale.

32. Codul de procedură penală al Republicii Moldova, nr.122-XV din 14.03.2003 // Monitorul Oficial al Republicii Moldova, 2003, nr.104-110/447, art.124, 260 şi 261.
33. Metodologia de efectuare a cercetării la faţa locului, examinării corporale şi a obiectelor, aprobată prin Ordin al Procurorului General (nepublicat).
34. Доценко С.М., Шпак В.Ф. Комплексная безопасность объекта: от теории к практике. - С.-Петербург: Полигон, 2000, с.16.
35. Alecu Gh. Criminalistică: Curs universitar. - Constanţa: Ovidius University Press, 2004, p.37.
36. Ghid privind criminalitatea informaţională, investigarea şi efectuarea urmăririi penale în privinţa infracţiunilor din domeniul informaticii şi telecomunicaţiilor, 2006, aprobat prin Ordin al Procurorului General (nepublicat).
37. *Măsuri de securitate* – folosirea unor proceduri, dispozitive sau programe informatice specializate, cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori / Legea Republicii Moldova privind prevenirea şi combaterea criminalităţii informatice, nr.20 din 03.02.2009 // Monitorul Oficial al Republicii Moldova, 2010, nr.11-12/17.
38. Este recomandată consemnarea detaliată a întregului proces de copiere, indicând echipamentele, programele şi mediile de stocare utilizate.
39. Dobrinoiu M. Provocarea legislativă a reţelelor WI-FI // Intelligence, 2009, nr.16.
40. Ярочкин В.Я. Информационная безопасность: Учебник для вузов. - Москва: Gaudeamus, 2004.
41. Gheorghita M., Brega Z., Vozniuc L., Stativca T., Malcoci N., Zaborot A., Cazangiu E., Ciobanu A., Lâsâi A., Sandu I., Iacub V. Grosu D. Ghid de expertize judiciare. - Chişinău: Î.I. „Angela Levinţa", 2005, p.77.
42. Ibidem, p.83.
43. Recomandări metodice privind metodologia de investigare a criminalităţii informaţionale şi a fraudelor prin Internet, 2007, Ordin al Procurorului General (nepublicat).
44. Convenţie privind criminalitatea informatică din 23 noiembrie 2001, Budapesta. Publicată în Monitorul Oficial al Republicii Moldova, 2004, nr.343, Partea I. Seria Tratatelor Europene nr.185; ratificată prin Legea Parlamentului Republicii Moldova nr.6-XVl din 02.02.2009.
45. Secţia Tehnologii Informaţionale şi Investigaţii ale Infracţiunilor în domeniul Informaticii.
46. Ordin al Procurorului General cu privire la aprobarea Planului comun de Acţiuni în domeniul prevenirii şi combaterii criminalităţii cibernetice, nr.103/428/105/198/58/168/47/104/184-10/G din 20 decembrie 2010 (nepublicat).
47. Instituţiile vizate sunt: Procuratura Generală, Ministerul Afacerilor Interne, Ministerul Tehnologiilor Informaţionale şi Comunicaţiilor, Centrul pentru Combaterea Crimelor Economice şi Corupţiei, Serviciul de Informare şi Securitate, Agenţia de Stat pentru Proprietatea Intelectuală, Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, Întreprinderea de Stat „Centrul de Telecomunicaţii Speciale", Institutul Naţional al Justiţiei.
48. Planul comun de Acţiuni în domeniul prevenirii şi combaterii criminalităţii cibernetice din 20 decembrie 2010 (nepublicat).
49. Infracţiunile informaţionale – parte integră a infracţiunilor economice; www.security.ase.md./rom/cerneiv.doc

Prezentat la 30.12.2010