FIŞA DISCIPLINEI
(doctorat)

Valabilă începând cu 2024/2025

1. **Date despre program**

Instituţia de învăţământ superior	Universitatea "Ştefan cel Mare" din Suceava
Şcoala doctorală	Ştiinţe Aplicate şi Inginereşti
Domeniul de studii de doctorat	Inginerie electronică, telecomunicaţii şi tehnologii informaţionale
Ciclul de studii	Doctorat
Programul de studii	Program de pregătire bazat pe studii universitare avansate

2. **Date despre disciplină**

Denumirea disciplinei	**SECURITATE CIBERNETICĂ**					
Titularul activităţilor de curs	Şef de lucrări univ. dr. ing. Doru BALAN					
Titularul activităţilor aplicative	Şef de lucrări univ. dr. ing. Doru BALAN					
Anul de studiu	I	Semestrul	I	Tipul de evaluare	Colocviu	
Regimul disciplinei	Categoria formativă a disciplinei DAP – disciplină de aprofundare; DPA – disciplină de pregătire avansată; DSI – discipline de sinteză					DPA
	Categoria de opţionalitate a disciplinei: DI - impusă, DO - opţională, DF - facultativă					DO

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

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

II Distribuţia fondului de timp pe semestru:	ore
II a)Studiul după manual, suport de curs, bibliografie şi notiţe	62
II b)Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	88
II c)Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	56
II d)Tutoriat	
III Examinări	2
IV Alte activităţi:	

Total ore studiu individual II (a+b+c+d)	206
Total ore pe semestru (I+II+III+IV)	250
Numărul de credite	10

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

Curriculum	• Studii de licenţă
Competenţe	• Masterat în inginerie

5. **Condiţii** (acolo unde este cazul)

Desfăşurare a cursului		• calculator portabil, videoproiector, note de curs în format editat, prezentări animaţii specifice
Desfăşurare aplicaţii	Seminar	• nu este cazul
	Laborator / Lucrări practice	• îndrumar de laborator, referate de laborator în format editat şi în format electronic, standuri experimentale, desktopuri - 10 buc. Software specializat
	Proiect	• nu este cazul

6. **Competenţe specifice acumulate**

Competenţe profesionale	-Capacitatea de identificare, formulare şi soluţionare într-o manieră creativă a problemelor de cercetare; -Abilităţi de documentare şi valorificare a lucrărilor ştiinţifice; -Capacitatea de a redacta lucrări ştiinţifice şi alte materiale academice la un nivel avansat, într-un stil adecvat domeniului de studiu şi cu respectarea rigorilor specifice acestuia la nivel naţional şi internaţional.

Competențe transversale	-Abilități de interrelaționare și de lucru în echipă; -Cunoștințe privind gândirea critică, inclusiv aptitudinea de a analiza, interpreta sau formula raționamente în diferite contexte.

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

Obiectivul general al disciplinei	Identificarea soluțiilor de securizare informațională și gestiunea resurselor specifice securității cibernetice. Vor fi identificate elementele de bază ale securității cibernetice pentru a proteja resursele digitale, folosind informații despre cele mai mari provocări de securitate cu care se confruntă comunicațiile de date în prezent. Formarea profesională în securitate cibernetică pentru a putea utiliza și dezvolta soluții de protejare și apărare a rețelelor de comunicații de date.

8. **Conținuturi**

CURS	Nr. ore	Metode de predare	Observații
1. Elemente de securitate cibernetică. Atacuri, vulnerabilități, concepte, tehnici. 2. Securizarea sistemelor informatice. Securitatea rețea. Comunicații wireless sigure. 3. Infrastructură de securitate în rețea 4. Securitizarea sistemelor de operate 5. Mecanisme de securitate la nivel de sistem și în rețea. Securitatea cloud. 6. Controlul accesului 7. Tehnologii firewall 8. Tehnologii și protocoale. Criptografie. 9. Prelucrare de informații pentru securizarea rețelei 10. Cadre de securitate informațională. Gestiune și conformitate. 11. Testarea securității în rețea 12. Evaluarea vulnerabilităților 13. Gestiunea riscurilor de securitate. Controale de securitate. 14. Investigații digitale și răspunsul la incidente cibernetice.	28	expunerea, prelegerea-dezbatere, demonstrația	

