R40 Anexa 1

FIŞA DISCIPLINEI
(masterat)

1. **Date despre program**

Instituţia de învăţământ superior	**Universitatea Ştefan cel Mare Suceava**
Facultatea	**Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor**
Departamentul	**Departamentul de Calculatoare Electronică şi Automatică**
Domeniul de studii	**Inginerie electronică şi telecomunicaţii**
Ciclul de studii	**Master**
Programul de studii	**Rețele de comunicații și calculatoare (RCC)**

2. **Date despre disciplină**

Denumirea disciplinei	CRIPTOGRAFIE ȘI SECURITATE CIBERNETICĂ					
Titularul activităţilor de curs	S.l..dr.ing. Doru Balan					
Titularul activităţilor aplicative	S.l..dr.ing. Doru Balan					
Anul de studiu	I	Semestrul	2	Tipul de evaluare	E	
Regimul disciplinei	Categoria formativă a disciplinei DSI – Discipline de sinteză; DAP – Discipline de aprofundare					DAP
	Categoria de opţionalitate a disciplinei: DI - impusă, DO - opţională, DF - facultativă					DI

3. **Timpul total estimat** (ore alocate activităţilor didactice)

I a) Număr de ore, pe săptămână	3	Curs	1	Seminar		Laborator	2	Proiect	
I b) Totalul de ore (pe semestru) din planul de învăţământ	42	Curs	14	Seminar		Laborator	28	Proiect	

II. Distribuţia fondului de timp pe semestru	ore
II.a) Studiul după manual, suport de curs, bibliografie şi notiţe	20
II.b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	32
II.b) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	28
II.d) Tutoriat	
III. Examinări	3
IV. Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	80
Total ore pe semestru (Ib+II+III+IV)	125
Numărul de credite	5

1. **Precondiţii** (acolo unde este cazul)

Curriculum	•
Competenţe	•

2. **Condiţii** (acolo unde este cazul)

Desfăşurare a cursului		• PC, videoproiector (prezentări PPT, software specializat)
Desfăşurare aplicaţii	Seminar	•
	Laborator	• PC, videoproiector, software specializat, suporturi electronice pentru aplicații, prezentări PPT, materiale pentru aplicații, referate, stații de lucru studenți etc..
	Proiect	•

3. **Competenţe specifice acumulate**

Competenţe profesionale	• C2. Utilizarea și administrarea sistemelor și rețelelor de comunicații și calculatoare • C3. Analiza, modelarea și rezolvarea problemelor real complexe, ce implică soluții specifice rețelelor de comunicații și calculatoare • Conceperea, proiectarea, implementarea și exploatarea rețelelor de comunicații și calculatoare și a bazelor de date

Competențe transversale	• CT1. Executarea unor sarcini profesionale complexe, în condiții de autonomie și independență Profesională, individual sau în grup

4. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	• •Înțelegerea rolului algoritmilor criptografici în procesul de securizare informațională a sistemelor și rețelelor de comunicații
	• Dezvoltarea abilităților de evaluare și asigurare a securității cibernetice

5. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
• Concepte fundamentale de securitate criptografică.	2	expunerea, prelegerea, dezbaterea	
• Sisteme criptografice utilizate pentru securizarea sistemelor și rețelelor de comunicații	2		
• Algoritmi criptografici de validare a autenticității. Protocoale criptografice de autentificare. Semnături digitale	2		
• Politici de securitate, analiza riscului, planificarea securității, auditul, certificarea Securitatea aplicațiilor canalelor de comunicații și sistemelor informatice	2		
• Atacuri, politici si mecanisme de securitate. Tipuri de atacuri de rețea. Prevenirea atacurilor la nivelul rețelei.	2		
• Echipamente de securitate informatică. Securizarea la nivel de switch și router. Sisteme firewall IDS/IPS.	2		
• Protocoale și arhitecturi de sisteme de monitorizare și avertizare	2		

