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 rețelelor wireless și a dispozitivelor mobile/SCC.IA.104			
2.2 Titularul activităţilor de curs				conf. univ. dr. ing. Elena Șerban			
2.3 Titularul activităţilor de aplicaţii				conf. univ. dr. ing. Elena Șerban			
2.4 Anul de studii[2]	I	2.5 Semestrul[3]	I	2.6 Tipul de evaluare[4]	C	2.7 Tipul disciplinei[5]	DA

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

3.1 Număr de ore pe săptămână	3	din care 3.2 curs	2	3.3a sem.	-	3.3b laborator	1	3.3c proiect	-
3.4 Total ore din planul de învăţământ[6]	42	din care 3.5 curs	28	3.6a sem.	-	3.6b laborator	14	3.6c proiect	-

Distribuţia fondului de timp[7]	Nr. ore
Studiul după manual, suport de curs, bibliografie şi notiţe	22
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	26
Pregătire seminarii/laboratoare/proiecte, teme, referate şi portofolii	22
Tutoriat[8]	10
Examinări[9]	3
Alte activităţi:	

3.7 Total ore studiu individual[10]	83
3.8 Total ore pe semestru[11]	125
3.9 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum[12]	●
4.2 de competenţe	●

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului[13]	● Sală
5.2 de desfăşurare a seminarului / laboratorului / proiectului[14]	● Rețea de calculatoare cu acces la Internet cu acces la mașinile virtuale puse la dispoziție de ENISA (referința bibliografică [1].

[1] *Licenţă / Master*

[2] *1-4 penrtru 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 completeaza 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*

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

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

6. Competenţele specifice acumulate[15]

	Număr de credite alocat disciplinei[16]:	**5**	Repartizare credite pe competenţe[17]
Competenţe profesionale	CP1	Cunoașterea conceptelor avansate din domeniul științei calculatoarelor și tehnologiei informației și capacitatea de a opera cu aceste concepte.	1
	CP2	Cercetarea științifică și practică privind securitatea sistemelor informatice complexe.	1
	CP3	Rezolvarea problemelor pe baza metodelor și tehnologiilor de securizare a sistemelor informatice complexe.	1
	CP4	Utilizarea de instrumente specifice domeniului în vederea identificării vulnerabilităților și a amenințărilor de securitate cibernetică.	1
	CP5	Proiectarea și dezvoltarea de soluții software cu un înalt grad de securitate orientate pe prevenția și răspunsul la incidente de securitate cibernetică.	0.5
	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.	0.25
	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.	-
	CT3	Dezvoltarea spiritului de creativitate, inițiativă și acțiune, pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.	0.25
	CTS		

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

7.1 Obiectivul general al disciplinei	• Introducerea de concepte, unelte și tehnici folosite pentru gestionarea incidentelor legate de dispozitivele mobile și prezentarea riscurilor de pe platformele mobile și a căilor de identificare și reducere a acestor riscuri, ca și tehnici pentru analizarea amenințărilor legate de platformele mobile și malware.
7.2 Obiective specifice	• Înțelegerea modului de funcționare a sistemelor de operare pentru dispozitive mobile și a modelelor și principiilor securității aplicațiilor mobile • Însușirea abilității de a analiza din punctul de vedere al securității cibernetice o aplicație mobilă • Însușirea abilității de a efectua analiză inversă pe o aplicație mobilă

8. Conţinuturi

8.1 Curs[18]	Metode de predare[19]	Observaţii
1. Tipuri de sisteme de operare pe dispozitive mobile și wearable (2 ore) 2. Aplicații pentru analiza dispozitivelor mobile (2 ore) 3. Vulnerabilități ale sistemelor de operare mobile (8 ore) 4. Metode de securizare ale dispozitivelor mobile (8 ore) 5. Elemente de forensics pentru dispozitive mobile (8 ore) **Total ore curs 28 ore**	Prezentare la tablă a problematicii studiate, utilizare videoproiector, discuţii cu studenţii	

Bibliografie curs:

[1] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational

[2] Bergman, N., Stanfield, M., Rouse, J., Scambray, J., et al. (2013). *Hacking Exposed Mobile: Security Secrets & Solutions*. McGraw Hill Osbourne Media: New York, NY.

[3] Androulidakis, I. (2012). *Mobile Phone Security and Forensics: A Practical Approach*. Springer: New York, NY.

