N. PLOTEANU,
Academia M.A.I. "Ştefan cel Mare"

ANALIZA FRAUDELOR INFORMAȚIONALE INVESTIGATE ÎN REPUBLICA MOLDOVA ÎN 2007

Fraudelor informaționale în Moldova, ca şi în toată lumea, conform statisticii mondiale se află într-o continuă creştere. Societatea trebuie să mobilizeze şi să utilizeze toate pârghiile legislative posibile pentru stoparea acestor momente negative, să informeze cetățenii despre măsurile şi mecanismele posibile de prevenire a fraudelor informaționale.

Până la mijlocul anilor '90, în fosta URSS, se considera că crimele computeriale sunt un atribut numai al țărilor occidentale, avansate în sfera tehnologiilor informaționale moderne şi, din cauza nivelului mic de informatizare a societății, adică slaba utilizare, în producție şi în relațiile sociale, a tehnologiilor informaționale moderne, lipseşte, în general. Anume acest fapt a şi dus la lipsa unor cercetări ştiințifice serioase în acest domeniu.

La noi în Moldova, numai pe parcursul ultimului deceniu, şi-au făcut apariția nişte avize, lucrări, rapoarte nesemnificative despre unele mici incidente ici-colo în domeniul fraudelor informatice, în timp ce Occidentul se cutremura de epidemiile virusologice şi atacurile hackerilor. Aceste informații poate că i-au pus în gardă pe legiuitori despre viitorul informatizării societății şi problemele juridice ce pot apărea.

Putem constata faptul că dezvoltarea societății merge după spirală – vechea formulă. Cu infracționalitatea informatică se întâmplă ca şi cu celelalte momente negative din societate, cum s-a întâmplat şi mai înainte, de exemplu, situația cu narcomania sau crima organizată, lupta cu aceste elemente sociale a început doar atunci când pierderile materiale de pe urma acestora au atins cantități enorme şi au început a se evidenția în fondul total de pierderi de pe urma crimelor obişnuite. Adică, până la anii '90, se spunea că nu există asemenea vicii în societatea noastră, iar după '90 nu ştim cum să ne luptăm cu amploarea acestor elemente negative în societate.[1]

Prima dată, despre problemele luptei cu crimele computeriale din spațiul țărilor CSI, au început să ridice problema specialiştii criminologi în Rusia, unde nivelul informatizării societății era mai înalt, în comparație cu alte state din comunitatea CSI, ştiința criminalistică, oficial, a menționat în iulie 1992 din momentul creării seminarului interdepartamental, care activează continuu "Criminalistica şi crima computerială", organizat de către procuratura Generală a Federației Ruse şi Centrul Expert-Criminalist al MAI din Rusia.

Republica Moldova, de asemenea, s-a ciocnit cu probleme din domeniul criminalității informatice; statistica mondială atenționează procentul exagerat al pirateriei software în țările Europei de sud-vest.

Eforturile depuse de conducerea țării noastre, în 2006-2007, pentru rezolvarea acestei probleme îi bucură chiar şi pe cei de la compania Microsoft, care se consideră cea mai afectată companie de pirateria software.

În cadrul seminarului-traning "Aplicarea legislației în domeniul protejării dreptului de autor asupra programelor computaționale", ce a avut loc la 28 noiembrie 2007, reprezentantul Business Software Alliance în Moldova, Oleg Efrim, a menționat că vânzările de soft licențiat, în 2007, în Republica Moldova, au întrecut prognoza companiei Microsoft. Dl Efrim, de asemenea, a menționat că este dispus ca în țară să fie create toate condițiile pentru ca pe viitor R. Moldova să îmbunătățească esențial situația privind pirateria software.[2]

Actualmente se cunosc o mulțime de clasificări ale riscurilor şi incidentelor computaționale. *O clasificare simplistă este o listă de termeni definiți pe plan internațional:*

1. Interceptarea cablurilor şi a semnalelor emise *(Wiretapping, Eavesdropping on Emanations);*

---

[1] N. Ploteanu, Definirea infracțiunilor informațional-computeriale, Conferința ştiințifico-practică internațională „Criminalitatea în Republica Moldova: Starea actuală, tendințele, măsurile de prevenire". Chişinău 18-19.04.2003.

[2] Лицензионное програмное обеспечение, Экономическое обозрение "ЛОГОС-ПРЕСС", nr.44, 30.11.2007, c.21.

2. Căutarea prin fişierele şterse *(Dumpster diving);*
3. Refuzarea serviciului *(Denial-of-service);*
4. Hărțuire *(Harassment);*
5. Mascare *(Masquerading);*
6. Pirateria software *(Software piracy);*
7. Copierea neautorizată de date *(Unauthorized data copying);*
8. Degradarea serviciului *(Degradation of service);*
9. Analiza traficului *(Traffic analysis);*
10. Uşi ascunse *(Trap doors);*
11. Canale ascunse *(Covert channels);*
12. Viruşi şi viermi *(Viruses and worms);*
13. Deturnarea sesiunii *(Session hijacking);*
14. Atacuri temporale *(Timing attacks);*
15. Forare *(Tunneling);*
16. Cal troian *(Trojan horses);*
17. Simulare IP *(IP spoofing);*
18. Bombe logice *(Logic bombs);*
19. Distrugerea datelor *(Data diddling);*
20. Tehnica tăierii salamului *(Salamis);*
21. Interceptarea parolelor *(Password sniffing);*
22. Privilegii excesive *(Excessprivileges);*
23. Scanare *(Scanning).*[3]

Statisticile companiilor ce activează în domeniul securității informaționale confirmă că, în majoritatea cazurilor, programele din compartimentul spyware sunt folosite pentru obținerea informațiilor strict confidențiale, cum ar fi:

a) parola de acces în sistemele informaționale sau fişiere;
b) loghinul (ID) personal în sistemul informațional;
c) numărul conturilor bancare;
d) datele personale confidențiale.

Se pare că este imposibil a lupta cu programele spy, dar specialiştii din domeniul securității informaționale sunt într-o continuă cercetare. În scopul prevenirii furturilor de informații de către spioni se recomandă:

a) utilizarea parolelor de unică folosință (autentificarea dublă);
b) utilizarea sistemelor de protecție activă, utilitare destinată depistării spionilor cu actualizarea regulată a bazelor cu coduri;
c) utilizarea tastierelor virtuale.

[3] Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică, USAID din România, Bucureşti, 2004.