FIŞA DISCIPLINEI

Anul universitar 2021-2022

Decan,
Prof. Vasile-Ion Manta

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică „Gheorghe Asachi” din Iaşi
1.2 Facultatea	Automatică şi Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare şi tehnologia informaţiei
1.5 Ciclul de studii[1]	Masterat
1.6 Programul de studii	Securitatea spațiului cibernetic

2. Date despre disciplină

2.1 Denumirea disciplinei/Cod				Securitatea spațiului cibernetic / SCC.IA.101			
2.2 Titularul activităţilor de curs				Conf.dr.ing. Mihai Horia Zaharia			
2.3 Titularul activităţilor de aplicaţii				Conf.dr.ing. Mihai Horia Zaharia			
2.4 Anul de studii[2]	1	2.5 Semestrul[3]	1	2.6 Tipul de evaluare[4]	examen	2.7 Tipul disciplinei[5]	DA

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

3.1 Număr de ore pe săptămână	4	din care 3.2 curs	2	3.3a sem.		3.3b laborator	2	3.3c proiect	
3.4 Total ore din planul de învăţământ[6]	56	din care 3.5 curs	28	3.6a sem.		3.6b laborator	28	3.6c proiect	

Distribuţia fondului de timp[7]	Nr. ore
Studiul după manual, suport de curs, bibliografie şi notiţe	27
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	26
Pregătire seminarii/laboratoare/proiecte, teme, referate şi portofolii	30
Tutoriat[8]	7
Examinări[9]	4
Alte activităţi:	

3.7 Total ore studiu individual[10]	94
3.8 Total ore pe semestru[11]	150
3.9 Numărul de credite	6

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum[12]	• Asamblare, Programarea Calculatoarelor, Sisteme de operare, retele de calculatoare, paradigme de programare
4.2 de competenţe	• Etică, deontologie, matematica, programare, administrare

---

1 *Licenţă / Master*

2 *1-4 pentru licenţă, 1-2 pentru master*

3 *1-8 pentru licenţă, 1-3 pentru master*

4 *Examen, colocviu sau VP A/R – din planul de învăţământ*

5 *DF - disciplină fundamentală, DID - disciplină în domeniu, DS – disciplină de specialitate sau DC - disciplină complementară - din planul de învăţământ*

6 *Este egal cu 14 săptămâni* x *numărul de ore de la punctul 3.1 (similar pentru 3.5, 3.6abc)*

7 *Liniile de mai jos se referă la studiul individual; totalul se completează la punctul 3.7.*

8 *Între 7 şi 14 ore*

9 *Între 2 şi 6 ore*

10 *Suma valorilor de pe liniile anterioare, care se referă la studiul individual.*

11 *Suma dintre numărul de ore de activitate didactică directă (3.4) şi numărul de ore de studiu individual (3.7); trebuie să fie egală cu numărul de credite alocat disciplinei (punctul 3.9)* x *24 de ore pe credit.*

12 *Se menţionează disciplinele obligatoriu a fi promovate anterior sau echivalente*

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului[13]	• Tablă, videoproiector
5.2 de desfăşurare a seminarului / laboratorului / proiectului[14]	• Debian buster, Pycharm,virtual box, imagini instalate Kali, Parrot, Damn Vulnerable Linux, Win8, docker, server vulnerabil pentru atac - mașina separata, router dispobibil pentru atac, malware pentru analiză, drept de supervisor la studenți

6. Competenţele specifice acumulate[15]

		Număr de credite alocat disciplinei[16]:	**6**
Competenţe profesionale	CP1	Cunoașterea conceptelor avansate din domeniul științei calculatoarelor și tehnologiei informației și capacitatea de a opera cu aceste concepte.	0.6
	CP2	Cercetarea științifică și practică privind securitatea sistemelor informatice complexe.	1.0
	CP3	Rezolvarea problemelor pe baza metodelor și tehnologiilor de securizare a sistemelor informatice complexe.	1.45
	CP4	Utilizarea de instrumente specifice domeniului în vederea identificării vulnerabilităților și a amenințărilor de securitate cibernetică.	1.1
	CP5	Proiectarea și dezvoltarea de soluții software cu un înalt grad de securitate orientate pe prevenția și răspunsul la incidente de securitate cibernetică.	1.5
	CP6		
	CPS1		
	CPS2		
Competenţe transversale	CT1	Aplicarea, în contextul respectării legislației, a drepturilor de proprietate intelectuală, a principiilor, normelor și valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă și responsabilă.	0.05
	CT2	Identificarea rolurilor și responsabilităților într-o echipă specializată, luarea deciziilor și atribuirea de sarcini, cu aplicarea de tehnici de relaționare și muncă eficientă în cadrul echipei.	0.15
	CT3	Dezvoltarea spiritului de creativitate, inițiativă și acțiune, pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.	0.15
	CTS		

