Protecția informației. Prevenirea și curmarea fraudelor informatice

Autor: Tatiana Busuncian
Dr., conferențiar universitar

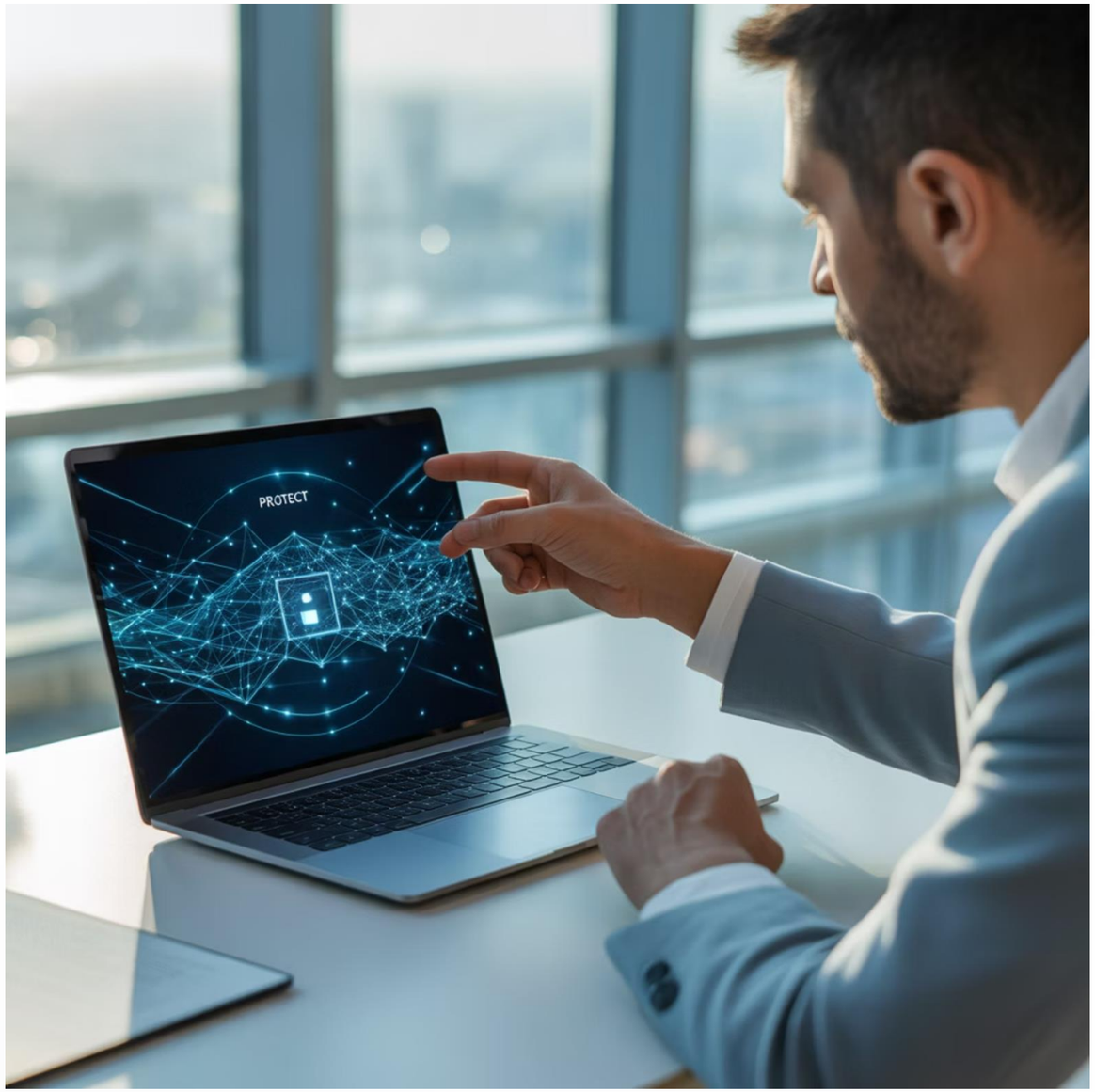
Chișinău 2026

Conținuturi și Obiective de referință

Obiective de referință:

- să definească caracteristicile securității informaționale
- să determine instrumentele și metodele de luptă cu amenințările cibernetice
- să evalueze motivele criminalității cibernetice și să descrie eforturile întreprinse pentru asigurarea securității informaționale
- să estimeze importanța prevenirii amenințărilor complexe și persistente la adresa securității informaționale

Termeni-cheie: securitate informațională, știri false, mediul informațional, pericol, politică



Asigurarea securității informaționale

> Spațiul informațional reprezintă o platformă confortabilă pentru pregătirea și efectuarea crimelor informatice, a actelor de terorism cibernetic și a altor acțiuni maliţioase, menite să afecteze, direct sau indirect, securitatea națională.

Penetrarea sistemelor informaționale sau de comunicații electronice ale autorităților administrației publice și ale altor instituții și întreprinderi de stat sau private poate duce la compromiterea confidențialității, integrității sau disponibilității informației sensibile. Această situație poate genera prejudicii financiare sau de altă natură, inclusiv afectarea securității statului.

În cazul Republicii Moldova, penetrarea sistemelor informatice aferente infrastructurii critice poate conduce la obținerea controlului neautorizat asupra acestor sisteme, afectând procesele economice, sociale, politice, informaționale și militare.

Misiuni primordiale în prevenirea agresiunilor cibernetice

Misiunile de prevenire și combatere a agresiunilor din mediul virtual, intern sau extern, sunt îndreptate spre sistemele informatice și de comunicații electronice de importanță statală. Acestea se realizează prin procese operaționale specifice:

01

Elaborarea propunerilor de securitate

Dezvoltarea și promovarea politicii de stat pentru asigurarea protecției informației clasificate în spațiul cibernetic

02

Crearea sistemelor guvernamentale

Asigurarea funcționării și securității sistemelor speciale de comunicații electronice

03

Asigurarea conducerii țării

Furnizarea de legătură guvernamentală, cifrată și secretă pentru autorități publice

