INSTITUTUL NAȚIONAL AL JUSTIȚIEI

Anexa nr.9
la Hotărîrea Consiliului INJ
nr.1/3 din 30 ianuarie 2015

CURRICULUM
la disciplina

„INVESTIGAREA INFRACŢIUNILOR CIBERNETICE”

(candidaţi la funcţii de judecători şi procurori)

AUTOR:
Veaceslav SOLTAN,
Procuror, şef al Secţiei tehnologii informaţionale
şi investigaţii ale infracţiunilor în
domeniul informaticii al Procuraturii Generale, formator INJ

_____ AVIZAT
Mariana PITIC, Șef Direcție instruire și cercetare

CHIŞINĂU 2015

I. PRELIMINARII

Apariţia, acum mai bine de 50 de ani, a primelor calculatoare electronice a declanşat o adevărată revoluţie în societatea umană. Consecinţa primordială a avansului tehnologic apărut a reprezentat-o tranziţia de la societatea industrială la societatea informaţională. Umanitatea a evoluat în ultimii 50 de ani mai mult decît în orice altă perioadă. Unealtă tehnologică în continuă perfecţionare, a cărei pătrundere în toate aspectele vieţii economice, sociale şi culturale a punctat această evoluţie, calculatorul electronic a devenit în ultimii ani o componentă normală a vieţii noastre.

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

Calculatoarele electronice nu au constituit o atracţie numai pentru cei interesaţi de dezvoltare, ci şi pentru cei care au văzut în exploatarea tehnologiei moderne un mod de a dobîndi foloase ne cuvenite. Analog modului în care noile tehnologii informaţionale sunt mai întîi aplicate vechilor sarcini industriale pentru perfecţionarea lor pentru ca apoi să dea naştere unor activităţi, procese şi produse noi, calculatoarele electronice au fost utilizate iniţial pentru a perfecţiona modul de comitere a unor infracţiuni tradiţionale, 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 dispoziţia conduitei criminale atît un nou obiect (informaţia, conţinută şi procesată de sistemele informatice) cît şi un nou instrument. El oferă un repertoriu deosebit de întins de tehnici şi strategii de înfăptuire a infracţiunilor, dar în acelaşi timp îmbogăţeşte sfera criminalităţii cu noi infracţiuni. Criminalitatea informatică prezintă numeroase elemente de diferenţiere faţă de fenomenul criminal tradiţional, ridicînd o serie de probleme în faţa autorităţilor responsabile pentru eradicarea acesteia.

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

Obiectivele generale ale acestei discipline vizează:

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

Avantajele pe care le prezintă cursul „Tehnologii informaţionale” pentru audienţi sunt următoarele:

- formularea obiectivelor este realizată în termeni de competenţe şi capacităţi;
- posibilitatea de a îmbogăţi registrul activităţilor de învăţare sugerate de curriculum în funcţie de obiectivele de referinţă definite şi de resursele disponibile la nivelul fiecărui audient;
- încurajarea cooperării dintre audienţi prin activităţi de grup cu asumarea de roluri individuale în vederea realizării unor aplicaţii specifice;
- conţinuturi adaptabile la resursele audienţilor.

Conţinuturile pentru curriculum-ul sunt concepute astfel încât să asigure un bagaj minim de cunoştinţe şi deprinderi din domeniul informaticii şi al tehnologiei informaţiei.

