

**INSTITUTUL NAȚIONAL AL JUSTIȚIEI**

*Anexa nr.25  
prin Hotărîrea Consiliului INJ  
nr.1/4 din 29.01.2016*

**CURRICULUM**

la disciplina

**„Investigarea infracțiunilor cibernetice”**

*(candidați la funcția de procuror)*

**AUTOR:**

**Veaceslav SOLTAN,**  
*Procuror, șef al Secției tehnologii informaționale  
și investigații ale infracțiunilor în domeniul informaticii  
al Procuraturii Generale, formator INJ*

\_\_\_\_\_ AVIZAT  
Șef Direcție instruire și cercetare

**CHIȘINĂU 2016**

## I. PRELIMINARII

Apariția, acum mai bine de 50 de ani, a primelor calculatoare electronice a declanșat o adevărată revoluție în societatea umană. Consecința primordială a avansului tehnologic apărut a reprezentat-o tranziția de la societatea industrială la societatea informațională. Umanitatea a evoluat în ultimii 50 de ani mai mult decât în orice altă perioadă. Unealtă tehnologică în continuă perfecționare, a cărei pătrundere în toate aspectele vieții economice, sociale și culturale a punctat această evoluție, calculatorul electronic a devenit în ultimii ani o componentă normală a vieții noastre.

Dezvoltarea tehnologică și utilizarea pe scară largă a sistemelor informatice a adus după sine și o serie de riscuri. Dependența din ce în ce mai accentuată a agenților economici, a instituțiilor publice și chiar a utilizatorilor individuali de sistemele informatice ce le gestionează în mare măsură resursele, face ca aceștia să fie tot mai vulnerabili la impactul pe care îl poate avea criminalitatea informatică.

Calculatoarele electronice nu au constituit o atracție numai pentru cei interesați de dezvoltare, ci și pentru cei care au văzut în exploatarea tehnologiei moderne un mod de a dobândi foloase ne cuvenite. Analog modului în care noile tehnologii informaționale sunt mai întâi aplicate vechilor sarcini industriale pentru perfecționarea lor pentru ca apoi să dea naștere unor activități, procese și produse noi, calculatoarele electronice au fost utilizate inițial pentru a perfecționa modul de comitere a unor infracțiuni tradiționale, pentru ca în cele din urmă să apară noi forme de încălcări ilicite, specifice domeniului informatic. Calculatorul electronic este un factor criminogen de prim ordin, ce pune la dispoziția conduitei criminale atât un nou obiect (informația, conținută și procesată de sistemele informatice) cât și un nou instrument. El oferă un repertoriu deosebit de întins de tehnici și strategii de înlăturare a infracțiunilor, dar în același timp îmbogățește sfera criminalității cu noi infracțiuni. Criminalitatea informatică prezintă numeroase elemente de diferențiere față de fenomenul criminal tradițional, ridicând o serie de probleme în fața autorităților responsabile pentru eradicarea acesteia.

În acest context, considerăm că prezentul curs va fi foarte folositor tuturor celor interesați de combaterea acestor fenomene periculoase pentru societatea noastră. Sperăm ca acest curs, dincolo de menirea sa de material informativ, să constituie un material de referință util în activitatea zilnică a destinatarilor lui. De asemenea, el este punctul de plecare pentru programe de perfecționare profesională a persoanelor implicate în acțiuni de combatere a criminalității informatice.

Obiectivele generale ale acestei discipline vizează:

- dezvoltarea deprinderilor moderne de utilizator;
- cunoașterea modului de utilizare a instrumentelor informatice;
- dezvoltarea deprinderilor de a lucra individual și în echipă,
- înțelegerea impactului tehnologiilor informatice în societate, precum și a conexiunilor dintre informatică și alte obiecte de studiu.

Avantajele pe care le prezintă cursul „Tehnologii informaționale” pentru audienți sunt următoarele:

- formularea obiectivelor este realizată în termeni de competențe și capacități;
- posibilitatea de a îmbogăți registrul activităților de învățare sugerate de curriculum în funcție de obiectivele de referință definite și de resursele disponibile la nivelul fiecărui audient;
- încurajarea cooperării dintre audienți prin activități de grup cu asumarea de roluri individuale în vederea realizării unor aplicații specifice;
- conținuturi adaptabile la resursele audienților.

Conținuturile pentru curriculum-ul sunt concepute astfel încât să asigure un bagaj minim de cunoștințe și deprinderi din domeniul informaticii și al tehnologiei informației.