04

Depistarea amenințărilor

Identificarea emițătorilor radio care periclitează securitatea de stat

Fraudele informatice: considerații generale

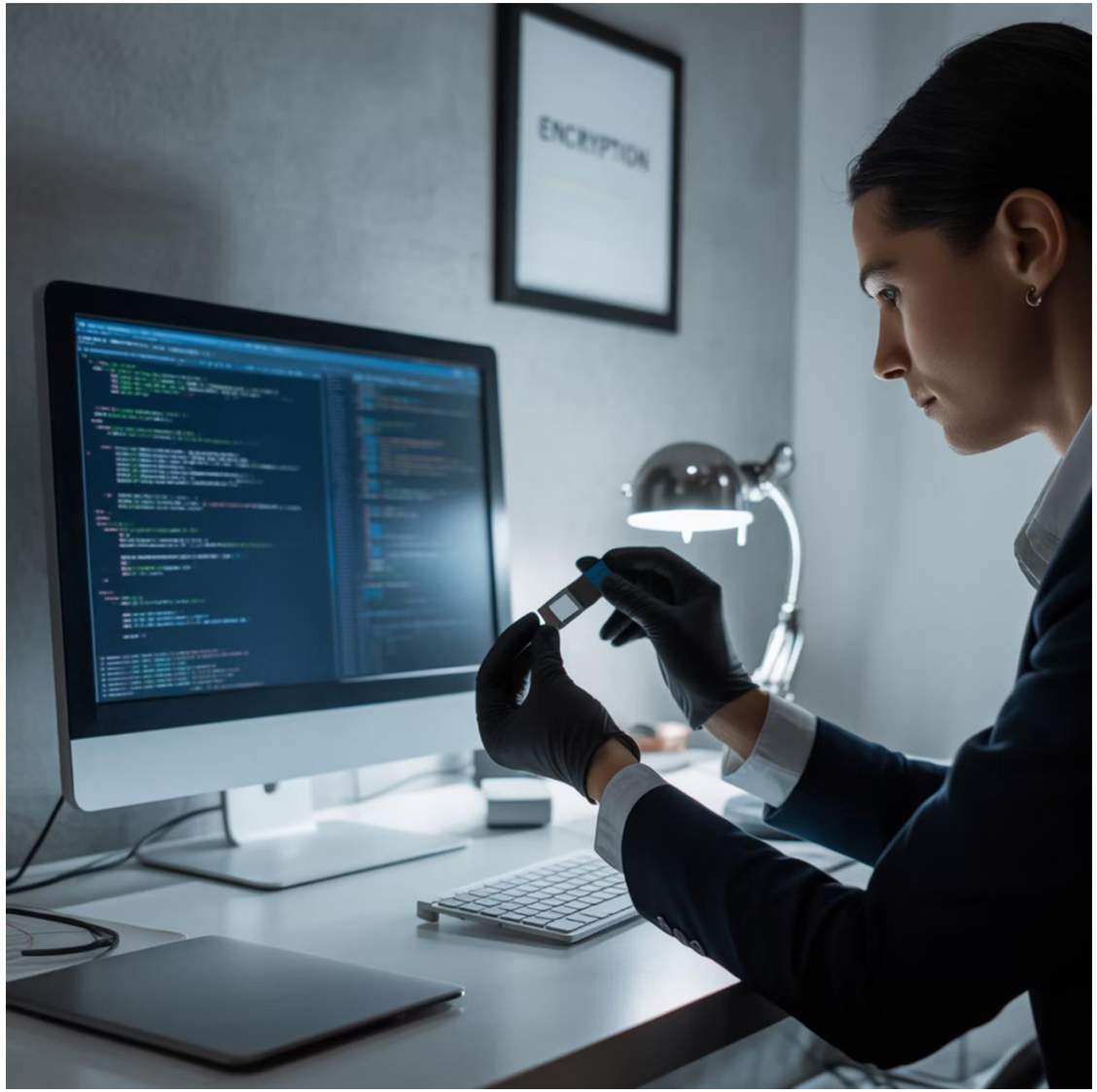
Definiția largă

Fraudele informatice reprezintă "orice infracțiune în care un calculator sau o rețea de calculatoare este obiectul unei infracțiuni, sau în care un calculator sau o rețea de calculatoare este instrumentul sau mediul de înfăptuire a unei infracțiuni"

Definiția restrânsă

"Orice infracțiune în care făptuitorul interferează, fără autorizare, cu procesele de prelucrare automată a datelor"

Alte definiții ale fraudelor informatice



"Orice incident legat de tehnica informatică în care o victimă a suferit sau ar fi putut să sufere un prejudiciu și din care autorul a obținut sau ar fi putut obține intenționat un profit."

"Orice acțiune ilegală în care un calculator constituie instrumentul sau obiectul delictului, sau, altfel spus, orice infracțiune al cărei mijloc sau scop este influențarea funcției calculatorului."

Formele fraudelor informatice

Momește și Schimbă
(Bait and Switch)

Scrisorile Nigeriene
(Frauda 419)

Facturarea falsă

Frauda Salam

Înființarea de Firme Fantomă

Momește și schimbă (Bait and Switch)

Este o formă de fraudă informatică în care făptuitorul ademenește potențiali clienți făcând publicitate unor produse care fie nu există în realitate, fie sunt ulterior schimbate cu produse aparent similare, dar cu calități net inferioare.

Fapta se realizează cel mai adesea prin intermediul sistemelor informatice și al rețelei Internet. Ademenirea clienților se poate face și prin mesaje de poștă electronică sau prin intermediul unei pagini web specializate.

⚠ Victimele sunt atrase de oferte aparent avantajoase, dar primesc produse de calitate inferioară sau nu primesc nimic

Scrisorile nigeriene (Frauda 419)

Sunt adesea cunoscute sub denumirea de "transferuri nigeriene" sau "Fraude cu avans" ori, pur și simplu, "înșelătorii 419" (după articolul din Codul Penal al Nigeriei care incriminează astfel de fapte).

Victimele vizate sunt persoane înstărite sau investitori din Europa, Asia, Australia sau America de Nord. Mijloacele de comitere variază de la scrisorile expediate prin poștă sau faxuri la email sau pagini web, în special după 1990.

Astfel de înșelăciuni își au originea în Nigeria și sunt pregătite astfel încât adresele de email, site-urile web, numerele de telefon sau fax să pară a aparține unor centre de afaceri, firme sau chiar instituții guvernamentale locale.

Depozite false (False Escrow)

O metodă sofisticată de fraudare în sistemele informatice prin care autorul, după ce câștigă o licitație de produse pe un site Internet specializat (gen eBay), solicită victimei utilizarea unui site de escrow "sigur" și "neutru".

Acest site aparent independent urmează să "depoziteze" bunurile (produsele – în general echipamente electronice) până la perfectarea aranjamentelor financiare.

⊗ **Atenție:** Site-ul de escrow este creat și controlat de infractor. La primirea bunurilor "în gaj", pagina web este închisă (dezactivată) iar contul șters.

Mailbombing - Atacul prin email

Este considerată cea mai veche metodă de atac cibernetic, deși esența sa este simplă și primitivă: un număr mare de mesaje de e-mail fac imposibilă lucrul cu cutiile poștale și, uneori, cu servere de mail întregi.

1

Execuția atacului

Multe programe au fost dezvoltate pentru acest scop. Chiar și un utilizator neexperimentat poate efectua un atac specificând doar e-mailul victimei, textul mesajului și numărul de mesaje necesare.

2

Mascarea identității

Multe astfel de programe permit ascunderea adresei IP reale a expeditorului, folosind servere de e-mail anonime.

3

Prevenirea

Atacul este ușor de prevenit prin filtre anti-spam eficiente și limitarea numărului de scrisori de la un expeditor.

Selectarea parolei prin forță brută

Următorul tip de atac este, de asemenea, simplu în concept. Atacatorul încearcă să găsească parole pentru sistemele de control al accesului prin încercări repetate.

Este evident că utilizatorii de sisteme de calcul nu sunt de obicei capabili să țină cont de combinații complexe de litere, cifre și semne lungi de până la o sută de caractere. Parola medie pentru accesarea sistemului nu depășește, de obicei, opt caractere, iar uneori un cuvânt sau o dată este folosită ca parolă.