[4] OWASP Mobile Security Testing Guide, https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide#tab=Main

[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*

[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)*

[5] Eric Butow, *Pro iOS Security and Forensics: Enterprise iPhone and iPad Safety*, Apress, 2018
[6] Nikolay Elenkov, *Android Security Internals: An In-Depth Guide to Android's Security Architecture*, No Starch Press, 2014
[7] Rohit Tamma, Oleg Skulkin, Heather Mahalik, Satish Bommisetty, *Practical Mobile Forensics - Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms*, Packt Publishing, 2018.

8.2a Seminar	Metode de predare[20]	Observaţii

8.2b Laborator	Metode de predare[21]	Observaţii
1. Prezentare instrumente de lucru (2 ore) 2. Familiarizare cu Android, AVD și ADB. Clonarea unei aplicații (2 ore) 3. Analiza aplicației clonate. Analiza simplelocker (2 ore) 4. Analiza drepturilor de acces pe un dispozitiv Android și un dispozitiv iOS (2 ore) 5. Extragerea datelor din dispozitive Android (2 ore) 6. Recuperarea datelor(2 ore) 7. Ram Memory dump pentru dispozitive Android (2 ore)	Rezolvare de probleme cu implemntare practică a soluției și discutarea situațiilor speciale	

8.2c Proiect	Metode de predare[22]	Observaţii

Bibliografie aplicaţii (seminar / laborator / proiect):

[1] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational
[2] Bergman, N., Stanfield, M., Rouse, J., Scambray, J., et al. (2013). *Hacking Exposed Mobile: Security Secrets & Solutions*. McGraw Hill Osbourne Media: New York, NY.
[3] Androulidakis, I. (2012). *Mobile Phone Security and Forensics: A Practical Approach*. Springer: New York, NY.
[4] OWASP Mobile Security Testing Guide, https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide#tab=Main
[5] Eric Butow, *Pro iOS Security and Forensics: Enterprise iPhone and iPad Safety*, Apress, 2018
[6] Nikolay Elenkov, *Android Security Internals: An In-Depth Guide to Android's Security Architecture*, No Starch Press, 2014
[7] Rohit Tamma, Oleg Skulkin, Heather Mahalik, Satish Bommisetty, *Practical Mobile Forensics - Third Edition: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms*, Packt Publishing, 2018.

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

Migrarea pe echipamente mobile și pătrunderea acestora în viața cotodiană, precum și extinderea trendului BYOD (Bring Your Own Device) și BYOC (Bring Your Own Cloud) aduce cu sine nevoia de securitate a datelor. Adopția accelerată a mobilității la nivel global are un impoact important asupra mediul economic care se confruntă cu provocări sporite pe zona de securitate. Totodată protecția datelor personale vehiculate în mediul mobil este o necesitate pentru fiecare utilizator, conștientizarea fiind un prim pas pentru o utilizare mai sigură a dispozitivelor mobile.
Cursuri legate de securitatea dispozitivelor mobile sunt prezente în numeroase programe de masterat din România (Cluj, București), Europa: (Oxford – Mobile Systems Security - https://www.cs.ox.ac.uk/softeng/subjects/MSS.html Aalto University - https://courses.aalto.fi/course/CS-E4310), dar și din SUA (XACS215 - Mobile Security, Stanford, USA, http://scpd.stanford.edu/search/publicCourseSearchDetails.do?method=load&courseId=13070857).

De asemenea, sunt firme care organizează cursuri care asigură și accesul la certificare în domeniul securității cibernetice a dispozitivelor mobile (https://www.sans.org/course/mobile-device-security-ethical-hacking).

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]:	50%	50% (minim 5)
		Teme de casă:	%	
		Alte activităţi[25]:	%	
		Evaluare finală:	50% (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	● Chestionar scris ● Răspuns oral ● Caiet de laborator (lucrări experimentale, referate) ● Demonstraţie practică		50% (minim 5)

[20] *Discuţii, dezbateri, prezentare şi/sau analiză de lucrări, rezolvare de exerciţii şi probleme*
[21] *Demonstraţie practică, exerciţiu, experiment*
[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.*

	sau realizări, prelucrarea şi interpretarea unor 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,

13.01.2021

Semnătura titularului de curs,

conf. univ. dr. ing. Elena Şerban

Semnătura titularului de aplicaţii,

conf. univ. dr. ing. Elena Şerban

Data avizării în departament,

13.01.2021

Director departament,

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.*