FIȘA DISCIPLINEI

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	**Calculatoare și tehnologia informației**
Ciclul de studii	**Master**
Programul de studii	**Știința și Ingineria Calculatoarelor (SIC)**

2. **Date despre disciplină**

Denumirea disciplinei	**SECURITATE AVANSATĂ A SISTEMELOR INFORMATICE**					
Anul de studiu	II	Semestrul	3	Tipul de evaluare	E	
Regimul disciplinei	Categoria formativă a disciplinei DF - fundamentală, DS - de specializare, DC – complementară					DS
	Categoria de opționalitate a disciplinei: DOB – obligatorie, DOP – opțională, DFA - facultativă					DOP

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

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

Distribuția fondului de timp pe semestru	ore
II. Studiu individual	97
III. Examinări	3
IV. Alte activități (precizați):	

Total ore studiu individual (II+III)	97
Total ore pe semestru (I.b+II+III+IV)	125
Numărul de credite	5

4. **Competențe specifice acumulate**

Competențe transversale	
Competențe profesionale	CP1 - efectuează cercetare științifică CP6 - aplica politici de securitate informatica CP8 - dezvolta aplicații de procesare de date

5. **Rezultatele învățării**

Cunoștințe	Aptitudini	Responsabilitate și autonomie
Studentul/absolventul descrie, identifică, sumarizează concepte și metode avansate privitoare la baze de date, modele și paradigme moderne de inginerie software , calculul cuantic și cunoaște rigorile științifice pentru elaborarea unei lucrări de cercetare, respectând normele etice.	Studentul / absolventul proiectează arhitecturi avansate de sisteme informatice utilizând mecanisme performanțe de securitate informatică.	Studentul / absolventul poate derula managementul proiectelor complexe cu preluarea diverselor roluri în echipă, asumându-și gestionarea și transformarea situațiilor de muncă complexe și imprevizibile prin noi abordări strategice adecvate.

6. **Obiectivele disciplinei** (reieșind din grila competențelor specifice acumulate)

Obiectivul general al disciplinei	● Identificarea și punerea în practică a unor soluții eficiente de securizare a sistemelor informatice
	● Însușirea tehnicilor de evaluare a nivelului de securitate a sistemelor informatice

7. **Conținutul predării și învățării**

Curs	Nr. ore	Metode de predare	Observații
● •Concepte fundamentale de criptografie și securitate a sistemelor informatice.	2	expunerea, prelegerea, dezbaterea	
● Sisteme criptografice utilizate pentru securizarea sistemelor informatice și rețelelor de comunicații	2		
● •Integritatea datelor. Gestiunea cheilor de securitate	2		
● •Autentificarea utilizatorilor. Controlul accesului în rețea.	2		
● •Securitatea comunicațiilor web. Securitatea rețelelor fără fir.	2		
● •Securitatea serviciilor de rețea. Securitatea IP.	2		
● •Incidente de securitate cibernetică. Evaluarea securității.	2		

Bibliografie minimală recomandată

[1] A. Graur and D. Voukalis, *Applied Channel Cryptography*. Media Mira, 2008.
[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Global Ed. Pearson Higher Ed, 2022.
[3] O. Santos, *End-to-End Network Security: Defense-in-Depth*. Cisco Press, 2007.
[4] W. Stallings and L. Brown, *Computer Security: Principles and Practice*. Prentice Hall, 2007.
[5] A. Kahate, *Cryptography and Network Security*, 3rd ed. McGraw Hill, 2013.
[6] W. Stallings, *Network Security Essentials: Applications and Standards*. Pearson Education, 2016.
[7] E. C. Thompson, *Cybersecurity Incident Response*. Apress, 2018.
[8] W. Mao, *Modern Cryptography: Theory and Practice*. Prentice Hall PTR, 2003.
[9] R. A. Grimes, *Hacking the Hacker*. Wiley, 2017.
[10] R. Oppliger, *Contemporary Cryptography*. Artech House Publishers, 2005.
[11] S.-P. Oriyano, *Penetration Testing Essentials*. Sybex, 2016.
[12] E. Vyncke and C. Paggen, *LAN Switch Security: What Hackers Know About Your Switches*. Cisco Press, 2007.
[13] W. Stallings, *Effective Cybersecurity*. Pearson Education, 2018.
[14] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed. John Wiley & Sons, 2020.
[15] J. R. Vacca, *Cloud Computing Security: Foundations and Challenges*, 2nd ed. CRC Press, 2021.