Vulnerabilitatea parolelor simple face ca această metodă să fie încă eficientă împotriva sistemelor slab protejate

Analiza vulnerabilităților parolelor

Parole bazate pe date

Când se folosește o dată, calculul devine simplu: opt cifre oferă doar 100.000.000 de combinații posibile. Însă:

- Primele/ultimele 4 cifre indică anul (1900-2050)
- Două cifre indică luna (1-12)
- Cifrele rămase indică ziua (1-31)

Se exclud datele invalide (ex: 31 februarie). La o rată de sortare de 100 parole pe secundă, durata atacului este de aproximativ 11 zile.

Atacuri asupra parolelor bazate pe cuvinte

Pentru fraze, totul este mai complicat. Chiar dacă considerăm alfabetul englezesc de 26 de litere (românesc - 31 de litere), o frază de opt caractere va consta din 208.827.064.576 de opțiuni (1.406.408.618.241 pentru limba română).

Limitarea vocabularului

Utilizatorul nu își poate aminti secvențe aleatorii - este suficient să sortezi cuvintele din dicționar (max. 200.000)

1

Contextul profesional

Majoritatea oamenilor au vocabulare mai mici, reducând opțiunile cu un ordin de mărime

2

Parole personale

Numele rudelor, animalelor de companie, orașelor sunt frecvent folosite ca parole

3

Crearea de parole sigure

Nu există motiv să ne bazăm pe modalități simple de obținere a parolei. Majoritatea utilizatorilor folosesc ca parolă secvențe aleatorii de caractere latine mari și mici, intercalate cu numere.

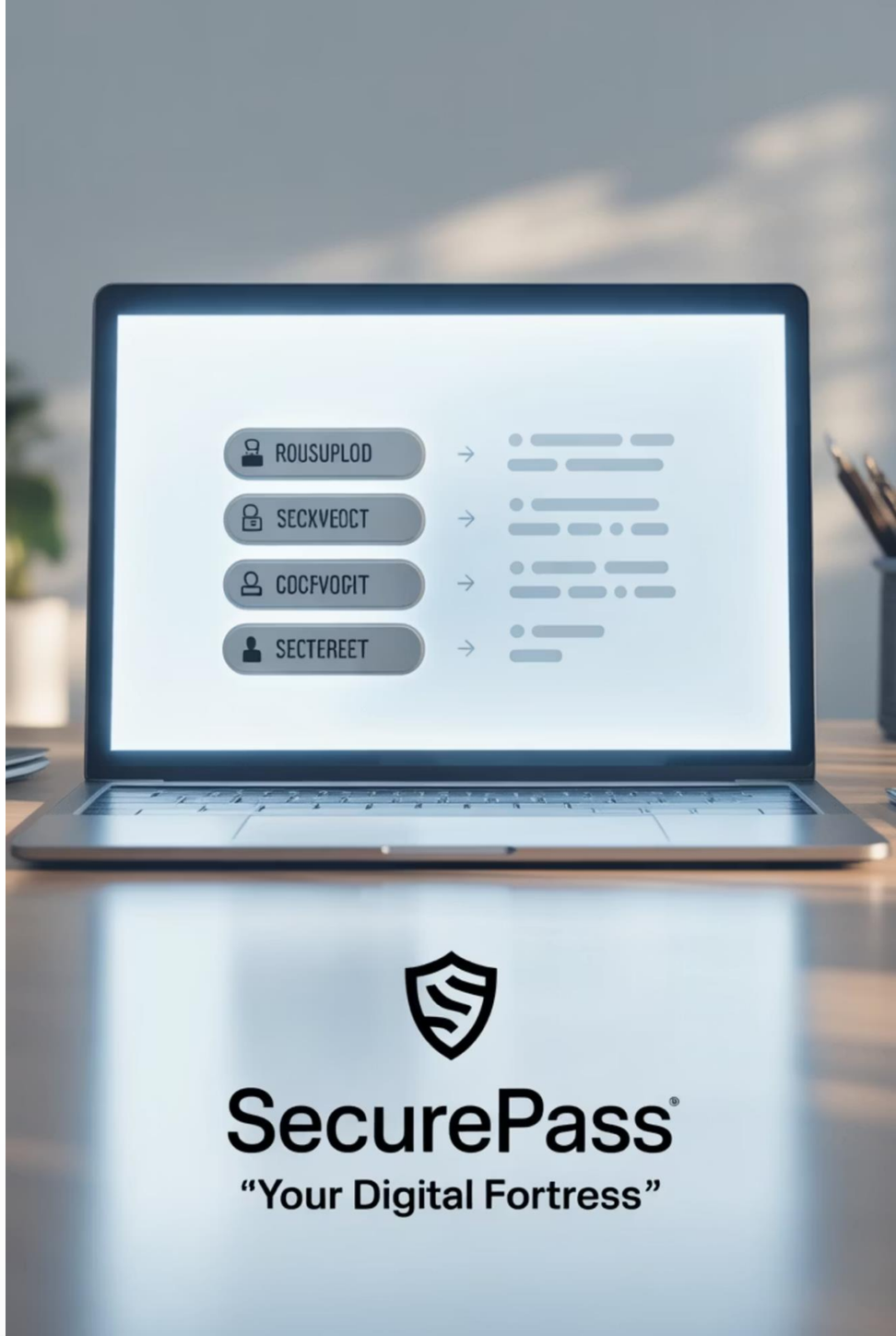
Metoda acronimului

Din primele litere ale expresiei "există un stejar verde lângă malul mării, un lanț de aur pe acel stejar", se obține parola "uldzzzndt" (9 litere)

Securitate maximă

Selectarea unei astfel de parole va necesita câteva trilioane de încercări, făcând atacul impracticabil

Parolele complexe generate prin metode mnemonice oferă securitate maximă păstrând ușurința de memorare



Programe malware specializate

Următorul tip de atac reprezintă o metodă mai sofisticată de obținere a accesului la informații clasificate - utilizarea de programe speciale pentru a funcționa pe computerul victimei.

Viruși informatici

Programe care se replică și infectează alte fișiere, putând cauza daune sistemului

Troieni

Software aparent legitim care ascunde funcționalități malițioase

Viermi de rețea

Programe care se răspândesc automat prin rețele fără intervenția utilizatorului

Sniffer și Rootkit-uri

Instrumente specializate pentru interceptarea și controlul sistemelor compromise

Aceste programe sunt concepute pentru a căuta și transfera informații secrete către proprietarul lor sau pentru a dăuna sistemului de securitate și performanței computerului victimei.

Recunoașterea rețelei (Network Intelligence)

În timpul unui astfel de atac, hackerul nu efectuează acțiuni distructive vizibile, dar poate obține informații confidențiale despre construcția și principiile de funcționare a sistemului informatic al victimei.

