Universitatea POLITEHNICA din Bucureşti
Facultatea de Stiinte Aplicate

FISA DISCIPLINEI
CRIMINALITATEA INFORMATICA (C.I.)

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea POLITEHNICA din Bucureşti
1.2 Facultatea	Facultatea de Stiinte Aplicate
1.3 Departamentul	Departamentul de Metode si Modele Matematice
1.4 Domeniul de studii	Stiinte Ingineresti Aplicate
1.5 Ciclul de studii	MASTER
1.6 Programul de studii/Calificarea	TCSI/ Specialist SIG/IT COD.COR 252901

2. Date despre disciplină

2.1 Denumirea disciplinei				CRIMINALITATEA INFORMATICA (C.I.)			
2.2 Titularul activităţilor de curs				lector dr. Emil Simion			
2.3 Titularul activităţilor de seminar				lector dr. Emil Simion			
2.4 Anul de studiu	II	2.5 Semestrul	I	2.6 Tipul de evaluare	Verificare	2.7 Regimul disciplinei	Obligatoriu

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână din care	1	3.2 curs	1	3.3 seminar/laborator	2
3.4 Total ore din planul de învăţământ din care	42	3.5 curs	14	3.6 seminar/laborator	28
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie şi notițe					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate					5
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					10
Tutoriat					0
Examinări					3
Alte activităţi					0

3.7 Total ore studiu individual	62
3.9 Total ore pe semestru	104
3. 10 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Nu este cazul
4.2 de competenţe	Nu este cazul

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului	Nu este cazul
5.2 de desfăşurare a seminarului	Prezenţa obligatorie la seminarii

6. Competenţe specifice acumulate

Competenţe profesionale	- Dezvoltarea capacităţii de a folosi în domeniul cercetării informatice cunoştinţe de matematică modernă; - Dezvoltarea abilităţilor de folosire a sistemelor de operare UNIX şi

	LINUX; - Dezvoltarea capacităţii de a proiecta şi administra reţele de calculatoare; - Dezvoltarea capacităţii de a proteja serverele de atacurile informatice si de a asigura un trafic informaţional securizat; - Dezvoltarea capacităţii de lucru în echipă; - Dezvoltarea capacităţii de cercetare ştiinţifică; - Aplicarea, în situaţii tipice, a metodelor de colectare si investigare a probelor rezultate din infractiunile de criminalitate informatica.
Competenţe transversale	Comportarea onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputaţia profesiei.

7. Obiectivele disciplinei (reieşind din grila de competenţe specifice acumulate)

7.1 Obiectivul general al disciplinei	Aplicarea, în situaţii tipice, a metodelor de colectare si investigare a probelor in cazul criminalitatii informatice.
4.2 Obiective specifice	**1. Cunoştinţe teoretice - Cunoaştere şi înţelegere:** Prezentarea tehnicilor şi metodelor utilizate in colectarea si investigarea probelor criminalitatii informatice. Cunoaşterea cadrului legislativ afferent domeniului informatic. . **2. Deprinderi dobândite - Explicare şi interpretare:** Formarea deprinderilor necesare colectarii si investigarii probelor rezultate in urma active de criminalitate informatica. **3. Abilităţi dobândite - Instrumental-aplicative:** Utilizarea instrumentelor de colectare şi analiza a probelor informatice. **4. Atitudinale:** Capacitatea de lucru în echipă pentru rezolvarea unor probleme practice. Responsabilitate şi corectitudine în activităţile desfăşurate.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1. Societatea informationala: ➢ semnatura electronica; ➢ marcare temporala; ➢ notariat electronic; ➢ arhivare electronica; ➢ ebanking; ➢ comert electronic; ➢ aparate de marcat electronice fiscale.	Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă); metodele de comunicare orală utilizată sunt metoda expozitivă şi metoda problematizării, utilizate frontal. Materialele de curs sunt: notele şi prezentările de curs, culegeri de probleme propuse (teoretice şi cu rezolvare pe calculator). Toate materialele sunt disponibile în format electronic, prin situl cursului.	3 ore
2. Infractiuni informatice in codul penal		1 ore
3. Investigatii asupra calculatoarelor: fake update exploits; email attachments exploits;		3 ore
4. Investigatii asupra terminalelor mobile		1 ore
5. Frauda bancara		1 ore
6. Investigatii asupra retelelor de comunicatii		3 ore