Bibliografie

1. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.
2. J. R. Vacca, Computer and Information Security Handbook, 3rd ed., Morgan Kaufmann, 2017.
3. S. Kumar and N. Tripathi, "Cybersecurity Threats and Countermeasures in the Industry 4.0 Era," IEEE Access, vol. 8, pp. 57460–57488, 2020, doi: 10.1109/ACCESS.2020.2982299.
4. NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, Version 1.1, Apr. 16, 2018. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.04162018.
5. ISO/IEC 27001:2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements, ISO, Geneva, Switzerland, 2013.
6. A. K. Sood and R. J. Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," IEEE Security & Privacy, vol. 11, no. 1, pp. 54–61, 2013, doi: 10.1109/MSP.2013.8.
7. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 20th ed., Wiley, 2015.
8. L. K. Gallon et al., "Machine Learning for Cybersecurity: A Comprehensive Survey," *IEEE Access*, vol. 8, pp. 181213–181239, 2020, doi: 10.1109/ACCESS.2020.3018026.
9. J. M. Hu, M. R. Refaei and A. Rayes, "Cybersecurity in 5G Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1454–1494, 2021, doi: 10.1109/COMST.2021.3062231.
10. Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," *IEEE Cloud Computing*, vol. 7, no. 2, pp. 43–56, 2020, doi: 10.1109/MCC.2020.2976543.
11. D. Kim and M. G. Solomon, Fundamentals of Information Systems Security, 4th ed. Burlington, MA, USA: Jones & Bartlett Learning, 2020.
12. P. W. Singer and A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know. New York, NY, USA: Oxford Univ. Press, 2021.
13. S. Harris, CISSP All-in-One Exam Guide, 9th ed. New York, NY, USA: McGraw-Hill Education, 2021.
14. R. Von Solms and J. Van Niekerk, Cybersecurity and Cyber Warfare: Concepts, Methodologies, Tools, and Applications, 2nd ed. Hershey, PA, USA: IGI Global, 2020.
15. J. L. Bayuk, Ed., Cybersecurity Policy Guidebook. Hoboken, NJ, USA: Wiley, 2022.
16. Cisco Networking Academy, Junior Cybersecurity Analyst. Cisco, 2023. [Online]. Available: https://www.netacad.com
17. Materiale de curs și bibliografice disponibile pe platforma Google Classroom, actualizate 2024

Bibliografie minimală

1. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.
2. Cisco Networking Academy, Junior Cybersecurity Analyst. Cisco, 2023. [Online]. Available: https://www.netacad.com
3. D. Kim and M. G. Solomon, Fundamentals of Information Systems Security, 4th ed. Burlington, MA, USA: Jones & Bartlett Learning, 2020.

Aplicații (Laborator/ lucrări practice)	Nr. ore	Metode de predare	Observații
LISTA LUCRĂRILOR DE LABORATOR			
1. Protecţia muncii. Prezentarea laboratorului. 2. Analiza mecanismelor criptografice. 3. Securitatea comunicațiilor wireless. 4.Controlul accesului. Autentificare și autorizare. 5. Analiza securității serviciilor de rețea. 6. Semnături și certificate digitale. 7. Evaluarea vulnerabilităților.	2 2 2 2 2 2 2	lucrări practice, experimentul	