01

Scanarea porturilor

Identificarea serviciilor active și a punctelor de intrare potențiale în sistem

02

Interogări DNS

Obținerea informațiilor despre structura domeniilor și subdomeniiilor organizației

03

Testarea proxy-urilor

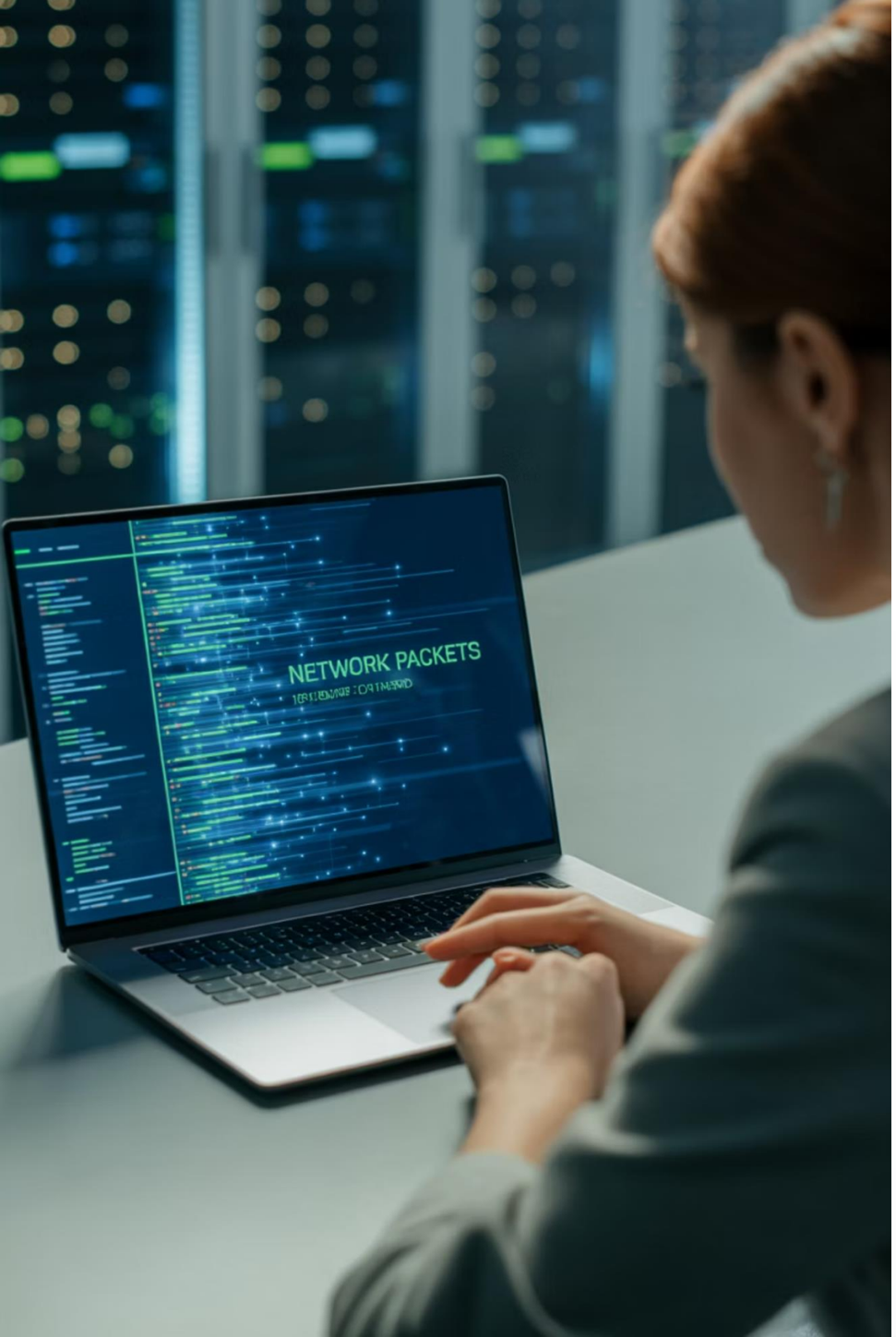
Verificarea prezenței și securității serverelor intermediare

04

Analiza rezultatelor

Construirea unei hărți detaliate a infrastructurii pentru atacuri viitoare

⚠ Informațiile obținute pot include adrese DNS, proprietari, servicii disponibile și niveluri de acces pentru utilizatori externi și interni



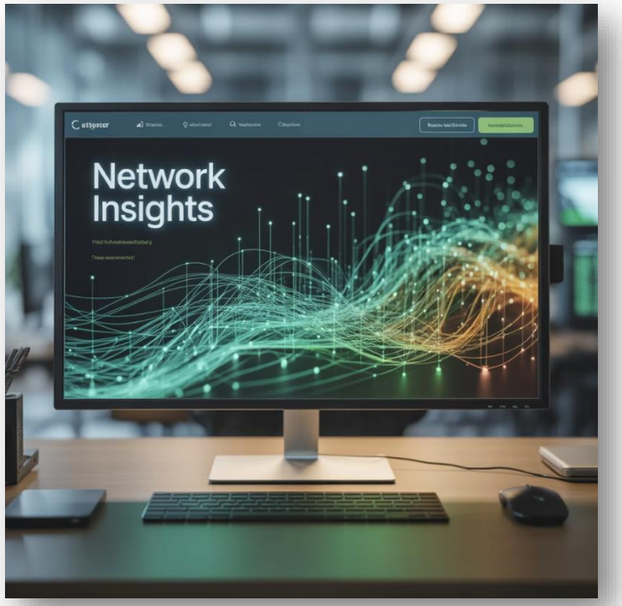
Sniffing pachetelor de rețea

Este un tip de atac destul de comun bazat pe funcționarea unei plăci de rețea în modul promiscuu. În acest mod, toate pachetele primite de placa de rețea sunt trimise pentru procesare către o aplicație specială.

Informații interceptate:

- Adresele sursă și destinație ale comunicațiilor
- Rutele prin care trec pachetele de date
- Conținutul neprotejat al comunicațiilor

Cel mai mare pericol: obținerea de login-uri și parole care pot fi folosite pentru intrarea ilegală în sistem



IP Spoofing - Uzurparea identității

Un tip obișnuit de atac în rețelele insuficient protejate, când un atacator își uzurpează identitatea unui utilizator autorizat, aflându-se în interiorul organizației sau în afara acesteia.

1

Metoda atacului

Hackerul folosește o adresă IP care este permisă în sistemul de securitate al rețelei

2

Vulnerabilitatea

Atacul este posibil dacă sistemul permite identificarea utilizatorului doar prin adresa IP

3

Consecințele

Obținerea accesului neautorizat la resurse și informații confidențiale

Prevenirea necesită implementarea de mecanisme suplimentare de autentificare, nu doar verificarea adresei IP

Atacul Man-in-the-Middle

> Din engleză "Bărbatul din mijloc" - un tip de atac când un atacator interceptează canalul de comunicație între două sisteme și obține acces la toate informațiile transmise.

Interceptarea	Modificarea	Obiectivele
Atacatorul se pozționează între două părți care comunică, interceptând toate datele	Informațiile pot fi modificate în mod activ pentru a atinge obiectivele atacatorului	Furtul sau falsificarea informațiilor, obținerea accesului la resurse de rețea

⚠ Astfel de atacuri sunt extrem de greu de urmărit, deoarece atacatorul se află de obicei în interiorul organizației

Atacuri prin injecție

Un atac de injecție implică introducerea unor comenzi sau date terță parte într-un sistem care rulează pentru a schimba cursul sistemului și, ca urmare, a obține acces la funcții și informații închise sau a destabiliza sistemul în ansamblu.

