

**INSTITUTUL NAȚIONAL AL JUSTIȚIEI**

**INVESTIGAREA INFRAȚIUNILOR CIBERNETICE**

**CURRICULUM**

**FORMATOR:**

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

**CHIȘINĂU - 2012**

## 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 desfășurare 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. OBIECTIVELE GENERALE ALE DISCIPLINEI

În baza studierii disciplinei „Tehnologii informaționale” audientul trebuie:

### ***La nivel de cunoaștere și înțelegere:***

- să identifice atribuțiile procurorului în procesul depistării și cercetării cazurilor de infracțiuni informaționale și a fraudelor comise prin Internet;
- să determine 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.

### ***La nivel de aplicare:***

- 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.

### ***La nivel de integrare:***

- 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. ADMINISTRAREA DISCIPLINEI

Codul disciplinei	Anul predării	Semestrul	Numărul de ore		Evaluarea	Responsabil de disciplină
			C	S		
		II	10	18	Colocviu diferențiat	V. Soltan

### IV. TEMATICA ȘI REPARTIZAREA ORIENTATIVĂ A ORELOR

#### a) Tematica și repartizarea orientativă a orelor de curs

Nr. crt.	Tema	Realizarea în timp (ore)
1	Reglementarea criminalității informatice. Conceptul de “criminalitate informatică”.	2
2	Infrațiuni informatice. Atacurile sistemelor informatice.	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
	<b>În total</b>	<b>10</b>

#### b) tematica și repartizarea orientativă a orelor de seminar

Nr. crt.	Tema	Realizarea în timp (ore)
1	Atacurile sistemelor informatice.	2
2	Reglementarea criminalității informatice. Conceptul de “criminalitate informatică”.	2
3	Infrațiuni informatice.	2
4	Organele abilitate cu funcții de depistare și documentare a infracțiunilor informaționale și fraudelor prin Internet	2
5	Calificarea și probatoriul infracțiunilor comise în sfera informației computerizate.	2
6	Considerații generale privind numirea expertizei.	2
7	Investigații informatice.	4
8	Practica internațională în investigarea infracțiunilor informatice.	2
	<b>În total</b>	<b>18</b>

