STUDIA UNIVERSITATIS MOLDAVIAE, 2017, nr.8(108)
Seria "Științe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.146-152

CZU: 343.139:004.7

MĂSURI TACTICE ȘI STRATEGICE DE DEPĂȘIRE A OBSTACOLELOR CARE ÎMPIEDICĂ BUNA DESFĂȘURARE A INVESTIGĂRII INFRACȚIUNILOR INFORMATICE

Mihail GHEORGHIȚĂ, Svetlana PURICI

Universitatea de Stat din Moldova

Una dintre sarcinile de bază ale investigării criminalității cibernetice este stabilirea tuturor circumstanțelor săvârșirii infracțiunii. Totuși, realizării acesteia deseori se opun persoanele care doresc eschivarea infractorului de la răspunderea penală. Nu doar distrugerea informației computerizate poate fi îndreptată în vederea ascunderii urmelor infracțiunii. Cu același scop poate fi efectuată blocarea sau modificarea informației. În acest din urmă caz infractorul va îndrepta investigarea într-o direcție greșită. Această metodă este cea mai periculoasă, deoarece infractorul își poate masca identitatea prin modificarea datelor din registrele electronice, prin preschimbarea adresei IP, precum și a pachetelor de date, fiind create probe false.

Cuvinte-cheie: *măsuri tactice, împotrivire, depășirea obstacolelor, provocare. probe digitale, distrugerea informației, simulare, infractor cibernetic.*

TACTICAL AND STRATEGIC MEASURES TO REMOVING THE OBSTACLES WHICH HELPS TO THE INVESTIGATION AGAINST OF CYBERCRIMES

One of the basic tasks of investigating cybercrime is to establish all the circumstances of the offense. However, when doing so, they often oppose people who want to escape the offender from criminal responsibility. Not just the destruction of computerized information can be directed to hide the traces of the offense. For the same purpose, blocking or changing information can be made. In the latter case, the offender will direct the investigation in the wrong direction. The latter method is the most dangerous, the offender can mask his identity by modifying the data in the electronic registers, changing the IP address, and data packets, creating false evidence.

Keywords: *tactical measures, resistance, overcoming obstacles, cause, digital samples, destruction of information, simulation, cybercriminal.*

Introducere

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

Progresul semnificativ de dezvoltare a tehnologiilor informaționale și a mijloacelor care formează spațiul cibernetic a devenit nu doar un beneficiu, dar a generat și apariția urmărilor negative, pericolelor legate de posibilitatea utilizării acestor tehnologii și mijloace în scopuri incompatibile cu sarcinile de asigurare a securității și stabilității internaționale.

Rezultate și discuții

1. Clasificarea obstacolelor care perturbă desfășurarea normală a procesului penal

Apărută la începutul anilor '90 ai secolul XX, teoria învingerii împotrivirii urmăririi penale ține de criminalistică și este inclusă în această știință ca o teorie particulară. La formarea acestei teorii au contribuit mai mulți criminaliști (Белкин Р. și alții) [1].

Una dintre sarcinile de bază ale investigării criminalității cibernetice este stabilirea tuturor circumstanțelor săvârșirii infracțiunii. Totuși, realizării acesteia deseori se opun persoanele care doresc eschivarea infractorului de la răspunderea penală, creând impedimente la realizarea sarcinilor de serviciu de către organele de drept [2, p.80].

În dependență de factorii care generează apariția obstacolelor ce perturbă desfășurarea normală a procesului penal, acestea pot fi clasificate în [3, p.13]:

1) obiective: care apar și acționează independent de voința persoanei (spre exemplu: condițiile meteorologice nefavorabile, care au generat distrugerea urmelor infracțiunii sau deteriorarea neprevăzută a mecanismului);

2) subiective: provocate de către făptuitor, de către alte persoane în interesele acestuia, precum şi greşelile/ omisiunile organului de urmărire penală;

3) *relativ obiective*: ele nu depind de voinţa anumitor persoane, însă pot fi luate în calcul de către acestea. Un exemplu ar fi particularităţile suporturilor de stocare a datelor electronice, care pot sta la baza distrugerii informaţiei.