1. **Identificarea vulnerabilității**

   Atacatorul caută puncte de intrare în aplicație unde datele utilizatorului nu sunt validate corespunzător

2. **Injectarea codului**

   Se introduc comenzi malițioase care vor fi executate de sistemul țintă

3. **Executarea**

   Sistemul execută comenzile injected, oferind atacatorului control parțial sau total

Un astfel de atac este cel mai popular pe Internet, dar poate fi efectuat și prin linia de comandă a sistemului local.

Tipuri specifice de injecție

SQL Injection

Modificarea parametrilor interogărilor SQL către baza de date. Cererea capătă un sens complet diferit și poate afișa informații confidențiale sau modifica/șterge date. Foarte frecvent pe site-urile care folosesc parametrii URL pentru construirea interogărilor SQL fără validare adecvată.

PHP Injection

O modalitate de a pirata site-urile care rulează pe PHP. Constă în executarea codului necesar pe partea de server a site-ului prin exploitarea vulnerabilităților în procesarea datelor de intrare.

Cross Site Scripting (XSS)

Similar cu injecția SQL, dar atacatorul nu modifică interogarea SQL, ci variabilele interne ale sistemului de operare, folosind deficiențe în procesarea parametrilor de intrare sau erori în configurarea aplicațiilor.

Inginerie socială

> Ingineria socială (din engleză Social Engineering) este utilizarea incompetenței sau neglijenței personalului pentru a obține acces la informații. Această metodă este de obicei folosită fără computer, folosind un telefon obișnuit, poștă sau contact direct.

Contactul inițial

Atacatorul stabilește contactul cu victima prin diverse mijloace de comunicare

Câștigarea încrederii

Se creează o atmosferă de încredere prin inducerea în eroare sau manipulare psihologică

Extragerea informației

Se obțin informațiile necesare care sunt greu de obținut prin alte metode mai riscante

⊗ **Vechea vorbă:** "Cea mai slabă verigă dintr-un sistem de securitate este Omul"

Cele mai periculoase amenințări IT

Acțiuni din interior

Amenințări provenite de la angajați cu acces privilegiat

Programe malware

Software malițios conceput pentru a compromite sistemele

Atacurile hackerilor

Intruziuni externe planificate și sofisticate

Neglijența angajaților

Erori umane care expun sistemele la riscuri

Spam

Comunicări nesolicitate care pot conține amenințări

Eșecuri hardware și software

Probleme tehnice care afectează securitatea

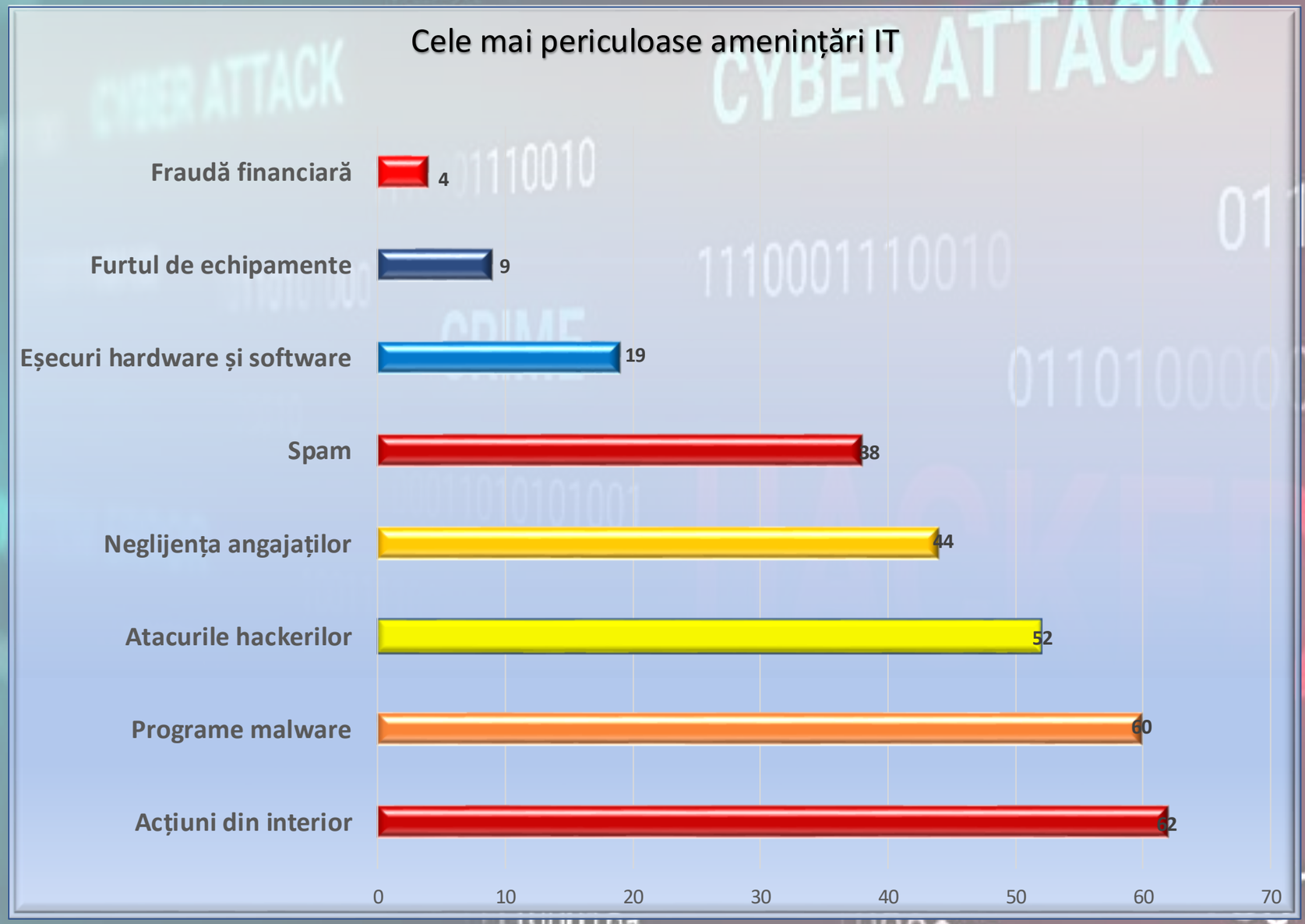
Furtul de echipamente

Pierderea fizică a dispozitivelor cu date sensibile

Fraudă financiară

Atacuri având ca scop obținerea de beneficii financiare ilegale

Cele mai periculoase amenințări IT



Subiecții fraudei informatice

Subiectul activ

Poate fi orice persoană care răspunde penal - persoana fizică care comite infracțiunea informatică și care poate fi trasă la răspundere penală conform legislației în vigoare

Subiectul pasiv

Persoana fizică sau juridică, proprietară sau utilizatoare a sistemului informatic accesat ilegal sau a datelor informatice vizate de infracțiunea comisă

Distincția între subiectul activ și cel pasiv este esențială pentru înțelegerea responsabilității juridice în cazul fraudelor informatice

Categoriile de fraude informatice conform Comitetului European

Raportul Comitetului European pentru probleme criminale evidențiază următoarele categorii principale de fraude informatice:

- Infracțiunea de fraudă informatică
  Orice ingerință într-un sistem informatic care influențează rezultatul și cauzează prejudicii

- Infracțiunea de fals în informatică
  Modificarea sau falsificarea datelor informatice cu intenție frauduloasă

