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	**Master**
Ciclul de studii	**Inginerie electronică şi telecomunicaţii**
Programul de studii	**Securitate cibernetică (SC)**

2. **Date despre disciplină**

Denumirea disciplinei	ATACURI CIBERNETICE ȘI PROTECȚIE CIBERNETICĂ					
Titularul activităţilor de curs	S.l. dr.ing. Doru Balan					
Titularul activităţilor aplicative	drd. Edi TIMOFTE					
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	4	Curs	2	Seminar		Laborator	2	Proiect	
I b) Totalul de ore (pe semestru) din planul de învăţământ	56	Curs	28	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	22
II.b) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	24
II.d) Tutoriat	
III. Examinări	3
IV. Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	66
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	Laborator	● • PC, videoproiector, software specializat, suporturi electronice pentru aplicaţii, prezentări PPT, materiale pentru aplicaţii, referate, 14 staţii de lucru etc..

3. **Competenţe specifice acumulate**

Competenţe 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
Competenţe transversale	CT3. Cunoaşterea problemelor contemporane şi recunoaşterea nevoii de formare continuă

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

Obiectivul general al disciplinei	● Dobândirea de către cursanți a cunoștințelor și abilităților necesare cunoașterii riscurilor și amenințărilor la care sunt supuse activitățile desfășurate în spațiul cibernetic și oferirea de soluții de prevenire și contracarare a acestora..

5. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
Atacuri cibernetice (12h) ● Noțiuni fundamentale de securitate informatică ● Considerente privind mecanismele de atac informatic ● Amenințări și vulnerabilități ale securității informaționale ● Tehnici de spargere de parolelor și contramăsuri ● Tehnici de inginerie socială și contramăsuri specifice ● Atacuri la nivelul rețelei și contramăsuri specifice ● Atacuri la nivelul aplicațiilor web și contramăsuri ● Atacuri asupra comunicațiilor fără fir și contramăsuri ● Atacuri asupra resurselor de comunicație mobile și măsuri de combatere. ● Atacuri asupra infrastructurilor critice, tehnologiilor operaționale și IoT. Măsuri de combatere și protecție ● Amenințări și contramăsuri pentru securitatea în cloud ● Fundamentele testelor de penetrare	1 1 1 1 1 1 1 1 1 1 1 1	prelegerea, conversația, exemplificarea.	
Protecție cibernetică (12h) ● Componente specifice securității rețelelor ● Concepte de securitate: Identificare, autentificare și autorizare ● Securitatea rețelei la nivel administrativ ● Securitatea rețelei la nivel fizic ● Tehnologii de securizare a rețelelor ● Securitatea mecanismelor de virtualizare și cloud ● Securitatea rețelei wireless ● Securitatea dispozitivelor mobile ● Securitate dispozitivelor IoT ● Tehnici, algoritmi și instrumente criptografice actuale folosite în securizarea rețelelor ● Securitatea datelor ● Monitorizarea traficului în rețea	1 1 1 1 1 1 1 1 1 1 1 1 1		
Elemente de investigație informatică (4h) ● Noțiuni de investigație criminalistică digitală ● Identificarea și preluarea datelor ● Investigații la nivel de sistem de operare și în rețea ● Investigarea atacurilor web, email și malware	1 1 1 1		

Bibliografie

● M. Chapple, Isc2 Cissp Certified Information Systems Security Professional Official Study Guide + Practice... Tests Bundle. S.L.: Wiley-Sybex, 2021

● M. Chapple, COMPTIA SECURITY+ CERTIFICATION KIT : exam sy0-601. S.L.: Wiley-Sybex, 2021.

● M. Walker, CEH Certified Ethical Hacker Practice Exams, Fifth Edition, McGraw Hill, 2022

● Wm Arthur Conklin, G. White, Cothren Cothren, L Roger Davis, and D. Williams, CompTIA Security+ All-in-One Exam Guide, Sixth Edition (Exam SY0-601) /. New York, N.Y.: Mcgraw-Hill Education, 2021.

● W. Stallings, CRYPTOGRAPHY AND NETWORK SECURITY : principles and practice, global edition. S.L.: Pearson Education Limited, 2022.

- 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.
- G. D. Singh, The ultimate Kali Linux book : perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire. Birmingham: Packt Publishing, 2022

Aplicaţii (~~Seminar~~ / laborator / ~~proiect~~)	Nr. ore	Metode de predare	Observaţii
● 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 si contramăsuri pentru securitatea în cloud	2		
● Configurare și gestionare firewall, IDS și VPN securizat	2		

Bibliografie

- 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 conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului**

- **Conţinutul disciplinei se regăseşte 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

- Identificarea principalelor tipuri de atacuri și vulnerabilități.
- Identificarea principalelor soluții de protecție cibernetică.

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicaţie
23.09.2022		

Data avizării în departament	Semnătura directorului de departament
26.09.2022	

Data aprobării în consiliul facultăţii	Semnătura decanului
30.09.2022	