Totodată, piedicile create la investigarea crimelor cercetate pot fi clasificate în *legale* (dreptul acuzatului de a nu da declaraţii, dreptul părţilor de a înainta cereri şi demersuri, lipsa răspunderii acuzatului în cazul depunerii declaraţiilor false, obligaţia organului de urmărire penală de a verifica versiunile apărării) şi *ilegale* (declaraţiile false ale martorilor, victimei). Cele legale, la rândul lor, pot fi divizate în *vădite* (spre exemplu, refuzul de a da declaraţii) şi *camuflate* – în care suspectul exteriorizează dorinţa de a contribui la stabilirea adevărului pe caz şi disponibilitatea de a acorda ajutorul necesar organului de urmărire penală, deşi intenţia sa este de a direcţiona urmărirea penală pe o cale greşită. Cele camuflate reprezintă o capcană periculoasă pusă în faţa organului de urmărire penală.

Cel mai des declaraţii false sunt depuse de către acuzat (72%), martori (18%), victimă (10%). Aceasta se datorează strategiei de comportare alese de către infractor, posibilităţilor lui, precum şi specificului infracţiunii investigate [3, p.26]. În majoritatea cazurilor, în cadrul audierii sale, acuzatul va palpa nivelul cunoştinţelor în domeniul tehnologiilor informaţionale de care dispune persoana care îl audiază. Ulterior, în baza acestei informaţii, el se va prezenta drept o persoană insuficient de capabilă de a utiliza sistemele informatice sau de a avea intenţii infracţionale.

Spre exemplu, apărarea Cal Troian urmăreşte aplicarea regulii *„in dubio pro reo"* ca şi complement al prezumţiei de nevinovăţie contestând identificarea făptuitorului şi având în practica judiciară şanse de succes doar în măsura în care practicienii şi instanţele cunosc şi înţeleg realităţile societăţii digitale. Aceasta mai cu seamă în cauzele în care trimiterea în judecată s-a făcut exclusiv pe baza probelor digitale incriminatoare prelevate din sistemul informatic al suspectului ori al inculpatului (ex.: fotografii cu minori în ipostaze sexuale explicite) şi fără a adresa corespunzător şi a elimina aspectele de posibil control de la distanţă asupra sistemului informatic, ori viruşii existenţi care ar fi putut comite fapta în mod automatizat, precum şi în cauzele în care percheziţia informatică nu este completată şi de alte procedee probatorii, precum: supravegherea operativă, documentarea profilului persoanei investigate, operaţiuni financiare în legătură cu fapta şi altele similare menite a-l plasa pe inculpat „la tastatură" la momentul comiterii faptei, ori a proba distinct fapta sub aspectul laturii subiective, aşa cum o indică de altfel manualele de bune practici în investigarea infracţiunilor de criminalitate informatică [4, p.168].

2. Scopurile influenţării activităţii de urmărire penală a crimelor săvârşite în domeniul criminalităţii cibernetice

Scopul cererilor şi demersurilor părţii apărării este îndreptat, de regulă, în vederea impunerii versiunii sale prezentând faptele suspectului ca fiind inofensive, urmărindu-se totodată de a supraîncărca organul de urmărire penală cu un volum mare de informaţie pentru a-l dezorienta. Doar examinarea acestora, de admitere sau de respingere, răpeşte mult timp şi sustrage organul de drept de la activitatea de bază a investigaţiei. O altă tehnică utilizată este de a încurca organul de urmărire penală în terminologie, precum şi în procesele utilizate în sistemele informatice; cu acest scop se înaintează demersuri cu privire la efectuarea diferitelor expertize.

Nu doar distrugerea informaţiei computerizate poate fi îndreptată în vederea ascunderii urmelor infracţiunii. Cu acelaşi scop poate fi efectuată blocarea sau modificarea informaţiei. În acest din urmă caz infractorul va îndrepta investigarea într-o direcţie greşită [5, p.3]. Această metodă este cea mai periculoasă, deoarece infractorul îşi poate masca identitatea prin modificarea datelor din registrele electronice, preschimbarea adresei IP, precum şi a pachetelor de date, fiind create probe false [6, p.152].