- Prejudicierea datelor sau programelor
  Distrugerea, deteriorarea sau alterarea informațiilor digitale

- Sabotajul informatic
  Acțiuni deliberate de perturbarea funcționării sistemelor informatice

- Accesul neautorizat
  Intrarea ilegală în sisteme informatice fără permisiunea proprietarului

- Interceptarea neautorizată
  Capturarea ilegală a comunicațiilor electronice în tranzit

Categorii suplimentare de infracțiuni informatice

- Reproducerea neautorizată a topografiilor

  Copierea ilegală a designului circuitelor integrate și componentelor electronice

- Reproducerea programelor protejate

  Copierea ilegală a software-ului protejat prin drepturi de autor

- Alterarea datelor fără drept

  Modificarea neautorizată a informațiilor din sisteme informatice

- Spionajul informatic

  Obținerea ilegală de informații confidențiale prin mijloace electronice

- Utilizarea neautorizată

  Folosirea ilegală a calculatoarelor și programelor informatice protejate

Clasificarea ONU pentru infracționalitatea informatică

Manualul Națiunilor Unite pentru prevenirea și controlul infracționalității informatice identifică cinci categorii principale:

01

Fraude prin manipularea calculatoarelor electronice

Modificarea neautorizată a proceselor de calcul pentru obținerea de avantaje ilegale

02

Fraude prin falsificarea de documente

Crearea sau modificarea documentelor electronice cu intenții frauduloase

03

Alterarea/modificarea programelor

Schimbarea neautorizată a codului software pentru a obține acces ilegal

04

Accesul neautorizat la sisteme

Intrarea ilegală în sisteme informatice protejate

05

Reproducerea neautorizată de programe

Copierea ilegală a software-ului protejat de lege

Rolul sistemelor informatice în fraude

Infracțiuni săvârșite cu ajutorul sistemelor informatice

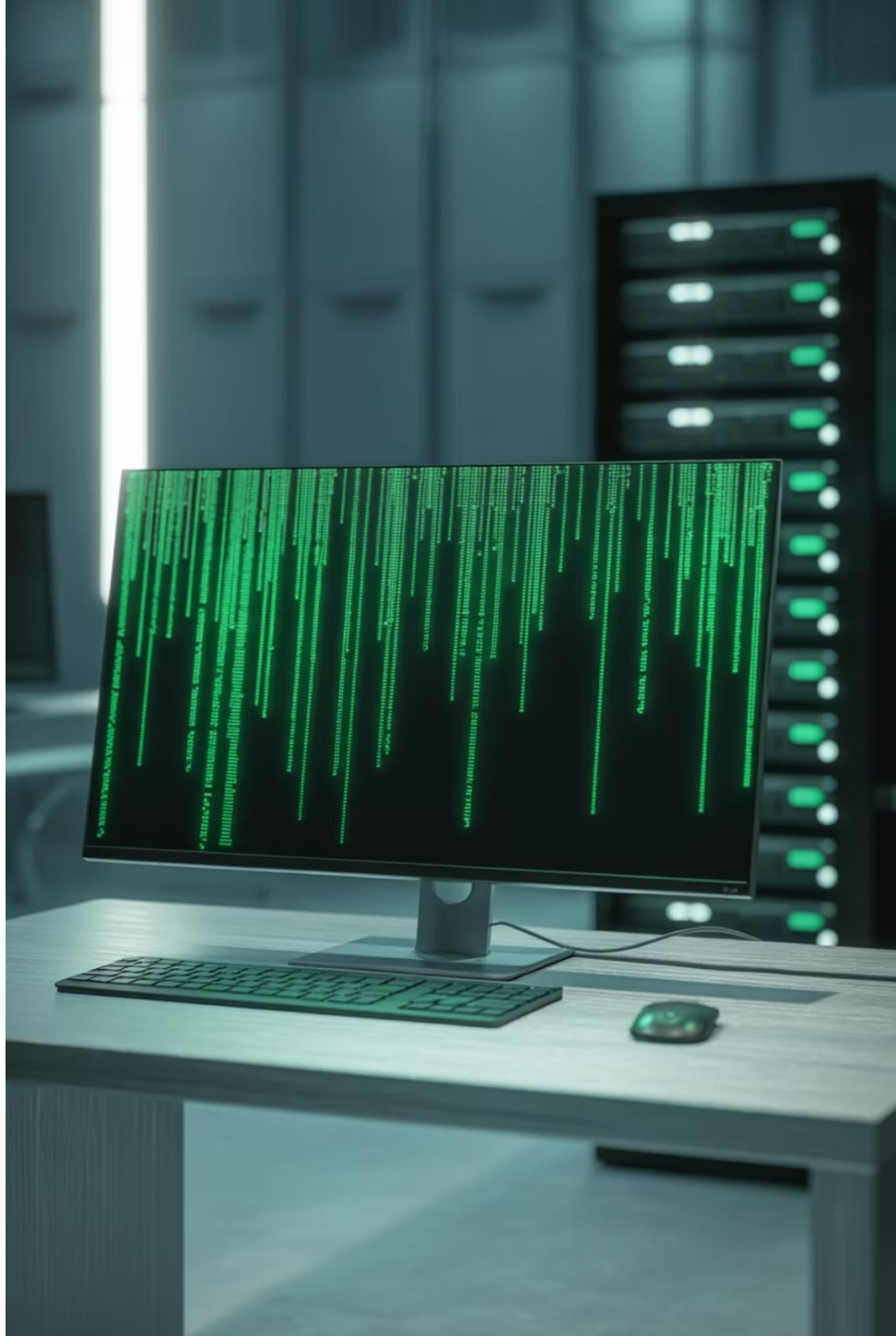
Sistemele informatice constituie un instrument de facilitare a comiterii infracțiunilor. Este vorba despre infracțiuni tradiționale, perfecționate prin utilizarea sistemelor informatice.

- Fraudă bancară electronică
- Înșelăciuni online
- Falsificarea de documente digitale
- Spionaj economic digital

Infracțiuni săvârșite prin intermediul sistemelor

Sistemele informatice, incluzând și datele stocate în acestea, constituie ținta infracțiunii.

- Atacuri asupra bazelor de date
- Sabotarea infrastructurii IT
- Furtul identității digitale
- Alterarea programelor software



OECD - Organizația pentru Cooperare și Dezvoltare

Organizația pentru Cooperare Economică și Dezvoltare (OECD) a fost una dintre primele organizații internaționale care a realizat un studiu privind armonizarea legislației în domeniu.

1983 - Primul raport OECD

Publicarea primului studiu comprehensive privind criminalitatea informatică la nivel internațional

Recomandări legislative

Propuneri pentru statele membre ale Uniunii Europene pentru armonizarea legilor naționale

Lista minimă de activități

Identificarea infracțiunilor care trebuie pedepsite: fraudarea, falsificarea, alterarea programelor, copyright-ul, interceptarea

OECD a stabilit bazele pentru cooperarea internațională în combaterea criminalității informatice

ONU - Organizația Națiunilor Unite

Organizația Națiunilor Unite s-a implicat activ în studiul și combaterea fenomenului criminalității informatice prin numeroase documente și inițiative.

