Nicolae PLOTEANU, Rodica GRINIUC,
Academia „Ştefan cel Mare" a MAI

INVESTIGAREA CRIMELOR COMPUTAȚIONALE

Abstract: Cybercrimes have a very big price on economical plan, so it is very necessary for contemporary society to study and investigate those crimes. This article contains definitions, obiections and models of investigation in stages of informational attacs and cybercrimes, from international practice.

Actualmente suntem martorii unor mari schimbări în accentele de bază ale dezvoltării socio-economice şi politice ale țării noastre. Cele mai recente proiecte informaționale au menirea de a accelera integrarea în Comunitatea Europeană şi informatizarea proceselor social-economice. Cele mai mari ecouri în viața social-economică actuală, în care sunt antrenate majoritatea instituțiilor de stat şi private, sunt Decretul preşedintelui Republicii Moldova şi Hotărârea Guvernului privitoare la "Strategia Națională de edificare a societății informaționale în RM" – "Moldova Electronică", stabilite ca priorități naționale.

Apariția numeroaselor companii ce acordă servicii în domeniul ***tehnologiilor informaționale*** este un atribut al societății noastre. Creşterea numărului de pagini WEB private în rețelele globale generează interesul față de Republica Moldova.

Explozia tehnologiilor informaționale, pe lângă efectele pozitive în viața social-economică şi politică a lumii, a dat naştere şi unor comportamente situate în afara legii, luând forme care nu au existat anterior. Sistemele informatice, care au schimbat radical modul de viață al oamenilor, au oferit noi ocazii, mult mai sofisticate, prin care legea poate fi încălcată; în acelaşi timp, au oferit mijloace noi de comitere a unor delicte tradiționale care până acum nu au mai fost experimentate.

Într-o societate care suportă repercusiunile economice şi sociale ale criminalității informatice, zilnic se face uz de calculatoare în aproape toate domeniile, de la controlul traficului aerian, feroviar şi circulația autobuzelor şi până la coordonarea serviciilor medicale şi securitatea națională. Cea mai măruntă dificultate în funcționarea acestor sisteme poate pune în pericol mii de vieți omeneşti, fapt care ne demonstrează incidența noilor tehnologii asupra ființei umane, pe de o parte, şi, pe de altă parte, dependența societății față de noile sisteme informatizate.

Marile rețele informatice au avut o ascensiune extrem de rapidă atât în plan național, cât, şi mai ales, în plan transnațional, făcând posibilă accesarea numeroaselor sisteme atât prin legăturile telefonice normale, cât şi prin intermediul telefoniei celulare. Accesul la bazele de date

tot mai numeroase a sporit şi vulnerabilitatea acestor sisteme, iar ocaziile de a face uz în mod abuziv sau de a le folosi în scopuri criminale, nu au întârziat să apară.

Criminalitatea informatică poate să aibă un preț foarte ridicat pe plan economic, dar şi în termenii securității umane. Problema definirii delictului informatic poate apărea ca o preocupare de noutate pentru societățile unde accesul noilor tehnologii s-a făcut cu întârziere şi unde statul nu a luat încă toate măsurile de protecție împotriva crimelor care pot fi comise cu ajutorul acestora.

Criminalitatea informatică reprezintă totalitatea faptelor comise în zona tehnologiilor informaționale, într-o anumită perioadă de timp bine determinată şi pe un anumit teritoriu. Ca orice fenomen social, criminalitatea informatică reprezintă un sistem cu proprietăți şi funcții proprii, distincte calitativ de cele ale elementelor componente.

Este cunoscut faptul că, în cercetarea criminologică, criminalitatea ca fenomen social cuprinde:

- criminalitatea reală – presupune totalitatea faptelor penale săvârşite pe un anumit teritoriu şi într-o anumită perioadă de timp;
- criminalitatea aparentă – cuprinde întregul set de infracțiuni semnalate organelor abilitate ale statului şi înregistrate ca atare;
- criminalitatea legală – reprezintă totalitatea faptelor de natură penală comise în spațiul tehnologiilor informaționale şi pentru care s-au pronunțat hotărâri judecătoreşti rămase definitive. Fiecare acest segment de criminalitate îşi are corespondența şi în criminalitatea informatică.