Orice nedescoperire a crimei şi neidentificare a făptuitorului acesteia permite infractorului să continue activitatea sa, dar şi practica negativă îi permite să înţeleagă erorile, pe care nu trebuie să le admită la săvârşirea unei crime analogice.

Influenţarea activităţii de urmărire penală a crimelor săvârşite în domeniul supus analizei, de regulă, urmăreşte scopurile [3, p.52]:

– de a prezenta infracţiunea săvârşită drept o activitate socialmente nepericuloasă, adică non-penală, comisă din curiozitate;

– de a reda fapta comisă drept o consecinţă întâmplătoare, în lipsa unei intenţii infracţionale, cauzată de lipsa la făptuitor a cunoştinţelor aprofundate în domeniul tehnologiilor avansate. Apărarea prin invocarea

nepriceperii utilizatorului, care susţine, spre exemplu, că nu a avut intenţia de a pune la dispoziţie materialele ilegal descărcate prin sistemele de partajare de fişiere [7] şi nu a ştiut că programul de partajare punea automat la dispoziţie în reţea documentele descărcate [8];

– de a demonstra că acţiunile făptuitorului sunt rezultatul unei constrângeri insurmontabile şi au fost săvârşite exclusiv în interesul societăţii;

– de a convinge despre onestitatea persoanei suspecte, care, ca şi organul de urmărire penală, doreşte să stabilească adevărul şi în final să-şi confirme nevinovăţia;

– de a demonstra părtinirea şi reaua-credinţă a persoanei care efectuează urmărirea penală, nedorinţa ei de a stabili toate circumstanţele cauzei;

– de a prezenta suspectul drept o victimă a crimei, datorită evoluţiei nefavorabile a circumstanţelor cauzei;

– de a argumenta necesitatea efectuării anumitor acţiuni procesuale în vederea îndreptării procesului penal într-un punct mort;

– de a argumenta inadmisibilitatea efectuării anumitor acţiuni (inclusiv procesuale) pentru ca anumite împrejurări la săvârşirea infracţiunii să rămână neidentificate;

– de a crea impresia despre incompetenţa persoanei care efectuează urmărirea penală (cum ar fi lipsa abilităţilor de a investiga o cauză complexă);

– de a forma o opinie publică pozitivă despre suspect.

La investigarea infracţiunilor informatice cele mai răspândite forme de opunere de rezistenţă sunt:

1) *Tăinuirea infracţiunii şi a probelor* (63%). În jumătate din cazuri de crime cibernetice infractorii tind să concentreze crearea obstacolelor în vederea ridicării şi cercetării suporturilor de stocare a informaţiei electronice. În acest scop năzuiesc să substituie suporturile respective şi să creeze impresia la examinarea acestora că nu a fost săvârşită infracţiunea.

Una dintre cauzele succesului activităţii de opunere a rezistenţei întru descoperirea infracţiunilor informatice este latenţa sporită a acestor categorii de crime. Multiple acţiuni în domeniul tehnologiilor informaţionale, precum şi datele informatice pot fi uşor depersonalizate. Totuşi, datele informatice nu sunt lipsite de anumite semne care să le individualizeze. Încă de la etapa pregătirii infracţiunii, făptuitorul întreprinde măsuri pentru a nu fi identificată crima, investigată şi descoperită [9, p.161]. Baza informaţională este foarte complicată pentru citire, de regulă, necesită decodificare şi doar după aceasta poate fi utilizată în investigaţie.

2) *Înscenarea* (27%). Cele mai des întâlnite înscenări pe cazurile de criminalitate informatică sunt:

- simularea faptului că informaţia a fost afectată în rezultatul utilizării proaste a acesteia de către persoanele care aveau drept de acces la ea;
- virusarea din neatenţie de către persoanele care aveau drept de acces la informaţia computerizată;
- defecţiunea suportului de stocare a informaţiei electronice, chipurile din motive independente de voinţa persoanelor;
- imitarea unei alte fapte prejudiciabile pentru a distrage atenţia organului de urmărire penală [6, p.152].

„Hackerii", care au abilităţi tehnice şi profesionale mai bune decât alte categorii de infractori cibernetici, preferă utilizarea înscenărilor, iar în unele cazuri şi a tăinuirii crimei.