Bibliografie

1. Pooya Farshim, E. Simion, *Innovative Security Solutions for Information Technology and Communications*, Springer Verlag, LNCS 10543, 2017, ISBN: 978-3-319-69283-8, DOI: 10.1007/978-3-319-69284-5.
2. A. Pătraşcu, E. Simion, *Applied cryptography and practical scenarios for cyber security defense*, Scientific Bulletin of University „Politehnica" of Bucharest, Series C: Electrical Engineering and Computer Science, vol 75, Iss. 4, 2012, ISSN 2286 – 3540, pp. 131-142.
3. A. Pătraşcu, E. Simion, *Critical Infrastructures Cyber Protection Using Kernel Based Supervised Learning Techniques*, MTA Review, Military Technical Academy Publishing House, vol.XXIV, no. 2, Jun. 2014, ISSN 1843-3391, pp. 59-66.
4. Nicu Bizon, Lucian Dascalescu, Naser M. Tabatabei, E. Simion et. al., *Autonomous Vehicles: Intelligent Transport Systems and Automotive Technologies*, Chapter 4: *Cyber Security Evaluation of Critical Infrastructures System*, pp 73-92, Publishing house of the University of Piteşti, 2013, ISBN: 978-606-560-327-1.
5. D. Maimuţ, A. Pătraşcu, E. Simion, *Cloud Computing in Cyberwarfare*, MTA Review, Military Technical Academy Publishing House, vol.XXII, no. 3, sept. 2012, ISSN 1843-3391, pp. 159-180.
6. W. Stalings, *Cryptography and Network Security: Principles and Practice (6th Edition)*- 6th Edition, 2013.

8.2 Seminar	Metode de predare	Observaţii
1. Continutul si forma unui raport de expertiza criminalistica	Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă); metoda de comunicare orală utilizată este metoda problematizării,utilizate frontal. Materialele didactice sunt postate pe platforma educaţională a UPB.	2 ore
2. Unelte de analiză a fisierelor binare: UltraEdit, Cryptool.		6 ore
3. Utilitare de analiza a probelor digitale: EnCase, FTK Recovery.		8 ore
4. Exercitii practice care urmaresc linia cursului		12

Bibliografie

1. Pooya Farshim, E. Simion, *Innovative Security Solutions for Information Technology and Communications*, Springer Verlag, LNCS 10543, 2017, ISBN: 978-3-319-69283-8, DOI: 10.1007/978-3-319-69284-5.
2. A. Pătraşcu, E. Simion, *Applied cryptography and practical scenarios for cyber security defense*, Scientific Bulletin of University „Politehnica" of Bucharest, Series C: Electrical Engineering and Computer Science, vol 75, Iss. 4, 2012, ISSN 2286 – 3540, pp. 131-142.
3. A. Pătraşcu, E. Simion, *Critical Infrastructures Cyber Protection Using Kernel Based Supervised Learning Techniques*, MTA Review, Military Technical Academy Publishing House, vol.XXIV, no. 2, Jun. 2014, ISSN 1843-3391, pp. 59-66.
4. Nicu Bizon, Lucian Dascalescu, Naser M. Tabatabei, E. Simion et. al., *Autonomous Vehicles: Intelligent Transport Systems and Automotive Technologies*, Chapter 4: *Cyber Security Evaluation of Critical Infrastructures System*, pp 73-92, Publishing house of the University of Piteşti, 2013, ISBN: 978-606-560-327-1.
5. D. Maimuţ, A. Pătraşcu, E. Simion, *Cloud Computing in Cyberwarfare*, MTA Review, Military

Technical Academy Publishing House, vol.XXII, no. 3, sept. 2012, ISSN 1843-3391, pp. 159-180.
1. W. Stalings, *Cryptography and Network Security: Principles and Practice (6th Edition)*- 6th Edition, 2013.

9. Coroborarea conţinuturilor disciplinei cu asteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale si angajatori reprezentativi din domeniul aferent programului

Intrând progresiv în era informaţiei, societăţile industrializate se găsesc în faţa unui paradox: pe de o parte, puterea şi influenţa Europei şi a Americii de Nord au crescut semnificativ, în principal datorită măiestriei modalităţilor prin care se controlează fluxurile de informaţii, precum şi valorii crescute a datelor procesate. Pe de altă parte, după cum au demonstrat-o deja criza Wikileaks, viermele Stuxnet, sau virusul WannaCry, apar noi ameninţări şi vulnerabilităţi care fac ca dependenţa noastră de sistemele informaţionale să fie crucială. De aceea, dezvoltarea atacurilor cibernetice, precum şi disponibilitatea online a instrumentelor utilizate în activitatea de piraterie conduce la obiective strategice importante şi cultivă necesitatea de a pregăti experţi pentru acest domeniu. Mediul în care trăim se schimbă în ritm alert, această evoluţie fiind rezultatul progresului în domeniul tehnologiilor informaţionale, precum şi al matematicii. **Cursul are ca obiectiv dobindirea competentelor necesare colectarii si investigarii probelor digitale, precum si al elaborarii rapoartelor de expertiza tehnica.**

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală
10.4 Curs	-cunoaşterea noţiunilor teoretice fundamentale; - cunoaşterea modului de aplicare a teoriei la probleme specifice; - analiza diferenţială a tehnicilor şi metodelor teoretice.	Examen final	50%
10.5 Seminar	- cunoasterea aplicarii, pe exemple concrete a elementelor teoretice exemplificate in cadrul cursului.	Activitate laborator	50%
10.6 Standard minim de performanţă			
Cunoaşterea noţiunilor teoretice de bază prezentate la curs şi rezolvarea unor probleme tip.			

Data completării **01.09.2018**

Semnătura titularului de curs
lector dr. Emil Simion

Semnătura titularului de aplicaţii
lector dr. Emil Simion

Data avizării în departament
.....

Semnătura sefului de department
prof. dr. Mircea Olteanu

Responsabil program master
lector dr. Emil Simion