1985 - Propuneri de concertare

Raportul privind acțiunile internaționale pentru combaterea activității criminale

1990 - Rezoluția canadiană

Introducerea de către Canada a rezoluției privind combaterea criminalității pe calculator

1990 - Declarația pentru victime

"Declarația Națiunilor Unite privind principiile de bază ale justiției aplicabile victimelor abuzului de putere"

Raportul "Provocarea fără frontiere"

Analiza comprehensivă a provocărilor transnaționale în combaterea criminalității informatice

Consiliul Europei și combaterea criminalității informatice

În completarea raportului OECD, Consiliul Europei a inițiat propriul studiu de caz pentru dezvoltarea cadrului legal privind combaterea criminalității informatice.

Comisia de experți în domeniul criminalității pe calculator a Consiliului a adoptat **Recomandarea R(89)9** care reprezintă un ghid de acțiune pentru statele membre ale Uniunii Europene.

Această recomandare a devenit fundamentul pentru harmonizarea legislației europene în domeniul criminalității informatice

Clasificarea Consiliului Europei - Lista minimală

Infracțiunile informatice sunt clasificate, potrivit recomandărilor Consiliului Europei, în opt categorii:

- Frauda informatică

  Orice ingerință într-un sistem informatic care influențează rezultatul, cauzând prejudicii
- Falsul informatic
- Prejudicierea datelor sau programelor
- Sabotajul informatic
- Accesul neautorizat
- Interceptarea neautorizată
- Reproducerea neautorizată de programe
- Reproducerea neautorizată de topografii

Provocări în combaterea fraudelor informatice

- Lipsa consensului global

  Absence unei definiții universale a "fraudelor informatice" și a motivației realizării acestor fapte

- Lipsa expertizelor specializate

  Insuficiența personalului autorizat din instituțiile cu atribuții de control în domeniu

- Cadrul legal inadecvat

  Inexistența normelor legale pentru accesul și investigația sistemelor informatice

- Lipsa armonizării legislative

  Neuniformitatea procedurilor de investigație la nivel internațional

- Caracterul transnațional

  Dificultăți în urmărirea infractorilor care operează în mai multe jurisdicții

- Tratate internaționale limitate

  Numărul redus de acorduri privind extrădarea și asistența mutuală

Elemente de prevenire a fraudelor informatice

Control intern eficace

Implementarea și dezvoltarea unui sistem robust de control intern pentru monitorizarea tuturor proceselor critice

Securizarea accesului

Protejarea riguroasă a accesului la sistemele informaționale prin autentificare multi-factor

Transparența activităților

Asigurarea transparenței și evaluarea procedurilor de achiziții publice și a tranzacțiilor cu risc major

Segregarea sarcinilor

Separarea responsabilităților și consolidarea supravegherii activităților ce implică riscuri majore

Principiul "patru ochi"

Implementarea procedurilor de control bazate pe verificarea independentă

Politica de recrutare

Stabilirea unei politici adecvate de recrutare și verificarea antecedentelor personalului

Cadrul legislativ în Republica Moldova

Curmarea fraudelor informatice în RM se bazează pe un cadru legislativ comprehensive:

Legea nr. 20/2009
"Privind prevenirea și combaterea criminalității informatice" - stabilește funcțiile autorităților și instituțiilor publice competente în domeniul prevenirii și combaterii fraudelor informatice

Legea nr. 91/2014
"Privind semnătura electronică și documentul electronic" - sporește nivelul de securitate a semnăturilor electronice și validarea documentelor digitale

Directiva 2006/24/CE
Păstrarea datelor generate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului

Directiva 2002/58/CE
"Privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice"

Concluzii principale

Complexitatea investigațiilor

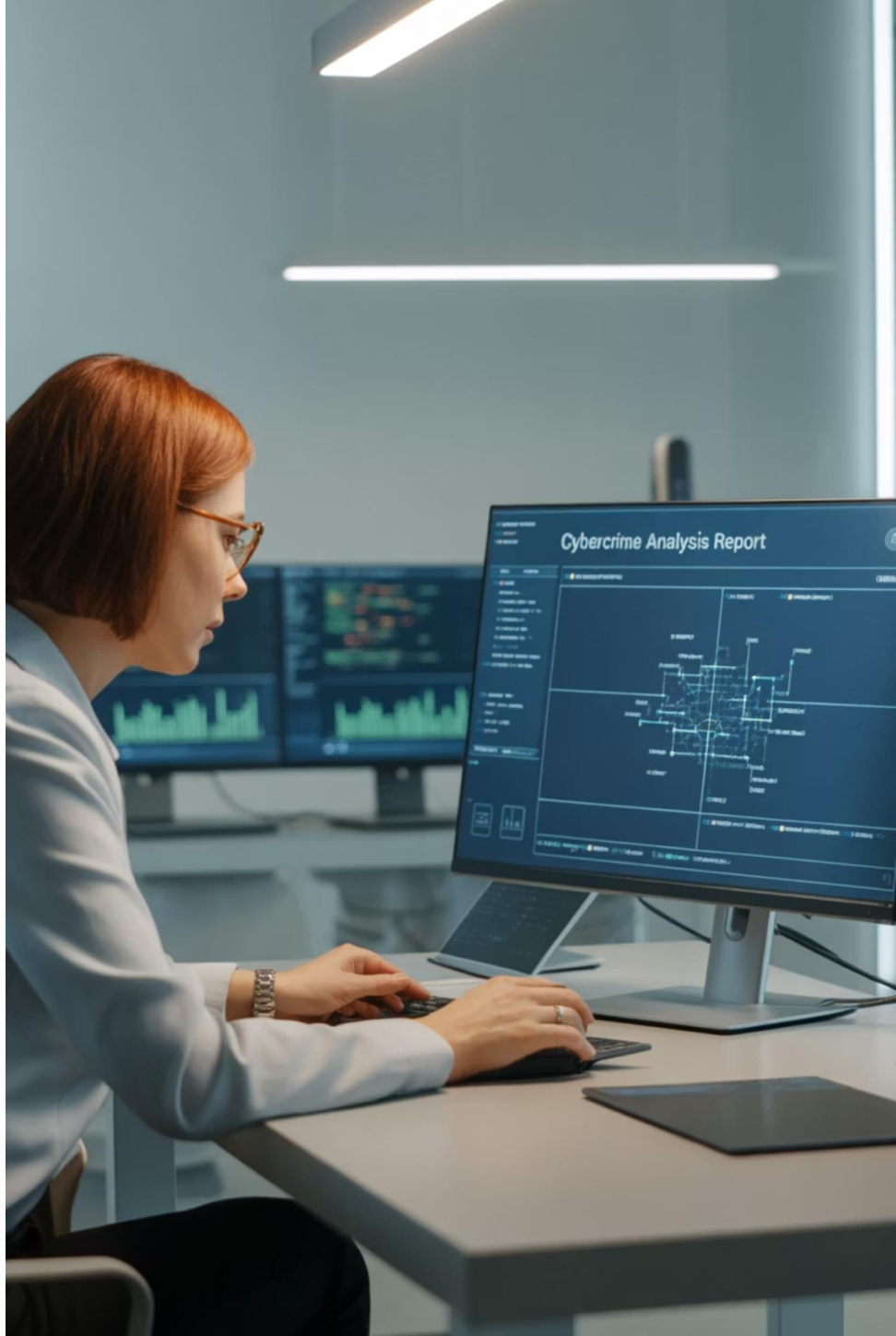
Un investigator în domeniul criminalității informatice poate lucra la maximum 3-4 cazuri pe lună, în timp ce un investigator tradițional poate soluționa între 40 și 50 de cazuri în aceeași perioadă de timp.