3) Formarea unei opinii publice favorabile infractorului (3%). Aceasta se efectuează nu doar prin utilizarea mijloacelor tradiţionale de informare în masă (periodică, televiziune şi radio), dar şi prin publicaţii în reţeaua Internet. Ea este specifică persoanelor care încalcă regulile de exploatare a sistemelor şi reţelelor informatice.

4) Influenţarea directă a organului de urmărire penală (7%). Organele de drept sunt învinuite pe nedrept în depăşirea atribuţiilor de serviciu, efectuarea defectuoasă a urmăririi penale şi altele. De regulă, partea apărării contestă prin toate căile posibile (la procuror, la procurorul ierarhic superior, la judecătorul de instrucţie etc.) legalitatea, temeinicia şi corectitudinea efectuării acţiunilor procesuale. Un alt reprezentant al organului de urmărire penală, cunoscând cauzele înlăturării de la efectuarea urmăririi penale a colegului său, este mai cooperant cu partea apărării şi va accepta mai uşor propunerile acesteia referitor la desfăşurarea procesului penal.

5) *Şantajarea victimei:* cu începerea/continuarea atacurilor cibernetice asupra resurselor informatice ale acesteia, cu răspândirea informaţiilor confidenţiale despre ea, care i-ar putea afecta reputaţia.

În cazul constatării de către apărător a unor greşeli admise de către organul de urmărire penală aceasta poate avea două finalităţi. În cel mai bun caz, avocatul o va arăta organului de urmărire penală. Totuşi, partea apărării va putea lăsa sub tăcere erorile admise până la momentul prielnic din punct de vedere tactic, chiar până la cercetarea judecătorească a cauzei, în speranţa folosirii lor pentru a „distruge dosarul" şi obţinerii unei sentinţe de achitare sau de încetare a procesului penal [6, p.184].

3. Calitățile persoanelor ce creează obstacole la efectuarea investigărilor privind infracțiunile informatice

Persoanelor care creează obstacole la efectuarea investigațiilor cu privire la crimele în domeniul informației computerizate (bănuiți – 61%, învinuiți – 42%, martori – 26%, părți vătămate – 7%, apărători – 21%, alți participanți la proces – 10%) le sunt caracteristice următoarele calități [3, p.77]:

– nivel sporit de rezistență la stres;
– abilitate de concentrare în situații critice;
– foarte critici în aprecierea situațiilor apărute;
– echilibrați emoțional;
– siguri în puterile lor intelectuale;
– nivel intelectual înalt.

Printre persoanele care împiedică buna desfășurare a procesului penal sunt:

– infractorul;
– apărătorul acestuia;
– rudele făptuitorului;
– prietenii, colegii de serviciu;
– persoanele care au temerea de a nu fi răspândită informația ce le poate afecta imaginea (în iunie 2011 hackerii au reușit să obțină acces la datele cardurilor bancare a 360.000 de persoane, ceea ce a fost confirmat recent de către oficialii băncii. Trei săptămâni la rând colaboratorii băncii nu au informat organele de drept, fapt ce a expus clienții la prejudicii și mai mari) [10].

În ultima perioadă, specific crimelor cibernetice este faptul că obstacole la investigarea infracțiunii sunt create de către persoane necunoscute infractorului. Aceasta sunt hackerii, care sunt predispuși la formarea unor mișcări în Internet în vederea neadmiterii tragerii la răspundere a altor „colegi de breaslă", în semn de solidaritate.

Printre instrumentele utilizate la crearea piedicilor în fața organului de urmărire penală putem regăsi:

– produsele program utilizate la comiterea infracțiunii, care nu lasă urme, făptuitorii le șterg instant și/sau criptează informația [11, p.63];
– când este imposibilă distrugerea urmelor sunt folosite softuri care fac inadmisibilă identificarea persoanei sau utilizarea accesării prin servere intermediare [12, p.158];
– programe care, în opinia infractorului, nu pot fi identificate de către sistemele de securitate;
– folosirea remailers, care reprezintă calculatoare ce primesc mesaje, pe care făptuitorii le redirecționează către adresa electronică de la destinație, ștergând toate datele despre expeditor [13, p.556];
– păstrarea datelor informatice la distanță [11, p.63];
– utilizarea manevrelor de distragere a atenției (de exemplu, atacuri cibernetice);
– utilizarea posibilităților tehnice de tăinuire a crimei, asigurate cu alte metode și mijloace (cum ar fi situația în care victimei îi este inconvenabilă atragerea atenției cu privire la crima săvârșită, având în vedere faptul că-i poate dăuna statutului său).