II. COMPETENŢE

Prin studiul disciplinei "Utilizarea tehnologiilor informaţionale în domeniul profesional" audientul va obține următoarele competențe:

- Să cunoască atribuţiile procurorului în procesul depistării şi cercetării cazurilor de infracţiuni informaţionale şi a fraudelor comise prin Internet;
- Să cunoască practica internațională în domeniul investigării infracțiunilor informatice;
- Să determine rolul tehnologiilor informaţionale în prevenirea şi combaterea infracţiunilor;
- Să relateze despre dispozitivele de calcul şi medii de stocare;
- Să determine metodele şi formele de bază de descoperire şi cercetare a infracţiunilor informaţionale.
- Să utilizeze în mod efectiv informaţia obţinută din sistemele informaţionale ale autorităţilor publice centrale şi locale pentru a stabili infractorul şi a dovedi faptul participării lui la comiterea infracţiunii;
- Să utilizeze în mod efectiv informaţia obţinută din reţelele Intranet şi Internet.
- Să aplice studiile de caz pe bază de dosare și soluționarea unor spețe.
- Să formuleze indicaţii concrete adresate ofiţerului de urmărire penală referitor la aspectele tactice şi tehnice de efectuare a acţiunilor de urmărire penală în cazurile infracţiunilor informaţionale;
- Să formuleze unele probleme care pot fi realizate în grupuri pe baza unor discuţii preliminare şi analiza problemei;
- Să întocmească corect formele statistice;
- Să dea apreciere probelor obţinute în rezultatul efectuării acţiunilor de urmărire penală şi să le utilizeze în procesul investigării;
- Să ia decizii optime în situaţii problematice de cercetare a infracţiunilor informaţionale.

III. PRINCIPALELE OBIECTIVE

La sfârşitul studiului disciplinei audientul va fi capabil să:

- descrie istoria atacurilor sistemelor informatice;
- enumere motivele şi tipurile de riscuri;
- clasifice riscurile şi incidentele;
- clasifice după lista de termeni;
- clasifice după lista de categorii;
- relateze despre listele empirice;
- relateze despre clasificările bazate pe acţiune;
- definească evenimentele, atacurile şi incidentele;
- enumere acţiunile;
- enumere ţintele;
- definească şi să enumere atacurile;
- enumere categoriile de unelte;
- determine noţiunea de cal troian ca program de atac;
- enumere categoriile de rezultate neautorizate.
- definească noţiunea de criminalitate informatică;
- sistematizeze categoriile de infracţiuni informatice din raportul Comitetului European;
- compare categoriile de infracţiuni informatice din manualul pentru prevenirea şi controlul infracţiunilor informatice al Naţiunilor Unite cu categoriile de infracţiuni informatice din studiul Comisiei Europene;
- aprecieze rolul criminalităţii informatice în societate.
- definească noţiunea de infracţiune informatică;
- clasifice infracţiunile informatice ;

- determine infracţiunile săvîrşite cu ajutorul sistemelor informatice;
- dezvolte responsabilităţi vizând utilizarea tehnicii de calcul în scopul accesului ilegal la un sistem informatic;
- relateze referitor regulilor de protecţie a sistemului informatic;
- determine evoluţia infracţiunilor.
- enumere organele care sunt abilitate cu atribuţii de depistare a infracţiunilor, inclusiv şi a infracţiunilor informaţionale şi fraudelor prin Internet;
- caracterizeze acţiunile ce se întreprind de către aceste organe;
- evalueze activitatea de prevenire şi combatere a infracţiunilor computerizate.
- definească noţiunea de probatoriu;
- descrie examinarea preliminară a tehnicii de calcul;
- justifice procesul examinării calculatorului.
- descrie atribuţiile procurorului în procesul depistării şi cercetării cazurilor infracţiunilor informaţionale şi a fraudelor comise prin Internet;
- aprecieze rolul serviciilor speciale în procesul depistării şi cercetării cazurilor infracţiunilor informaţionale;
- proiecteze aplicaţii pentru rezolvarea unor probleme utilizând instrumentele specifice de prelucrare a datelor.
- definească noţiunea de expertiză;
- enumere întrebările în faţa expertizei tehnico-programiste;
- justifice întrebările puse la soluţionarea expertizei în utilizarea tehnicii de calcul.
- definească noţiunea de *investigaţii informatice*;
- descrie modelele de bune practici în domeniul investigaţiilor criminalistice de natură informatică;
- identifice principalele caracteristici a investigaţiilor informatice;
- relateze referitor instrumentelor necesare pentru investigaţii.

