

FIȘA DISCIPLINEI

(masterat)

1. Date despre program

Instituția de învățământ superior	Universitatea Ștefan cel Mare Suceava
Facultatea	Facultatea de Inginerie Electrică și Știința Calculatoarelor
Departamentul	Departamentul de Calculatoare Electronică și Automatică
Domeniul de studii	Inginerie Electronică, Telecomunicații și Tehnologii Informaționale
Ciclul de studii	Master
Programul de studii	Securitate Cibernetică (SC)

2. Date despre disciplină

Denumirea disciplinei	ATACURI CIBERNETICE ȘI PROTECȚIE CIBERNETICĂ				
Titularul activităților de curs	S.I. dr.ing. Doru Balan				
Titularul activităților aplicative	drd. Edi TIMOFTE				
Anul de studiu	I	Semestrul	2	Tipul de evaluare	E
Regimul disciplinei	Categorია formativă a disciplinei DSI – Discipline de sinteză; DAP – Discipline de aprofundare				DAP
	Categorია de opționalitate a disciplinei: DI - impusă, DO - opțională, DF - facultativă				DI

3. Timpul total estimat (ore alocate activităților didactice)

I a) Număr de ore, pe săptămână	4	Curs	2	Seminar		Laborator	2	Proiect	
I b) Totalul de ore (pe semestru) din planul de învățământ	56	Curs	28	Seminar		Laborator	28	Proiect	

II. Distribuția fondului de timp pe semestru	ore
II.a) Studiul după manual, suport de curs, bibliografie și notițe	20
II.b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren	22
II.b) Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	24
II.d) Tutoriat	
III. Examinări	3
IV. Alte activități (precizați):	

Total ore studiu individual II (a+b+c+d)	66
Total ore pe semestru (Ib+II+III+IV)	125
Numărul de credite	5

1. Precondiții (acolo unde este cazul)

Curriculum	•
Competențe	•

2. Condiții (acolo unde este cazul)

Desfășurare a cursului	• PC, videoproiector (prezentări PPT, software specializat)
Desfășurare aplicații	Laborator • • PC, videoproiector, software specializat, suporturi electronice pentru aplicații, prezentări PPT, materiale pentru aplicații, referate, 14 stații de lucru etc..

3. Competențe specifice acumulate

Competențe profesionale	C4 - Însușirea tehnicilor de operare și utilizare a aparaturii și aplicațiilor profesionale specifice ariei Securității Cibernetice C5 - Identificarea și combaterea riscurilor și pericolelor privind expunerea sistemelor informatice la atacuri cibernetice C6 - Soluționarea incidentelor de securitate folosind instrumente specifice, proiectarea și dezvoltarea de instrumente și aplicații specifice securității cibernetice
Competențe transversale	•

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observații
• Elemente de securizarea rețelei de calculatoare	2	prelegerea, conversația, exemplificarea.	
• Amenințări la securitatea rețelei. Vulnerabilități. și atacuri.	2		
• Controlul securității rețelei. Protocoale și dispozitive	2		
• Politici de securitate. Proiectare și implementare.	2		
• Securitatea datelor și monitorizarea traficului	2		
• Revizuirea securității informațiilor	2		
• Identificarea vulnerabilităților. Riscuri de securitate.	2		
• Verificarea vulnerabilităților. Vectori de atac local.	2		
• Vectori de atac bazat pe principiul ingineriei sociale	2		
• Gestionare atacuri și răspunsul la incidente cibernetice	2		
• Atacuri la nivel de aplicații web și contramăsuri	2		
• Backup și recuperare de date	2		
• Amenințări și contramăsuri pentru securitatea în cloud	2		
• Configurare și gestionare firewall, IDS și VPN securizat	2		
Bibliografie			
<ul style="list-style-type: none"> • M. Walker, CEH Certified Ethical Hacker Practice Exams, Fifth Edition, McGraw Hill, 2022 • Wm Arthur Conklin and G. B. White, CompTIA security+ exam guide, (Exam SY0-601). New York: Mcgraw-Hill Education, 2021. • Y. Ozkaya, CYBERSECURITY - ATTACK AND DEFENSE STRATEGIES - : counter modern threats and employ state-of-the... -art tools and techniques to protect your organiza. S.L.: Packt Publishing Limited, 2019. • M. D. Paul W Browning, 101 Labs - CompTIA Security+. Reality Press Ltd., 2021. 			

6. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- **Conținutul disciplinei se regăsește în curricula disciplinelor similare de la facultăți 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, orală sau evaluare de referate de studiu	40
Laborator	Media notelor acordate la lucrări practice	Evaluare continuă (prin metode orale, probe practice, sau proiecte de studiu)	50
Standard minim de performanță			
<ul style="list-style-type: none"> • Identificarea principalelor tipuri de atacuri și vulnerabilități. • Identificarea principalelor soluții de protecție cibernetică. 			

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicație
18.09.2024		

Data avizării	Semnătura responsabilului de program
20.09.2024	

Data avizării în departament	Semnătura directorului de departament
23.09.2024	

Data aprobării în consiliul facultății	Semnătura decanului
27.09.2024	