Bibliografie

- Adrian Graur, Dimitris Voukalis, Applied Channel Cryptography, Media Mira, 2008
- William Stallings, Cryptography and Network Security: Principles and Practice, 8th Edition, 2022
- Omar Santos,. End-to-End Network Security: Defense-in-Depth. Cisco Press, 2007
- W. Stallings, Lawrie Brown, Computer Security: Principles and Practice. Prentice Hall, 2007
- Atul Kahate Cryptography and Network Security, McGraw Hill; Third edition, 2013
- William Stallings, Network Security Essentials: Applications and Standards, Pearson Education, 2016
- Eric C. Thompson, Cybersecurity Incident Response, Apress, 2018
- Wenbo Mao, Modern Cryptography: Theory and Practice, Prentice Hall PTR, 2003
- Roger A. Grimes, Hacking the Hacker, Wiley, 2017
- Rolf Oppliger, Contemporary Cryptography, Artech House Publishers, 2005
- Sean–Philip Oriyano, Penetration Testing Essentials, Sybex, 2016
- E. Vyncke, Ch. Paggen, LAN Switch Security: What Hackers Know About Your Switches. Cisco Press, 2007
- William Stallings, Effective Cybersecurity, Pearson Education, 2018

Aplicaţii (~~Seminar~~ / laborator / ~~proiect~~)	Nr. ore	Metode de predare	Observaţii
• Resurse pentru asigurarea securității criptografice	2	- activitatea se face la nivel de subgrupă; - expunere pe scurt a noţiunilor teoretice, abordarea temelor de către grupuri de studenţi, aplicaţii demonstrative, probleme rezolvate; - utilizarea materialelor suport în format electronic, accesibile pe web.	
• Analiza unui sistem criptografic simetric	2		
• Analiza unui sistem criptografic asimetric	2		
• Instrumente și mecanisme de securitate.	2		
• Securizarea serviciilor și a transferului de date	2		
• Securitatea comunicațiilor web.	2		
• Controlul accesului in rețea.	2		
• Comunicații wireless securizate.	2		
• Sisteme de detecție a intruziunilor	2		
• Vulnerabilități ale aplicațiilor web. Proiecte OWASP.	2		
• Aplicație web vulnerabilă. Aplicații web sigure.	2		
• Echipamente de infrastructură. Resurse de tip NGFW.	2		
• Vulnerabilități sisteme de operare. Teste de penetrare.	2		
• Identificarea, alertarea și eliminarea vulnerabilităților și amenințărilor de securitate. Auditul de securitate.	2		

Bibliografie
• Atul Kahate, Cryptography and Network Security, McGraw Hill; Third edition, 2013 • William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, 2016 • William Stallings, Lawrie Brown, Computer Security: Principles and Practice. Prentice Hall, 2007 • Roger A. Grimes, Hacking the Hacker, Wiley, 2017 • Sean–Philip Oriyano, Penetration Testing Essentials, Sybex, 2016 • Eric C. Thompson, Cybersecurity Incident Response, Apress, 2018

6. **Coroborarea conținuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului**

• **Conținutul disciplinei se regăsește în curricula disciplinelor similare de la toate facultățile de profil din țară și din străinătate.**

7. **Evaluare**

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Nota acordată participarea activă în timpul cursurilor	Evaluare continuă	*10*
	Nota acordată la examinarea finală	Evaluare prin probă finală scrisă și orală, evaluare de referate de studiu	*40*
Seminar			
Laborator	Media notelor acordate la lucrări practice	Evaluare continuă (prin metode orale, probe practice, sau proiecte)	*50*
Proiect			
Standard minim de performanţă			
• **Identificarea principalelor principii teoretice fundamentale ale criptografiei moderne** • **Înțelegerea rolului algoritmilor de criptare și decriptare specifici diverselor sisteme de securizare informațională.**			

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicaţie
23.09.2022		

Data avizării în departament	Semnătura directorului de departament

Data aprobării în consiliul facultăţii	Semnătura decanului