IV. ADMINISTRAREA DISCIPLINEI

Denumirea disciplinei	Formator	Semestrul	Total ore	Ore curs	Ore practice	Evaluarea
Investigarea infracţiunilor cibernetice	**Veaceslav SOLTAN**	**II**	**24**	**8**	**16**	**colocviu diferențiat**

V. TEMATICA ŞI REPARTIZAREA ORIENTATIVĂ A ORELOR

Nr. d/o	TEMATICA	Ore curs	Ore practice
1.	Reglementarea criminalităţii informatice. Conceptul de “criminalitate informatică”.	2	2
2.	Infracţiuni informatice. Atacurile sistemelor informatice.	2	2
3.	Atribuţiile procurorului în procesul depistării şi cercetării cazurilor infracţiunilor informaţionale şi a fraudelor comise prin Internet.	-	2
4.	Investigaţii informatice.	2	2
5.	Practica internaţională în investigarea infracţiunilor informatice.	2	2
6.	Organele abilitate cu funcţii de depistare şi documentare a infracţiunilor informaţionale şi fraudelor prin Internet	-	2

7.	Calificarea şi probatoriul infracţiunilor comise în sfera informaţiei computerizate.	-	2
8.	Consideraţii generale privind numirea expertizei.	-	2
TOTAL		**8**	**16**

VI. UNITĂŢI TEMATICE

Unităţi tematice	**Strategii didactice/ Resurse logistice**	**Lucrul individual**
Tema 1. Reglementarea criminalităţii informatice. Conceptul de "criminalitate informatică".		
Ore curs 1. Definiţia criminalităţii informatice. 2. Categoriile de sistematizare ale criminalităţii informatice. 3. Categoriile de infracţiuni informatice din manualul pentru prevenirea şi controlul infracţiunilor informatice al Naţiunilor Unite cu categoriile de infracţiuni informatice din studiul Comisiei Europene; *Ore practice* 1) Descrierea istoriei atacurilor sistemelor informatice; 2) Enumerarea motivelor şi tipurile de riscuri; 3) Sistematizarea categoriilor de infracţiuni informatice din raportul Comitetului European; 4) Aprecierea rolului criminalităţii informatice în societate 5) Definirea noţiunii de infracţiune informatică;	Curs-prelegere Proiector/laptop Seminare Studiu de caz Tablă flipchart	*Ore curs* Brainstorming. Lectura surselor din Lista bibliografică. *Ore practice* 1) Proiecte. 2) Teste aplicative pentru a măsura gradul de însuşire al noţiunilor strict teoretice. 3) Probleme. 4) Analiza generalizărilor practicii judiciare.
Tema 2. Infracţiuni informatice. Atacurile sistemelor informatice.		
Ore curs 1. Clasificarea infracţiunilor informatice. 2. Atacurile sistemelor informatice**.** 3. Determinarea infracţiunilor săvîrşite cu ajutorul sistemelor informatice; 4. Accesul ilegal la un sistem informatic. 5. Art.260-260^6 CP 6. Încălcarea regulilor de securitate la diferite sisteme informaţionale. 7. Acces neautorizat la reţelele şi serviciile de telecomunicaţii 8. Evoluţia infracţiunilor. *Ore practice* 1) Clasificarea după lista de termeni; 2) Clasificarea după lista de categorii; 3) Relatarea listelor empirice; 4) Clasificările bazate pe acţiune; 5) Definirea evenimentelor, atacurilor şi incidentelor;	Curs-prelegere Proiector/laptop Seminare Studiu de caz Tablă flipchart	*Ore curs* Brainstorming. Lectura surselor din Lista bibliografică. *Ore practice* 1) prezentarea rezultatelor; 2) susţinerea tezelor