Bibliografie

1. W. Easttom, *Computer Security Fundamentals*, 4th ed., Pearson, 2021.
2. D. W. Misner and S. Bach, *Hands-On Ethical Hacking and Network Defense*, Cengage Learning, 2020.
3. R. Gupta and B. Gupta, *Hands-On Cybersecurity for Architects*, Packt Publishing, 2018.
4. J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, 3rd ed., Syngress, 2019.
5. P. Engebretson, *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*, 2nd ed., Syngress, 2018.
6. D. Upton, *Digital Forensics and Incident Response: A Practical Guide to Deploying Digital Forensic Techniques in the Enterprise*, Packt Publishing, 2020
7. W. Pollock, *Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali*, No Starch Press, 2019.
8. Cisco Networking Academy, Junior Cybersecurity Analyst. Cisco, 2023. [Online]. Available: https://www.netacad.com
9. Materiale şi bibliografice disponibile pe platforma Google Classroom, actualizate 2024

Bibliografie minimală

1. Cisco Networking Academy, Junior Cybersecurity Analyst. Cisco, 2023. [Online]. Available: https://www.netacad.com
2. Îndrumar de laborator în format electronic

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

Conţinutul disciplinei este în concordanţă cu conţinutul disciplinelor similare, opţionale sau facultative, de la programele de studiu din cadrul aceluiaşi domeniu, de la alte universităţi din ţară (Universitatea "Politehnica" din Bucureşti; Universitatea "Gh. Asachi Iaşi") şi străinătate (University of Limerick, IR; Michigan State University, USA).

10. **Evaluare**

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Claritatea, coerența și concizia prezentării clare de rezolvare a unei probleme pe tematica tezei de doctorat.	Examen oral	60%
Laborator / Lucrări practice	Aplicarea corectă a conceptelor la planificarea măsurărilor și modelarea datelor experimentale.	Rezolvarea de lucrări practice	40%

10.1. Standard minim de performanţă evaluare la curs

- însușirea principalelor noțiuni, teorii;
- abilități si cunoștințe teoretice necesare pentru planificarea experimentelor.

10.2. Standard minim de performanţă evaluare la activitatea aplicativă

- aplicarea corectă a conceptelor la rezolvarea unor probleme simple;
- alegerea corectă a metodelor specifice de programare a experimentelor şi optimizare a procesului.

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicație
20.09.2024		

Data avizării în consiliul SDSAI	Semnătura directorului SDSAI
23.09.2024	

Data avizării	Semnătura responsabilului de domeniu
23.09.2024	

Data aprobării în CSUD	Semnătura directorului CSUD
24.09.2024	

FIŞA DISCIPLINEI

Valabilă începând cu 2024/2025

1. Date despre program

Instituţia de învăţământ superior	Universitatea "Ştefan cel Mare" din Suceava
Şcoala doctorală	Ştiinţe Aplicate şi Inginereşti
Domeniul de studii de doctorat	Inginerie electronică, telecomunicaţii şi tehnologii informaţionale
Ciclul de studii	Doctorat
Programul de studii	Program de pregătire bazat pe studii universitare avansate

2. Date despre disciplină

Denumirea disciplinei	**COMPATIBILITATE ELECTROMAGNETICĂ**				
Titularul activităţilor de curs	Conf. univ. dr. ing. Eugen COCA				
Titularul activităţilor aplicative	Conf. univ. dr. ing. Eugen COCA				
Anul de studiu	I	Semestrul	I	Tipul de evaluare	Colocviu
Regimul disciplinei	Categoria formativă a disciplinei DAP – disciplină de aprofundare; DPA – disciplină de pregătire avansată; DSI – discipline de sinteză				DPA
	Categoria de opţionalitate a disciplinei: DI - impusă, DO - opţională, DF - facultativă				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	2	Laborator / Lucrări practice		Proiect	
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	28	Laborator / Lucrări practice		Proiect	

II Distribuţia fondului de timp pe semestru:	ore
II a)Studiul după manual, suport de curs, bibliografie şi notiţe	62
II b)Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	88
II c)Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	92
II d)Tutoriat	-
III Examinări	2
IV Alte activităţi:	-

