FIŞA DISCIPLINEI

1. **Date despre program**

Instituţia de învăţământ superior	Universitatea "Ştefan cel Mare" din Suceava
Facultatea	Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor
Departamentul	Departamentul de Calculatoare, Electronică şi Automatică
Domeniul de studii	Inginerie electronică, telecomunicaţii şi tehnologii informaţionale
Ciclul de studii	Master
Programul de studii	Rețele de Comunicații și Calculatoare

2. **Date despre disciplină**

Denumirea disciplinei	**CRIPTOGRAFIE ȘI SECURITATE CIBERNETICĂ**					
Titularul activităților de curs	Ș.l. dr. ing. Doru BALAN					
Titularul activităților aplicative	Ș.l. dr. ing. Doru BALAN					
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: DO - obligatorie (impusă), DA - opţională (la alegere), DL - facultativă (liber aleasă)					DO

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

I a) Număr de ore, pe săptămână	3	Curs	1	Seminar		Laborator	2	Proiect	
I.b) Totalul de ore (pe semestru) din planul de învăţământ	42	Curs	14	Seminar		Laborator	28	Proiect	

II. Distribuţia fondului de timp pe semestru	ore
II.a) Studiul după manual, suport de curs, bibliografie şi notiţe	10
II.b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	9
II.c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	8
II.d) Tutoriat	
III. Examinări	3
IV. Alte activităţi: (pregatire examen și teste)	56

Total ore studiu individual II (a+b+c+d)	27
Total ore pe semestru (I+II+III+IV)	128
Numărul de credite	5

4. **Precondiţii** (acolo unde este cazul)

Curriculum	
Competenţe	

5. **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, etc.

6. **Competenţe specifice acumulate**

Competenţe profesionale	C1. Operarea cu concepte şi metode ştiinţifice în tehnologia informației şi a comunicaţiilor C3. Analiza, modelarea şi rezolvarea problemelor real complexe, ce implică soluţii specifice reţelelor de comunicaţii şi calculatoare
Competenţe transversale	CT.3. Cunoaşterea problemelor contemporane şi recunoaşterea nevoii de formare continuă

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

Obiectivul general al disciplinei	• Însușirea principiilor teoretice fundamentale ale criptografiei moderne
	• Înţelegerea algoritmilor de criptare și decriptare specifici diverselor sisteme de securizare informațională.
	• Dezvoltarea abilităților de proiectare a unor tehnici de comunicaţie sigure.
Obiective specifice	• Înţelegerea criptografiei ca o necesitate în domenii diverse ale societății moderne: IT, economic (îndeosebi comercial), militar etc.
	• Prezentarea diferitelor modalităţi folosite pentru criptarea şi codificarea mesajelor de-a lungul istoriei;
	• Prezentarea matematică a algoritmilor de criptare şi, acolo unde este cazul, demonstrarea principiilor ce le utilizează.
	• Dezvoltarea abilităților privind criptarea şi decriptarea mesajelor;
	• Identificarea modalităţilor de criptare a datelor în funcţie de domeniul de utilizare;
	• Verificarea corectitudinii mesajelor criptate și interpretarea rezultatelor obținute;
	• Capacitatea de dezvoltare a aplicațiilor complexe din domeniul criptografiei sub forma unui proiect.
	• Manifestarea interesului faţă de ideea de rezolvare a problemelor din domeniul criptografiei şi criptologiei;
	• Dezvoltarea capacității de lucru în echipă;

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
• Noțiuni fundamentale de criptografie.	2	expunerea, prelegerea, dezbaterea	
• Sisteme criptografice simetrice, asimetrice și cu cheie publică	2		
• Algoritmi criptografici de validare a datelor. 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 si 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		
Total	14		

Bibliografie:

1. Adrian Graur, Dimitris Voukalis, Applied Channel Cryptography, Media Mira, 2008
2. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, 2016
3. Omar Santos,. End-to-End Network Security: Defense-in-Depth. Cisco Press, 2007
4. W. Stallings, Lawrie Brown, Computer Security: Principles and Practice. Prentice Hall, 2007
5. Atul Kahate Cryptography and Network Security, McGraw Hill; Third edition, 2013
6. William Stallings, Network Security Essentials: Applications and Standards, Pearson Education, 2016
7. Eric C. Thompson, Cybersecurity Incident Response, Apress, 2018
8. Wenbo Mao, Modern Cryptography: Theory and Practice, Prentice Hall PTR, 2003
9. Roger A. Grimes, Hacking the Hacker, Wiley, 2017
10. Rolf Oppliger, Contemporary Cryptography, Artech House Publishers, 2005
11. Sean–Philip Oriyano, Penetration Testing Essentials, Sybex, 2016
12. E. Vyncke, Ch. Paggen, LAN Switch Security: What Hackers Know About Your Switches. Cisco Press, 2007
13. William Stallings, Effective Cybersecurity, Pearson Education, 2018

Laborator	Nr. ore	Metode de predare	Observaţii
• Analiza unui sistem criptografic simetric	2	- activitatea se face la nivel de semi-grupă; - expunere pe scurt a noţiunilor teoretice, abordarea temelor de către grupuri de studenţi, aplicaţii demonstrative, probleme rezolvate; - utilizarea materialelor suport în format electronic, accesibile pe web.	
• Analiza unui sistem criptografic asimetric	2		
• Metode securizate de autentificare a utilizatorilor	2		
• Securitatea comunicațiilor. Auditul de securitate.	2		
• Securizarea serviciilor şi a transferului de date	2		
• Atacuri, politici si mecanisme de securitate	2		
• Vulnerabilități ale aplicațiilor web	2		
• Securitatea sistemelor de operare. Teste de vulnerabilitate..	2		
• Securitatea bazelor de date. Teste de penetrare	2		
• Securitatea rețelelor. Soluții VPN.	2		
• Securitatea utilizatorilor. Acces. Privilegii.	2		
• Securizarea echipamentelor de infrastructură de rețea	2		
• Comunicații wireless securizate	2		
• Concluzii, analiza rezultatelor	2		
Total	28		

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

9. **Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului**

Conținutul disciplinei se regăsește în curricula disciplinelor similare de la toate facultățile de profil din țară și din străinătate.

10. **Evaluare**

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Înțelegerea rolului algoritmilor de criptare și decriptare specifici diverselor sisteme de securizare informațională	Evaluare continuă	*10*
	Nota acordată la examinarea finală	Evaluare prin probă finală scrisă și orală, evaluare de referate de studiu	*50*
Laborator	Gradul de realizare a lucrărilor practice	Evaluare continuă (prin metode orale, probe practice, proiecte)	*40*
Standard minim de performanţă			
•Identificarea principalelor principii teoretice fundamentale ale criptografiei moderne •Înțelegerea rolului algoritmilor de criptare și decriptare specifici diverselor sisteme de securizare informațională.			

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicaţie
21.09.2020		

Data avizării în departament	Semnătura directorului de departament
25.09.2020	

Data aprobării în consiliul facultăţii	Semnătura decanului
01.10.2020	