## II. COMPETENȚE

Prin studiul disciplinei “Utilizarea tehnologiilor informaționale în domeniul profesional” audientul va obține următoarele competențe:

- Să cunoască atribuțiile procurorului în procesul depistării și cercetării cazurilor de infracțiuni informaționale și a fraudelor comise prin Internet;
- Să cunoască practica internațională în domeniul investigării infracțiunilor informatice;
- Să determine rolul tehnologiilor informaționale în prevenirea și combaterea infracțiunilor;
- Să relateze despre dispozitivele de calcul și medii de stocare;
- Să determine metodele și formele de bază de descoperire și cercetare a infracțiunilor informaționale.
- Să utilizeze în mod efectiv informația obținută din sistemele informaționale ale autorităților publice centrale și locale pentru a stabili infractorul și a dovedi faptul participării lui la comiterea infracțiunii;
- Să utilizeze în mod efectiv informația obținută din rețelele Intranet și Internet.
- Să aplice studiile de caz pe bază de dosare și soluționarea unor spețe.
- Să formuleze indicații concrete adresate ofițerului de urmărire penală referitor la aspectele tactice și tehnice de efectuare a acțiunilor de urmărire penală în cazurile infracțiunilor informaționale;
- Să formuleze unele probleme care pot fi realizate în grupuri pe baza unor discuții preliminare și analiza problemei;
- Să întocmească corect formele statistice;
- Să dea apreciere probelor obținute în rezultatul efectuării acțiunilor de urmărire penală și să le utilizeze în procesul investigării;
- Să ia decizii optime în situații problematice de cercetare a infracțiunilor informaționale.

## III. PRINCIPALELE OBIECTIVE

La sfârșitul studiului disciplinei audientul va fi capabil să:

- descrie istoria atacurilor sistemelor informatice;
- enumere motivele și tipurile de riscuri;
- clasifice riscurile și incidentele;
- clasifice după lista de termeni;
- clasifice după lista de categorii;
- relateze despre listele empirice;
- relateze despre clasificările bazate pe acțiune;
- definească evenimentele, atacurile și incidentele;
- enumere acțiunile;
- enumere țintele;
- definească și să enumere atacurile;
- enumere categoriile de unelte;
- determine noțiunea de cal troian ca program de atac;
- enumere categoriile de rezultate neautorizate.
- definească noțiunea de criminalitate informatică;
- sistematizeze categoriile de infracțiuni informatice din raportul Comitetului European;
- compare categoriile de infracțiuni informatice din manualul pentru prevenirea și controlul infracțiunilor informatice al Națiunilor Unite cu categoriile de infracțiuni informatice din studiul Comisiei Europene;
- aprecieze rolul criminalității informatice în societate.
- definească noțiunea de infracțiune informatică;
- clasifice infracțiunile informatice ;

- determine infracțiunile săvârșite cu ajutorul sistemelor informatice;
- dezvolte responsabilități vizând utilizarea tehnicii de calcul în scopul accesului ilegal la un sistem informatic;
- relateze referitor regulilor de protecție a sistemului informatic;
- determine evoluția infracțiunilor.
- enumere organele care sunt abilitate cu atribuții de depistare a infracțiunilor, inclusiv și a infracțiunilor informaționale și fraudelor prin Internet;
- caracterizeze acțiunile ce se întreprind de către aceste organe;
- evalueze activitatea de prevenire și combatere a infracțiunilor computerizate.
- definească noțiunea de probatoriu;
- descrie examinarea preliminară a tehnicii de calcul;
- justifice procesul examinării calculatorului.
- descrie atribuțiile procurorului în procesul depistării și cercetării cazurilor infracțiunilor informaționale și a fraudelor comise prin Internet;
- aprecieze rolul serviciilor speciale în procesul depistării și cercetării cazurilor infracțiunilor informaționale;
- proiecteze aplicații pentru rezolvarea unor probleme utilizând instrumentele specifice de prelucrare a datelor.
- definească noțiunea de expertiză;
- enumere întrebările în fața expertizei tehnico-programiste;
- justifice întrebările puse la soluționarea expertizei în utilizarea tehnicii de calcul.
- definească noțiunea de *investigații informatice*;
- descrie modelele de bune practici în domeniul investigațiilor criminalistice de natură informatică;
- identifice principalele caracteristici a investigațiilor informatice;
- relateze referitor instrumentelor necesare pentru investigații.