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	• Securitatea cibernetică se referă la totalitatea practicilor, metodelor și mijloacelor tehnice utilizate în protecția, calculatoarelor, serverelor, dispozitivelor mobile, sistemelor electronice, rețelelor de comunicații precum și a datelor indiferent de zona de păstrare împotriva atacurilor.
7.2 Obiective specifice	• Să înțeleagă și să poată aplica noile dezvoltări specifice domeniului • Să aibă abilitatea de a investiga, analiza și sintetiza un volum mare de informații complexe • Să aibă abilitatea de a evalua noi concepte teoretice și practice dar și de a își prezenta și justifica propunerile și evaluările proprii atât la nivel teoretic cât și practic

[13] *Tablă, videoproiector, flipchart, materiale didactice specifice etc.*

[14] *Tehnică de calcul, pachete software, standuri experimentale, etc.*

[15] *Competenţele din Grilele G1 şi G1bis ale programului de studii, adaptate la specificul disciplinei, pentru care se repartizează credite (www.rncis.ro sau site-ul facultăţii)*

[16] *Din planul de învăţământ*

[17] *Creditele alocate disciplinei se distribuie pe competenţe profesionale şi transversale în funcţie de specificul disciplinei*

	• Să dezvolte o gândire critică la nivelul materiei studiate atât din punct de vedere practic cât și teoretic • Să își însușească deontologia generală dar și cea specifică respectivei discipline • Să își dezvolte abilitatea de autodepășire continuă • Să aibă abilitatea de a trece prin toate fazele de la idee până la cea de prototip funcțional pentru subiectul materiei studiate • Să se adapteze rapid la orice schimbări apărute atât la nivel situațional, profesional cât și la nivelul câmpului de studiu specific materiei studiate • Să fie capabil să înțeleagă, aplice și verifice aplicarea standardelor de calitate și tehnice asociate respectivei materii

8. Conţinuturi

8.1 Curs[18]	Metode de predare[19]	Observaţii
1. Cybersecurity - termeni definitii si concepte 2. Razboi informatic si legislatia asociata Inclusiv Gdpr - protecția date personale 3. Crearea unei echipe de lucrurosie-albastră 4. PKI 5. DSS 6. Securitatea unui dispozitiv de calcul conectat la Internet 7. Honeypot & SeLinux 8. Valoarea informatiei, modelarea si evaluarea amenintarilor de securitate 9. Auditarea unei organizatii utilizand Octave 10. Securitatea cloud-ului 11. Confidentializatea datelor personale in viitorul ciberspatiu 12. Securitatea dispozitivelor mobile 13. Sisteme de securitate fizică 14. Analiză malware	Tablă, videoproiector	
Bibliografie curs: 1. George Kostopoulos - Cyberspace and Cybersecurity Second Edition, Taylor & Francis - CRC, Boca Raton, 2018 2. Jeff Kosseff, Cybersecurity Law, Willey, 2017 3. Michael Erbschloe, Threat Level Red Cybersecurity Research Programs of the U.S. Government, Taylor & Francis - CRC, Boca Raton, 2017 4. Mohssen Mohammed, Habib-ur Rehm, Honeypotsand Route Collecting Internet Attacks, Taylor & Francis - CRC, Boca Raton, 2016 5. Prakhar Prasad, Mastering Modern Web Penetration Testing, Packt, 2016 6. Christopher J. Alberts Audrey J. Dorofee, OCTAVESM Method Implementation Guide Version 2.0, 2001 7. NIST (Authors: P. Mell and T. Grance), "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology Laboratory (October 7 2009). 8. J. Camp. (2001), “Trust and Risk in Internet Commerce,” MIT Press 9. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing, ver3, 2011		
8.2a Seminar	Metode de predare[20]	Observaţii
8.2b Laborator	Metode de predare[21]	Observaţii