Metodele și mijloacele de depășire a rezistenței opuse trebuie selectate în dependență de caracterul și specificul obstacolelor.

În literatura juridică activitatea organului de urmărire penală îndreptată în vederea învingerii împotrivirii la efectuarea procesului penal sunt folosiți doi termeni: „*neutralizarea obstacolelor*" [14, p.75] și „*depășirea obstacolelor*" [15, p.77].

Depășirea obstacolelor la investigarea infracțiunilor informatice presupune rezolvarea următoarelor sarcini și aplicarea următoarelor măsuri:

✓ asigurarea confidențialității la colectarea informațiilor despre crima comisă și suspecți, acțiunile procesuale planificate sau realizate [16, p.236] (prin limitarea/interzicerea conectării/deconectării la rețeaua Internet a sistemelor informatice – obiect al crimei; prin continuarea activității online a victimei pentru a nu atrage atenția la investigațiile efectuate; prin planificarea cronologiei activităților procesuale, astfel încât acțiunile față de persoanele care pot divulga datele investigațiilor să fie realizate în ultimă instanță; prin efectuarea percheziților sau ridicărilor în perioada de timp când poate fi evitată prezența masivă de martori; prin efectuarea controlului permanent al tuturor mesajelor electronice expediate de către subdiviziunea care efectuează investigația pe caz; prin stabilirea defecțiunilor în sistemul de securitate a informației în sistemele informatice ale victimei, precum și pericolele ascunse în sistemele informatice accesate neautorizat);

✓ colectarea datelor despre persoanele care au acces la documente şi care pot întreprinde acţiuni în vederea distrugerii probelor (organul de urmărire penală, precum şi judecătorul de instrucţie va trebui să menţioneze cât mai puţină informaţie despre investigaţiile efectuate şi persoanele suspecte în actele procesuale care vor fi prezentate persoanelor terţe – furnizori de servicii internet, operatori de telefonie etc.);

✓ stabilirea informaţiilor necesare pentru pornirea urmăririi penale, precum şi pe parcursul procesului penal;

✓ identificarea surselor din care pot fi dobândite probe;

✓ planificarea efectuării măsurilor speciale de investigaţii îndreptate în vederea obţinerii informaţiilor, care pot fi utilizate la învingerea impedimentelor cu privire la investigarea cazului. Astfel de date pot viza personalitatea infractorului, persoanele care pot oferi ajutor făptuitorului, informaţiile cu privire la activităţile planificate de către infractorul cibernetic [3, p.154];

✓ ofiţerul de urmărire penală trebuie să colaboreze cu organul care efectuează activitatea specială de investigaţii, să-l orienteze cu privire la informaţiile care trebuie colectate, să monitorizeze continuu activitatea acestuia şi să verifice corectitudinea informaţiilor prezentate [17, p.240];

✓ anticiparea posibilelor piedici care pot apărea la colectarea materialelor, precum şi a comportamentului infractorului [18, p.190], planificarea şi realizarea acţiunilor de zădărnicire a acestora, inclusiv măsuri de ordin tehnic (identificarea softurilor speciale destinate pentru prevenirea accesului neautorizat la informaţie, instalarea filtrelor) [2, p.152];

✓ planificarea şi efectuarea activităţilor de depăşire a obstacolelor deja existente, cu implicarea specialistului în domeniul tehnologiilor informaţionale;

✓ organizarea şi întreprinderea acţiunilor îndreptate în vederea învingerii piedicilor legate de efectuarea urmăririi penale trebuie pusă în sarcina ofiţerului de urmărire penală sau a conducătorului grupului de urmărire penală [18, p.216];

