

## 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

### 2. Date despre disciplină

Denumirea disciplinei	PRACTICĂ PROFESIONALĂ 2				
Titularul activităților de curs					
Titularul activităților aplicative	S.I. dr.ing. BALAN Doru				
Anul de studiu	1	Semestrul	2	Tipul de evaluare	C
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		Curs		Seminar		Laborator		Proiect	
I b) Totalul de ore (pe semestru) din planul de învățământ		Curs		Seminar		Laborator		Proiect	

II. Distribuția fondului de timp pe semestru	ore
II.a) Studiul după manual, suport de curs, bibliografie și notițe	
II.b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren	
II.b) Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	6
II.d) Tutoriat	1
III. Examinări	3
IV. Alte activități (precizați): Activități parțial asistate (conform planului de învățământ, 10 ore pe săpt.)	140

Total ore studiu individual II (a+b+c+d)	7
Total ore pe semestru (Ib+II+III+IV)	150
Numărul de credite	6

### 1. Precondiții (acolo unde este cazul)

Curriculum	•
Competențe	•

### 2. Condiții (acolo unde este cazul)

Desfășurare a cursului	•	
Desfășurare aplicații	Seminar	•
	Laborator	•
	Proiect	•
	Activități parțial asistate	• Studentii pot face practica atât pe cont propriu, cât și prin intermediul facultății, în limita locurilor oferite acesteia de diverse organizații, cu condiția realizării celor 140 de ore prevăzute în planul de învățământ.

### 3. Competențe specifice acumulate

Competențe 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 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	CT1. Executarea unor sarcini profesionale complexe, în condiții de autonomie și independență profesională individual sau în grup CT2. Managementul proiectelor complexe și utilizarea a diverse moduri de comunicare scrisă și orală

#### 4. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

Obiectivul general al disciplinei	Pregătirea de specialiști pentru integrarea rapidă pe piața muncii. Disciplina are o componentă orientată preponderent spre formarea și aprofundarea competențelor profesionale (ingineresti) în domeniul securității cibernetice.
	•

#### 5. Conținuturi

Curs	Nr. ore	Metode de predare	Observații
•			
•			
•			
Bibliografie			
•			

Aplicații (Seminar / laborator / proiect/activități parțial asistate)	Nr. ore	Metode de predare	Observații
<ul style="list-style-type: none"> <li>Efectuarea de teste de penetrare, atunci când sunt simulate diverse tipuri de atacuri pentru a căuta vulnerabilități și pentru a putea fi exploatare.</li> <li>Cercetarea celor mai recente tendințe de securitate a tehnologiei informației (IT)</li> <li>Dezvoltarea de standarde de securitate și a celor mai bune practici pentru organizația lor.</li> <li>Recomandarea de îmbunătățiri de securitate personalului de conducere sau personalului informatic superior.</li> <li>Instruirea utilizatorilor de computere atunci când au nevoie să instaleze sau să afle despre noi produse și proceduri de securitate.</li> <li>Instruirea cu privire la securitatea IT și cu cele mai recente metode pe care atacatorii le utilizează pentru a se infiltra în sistemele informatice.</li> <li>Cercetarea noilor tehnologii de securitate pentru a decide ce le va proteja cel mai eficient organizația.</li> <li>Crearea de planuri de recuperare și de restabilire a funcționării corecte în caz de dezastru al organizației lor, în ceea ce privește securitatea cibernetice, o procedură pe care ceilalți angajații o urmează în caz de urgență.</li> <li>Dezvoltarea abilităților tehnice de bază dar și specializate putându-se integra fără dificultate în contextul de afaceri, politic și juridic al securității cibernetice.</li> </ul>	Durata practicii este de 140 ore / activități parțial asistate [14 săptămâni x 10 ore/săpt.] și se desfășoară pe parcursul anului I de studii, sem 2.	Învățare prin probleme și aplicații practice; lucrul în grup într-o entitate economică; lucrul individual; observație și acțiune.	<ul style="list-style-type: none"> <li>- Studenții vor efectua stagiul de practică pe cont propriu. Organizația la care va face practica va fi aleasă de fiecare student în parte, potrivit indicațiilor primite de la responsabilii de practică, posibilităților sale de a efectua practica, specificului specializării și preferințelor sale pentru un anumit tip de activitate</li> <li>- Documentele care trebuie întocmite de către student: <ul style="list-style-type: none"> <li>• un portofoliu de practică - în care va consemna activitatea zilnică, în conformitate cu problematica indicată;</li> </ul> </li> </ul>
Bibliografie			
<ul style="list-style-type: none"> <li>• Documentele organizației</li> <li>• Legislația aplicabilă în vigoare la data efectuării practicii (legi, regulamente, norme de aplicare)</li> <li>• Bibliografia recomandată la disciplinele parcurse în sem. 1.</li> </ul>			

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

• Pregătirea viitorilor specialiști în domeniul securității cibernetice în concordanță cu normele în vigoare.
---

#### 7. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs			
Seminar			

Laborator			
Proiect			
Activități parțial asistate	- capacitatea de aplicare în practică, în contexte diferite, a cunoștințelor învățate; - capacitatea de analiză, de interpretare personală, originalitatea, creativitatea.	Evaluare orală	50% Prezentare activități realizate în timpul practicii 50% Portofoliul de practică
Standard minim de performanță			
<ul style="list-style-type: none"> <li>Studentul trebuie să fie capabil să facă o autoevaluare pertinentă, în scris (în cadrul portofoliului de practică) și oral (la colocviul de practică), a propriilor activități și să demonstreze capacitate de sistematizare și argumentare a propriilor opinii formate în stagiul de practică</li> </ul>			

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicație
23.09.2022		

Data avizării în departament	Semnătura directorului de departament
26.09.2022	

Data aprobării în consiliul facultății	Semnătura decanului
30.09.2022	