FIŞA DISCIPLINEI
Anul universitar 2021-2022

Decan,
Prof. Vasile-Ion Manta

1. Date despre program

1.1 Instituția de învățământ 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 spaţiului cibernetic

2. Date despre disciplină

2.1 Denumirea disciplinei/Cod	Metode de securitate bazate pe hardware şi virtualizare						
2.2 Titularul activităților de curs	Conf. dr. ing. Andrei Stan						
2.3 Titularul activităților de aplicații	Conf. dr. ing. Andrei Stan						
2.4 Anul de studii[2]	1	2.5 Semestrul[3]	1	2.6 Tipul de evaluare[4]	E	2.7 Tipul disciplinei[5]	DA

3. Timpul total estimat al activităților 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 învățământ[6]	42	din care 3.5 curs	28	3.6a sem.		3.6b laborator	14	3.6c proiect	

Distribuția fondului de timp[7]	Nr. ore
Studiul după manual, suport de curs, bibliografie şi notițe	30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	34
Pregătire seminarii/laboratoare/proiecte, teme, referate şi portofolii	24
Tutoriat[8]	14
Examinări[9]	6
Alte activități:	

3.7 Total ore studiu individual[10]	108
3.8 Total ore pe semestru[11]	150
3.9 Numărul de credite	6

4. Precondiții (acolo unde este cazul)

4.1 de curriculum[12]	●
4.2 de competențe	●

5. Condiții (acolo unde este cazul)

5.1 de desfăşurare a cursului[13]	● Sală de curs dotată cu videoproiector, tablă şi acces internet
5.2 de desfăşurare a seminarului / laboratorului / proiectului[14]	● Sală de laborator cu calculatoare şi acces la internet ● Sisteme de operare: Linux cu pachete software pentru emulare şi virtualizare (OVP, QEMU, KVM, VirtualBOX) ● Sisteme de dezvoltare cu microcontroler şi/sau FPGA

6. Competenţele specifice acumulate[15]

[1] *Licență / Master*
[2] *1-4 penrtru licență, 1-2 pentru master*
[3] *1-8 pentru licență, 1-3 pentru master*
[4] *Examen, colocviu sau VP A/R – din planul de învățământ*
[5] *DF - disciplină fundamentală, DID - disciplină în domeniu, DS – disciplină de specialitate sau DC - disciplină complementară - din planul de învățământ*
[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 menționează 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.*
[15] *Competențele din Grilele G1 şi G1bis ale programului de studii, adaptate la specificul disciplinei, pentru care se repartizează credite (www.rncis.ro sau site-ul facultății)*

		Număr de credite alocat disciplinei[16]:	**6**

			Repartizare credite pe competențe[17]
Competenţe profesionale	CP1	Cunoașterea conceptelor avansate din domeniul ştiinţei calculatoarelor şi tehnologiei informaţiei şi capacitatea de a opera cu aceste concepte.	1.2
	CP2	Cercetarea ştiinţifică şi practică privind securitatea sistemelor informatice complexe.	1.2
	CP3	Rezolvarea problemelor pe baza metodelor şi tehnologiilor de securizare a sistemelor informatice complexe.	1.0
	CP4	Utilizarea de instrumente specifice domeniului în vederea identificării vulnerabilităţilor şi a ameninţărilor de securitate cibernetică.	1.0
	CP5	Proiectarea şi dezvoltarea de soluţii software cu un înalt grad de securitate orientate pe prevenţia şi răspunsul la incidente de securitate cibernetică.	0.8
	CP6		
	CPS1		
	CPS2		
Competenţe transversale	CT1	Aplicarea, în contextul respectării legislaţiei, a drepturilor de proprietate intelectuală, a principiilor, normelor şi valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă şi responsabilă.	0.3
	CT2	Identificarea rolurilor şi responsabilităţilor într-o echipă specializată, luarea deciziilor şi atribuirea de sarcini, cu aplicarea de tehnici de relaţionare şi muncă eficientă în cadrul echipei.	0.3
	CT3	Dezvoltarea spiritului de creativitate, iniţiativă şi acţiune, pentru actualizarea cunoştinţelor profesionale, economice şi de cultură organizaţională.	0.2
	CTS		

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

7.1 Obiectivul general al disciplinei	• Familiarizarea studenţilor cu metode şi mijloace hardware şi cu soluţii de virtualizare pentru asigurarea securităţii sistemelor de calcul
7.2 Obiective specifice	• Cunoaşterea tipurilor de vulnerabilităţi, atacuri şi contramăsuri hardware • Dezvoltarea de soluţii hardware pentru creşterea securităţii • Evaluarea măsurilor de securitate hardware