✓ în vederea constatării existenţei cazurilor de influenţare necuvenită a angajaţilor organelor de drept şi anihilării acestora, efectuarea concomitentă a câtorva măsuri procesuale care se dublează, identificarea surselor de influenţare, stabilirea scopului şi sarcinilor acesteia, strecurarea informaţiilor false cu privire la activităţile planificate de către suspect, alegerea unei măsuri preventive mai severe;

✓ ridicarea sistemelor şi dispozitivelor informatice utilizate la comiterea infracţiunii chiar la etapa incipientă a procesului penal. Este o măsură-cheie menită să prevină apariţia şi efectul negativ al obstacolelor la investigaţie [19, p.167];

✓ colectarea probelor suplimentare. Organul de urmărire penală trebuie să acorde o atenţie sporită identificării făptuitorului real, spre exemplu: neputându-se prezuma din simpla prezenţă a materialelor ilegale în sistemul informatic aparţinând suspectului ori inculpatului că acesta se face vinovat de comiterea faptei, în lipsa unor probe suplimentare pe cât posibil de altă natură decât informatică [4, p.168].

Luând în considerare complexitatea şi rafinamentul activităţii de zădărnicire a investigării crimelor informatice, măsurile de învingere a acestora trebuie să fie organizate minuţios şi la nivel superior, cu utilizarea operaţiunilor tactice [20, p.295].

În acest sens, de cele mai deseori este necesară utilizarea posibilităţilor tehnice ale sistemelor informatice şi ale produselor program, pentru a bloca accesul ilegal al persoanelor interesate la informaţia computerizată aflată în reţele informatice.

Astfel de operaţiuni tactice, specifice acestor categorii de crime, sunt [3, p.165]:

– ridicarea purtătorilor de stocare a informaţiei computerizate în legătură cu care au fost săvârşite faptele ilegale;
– înaintarea acuzării bănuitului şi audierea acestuia.

4. Alibiul digital

Autorul rus H.A. Иванов menţionează despre „*alibiul digital*", şi anume: despre activitatea suspectului la calculator în momentul săvârşirii infracţiunii [21, p.31].

Practica denotă că stabilirea faptului absenţei persoanei bănuite la locul săvârşirii infracţiunii în timpul când aceasta s-a produs încă nu înseamnă că persoana respectivă nu are nicio atribuţie la fapta săvârşită. Persoana putea să nu apară în calitate de executor nemijlocit al infracţiunii, ci să fie complice al acesteia în calitate de organizator sau instigator. Posibilităţile tehnice moderne, aflate „în serviciul" infractorilor (de exemplu, mijloacele de telefonie mobilă, Internetul, Skype etc.) permit organizatorului infracţiunii să ţină sub control

situaţia criminală, să coordoneze acţiunile complicilor, să le dirijeze pe măsura parvenirii din partea lor a unor semnale urgente şi să elaboreze în baza analizei lor indicaţiile de rigoare. Înaintarea (declararea) alibiului are ca scop împotrivirea de a stabili adevărul în cauză şi încercarea de a influenţa sistemul probatoriu în folosul său. Alibi înseamnă altundeva, în altă parte [2, p.87].

Tot mai des, bănuiţii, când fac referinţă la „*alibiul digital*", motivează prin faptul că în momentul săvârşirii infracţiunii ei lucrau la calculatorul personal (se foloseau de telefoanele mobile personale, se aflau în perimetrul de observaţie al camerelor de supraveghere, se conectau la reţelele informatice prin autorizare personală), care în realitate se afla în altă parte. Acesta şi îl putem numi „*alibi digital*". În astfel de cazuri, organul de urmărire penală trebuie să efectueze în primul rând acţiunea tactică de audiere a persoanei care invocă „*alibiul digital*". Aici, organul de urmărire penală urmează să stabilească legătura directă dintre localizarea bănuitului în momentul săvârşirii infracţiunii şi sistemul electronic aflat la distanţă, în alt loc, făcând loc apariţiei noţiunii de *urme virtuale* [22]. În astfel de situaţii, sub incidenţa urmelor materiale cad amprentele papilare de pe tastatură, urme formate în urma secreţiilor sudoripare, etc. Timpul formării acestor urme este extrem de greu de stabilit, datorită interacţiunii permanente a persoanei cu dispozitivele externe ale sistemului informatic. Urmele ideale rămân totuşi a fi în mintea şi conştiinţa persoanei, cea care nemijlocit manipulează cu un sistem informatic concret.