#### IV. ADMINISTRAREA DISCIPLINEI

Denumirea disciplinei	Formator	Semestrul	Total ore	Ore curs	Ore practice	Evaluarea
Investigarea infracțiunilor cibernetice	Veaceslav SOLTAN	II	18	4	14	colocviu

#### V. TEMATICA ȘI REPARTIZAREA ORIENTATIVĂ A ORELOR

Nr. d/o	TEMATICA	Ore curs	Ore practice
1.	Reglementarea criminalității informatice. Conceptul de “criminalitate informatică”.	2	-
2.	Infracțiuni informatice. Atacurile sistemelor informatice.	2	2
3.	Atribuțiile procurorului în procesul depistării și cercetării cazurilor infracțiunilor informaționale și a fraudelor comise prin Internet.	-	2
4.	Investigații informatice.	-	2
5.	Practica internațională în investigarea infracțiunilor informatice.	-	2
6.	Organele abilitate cu funcții de depistare și documentare a infracțiunilor informaționale și fraudelor prin Internet	-	2

7.	Calificarea și probatoriul infracțiunilor comise în sfera informației computerizate.	-	2
8.	Considerații generale privind numirea expertizei.	-	2
<b>TOTAL</b>		<b>4</b>	<b>14</b>

## VI. UNITĂȚI TEMATICE

Unități tematice	Strategii didactice/ Resurse logistice	Lucrul individual
<b>Tema 1. Reglementarea criminalității informatice. Conceptul de “criminalitate informatică”.</b>		
<p style="text-align: center;"><i>Ore curs</i></p> <p>1. Definiția criminalității informatice. 2. Categoriile de sistematizare ale criminalității informatice. 3. Categoriile de infracțiuni informatice din manualul pentru prevenirea și controlul infracțiunilor informatice al Națiunilor Unite cu categoriile de infracțiuni informatice din studiul Comisiei Europene; <i>Audienții necesită să:</i> 1) Descrie istoria atacurilor sistemelor informatice; 2) Enumere motivele și tipurile de riscuri; 3) Sistematizeze categoriile de infracțiuni informatice din raportul Comitetului European; 4) Aprecieze rolul criminalității informatice în societate 5) Definească noțiunii de infracțiune informatică;</p>	Curs-prelegere Proiector/laptop	<p style="text-align: center;"><i>Ore curs</i></p> <p>Brainstorming. Lectura surselor din Lista bibliografică.</p>
<b>Tema 2. Infracțiuni informatice. Atacurile sistemelor informatice.</b>		
<p style="text-align: center;"><i>Ore curs</i></p> <p>1. Clasificarea infracțiunilor informatice. 2. Atacurile sistemelor informatice. 3. Determinarea infracțiunilor săvârșite cu ajutorul sistemelor informatice; 4. Accesul ilegal la un sistem informatic. 5. Art.260-260<sup>6</sup> CP 6. Încălcarea regulilor de securitate la diferite sisteme informaționale. 7. Acces neautorizat la rețelele și serviciile de telecomunicații 8. Evoluția infracțiunilor.</p> <p style="text-align: center;"><i>Ore practice</i></p> <p>1) Clasificarea după lista de termeni; 2) Clasificarea după lista de categorii; 3) Relatarea listelor empirice; 4) Clasificările bazate pe acțiune; 5) Definirea evenimentelor, atacurilor și incidentelor; 6) Enumerarea acțiunilor;</p>	Curs-prelegere Proiector/laptop	<p style="text-align: center;"><i>Ore curs</i></p> <p>Brainstorming. Lectura surselor din Lista bibliografică.</p>
<p style="text-align: center;"><i>Ore practice</i></p> <p>1) Clasificarea după lista de termeni; 2) Clasificarea după lista de categorii; 3) Relatarea listelor empirice; 4) Clasificările bazate pe acțiune; 5) Definirea evenimentelor, atacurilor și incidentelor; 6) Enumerarea acțiunilor;</p>	Seminare Studiu de caz Tablă flipchart	<p style="text-align: center;"><i>Ore practice</i></p> <p>1) prezentarea rezultatelor; 2) susținerea tezelor</p>