Aplicații (~~Seminar~~ / laborator / ~~proiect~~)	Nr. ore	Metode de predare	Observații
● Resurse pentru asigurarea securității sistemelor informatice	2	- activitatea se face la nivel de semi-grupă; - expunere pe scurt a noțiunilor teoretice, abordarea temelor de către grupuri de studenți, aplicații demonstrative, probleme rezolvate; - utilizarea materialelor suport în format electronic, accesibile pe web.	
● Analiza unui sistem criptografic	2		
● Instrumente și mecanisme de securitate.	2		
● Tehnici/ Tactici/ Abilități de securizare pentru combaterea unui atac informatic.	2		
● Vulnerabilitățile sistemelor informatice. Teste de penetrare. Auditul de securitate. Poligon de securitate cibernetică.	2		
● Securizarea serviciilor și a transferului de date	2		
● Echipamente de infrastructură de rețea. Protecția integrată – terminal, server, gateway, cloud - prin resurse de tip NGFW	2		

Bibliografie minimală recomandată

[1] A. Kahate, *Cryptography and Network Security*, 3rd ed. McGraw Hill, 2013.
[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Global Ed. Pearson Higher Ed, 2022.
[3] W. Stallings and L. Brown, *Computer Security: Principles and Practice*. Prentice Hall, 2007.
[4] R. A. Grimes, *Hacking the Hacker*. Wiley, 2017.
[5] S.-P. Oriyano, *Penetration Testing Essentials*. Sybex, 2016.
[6] E. C. Thompson, *Cybersecurity Incident Response*. Apress, 2018.
[7] M. Sikorski and A. Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press, 2012..
[8] P. Kim, *The Hacker Playbook 3: Practical Guide to Penetration Testing*. Secure Planet LLC, 2018*)*.
[9] D. Stuttard and M. Pinto, *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*, 2nd ed. John Wiley & Sons, 2011..
[10] C. Sanders, *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*, 3rd ed. No Starch Press, 2017.

8. **Evaluare**

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Evaluare finală	Înțelegerea conceptelor avansate de criptografie și securitate - Studentul descrie concepte fundamentale și avansate de criptografie, explică rolul acestora în securizarea sistemelor informatice și a rețelelor. (CP6, CT6) Analiza mecanismelor de protecție a datelor și autentificare - Studentul identifică metode de protejare a integrității datelor, explică gestiunea cheilor de securitate și mecanismele de autentificare și control al accesului. (CP6, CP8) Evaluarea securității comunicațiilor și serviciilor de rețea - Studentul analizează riscurile și măsurile de protecție pentru comunicații web, rețele wireless, servicii IP și infrastructuri de rețea. (CP6, CT6) Investigarea incidentelor și aplicarea standardelor de evaluare - Studentul identifică tipuri de incidente de securitate cibernetică și aplică standarde pentru evaluarea nivelului de securitate al sistemelor. (CP6, CP1)	Evaluare prin probă finală scrisă, orală sau evaluare de referate de studiu	50
Evaluare finală	Aplicarea resurselor și instrumentelor de securitate - Studentul utilizează resurse și instrumente specifice pentru asigurarea securității sistemelor informatice. (CP6, CP8) Analiza și testarea sistemelor criptografice - Studentul analizează funcționarea unui sistem criptografic și aplică teste de penetrare pentru identificarea vulnerabilităților. (CP6, CP1) Implementarea mecanismelor de protecție în rețele și servicii - Studentul securizează serviciile și transferul de date, configurând infrastructura de rețea cu protecție integrată (terminal, server, gateway, cloud). (CP5, CP6) Gestionarea incidentelor și auditul de securitate - Studentul identifică, alertează și elimină amenințările, derulează auditul de securitate și propune măsuri de remediere. (CP6, CT6)	Evaluare continuă (prin metode orale, probe practice sau proiecte)	50

Fișa disciplinei include, dacă este cazul, elemente adaptate persoanelor cu dizabilități, în funcție de tipul și gradul acestora.

Data completării	Grad didactic, nume, prenume, semnătura titularului de curs	Grad didactic, nume, prenume, semnătura titularului de aplicație
18.09.2026	S.l..dr.ing. Doru Balan	S.l..dr.ing. Doru Balan

Data avizării	Grad didactic, nume, prenume, semnătura responsabilului de program
24.09.2026	prof. dr. ing. Stefan-Gheorghe PENTIUC

Data avizării în departament	Grad didactic, nume, prenume, semnătura directorului de departament
24.09.2026	Prof. dr. ing. Ovidiu-Andrei SCHIPOR

Data aprobării în consiliul facultății	Grad didactic, nume, prenume, semnătura decanului
25.09.2026	Prof. dr. ing. Laurențiu- Dan MILICI