[18] *Titluri de capitole şi paragrafe*

[19] *Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuţii cu studenţii (pentru fiecare capitol, dacă este cazul)*

[20] *Discuţii, dezbateri, prezentare şi/sau analiză de lucrări, rezolvare de exerciţii şi probleme*

[21] *Demonstraţie practică, exerciţiu, experiment*

1. Auditare stație de lucru cu MS Windows 2. Instrumente specifice securizarii Linux 3. Auditarea utilizând comenzi Linux 4. RSA & PKI 5. Faza de Recunoaștere - Enumerare Resurse și Infrastructură 6. Utilizare Metasploit 7. Faza de Recunoaștere - Analiză vulnerabilități pentru diverse servere Web. 8. Utilizare Python pentru recunoaștere 9. Dezvoltarea de programe pentru injecție și exploatare utilizând Python 10. Analiza de securitate nori - ScoutSuite 11. Analiză și atac rețele WiFi 12. Analiza de log-uri de securitate 13. SeLinux 14. Analiza de executabil utilizând Ghidra	Tablă, interacțiune directă	
8.2c Proiect	Metode de predare[22]	Observaţii
Bibliografie aplicaţii (seminar / laborator / proiect): 1. Ross J. Anderson Security Engineering Second Edition, Wiley Publishing, Inc. Indianapolis, 2008 2. Earnest Wish, Leo, Python Application Hacking Essentials,2015 3. J. McDermott, (2009) "Security Requirements for Virtualization in Cloud Computing," presented at the ACSAC Cloud Security Workshop, Honolulu, Hawaii, USA, 2009.		

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului[23]

Având în vedere înlocuirea războiului rece cu cel asimetric bazat pe atacuri informatice declanșat acum cinci ani la nivel internațional relevanța cunoștințelor legate de cybersecuritate este imediată. În acest context nu se poate concepte un specialist IT fără astfel de cunoștințe. Materia permite dezvoltarea completă a abilităților necesare atât pentru evaluarea securității prin Octave cât și testarea prin penetrare a unei organizații dar și a unei aplicații aflate în dezvoltare și datorită problemelor discutate la curs acoperă și problemele de selecție de personal cât și aplicarea integrată a SIEM într-o organizație.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare		10.3 Pondere din nota finală
10.4a Examen / Colocviu	• Cunoştinţe teoretice şi practice însuşite (cantitatea, corectitudinea, acurateţea)	Teste pe parcurs[24]:	%	75% (minim 5)
		Teme de casă:	33.(3)%	
		Alte activităţi[25]: proiect	33.(3)%	
		Evaluare finală:	33.(3)% (minim 5)	
10.4b Seminar	• Frecvenţa/relevanţa intervenţiilor sau răspunsurilor	Evidenţa intervenţiilor, portofoliu de lucrări (referate, sinteze ştiinţifice)		% (minim 5)
10.4c Laborator	• Cunoaşterea aparaturii, a modului de utilizare a instrumentelor specifice; evaluarea unor instrumente sau realizări, prelucrarea şi interpretarea unor	• Chestionar scris • Răspuns oral • Demonstraţie practică		25% (minim 5)

22 *Studiu de caz, demonstraţie, exerciţiu, analiza erorilor etc.*

23 *Legătura cu alte discipline, utilitatea disciplinei pe piaţa muncii*

24 *Se va preciza numărul de teste şi săptămânile în care vor fi susţinute.*

25 *Cercuri ştiinţifice, concursuri profesionale etc.*

	rezultate		
10.4d Proiect	• Calitatea proiectului realizat, corectitudinea documentaţiei proiectului, justificarea soluţiilor alese	• Autoevaluarea, prezentarea şi/sau susţinerea proiectului • Evaluarea critică a unui proiect	% (minim 5)
10.5 Standard minim de performanţă[26]			

Data completării, Semnătura titularului de curs, Semnătura titularului de aplicaţii,

13.01.2021 Conf.dr.ing. Mihai Horia Zaharia Conf.dr.ing. Mihai Horia Zaharia

Data avizării în departament, Director departament,

13.01.2021 Conf.dr.ing. Andrei Stan

[26] *Se particularizează la specificul disciplinei standardul minim de performanţă din grila de competenţe a programului de studii, dacă este cazul.*