<p>7) Enumerarea țințelor;  8) Enumerarea categoriile de unelte;  9) Determinarea noțiunii de cal troian ca program de atac;  10) Enumerarea categoriilor de rezultate neautorizate.</p>		
<p><b>Tema 3. Atribuțiile procurorului în procesul depistării și cercetării cazurilor infracțiunilor informaționale și a fraudelor comise prin Internet.</b></p>		
<p style="text-align: center;"><i>Ore practice</i></p> <p>1. Procurorul-conducător al procuraturii teritoriale, specializate și subdiviziunilor Procuraturii Generale.  2. Procurorii responsabili de aplicarea și respectarea în teritoriu a legislației privind prevenirea și combaterea infracțiunilor comise în sfera informației computerizate.</p>	<p>Seminare  Studiu de caz  Tablă flipchart</p>	<p style="text-align: center;"><i>Ore practice</i></p> <p>1) Proiecte.  2) Teste aplicative pentru a măsura gradul de însușire al noțiunilor strict teoretice.  3) Probleme.  4) Analiza generalizărilor practicii judiciare.</p>
<p><b>Tema 4. Investigații informatice.</b></p>		
<p><i>Repere de conținut:</i></p> <p>1. Dezvoltarea responsabilităților vizând utilizarea tehnicii de calcul în scopul accesului ilegal la un sistem informatic;  2. Determinarea evoluției infracțiunilor.  3. Justificarea procesului de examinarea a calculatorului.</p> <p style="text-align: center;"><i>Ore practice</i></p> <p>1) relateze referitor regulilor de protecție a sistemului informatic;  2) Enumerarea organelor care sunt abilitate cu atribuții de depistare a infracțiunilor, inclusiv și a infracțiunilor informaționale și fraudelor prin Internet;  3) Caracterizarea acțiunilor ce se întreprind de către aceste organe;  4) Evaluarea activității de prevenire și combatere a infracțiunilor computerizate.  5) Descrierea examinării preliminare a tehnicii de calcul;</p>	<p>Seminare  Studiu de caz  Tablă flipchart</p>	<p>Lectura surselor din Lista bibliografică.</p> <p style="text-align: center;"><i>Ore practice</i></p> <p>1) Studiu de caz.  2) Referate/rezumate.  3) Teste aplicative.  4) Elaborarea tezelor anuale.  5) Elaborarea tezelor de licență.</p>
<p><b>Tema 5. Practica internațională în investigarea infracțiunilor informatice.</b></p>		
<p><i>Repere de conținut:</i></p> <p>1. Definirea noțiunii de <i>investigații informatice</i>;  2. Identificarea principalelor caracteristici a investigațiilor informatice;</p> <p style="text-align: center;"><i>Ore practice</i></p> <p>1) Descrierea modelelor de bune practici în domeniul investigațiilor criminalistice de natură informatică;  2) Relatarea referitor la instrumentele necesare</p>	<p>Seminar  Studiu de caz  Tablă flipchart</p>	<p>Lectura surselor din Lista bibliografică.</p> <p style="text-align: center;"><i>Ore practice</i></p> <p>1) rezolvarea exercițiilor practice;  2) aplicații practice privind utilizarea unor</p>

pentru investigații.		accesorii ale diferitor sisteme de operare 3) prezentarea rezultatelor.
<b>Tema 6. Organele abilitate cu funcții de depistare și documentare a infracțiunilor informaționale și fraudelor prin Internet</b>		
<i>Ore practice</i> 1) Descrierea atribuțiilor procurorului 2) Procesul depistării și cercetării cazurilor infracțiunilor informaționale și a fraudelor comise prin Internet; 3) Aprecierea rolului serviciilor speciale în procesul depistării și cercetării cazurilor infracțiunilor informaționale;	Seminare Studiu de caz Tablă flipchart	<i>Ore practice</i> 1) Soluționarea spețelor. 2) Examinarea sistemelor. 3) Întocmirea proiectelor de acte pentru înregistrare.
<b>Tema 7. Calificarea și probatoriul infracțiunilor comise în sfera informației computerizate.</b>		
<i>Ore practice</i> 1) Definirea noțiunii de probatoriu; 2) Probatoriul infracțiunilor comise în sfera informației computerizate. 3) Descrierea examinării preliminare a tehnicii de calcul; 4) Justificarea procesului examinării calculatorului. 5) Proiectarea de aplicații pentru rezolvarea unor probleme utilizând instrumentele specifice de prelucrare a datelor.	Seminare Studiu de caz Tablă flipchart	<i>Ore practice</i> 1) Teste aplicative. 2) Imagini grafice. 3) Analiza datelor statistice. 4) Desene. 5) Aplicații practice.
<b>Tema 8. Considerații generale privind numirea expertizei.</b>		
<i>Ore practice</i> 1) Definirea noțiunii de expertiză; 2) Enumerarea întrebărilor în fața expertizei tehnico-programiste; 3) Justificarea întrebărilor puse la soluționarea expertizei în utilizarea tehnicii de calcul.	Seminare Studiu de caz Tablă flipchart	<i>Ore practice</i> 1. Teste aplicative. 2. Imagini grafice. 3. Analiza datelor statistice. 4. Desene. 5. Aplicații practice.