8. Conținuturi

8.1 Curs[18]	Metode de predare[19]	Observații
1. (2h) Circuite electronice digitale – elemente moderne de proiectare (ASIC, FPGA, PCB, embedded systems, SoC, DFT, DFD, bootloaders) 2. (2h) Securitatea hardware vs încrederea în componenta hardware. Standarde de securitate: The Orange Book, NIST-FIPS 140-2 3. (2h) Atacuri, vulnerabilităţi, contramăsuri. Tipuri de atacuri hardware (troieni hardware, erori de proiectare, erori ale mediilor şi uneltelor de proiectare), piraterie, inginerie inversă 4. (2h) Atacuri pe canale alternative: putere consumată, lanţuri de scanare, trasare memorii cache 5. (4h) Elemente de criptografie modernă: cifruri pe blocuri de date, standardul AES, curbe eliptice, algoritmii de multiplicare Montgomery şi Karatsuba, funcţii hash. Implementări hardware 6. (2h) Tehnologii pentru implementarea securităţii hardware: Intel Trusted Execution Technology, ARMTrustZone, Texas InstrumentsM-Shield 7. (4h) Specificaţia Trusted Platform Module (TPM) 8. (2h) Sisteme reconfigurabile, reconfigurare parţială, arhitectura TinyTPM 9. (2h) Maşini virtuale: taxonomie hipervizoare, proprietăţi, management resurse	Cursul se predă folosind videoproiectorul şi tabla şi implică discuţii cu studenţii pe marginea subiectelor prezentate.	

[16] *Din planul de învățământ*

[17] *Creditele alocate disciplinei se distribuie pe competențe profesionale și transversale în funcție de specificul disciplinei*

[18] *Titluri de capitole și paragrafe*

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

10. (4h) Suport pentru virtualizare în microprocesoarele moderne: Virtual machine monitor (VMM), SVM (Secure Virtual Machine) Hardware, Virtualization Support, Guest Mode, External Access Protection, Interrupt Support, Restartable Instructions, Nested Paging 11. (2h) Tehnologii complementare pentru asigurarea integrității sistemelor de calcul: Secure Memory Encryption (SME), Machine Check Architecture (MCA)		
Bibliografie curs: Bhunia, Swarup. Hardware Security: A Hands-on Learning Approach. 1st edition. Cambridge, MA: Elsevier, 2018 Debdeep Mukhopadhyay, Rajat Subhra Chakraborty Hardware Security: Design, Threats, and Safeguards 1st Edition, Chapman and Hall/CR, 2014 Jim Smith, Ravi Nair Virtual Machines: Versatile Platforms for Systems and Processes, Morgan Kaufmann, 2005		
8.2a Seminar	Metode de predare[20]	Observații
8.2b Laborator	Metode de predare[21]	Observații
1. (4h) Proiectarea hardware a AES; optimizarea algoritmică și a implementării AES pe o platformă FPGA 2. (6h) Proiectarea unei arhitecturi Trusted Platform Module (TPM) pe un sistem cu microcontroler 3. (4h) Emularea RISC-V ISA folosind QEMU pe sisteme native x86		
8.2c Proiect	Metode de predare[22]	Observații
Bibliografie aplicații (seminar / laborator / proiect): Bhunia, Swarup. Hardware Security: A Hands-on Learning Approach. 1st edition. Cambridge, MA: Elsevier, 2018 Debdeep Mukhopadhyay, Rajat Subhra Chakraborty Hardware Security: Design, Threats, and Safeguards 1st Edition, Chapman and Hall/CR, 2014 Jim Smith, Ravi Nair Virtual Machines: Versatile Platforms for Systems and Processes, Morgan Kaufmann, 2005		

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului[23]

●

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare		10.3 Pondere din nota finală
10.4a Examen / Colocviu	● Cunoștințe teoretice și practice însușite (cantitatea, corectitudinea, acuratețea)	Teste pe parcurs[24]:	%	50 % (minim 5)
		Teme de casă:	50 %	
		Alte activități[25]:	%	
		Evaluare finală:	50 % (minim 5)	
10.4b Seminar	● Frecvența/relevanța intervențiilor sau răspunsurilor	Evidența intervențiilor, portofoliu de lucrări (referate, sinteze științifice)		% (minim 5)
10.4c Laborator	● Cunoașterea aparaturii, a modului de utilizare a instrumentelor specifice; evaluarea unor instrumente sau realizări, prelucrarea și interpretarea unor rezultate	● Răspuns oral ● Demonstrație practică		50 % (minim 5)
10.4d Proiect	● Calitatea proiectului realizat, corectitudinea documentației proiectului, justificarea soluțiilor alese	● Autoevaluarea, prezentarea și/sau susținerea proiectului ● Evaluarea critică a unui proiect		% (minim 5)
10.5 Standard minim de performanță[26] ● Cunoașterea tipurilor de vulnerabilităţi, atacuri și contramăsuri hardware				

[20] *Discuții, dezbateri, prezentare și/sau analiză de lucrări, rezolvare de exerciții și probleme*
[21] *Demonstrație practică, exercițiu, experiment*
[22] *Studiu de caz, demonstrație, exercițiu, analiza erorilor etc.*
[23] *Legătura cu alte discipline, utilitatea disciplinei pe piața muncii*
[24] *Se va preciza numărul de teste și săptămânile în care vor fi susținute.*
[25] *Cercuri științifice, concursuri profesionale etc.*
[26] *Se particularizează la specificul disciplinei standardul minim de performanță din grila de competențe a programului de studii, dacă este cazul.*

● Implementarea de soluţii hardware pentru creşterea securităţii

Data completării,
13.01.2021

Semnătura titularului de curs,
Conf. dr. ing. Andrei Stan

Semnătura titularului de aplicații,
Conf. dr. ing. Andrei Stan

Data avizării în departament,

13.01.2021

Director departament,

Conf.dr.ing. Andrei Stan