Necesitatea armonizării

Elaborarea tehnicilor și metodologiilor de cercetare a infracțiunilor informatice. Armonizarea legislației cu cea internațională trebuie să vizeze dreptul de autor, confidențialitatea datelor, prevenirea și combaterea fraudelor informatice.

Stadiul dezvoltării în RM

Republica Moldova se află în prima etapă de dezvoltare a ramurii respective și întâmpină mari greutăți în dezvoltarea ulterioară. Pentru a construi o societate informațională sănătoasă, statul trebuie să ia toate măsurile necesare pentru asigurarea securității.



Concluzii finale

> Orice atac nu este altceva decât o încercare de a folosi imperfecțiunea sistemului de securitate al victimei fie pentru a obține informații, fie pentru a dăuna sistemului.

Profesionalismul atacatorului

Competențele tehnice și cunoștințele specializate ale hackerilor determină succesul atacurilor

Valoarea informațiilor

Importanța și sensibilitatea datelor țintite motivează intensitatea și persistența atacurilor

Atenția la securitate

Gradul insuficient de atenție acordat problemelor de securitate la nivelul organizației

Competența insuficientă

Lipsa de experiență a administratorilor de sistem și imperfecțiunile software-ului creează vulnerabilități

Sarcini de autoevaluare

1 Informație analitică

Prezentarea unei analize comprehensive privind prevenirea și curmarea fraudelor informatice, inclusiv studii de caz și statistici relevante

2 Instrumente și metode

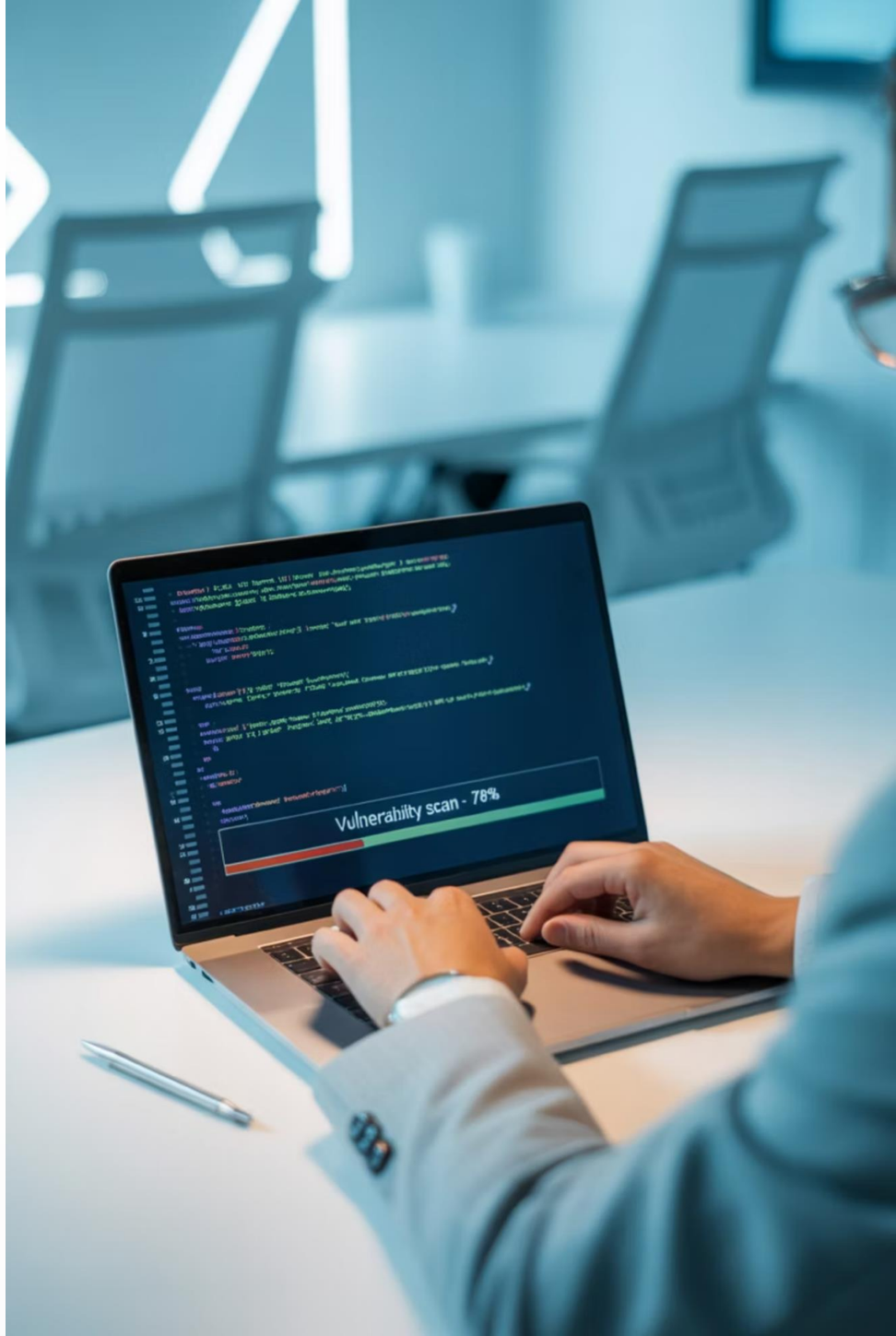
Determinați și descrieți instrumentele și metodele eficiente de luptă cu amenințările cibernetice, inclusiv tehnologiile emergente

3 Motivele criminalității

Evaluați și analizați motivele principale ale criminalității cibernetice din perspectiva psihologică, economică și tehnologică

4 Eforturile de securitate

Descrieți în detaliu eforturile întreprinse la nivel național și internațional pentru asigurarea securității informaționale și de securitate națională



Teme pentru lucru individual

1	Structuri de securitate democratică Analiza structurilor de securitate într-o societate democratică și rolul acestora în protejarea drepturilor cetățenilor
2	Hârțuirea electronică Studiul infracțiunilor pe Internet cu focus pe hârțuirea electronică și impactul asupra victimelor
3	Proprietatea intelectuală online Considerații privind protecția drepturilor de proprietate intelectuală pe Internet în era digitală
4	Politica informațională și integrarea europeană Politica și strategia de stat în domeniul informațional în contextul integrării europene a Republicii Moldova
5	Protecția sistemelor informaționale Metodologii și tehnologii avansate pentru protecția și securitatea sistemelor informaționale moderne

Bibliografie

Lucrări academice

- Oprea D. Protecția și securitatea sistemelor informaționale. Suport de curs, Iași, 2017
- Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică. București 2004, 71 p.

Cadru legal

- Legea nr. 286/2009 privind noul Cod Penal, publicată în Monitorul Oficial nr. 510 din 24 iulie 2009, în vigoare de la 1 februarie 2014

Resurse online

Înșelăciune prin sisteme informatice, fraudă informatică și fals informatic. Percheziții domiciliare

www.juridice.ro/295789/diicot-inselaciune-prin-sisteme-informatice