6) Enumerarea acţiunilor; 7) Enumerarea ţintelor; 8) Enumerarea categoriile de unelte; 9) Determinarea noţiunii de cal troian ca program de atac; 10) Enumerarea categoriilor de rezultate neautorizate.		
Tema 3. Atribuţiile procurorului în procesul depistării şi cercetării cazurilor infracţiunilor informaţionale şi a fraudelor comise prin Internet.		
Ore curs 1. Procurorul-conducător al procuraturii teritoriale, specializate şi subdiviziunilor Procuraturii Generale. 2. Procurorii responsabili de aplicarea şi respectarea în teritoriu a legislaţiei privind prevenirea şi combaterea infracţiunilor comise în sfera informaţiei computerizate.	Curs-prelegere Proiector/laptop	*Ore curs* Brainstorming. Lectura surselor din Lista bibliografică.
Tema 4. Investigaţii informatice.		
Ore curs 1. Dezvoltarea responsabilităţilor vizând utilizarea tehnicii de calcul în scopul accesului ilegal la un sistem informatic; 2. Determinarea evoluţiei infracţiunilor. 3. Justificarea procesului de examinarea a calculatorului. *Ore practice* 1) relateze referitor regulilor de protecţie a sistemului informatic; 2) Enumerarea organelor care sunt abilitate cu atribuţii de depistare a infracţiunilor, inclusiv şi a infracţiunilor informaţionale şi fraudelor prin Internet; 3) Caracterizarea acţiunilor ce se întreprind de către aceste organe; 4) Evaluarea activităţii de prevenire şi combatere a infracţiunilor computerizate. 5) Descrierea examinării preliminare a tehnicii de calcul;	Curs-prelegere Proiector/laptop Seminare Studiu de caz Tablă flipchart	*Ore curs* Brainstorming. Lectura surselor din Lista bibliografică. *Ore practice* 1) Studiu de caz. 2) Referate/rezumate. 3) Teste aplicative. 4) Elaborarea tezelor anuale. 5) Elaborarea tezelor de licenţă.
Tema 5. Practica internaţională în investigarea infracţiunilor informatice.		
Ore curs 1. Definirea noţiunii de *investigaţii informatice*; 2. Identificarea principalelor caracteristici a investigaţiilor informatice; *Ore practice* 1) Descrierea modelelor de bune practici în domeniul investigaţiilor criminalistice de natură informatică; 2) Relatarea referitor la instrumentele necesare pentru investigaţii.	Curs-prelegere Proiector/laptop Seminare Studiu de caz Tablă flipchart	*Ore curs* Brainstorming. Lectura surselor din Lista bibliografică. *Ore practice* 1) rezolvarea exerciţiilor practice; 2) aplicaţii practice privind utilizarea unor accesorii ale diferitor sisteme de operare 3) prezentarea rezultatelor;

		4) rezolvarea fişelor de lucru;
Tema 6. Organele abilitate cu funcţii de depistare şi documentare a infracţiunilor informaţionale şi fraudelor prin Internet		
Ore practice 1) Descrierea atribuţiilor procurorului 2) Procesul depistării şi cercetării cazurilor infracţiunilor informaţionale şi a fraudelor comise prin Internet; 3) Aprecierea rolului serviciilor speciale în procesul depistării şi cercetării cazurilor infracţiunilor informaţionale;	Seminare Studiu de caz Tablă flipchart	*Ore practice* 1) Soluționarea spețelor. 2) Examinarea sistemelor. 3) Întocmirea proiectelor de acte pentru înregistrare.
Tema 7. Calificarea şi probatoriul infracţiunilor comise în sfera informaţiei computerizate.		
Ore practice 1) Definirea noţiunii de probatoriu; 2) Probatoriul infracţiunilor comise în sfera informaţiei computerizate. 3) Descrierea examinării preliminare a tehnicii de calcul; 4) Justificarea procesului examinării calculatorului. 5) Proiectarea de aplicaţii pentru rezolvarea unor probleme utilizând instrumentele specifice de prelucrare a datelor.	Seminare Studiu de caz Tablă flipchart	*Ore practice* 1) Teste aplicative. 2) Imagini grafice. 3) Analiza datelor statistice. 4) Desene. 5) Aplicaţii practice.
Tema 8. Consideraţii generale privind numirea expertizei.		
Ore practice 1) Definirea noţiunii de expertiză; 2) Enumerarea întrebărilor în faţa expertizei tehnico-programiste; 3) Justificarea întrebărilor puse la soluţionarea expertizei în utilizarea tehnicii de calcul.	Seminare Studiu de caz Tablă flipchart	*Ore practice* 1. Teste aplicative. 2. Imagini grafice. 3. Analiza datelor statistice. 4. Desene. 5. Aplicaţii practice.