În urma analizei logice a tutror informaţiilor pe un caz concret organul de urmărire penală elaborează versiunile:

1) bănuitul (învinuitul) posedă „*alibiu digital*";
2) bănuitul (învinuitul) nu posedă „*alibiu digital*";
3) „*alibiul digital*" al bănuitului (învinuitului) a fost falsificat.

Atragerea specialistului la identificarea unei sau altei versiuni este indispensabilă. Astfel, organul de urmărire penală poate apela la cunoştinţele specialistului în momentul audierii, chiar şi la pregătirea întrebărilor care vor fi adresate bănuitului. În momentul audierii, cercetării la faţa locului poate fi chiar indicată participarea specialistului pentru a explica şi a ajuta la identificarea circumstanţelor aferente cazului, la fixarea şi ridicarea probelor, precum şi la monitorizarea celor relatate de către bănuit, pentru a evita dezorientarea organului de urmărire penală. În asemenea cazuri, organul de urmărire penală trebuie să determine profilul necesar de cunoştinţe speciale ale specialistului pe care îl va atrage în cadrul acţiunilor procesuale, deoarece este imposibil ca cel din urmă să posede cunoştinţe în toate domeniile informaţiilor computerizate [23].

De asemenea, la verificarea versiunilor „*alibiului digital*" organul de urmărire penală va atrage atenţia dacă bănuitul real posedă aptitudini speciale profesionale în domeniul tehnologiilor informaţionale (deţinerea diplomei, verificarea notelor obţinute, descrierea competenţelor şi experienţei de către colegii de serviciu, stimulările angajatorului, stagiul de lucru, practică anumit hobby în domeniu). În scopuri criminalistice putem obţine „portretul psihologic" şi chiar date de identificare (nume, data, anul naşterii), precum şi numerele de telefoane, adrese electronice ale persoanei care invocă „*alibiul digital*" din informaţia plasată de către aceasta în reţeaua Internet, şi anume: în reţelele sociale (ex. Facebook, Instagram, Odnoklassniki, Vkontakte etc). Toată această informaţie este publică, se regăseşte în reţeaua Internet, ceea ce nu necesită autorizare, astfel uşurând considerabil lucrul organului de urmărire penală.

După demascarea „alibiului fals" (una dintre formele cele mai răspândite de împotrivire), bănuitului, învinuitului i se propune să relateze obiectiv despre cele săvârşite şi rolul lui în infracţiunea cercetată [2, p.91].

Concluzii

Au dispărut timpurile când hackerii erau profesionişti şi, având cunoştinţe performante în ceea ce priveşte echipamentele informatice, puteau face minuni cu ajutorul codurilor de program. Acum orice adolescent studios, curios, dar nu deosebit de împovărat de principii morale, este capabil să creeze utilizatorilor obişnuiţi o mulţime de probleme.

Unui intrus, pentru a avea acces la informaţii confidenţiale, uneori chiar nu-i este nevoie de competenţe particulare şi abilităţi. În multe cazuri, acţionează factorul uman, cum ar fi o bucată de hârtie pe monitor sau sub sticlă lângă tastatură în care este scrisă parola. Parolele, de obicei, nu posedă prea multă originalitate. Şi în adâncimile Internetului se poate găsi întotdeauna un program care îşi va asuma munca de rutină de identificare a celor mai evidente parole.

Orice nedescoperire a crimei şi neidentificare a făptuitorului acesteia permite infractorului să continue activitatea sa, dar şi practica negativă îi permite să înţeleagă erorile, pe care nu trebuie să le admită la săvârşirea unei crime analogice.

Astfel, metodele şi mijloacele de depăşire a rezistenţei opuse trebuie selectate în dependenţă de caracterul şi specificul obstacolelor.

La investigarea infracţiunilor informatice cele mai răspândite forme de opunere de rezistenţă sunt tăinuirea infracţiunii şi a probelor, înscenarea, formarea unei opinii publice favorabile infractorului, şantajarea victimei.