## VII. EVALUAREA

Evaluarea se va efectua continuu și la final.

### A. Evaluarea continuă

- participarea audiențelor în cadrul orelor de curs și a celor practice;
- realizarea activităților individuale;
- identificarea principalelor caracteristici a investigațiilor informatice.
- aplicații pentru rezolvarea unor probleme utilizând instrumente specifice de probatoriu.
- codificarea și decodificarea informației de text;
- estimare a cantității de informație în fișierele de text;
- identificare și explicare destinației componentelor de bază ale calculatorului și fluxurilor de informație;
  - identificarea obiectivelor de măsurare a cunoștințelor, capacităților și competențelor/aptitudinilor profesionale;
  - pregătirea unui referat științific și/sau aplicativ pe o problemă propusă pentru activitățile individuale.

**B. Evaluarea finală** se va efectua ca colocviu la finele semestrului prin soluționarea testelor și investigarea crimelor cibernetice.

## VIII. BIBLIOGRAFIE

### *Acte legislative și normative:*

1. Convenția Consiliului Europei asupra Criminalității Informatice, semnată la Budapesta la 23 noiembrie 2001.
2. Codul penal al Republicii Moldova, nr. 985-XV din 18.04.2002;
3. Codul de procedură penală al Republicii Moldova nr. 122-XV din 14.03.2003;
4. Codul contravențional al Republicii Moldova nr. 218-XVI din 24.10.2008;
5. Legea cu privire la informatică nr.1069-XIV din 22.06.2000;
6. Legea cu privire la informatizare și la resursele informaționale de stat, nr. 467-XV din 21.11.2003;
7. Legea cu privire la documentul electronic și semnătura digitală nr.264-XV din 15.07.2004;
8. Legea privind comerțul electronic nr. 284-XV din 22.07.2004 ;
9. Legea comunicațiilor electronice nr. 241-XVI din 15.11.2007;
10. Legea privind prevenirea și combaterea criminalității informatice nr. 20-XVI din 03.02.2009;
11. Legea pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică nr. 6-XVI din 02.02.2009;
12. Legea cu privire la serviciile de plată și moneda electronică nr. 114 din 18.05.2012.

### *Jurisprudență/Practica judiciară:*

13. Convenția Uniunii Internaționale a Telecomunicațiilor.
14. Constituția Uniunii Internaționale de Telecomunicații.
15. Recomandarea R(85)10 cuprinzând normele de aplicare a Convenției Europene de Asistență Mutuală în Materie Infrațională, cu referire la comisiile rogatorii privind interceptarea telecomunicațiilor;
16. Recomandarea R(88)2 privind pirateria în contextul existenței drepturilor de autor și a drepturilor conexe;
17. Recomandarea R(87)15 privind reglementarea utilizării datelor personale în munca de poliție;
18. Recomandarea R(89)9 privind unele norme care trebuie aplicate de statele membre pentru combaterea criminalității informatice.
19. Recomandarea R(95)4 privind protecția datelor personale în domeniul serviciilor de telecomunicații;
20. Recomandarea R(95)13 privind aspecte de procedură penală în legătură cu Tehnologia Informației;

### *Literatură didactică și științifică:*

21. Achim, Gheorghe, Metodologia investigării criminalistice a fraudelor informatice, Editura Omnia, 2000
22. Amza, Tudor, Amza, Cosmin-Petronel, Criminalitatea informatică, Ed. Lumina Lex, 2003
23. Bica, Gheorghe, Mihail, Gheorghe, Infrațiuni săvârșite prin calculator, în Revista de Drept Penal 4/1996, p. 85-88.
24. Hanga, Vladimir, Calculatoarele în serviciul dreptului, Ed. Lumina Lex, București, 1996.
25. VasIU, Ioana, Infrațiuni comise prin calculator, în Revista de Drept Penal, nr. 2/1996
26. Alexei Barbăneagră, Codul Penal al Republicii Moldova, Comentariu, Editura ARC, 2003