

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 și telecomunicații
Ciclul de studii	Master
Programul de studii	Securitate cibernetică (SC)

2. Date despre disciplină

Denumirea disciplinei	Securitatea criptografică a sistemelor și a rețelelor de comunicații				
Titularul activităților de curs	S.l.dr.ing. Doru Balan				
Titularul activităților aplicative	S.l.dr.ing. Doru Balan				
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	3	Curs	1	Seminar		Laborator	1	Proiect	1
I b) Totalul de ore (pe semestru) din planul de învățământ	42	Curs	14	Seminar		Laborator	14	Proiect	14

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	32
II.b) Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	28
II.d) Tutoriat	
III. Examinări	3
IV. Alte activități (precizați):	

Total ore studiu individual II (a+b+c+d)	80
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	Seminar	•
	Laborator	• •PC, videoproiector, software specializat, suporturi electronice pentru aplicații, prezentări PPT, materiale pentru aplicații, referate, 14 stații de lucru etc.
	Proiect	• •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	• C3. Analiza, modelarea și rezolvarea problemelor real complexe, ce implică soluții specifice rețelelor de comunicații și calculatoare
-------------------------	---

	<ul style="list-style-type: none"> ● C4. Înșușirea tehnicilor de operare și utilizare a aparaturii și aplicațiilor profesionale specifice ariei Securității Cibernetice
Competențe transversale	<ul style="list-style-type: none"> ● CT.1 Executarea unor sarcini profesionale complexe, în condiții de autonomie și independență profesională individual sau în grup

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

Obiectivul general al disciplinei	<ul style="list-style-type: none"> ● Înțelegerea rolului algoritmilor criptografici în procesul de securizare informațională a sistemelor și rețelelor de comunicații
	<ul style="list-style-type: none"> ● Dezvoltarea abilităților de evaluare și asigurare a securității cibernetice

5. Conținuturi

Curs	Nr. ore	Metode de predare	Observații
● Concepte fundamentale de securitate criptografică.	2	expunerea, prelegerea, dezbateră	
● 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 și 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			
<ul style="list-style-type: none"> ● 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 			

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observații
● Resurse pentru asigurarea securității criptografice a sistemelor și rețelelor de comunicații	2	- activitatea se face la nivel de subgrupă; - 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 sistemelor criptografice utilizate pentru securizarea sistemelor și rețelelor de comunicații	2		
● Securizarea serviciilor la nivelul sistemelor informatice și a transferului de date în rețea	2		
● Securitatea comunicațiilor la nivelul resurselor web. Serviciu de securitate. Certificate digitale.	2		
● Securitatea sistemelor și rețelelor. Controlul accesului.	2		
● Securizarea rețelelor de comunicație. Resurse de tip NGFW.	2		
● Comunicații wireless securizate	2		
Bibliografie			
<ul style="list-style-type: none"> ● Atul Kahate, Cryptography and Network Security, McGraw Hill; Third edition, 2013 ● William Stallings, Cryptography and Network Security: Principles and Practice, 8th Edition, 2022 ● William Stallings, Lawrie Brown, Computer Security: Principles and Practice. Prentice Hall, 2007 ● Sean-Philip Oriyano, Penetration Testing Essentials, Sybex, 2016 			

● Eric C. Thompson, Cybersecurity Incident Response, Apress, 2018			
Aplicații (Seminar/laborator/proiect)	Nr. ore	Metode de predare	Observații
● Politici și mecanisme de securitate criptografică	2	- activitatea se face la nivel de subgrupă; - 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.	
● Proiectarea unui sistem criptografic pentru securizarea unui sistem sau a unei rețele de comunicații	2		
● Identificare tehnici/ Stabilire tactici/ Dezvoltare abilități de securizare pentru combaterea unui atac informatic	2		
● Identificare vulnerabilități ale aplicațiilor web. Dezvoltare de resurse web sigure. Proiecte OWASP.	2		
● Securitatea sistemelor de operare. Teste de vulnerabilitate..	2		
● Securitatea bazelor de date. Teste de penetrare	2		
● Soluții integrate de securizare a utilizatorilor, datelor și rețelelor de comunicații. Acces. Privilegii. Soluții VPN.	2		
Total		14	

Bibliografie:

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

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 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, orală sau evaluare de referate de studiu	40
Seminar			
Laborator	Media notelor acordate la lucrări practice	Evaluare continuă (prin metode orale, probe practice sau proiecte)	25
Proiect	Media notelor acordate la proiecte de studiu	Evaluare continuă (prin metode orale, probe practice sau proiecte)	25

Standard minim de performanță

- **Identificarea principalelor principii fundamentale de securitate criptografică**
- **Înțelegerea rolului algoritmilor criptografici pentru securizarea sistemelor și rețelelor de comunicații.**

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	