Diferența dintre criminalitatea informatică reală şi criminalitatea informatică aparentă reprezintă ***cifra neagră*** a acestui nou gen de crimă şi ea cuprinde toate faptele sancționate de legiuitor, dar care, din anumite motive, rămân nedescoperite de către organele abilitate ale justiției penale.

Dacă în cadrul criminalității generale se apreciază că cifra neagră reprezintă un important segment de fapte penale nedescoperite, în cadrul criminalității informatice, procentul acesteia tinde să fie în jur de 90%. Această rată extrem de ridicată a crimelor nedescoperite se datorează faptului că infracțiunea informatică este un act ilegal mai recent sancționat şi se află ascuns în spatele noilor tehnologii informaționale.

Investigarea criminalistică a sistemelor informatice prezintă o serie de particularități care o diferențiază în mod fundamental de alte tipuri de investigații. Investigarea criminalistică a sistemelor informatice poate fi definită ca: utilizarea de metode ştiințifice şi certe de asigurare, colectare, validare, identificare, analiză, interpretare, documentare şi prezentare a probelor de natură digitală, obținute din surse de natură informatică în scopul facilitării descoperirii

adevărului în cadrul procesului penal.

Un algoritm din practica investigațiilor criminalistice de natură informatică cuprinde următorii paşi:

1. Identificarea incidentului – recunoaşterea unui incident şi determinarea tipului acestuia. Nu reprezintă efectiv o etapă a investigației criminalistice, dar are un impact semnificativ asupra următoarelor etape.
2. Pregătirea investigației – pregătirea instrumentelor, verificarea procedurilor, obținerea documentelor ce permit percheziția etc.
3. Formularea strategiei de abordare – formularea unei strategii în funcție de tehnologia implicată şi de posibilele consecințe asupra persoanelor şi instituțiilor implicate. Scopul formulării acestei strategii este să maximizeze potențialul obținerii de probe relevante, minimizând în acelaşi timp impactul negativ asupra victimei.
4. Asigurarea probelor – izolarea, asigurarea şi păstrarea probelor de natură fizică şi digitală. Aceasta include îndepărtarea celor care ar putea denatura probele în orice fel.
5. Colectarea probelor – înregistrarea ambianței fizice şi copierea probelor digitale, folosind practici şi proceduri comune şi acceptate.
6. Examinarea probelor – examinarea în profunzime a probelor în căutarea elementelor care sunt în legătură cu fapta penală investigată. Acest lucru presupune localizarea şi identificarea probelor, precum şi documentarea fiecărui pas în scopul facilitării analizei.
7. Analiza probelor – determinarea semnificației probelor şi relevarea concluziilor cu privire la fapta investigată.
8. Prezentarea probelor – sintetizarea concluziilor şi prezentarea lor într-un mod inteligibil pentru nespecialişti. Această sinteză trebuie susținută de o documentație tehnică detaliată.
9. Restituirea probelor – dacă este cazul, returnarea către proprietarii de drept a obiectelor reținute în timpul investigației. Dacă este cazul, determinarea, în funcție de prevederile legilor procedurale penale, a confiscării obiectelor.

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*:

1. Autenticitate (dovada sursei de proveniență a probelor);
2. Credibilitate (lipsa oricăror dubii asupra credibilității şi solidității probelor);
3. Completitudine (prelevarea tuturor probelor existente şi integritatea acestora);
4. Lipsa interferențelor şi a contaminării probelor ca rezultat al investigației sau al

manipulării probelor după ridicarea acestora.

Bibliografia:

1. Tudor Anza, Criminolodie – Tratat de teorie şi politică criminologică, Editura Lumina Lex, Bucureşti, 2002.
2. Tudor Amza Criminolodie, Editura Lumina Lex, Bucureşti, 1998.
3. Statele Unite ale Americii, legea infracțiunilor prin computer, NMSA 1978, cap. 30, art. 45-1 până la art. 45-7.
4. Serge Ia Doran şi Philippe Rosé, Cyber-Mafia, Editura Antet, Bucureşti, 1998, p. 164.
5. „Ghidul introductiv pentru aplicarea dispozițiilor referitoare la criminalitatea informatică”, Bucureşti, 2004.