VII. EVALUAREA

Evaluarea se va efectua continuu şi la final.

A. Evaluarea continuă

- participarea audienţilor în cadrul orelor de curs şi a celor practice;
- realizarea activităţilor individuale;
- identificarea principalelor caracteristici a investigaţiilor informatice.
- aplicaţii pentru rezolvarea unor probleme utilizând instrumente specifice de probatoriu.
- codificarea şi decodificarea informaţiei de text;
- estimare a cantităţii de informaţie în fişierele de text;
- identificare şi explicare destinaţiei componentelor de bază ale calculatorului şi fluxurilor de informaţie;
- identificarea obiectivelor de măsurare a cunoştinţelor, capacităţilor şi competenţelor/aptitudinilor profesionale;
- pregătirea unui referat ştiinţific şi/sau aplicativ pe o problemă propusă pentru activităţile individuale.

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

VIII. BIBILIOGRAFIE

Acte legislative şi normative:

1. Convenţia Consiliului Europei asupra Criminalităţii 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 contravenţional 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 şi la resursele informaţionale de stat, nr. 467-XV din 21.11.2003;
7. Legea cu privire la documentul electronic şi semnătura digitală nr.264-XV din 15.07.2004;
8. Legea privind comerţul electronic nr. 284-XV din 22.07.2004 ;
9. Legea comunicaţiilor electronice nr. 241-XVI din 15.11.2007;
10. Legea privind prevenirea şi combaterea criminalităţii informatice nr. 20-XVI din 03.02.2009;
11. Legea pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică nr. 6-XVI din 02.02.2009;
12. Legea cu privire la serviciile de plată şi moneda electronică nr. 114 din 18.05.2012.

Jurisprudenţă/Practica judiciară:

13. Convenţia Uniunii Internaţionale a Telecomunicaţiilor.
14. Constituţia Uniunii Internaţionale de Telecomunicaţii.
15. Recomandarea R(85)10 cuprinzând normele de aplicare a Convenţiei Europene de Asistenţă Mutuală în Materie Infracţională, cu referire la comisiile rogatorii privind interceptarea telecomunicaţiilor;
16. Recomandarea R(88)2 privind pirateria în contextul existenţei drepturilor de autor şi a drepturilor conexe;
17. Recomandarea R(87)15 privind reglementarea utilizării datelor personale în munca de poliţie;
18. Recomandarea R(89)9 privind unele norme care trebuie aplicate de statele membre pentru combaterea criminalităţii informatice.
19. Recomandarea R(95)4 privind protecţia datelor personale în domeniul serviciilor de telecomunicaţii;
20. Recomandarea R(95)13 privind aspecte de procedură penală în legătură cu Tehnologia Informaţiei;

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, Infracţiuni săvîrşite prin calculator, în Revista de Drept Penal 4/1996, p. 85-88.
24. Hanga, Vladimir, Calculatoarele în serviciul dreptului, Ed. Lumina Lex, Bucureşti,1996.
25. Vasiu, Ioana, Infracţiuni comise prin calculator, în Revista de Drept Penal, nr. 2/1996
26. Alexei Barbăneagră, Codul Penal al Republicii Moldova, Comentariu, Editura ARC, 2003.