## V. OBIECTIVE DE REFERINȚĂ ȘI CONȚINUTURI

OBIECTIVELE DE REFERINȚĂ	CONȚINUTURI
<ul style="list-style-type: none"> <li>- să descrie istoria atacurilor sistemelor informatice;</li> <li>- să enumere motivele și tipurile de riscuri;</li> <li>- să clasifice riscurile și incidentele;</li> <li>- să clasifice după lista de termeni;</li> <li>- să clasifice după lista de categorii;</li> <li>- să relateze despre listele empirice;</li> <li>- să relateze despre clasificările bazate pe acțiune;</li> <li>- să definească evenimentele, atacurile și incidentele;</li> <li>- să enumere acțiunile;</li> <li>- să enumere țintele;</li> <li>- să definească și să enumere atacurile;</li> <li>- să enumere categoriile de unelte;</li> <li>- să determine noțiunea de cal troian ca program de atac;</li> <li>- să enumere categoriile de rezultate neautorizate.</li> </ul>	<p><b><i>Atacurile sistemelor informatice.</i></b></p> <ul style="list-style-type: none"> <li>• Riscurile.</li> <li>• Clasificarea riscurilor și incidentelor.</li> <li>• Clasificarea ca listă de termeni.</li> <li>• Listă de categorii.</li> <li>• Categoriile de rezultate.</li> <li>• Liste empirice.</li> <li>• Clasificări bazate pe acțiune.</li> <li>• Evenimente, atacuri și incidente.</li> <li>• Acțiuni.</li> <li>• Ținte.</li> <li>• Atacuri.</li> <li>• Unelte.</li> <li>• Cal troian.</li> <li>• Rezultate neautorizate.</li> </ul>
<ul style="list-style-type: none"> <li>- să definească noțiunea de criminalitate informatică;</li> <li>- să sistematizeze categoriile de infracțiuni informatice din raportul Comitetului European;</li> <li>- să 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;</li> <li>- să aprecieze rolul criminalității informatice în societate.</li> </ul>	<p><b><i>Reglementarea criminalității informatice. Conceptul de “criminalitate informatică”.</i></b></p> <ul style="list-style-type: none"> <li>• Definiția criminalității informatice.</li> <li>• Categoriile de sistematizare ale criminalității informatice.</li> </ul>
<ul style="list-style-type: none"> <li>- să definească noțiunea de infracțiune informatică;</li> <li>- să clasifice infracțiunile informatice ;</li> <li>- să determine infracțiunile săvârșite cu ajutorul sistemelor informatice;</li> <li>- să dezvolte responsabilități vizând utilizarea tehnicii de calcul în scopul accesului ilegal la un sistem informatic;</li> <li>- să relateze referitor regulilor de protecție a sistemului informatic;</li> <li>- să determine evoluția infracțiunilor.</li> </ul>	<p><b><i>Infracțiuni informatice.</i></b></p> <ul style="list-style-type: none"> <li>• Clasificarea infracțiunilor informatice.</li> <li>• Infracțiuni săvârșite cu ajutorul sistemelor informatice.</li> <li>• Accesul ilegal la un sistem informatic.</li> <li>• Introducerea sau răspîndirea programelor virulente.</li> <li>• Încălcarea regulilor de securitate la diferite sisteme informaționale.</li> <li>• Acces neautorizat la rețelele și serviciile de telecomunicații.</li> <li>• Evoluția infracțiunilor.</li> </ul>
<ul style="list-style-type: none"> <li>- să enumere organele care sunt abilitate cu atribuții de depistare a infracțiunilor, inclusiv și a infracțiunilor informaționale și fraudelor prin Internet;</li> <li>- să caracterizeze acțiunile ce se întreprind de către aceste organe;</li> </ul>	<p><b><i>Organele abilitate cu funcții de depistare și documentare a infracțiunilor informaționale și fraudelor prin Internet.</i></b></p>

- să evalueze activitatea de prevenire și combatere a infracțiunilor computerizate.	
- să definească noțiunea de probatoriu; - să descrie examinarea preliminară a tehnicii de calcul; - să justifice procesul examinării calculatorului.	<b>Probatoriul infracțiunilor comise în sfera informației computerizate.</b>
- să descrie atribuțiile procurorului în procesul depistării și cercetării cazurilor infracțiunilor informaționale și a fraudelor comise prin Internet; - să aprecieze rolul serviciilor speciale în procesul depistării și cercetării cazurilor infracțiunilor informaționale; - să proiecteze aplicații pentru rezolvarea unor probleme utilizând instrumentele specifice de prelucrare a datelor.	<b>Atribuțiile procurorului în procesul depistării și cercetării cazurilor infracțiunilor informaționale și a fraudelor comise prin Internet.</b> <ul style="list-style-type: none"> <li>• Procurorul-conducător al procuraturii teritoriale, specializate și subdiviziunilor Procuraturii Generale.</li> <li>• Procurorii responsabili de aplicarea și respectarea în teritoriu a legislației privind prevenirea și combaterea infracțiunilor comise în sfera informației computerizate.</li> </ul>
- să definească noțiunea de expertiză; - să enumere întrebările în fața expertizei tehnico-programiste; - să justifice întrebările puse la soluționarea expertizei în utilizarea tehnicii de calcul.	<b>Considerații generale privind numirea expertizei.</b>
- să definească noțiunea de <i>investigații informatice</i> ; - să descrie modelele de bune practici în domeniul investigațiilor criminalistice de natură informatică; - să identifice principalele caracteristici a investigațiilor informatice; - să relateze referitor instrumentelor necesare pentru investigații.	<b>Investigații informatice. Practica internațională în investigarea infracțiunilor informatice.</b>