Referinţe:

1. БЕЛКИН, Р.С. *Криминалестическое обеспечение деятельности криминальной милиции и органов предварительного расследования.* Москва: Новый Юрист, 1997. 400 с.
2. GHEORGHIŢĂ, M. *Tratat de Metodică criminalistică.* Chişinău: CEP USM, 2015. 531 p.
3. КОСЫНКИН, А.А. *Преодоление противодействия расследованию преступлений в сфере компьютерной информации:* Монография. Москва: Юрлитинформ, 2013, с.216.
4. PURICI, S. *In dubio pro reo:* Apărarea Cal Troian în cauzele de criminalitate informatică. În: *Penalmente* (Bucureşti), 2016, nr.2.
5. ГАЛКИН, А.И. Компьютерная информация как обьект уголовно-правовой защиты. В: *Следователь. Федеральное издание* (Москва), 2009, №4.
6. ОСИПЕНКО, А.Л. О характеристике способов совершения сетевых компьютерных преступлений. В: *Вестник криминалистики* (Москва), 2009, №.4(32).
7. *United States vs Dodd, 598 F.3d 449, 451-53 (8th Cir. 2010).*
8. *United States vs Creel783 F.3d 1357, 1357 (11th Cir. 2015).*
9. ГОЛОВИН, А. Ю. *Криминалистическая систематика.* Москва: ЛексЭст, 2002.
10. *Крупные атаки хакеров в 2001-2016 годах: хронология,* ТАСС, 29 august 2016. Disponibil pe http://tass.ru/info [Accesat: 15.06.2017].
11. МЕНЖЕГА, М.М. *Методика расследования создания и использования вредоносных программ для ЭВМ.* Москва: Юрлитинформ, 2010. 168 с.
12. AMZA, T., AMZA, C.P. *Criminalitatea Informatică*. Bucureşti: Lumina LEX, 2003. 509 p.
13. ШУРУХНОВ, Н.Г. *Криминалистика:* Учебное пособие. Москва: Юристь, 2005. 639 с.
14. СИДОРЕНКО, Е.В. Взаимодействие государственного обвинителя и оперативных работников в нейтрализаци преступного пртиводействия осушествлению судебного рассмотрения уголовного дела. В: *Криминалистический вестник,* 2005, №4.
15. ТЕПУКОВ, А.В. Преодоление противодействия доказыванию по уголовным делам в отношении прокуроров, руководителей следственных органов и следователей. В: *Закон и право,* 2009, №6.
16. БАБАЕВА, Э.У. *Проблемы теории и практики преодоления противодействия уголовному преследованию.* Москва: Юрлитинформ, 2006, с.312.
17. КРИВЕНКО, А.И. *Теория и практика взаимодействия следователя с органами, осушествляющими оперативно-розыскную деятельность.* Москва: Юрлитинформ, 2008, с.240.
18. РАТИНОВ, А.Р. *Судебная психология для следователей.* Москва: Юрлитинформ, 2001, с.352.
19. СТАРИЧКОВ, М.В. Тактика проведения обыска, связанного с изъятием носителей компьютерной информации. В: *Криминалистика: актуальные вопросы теории и практики: Сборник седьмой Всероссийской науч.-практ. конференции.* Ростов-на-Дону, 2010.
20. МЕРЕЦКИЙ, Н.Е. Опыт использования тактических комбинаций при расследовании преступлений. В: *Актуальные вопросы криминалистического обеспечения судопроизводства: Материалы Всероссийской науч.-практ. конференции.* Иркутск, 2010.
21. ИВАНОВ, Н.А. Применение специальных познаний при проверке «цифрового алиби». В: *Информационное право,* 2006, №4.
22. МЕЩЕРЯКОВ, В.А. *Преступления в сфере компьютерной информации: правовой и криминалистический анализ.* Москва, 2001; КРАСНОВА Л.Б. *Компьютерные объекты в уголовном процессе и криминалистике.* Воронеж, 2005, с.152.
23. ПОНОМАРЕВ, И.П. Цифровое алиби. В: *Воронежские криминалистические чтения*: Сборник научных трудов. Том.12. Воронеж: Изд-во Воронежского государственного университета, 2010, с.275.

Prezentat la 19.06.2017