Total ore studiu individual II (a+b+c+d)	242
Total ore pe semestru (I+II+III+IV)	300
Numărul de credite	**12**

4. Precondiţii (acolo unde este cazul)

Curriculum	• Studii de licenţă
Competenţe	• Masterat în inginerie

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• calculator portabil, videoproiector, note de curs în format editat, prezentări animaţii specifice
Desfăşurare aplicaţii	Seminar	• nu este cazul
	Laborator / Lucrări practice	• îndrumar de laborator, referate de laborator în format editat şi în format electronic, standuri experimentale, desktopuri - 10 buc. Software specializat
	Proiect	• nu este cazul

6. Competenţe specifice acumulate

Competenţe profesionale	- Capacitatea de identificare, formulare şi soluţionare într-o manieră creativă a problemelor de cercetare; - Abilităţi de documentare şi valorificare a lucrărilor ştiinţifice; - Capacitatea de a redacta lucrări ştiinţifice şi alte materiale academice la un nivel avansat, într-un stil adecvat domeniului de studiu şi cu respectarea rigorilor specifice acestuia la nivel naţional şi internaţional.

Competenţe transversale	- Abilităţi de interrelaţionare şi de lucru în echipă; - Cunoştinţe privind gândirea critică, inclusiv aptitudinea de a analiza, interpreta sau formula raţionamente în diferite contexte.

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

Obiectivul general al disciplinei	Însuşirea bazelor teoretice ale compatibilităţii electromagnetice, despre protejarea echipamentelor, încercarea echipamentelor şi determinarea gradului de imunitate la perturbaţii al acestora, cunoaşterea tehnicilor de încercare şi testate specifice echipamentelor electrice.

8. **Conţinuturi**

CURS	Nr. ore	Metode de predare	Observaţii
1. Perturbaţii de mod comun şi de mod diferenţial 2. Cuplaje în electronică. Apariţie, ecranare, principii de conectare la masă a circuitelor electronice. Ecranarea cablurilor. 3. Masa în electronică şi cuplajul parazit prin circuitul de masă. Metode de identificare şi eliminare a cuplajelor parazite. 4. Alimentări în curent continuu / alternativ. Decuplarea alimentărilor în curent continuu. Protecţia liniilor de curent alternativ la supratensiuni. 5. Perturbaţii pe căile de alimentare. Metode de identificare, măsurare şi protecţie. 6. Ecrane electromagnetice, studiul ecranelor EM prin metoda impedanţelor, tehnologii de realizare a ecranelor electromagnetice. 7. Tehnica măsurării standardizate a perturbaţiilor radiate şi imunităţii în laboratoare acreditate. 8. Standardizarea în domeniul compatibilităţii electromagntice. Standarde armonizate. Metode de determinare a conformităţii cu standardele în vederea obţinerii marcajului de conformitate CE: 9. Măsurări în camera anecoică. Laboratoare EMC acreditate conform ISO/EN 17025.	28	expunerea, prelegerea-dezbatere, demonstraţia	

Bibliografie

1. Clayton R. Paul, Robert C. Scully, Mark A. Steffka, "Introduction to Electromagnetic Compatibility", 3rd Edition, Wiley, 2022
2. Kenneth L. Kaiser, " Electromagnetic Compatibility Handbook ", CRC Press, 2004
3. Cehan, V.; "Compatibilitate electromagnetica", U.T. Iaşi, Facultatea de electronică şi telecomunicaţii, Note de curs, 2018
4. Radu, S., "Introducere în compatibilitate electromagnetică", Volumul 1, Ed. Gh. Asachi, Iaşi, 1995, ISBN 973-9178-25-1
5. Degauque, P.; "Compatibilite electromagnetique", Ed. Dunod, Paris, 1990, ISBN 2-04-018807-x
6. Rowe, H., E., "Signals and Noise in Communication Systems", Van Nostrand, Princeton, New Jersey, ISBN B0000CMWVT, 1965
7. Materiale de curs şi bibliografice disponibile pe platforma Google Classroom, actualizate 2024