## VI. SUGESTII PENTRU LUCRUL INDIVIDUAL AL STUDENȚILOR

Subiecte/probleme	Forme de realizare	Modalități de evaluare
1. Reglementarea criminalității informatice. Conceptul de "criminalitate informatică".	1. Proiecte. 2. Teste aplicative pentru a măsura gradul de însușire al noțiunilor strict teoretice. 3. Probleme. 1. Analiza generalizărilor practicii judiciare.	- prezentarea rezultatelor; - elaborarea articolelor; - rezolvarea problemelor; - rezolvarea testelor aplicative.
2. Investigarea infracțiunilor informatice.	1. Studiu de caz. 2. Referate/rezumate. 3. Teste aplicative. 4. Elaborarea tezelor anuale. 5. Elaborarea tezelor de licență.	- elaborarea articolelor; - prezentarea rezultatelor; - susținerea tezelor anuale; - susținerea tezelor de licență.

## VII. EVALUAREA DISCIPLINEI

Evaluări sumative periodice: testări.

### Mostre de teste:

#### Testul nr.1

##### **Subiectul I: Atacurile sistemelor informatice. Reglementarea criminalității informatice.**

- 1.1. Descrieți atacurile sistemelor informatice. Enumerați motivele și tipurile de riscuri.
- 1.2. Analizați categoriile infracțiunilor informatice.
- 1.3. Baza de date a MAE a fost atacată de la o stație de lucru determinați adresa fizică a calculatorului atacator.

##### **Subiectul II: Probatoriul infracțiunilor comise în sfera informației computerizate.**

- 2.1. Definiți noțiunile de infracțiune și probatoriu, explicați esența și importanța lui în descoperirea și investigarea infracțiunilor.
- 2.2. Clasificați infracțiunile informatice.
- 2.3. Proiectați aplicații pentru rezolvarea unor probleme utilizând instrumente specifice de probatoriu.

##### **Subiectul III: Atribuțiile procurorului în procesul depistării și cercetării cazurilor infracțiunilor informaționale și a fraudelor comise prin Internet. Numirea expertizei. Investigații informatice.**

- 3.1. Descrieți atribuțiile procurorului în procesul depistării și cercetării cazurilor infracțiunilor informaționale și a fraudelor comise prin Internet.
- 3.2. Identificați principalele caracteristici a investigațiilor informatice.
- 3.3. Justificați întrebările puse la soluționarea expertizei în utilizarea tehnicii de calcul.
- 3.4. Vasile – colaboratorul Întreprinderii „Romsym” din Internet a copiat o informație care conține viruși pe USB-drive, după aceea informația a fost transmisă la câțiva colaboratori, ca urmare calculatoarele au fost infectate. Argumentați dacă există în acțiunile lui Vasile temeii pentru tragerea la răspundere.

## VIII. REFERINȚE BIBLIOGRAFICE

1. Achim, Gheorghe, Metodologia investigării criminalistice a fraudelor informatice, Editura Omnia, 2000
2. Amza, Tudor, Amza, Cosmin-Petronel, Criminalitatea informatică, Ed. Lumina Lex, 2003
3. Bica, Gheorghe, Mihail, Gheorghe, Infracțiuni săvârșite prin calculator, în Revista de Drept Penal 4/1996, p. 85-88.
4. Hanga, Vladimir, Calculatoarele în serviciul dreptului, Ed. Lumina Lex, București, 1996.
5. VasIU, Ioana, Infracțiuni comise prin calculator, în Revista de Drept Penal, nr. 2/1996
6. Alexei Barbăneagră, Codul Penal al Republicii Moldova, Comentariu, Editura ARC, 2003
7. Ministerul Comunicațiilor și Tehnologiei Informației, [www.guv.ro](http://www.guv.ro).
8. Ministerul Comunicațiilor și Tehnologiei Informației, [www.mcti.ro](http://www.mcti.ro).