Bibliografie minimală

1. Clayton R. Paul, Robert C. Scully, Mark A. Steffka, "Introduction to Electromagnetic Compatibility", 3rd Edition, Wiley, 2022
2. Cehan, V.; "Compatibilitate electromagnetica", U.T. Iaşi, Facultatea de electronică şi telecomunicaţii, Note de curs, 2018

Aplicaţii (Laborator/ lucrări practice)	Nr. ore	Metode de predare	Observaţii
LISTA LUCRĂRILOR DE LABORATOR			
1. Protecţia muncii. Prezentarea laboratorului şi a ciclului de lucrări.	2	lucrări practice, experimentul	
2. Utilizarea echipamentelor din laboratorul de compatibilitate electromagnetică (setare iniţială, configurare, mesaje de eroare, comandă folosind instrucţiuni GPIB)	2		
3. Măsurarea perturbaţiilor radiate ale echipamentelor multimedia conform EN 55032.	2		
4. Măsurări de perturbaţii electromagnetice radiate în spectrul reglementat conform EN 55032.	2		
5. Teste de imunitate la descărcări electrostatice, conform EN 61000-4-2.	2		
6. Teste de imunitate la perturbaţii radiate, conform EN 61000-4-3.	2		
7. Teste de imunitate la scăderi de tensiune şi întreruperi de scurtă durată, conform EN 61000-4-11.	2		

Bibliografie

1. Clayton R. Paul, Robert C. Scully, Mark A. Steffka, "Introduction to Electromagnetic Compatibility, 3rd Edition", Wiley,2022
2. Cehan, V.; "Compatiblitate electromagnetica", U.T. Iasi, Facultatea de electronică şi telecomunicaţii, Note de curs, 2010
3. Degauque, P.; "Compatibilite electromagnetique", Ed. Dunod, Paris, 1990, ISBN 2-04-018807-x
4. Rowe, H., E., "Signals and Noise in Communication Systems", Van Nostrand, Princeton, New Jersey, ISBN B0000CMWVT, 1965
5. Materiale şi bibliografice disponibile pe platforma Google Classroom, actualizate 2024

Bibliografie minimală

1. Cehan, V.; "Compatiblitate electromagnetica", U.T. Iasi, Facultatea de electronică şi telecomunicaţii, Note de curs, 2010
2. Îndrumar de laborator în format electronic

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

Conţinutul disciplinei este în concordanţă cu conţinutul disciplinelor similare, opţionale sau facultative, de la programele de studiu din cadrul aceluiaşi domeniu, de la alte universităţi din ţară (Universitatea "Politehnica" din Bucureşti; Universitatea "Gh. Asachi Iaşi") şi străinătate (University of Limerick, IR; Michigan State University, USA).

10. **Evaluare**

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Capacitatea de a rezolva probleme pe tematica tezei de doctorat prin aplicarea noţiunilor de compatibilitate electromagnetică	Examen oral	60%
Laborator / Lucrări practice	Abilitatea de a aplica teste şi măsurători specifice	Rezolvarea de lucrări practice	40%

10.1. Standard minim de performanţă evaluare la curs

- însuşirea principalelor noţiuni, teorii;
- abilităţi si cunostinte teoretice necesare pentru planificarea experimentelor.

10.2. Standard minim de performanţă evaluare la activitatea aplicativă

- aplicarea corectă a conceptelor la rezolvarea unor probleme simple;
- alegerea corectă a metodelor specifice de programare a experimentelor şi optimizare a procesului.

Data completării	Semnătura titularului de curs	Semnătura titularului de aplicaţie
20.09.2024		

Data avizării	Semnătura responsabilului de domeniu
23.09.2024	

Data avizării în consiliul SDSAI	Semnătura directorului SDSAI
23.09.2024	

Data aprobării în CSUD	Semnătura directorului CSUD
24.09.2024	