

FIȘA DISCIPLINEI

An universitar 2026 / 2027

1. Date despre program

Instituția de învățământ superior	Universitatea Maritimă din Constanța
Facultatea	Electromecanică Navală
Departamentul	Științe inginerești în domeniul mecanic și mediu
Domeniul de studii	Inginerie mecanică
Ciclul de studii	Master
Programul de studii/calificarea	Inginerie mecanică maritimă avansată

2. Date despre disciplină

Denumirea disciplinei	Introducere în securitate cibernetică				
Titularul activităților de curs	Conf.univ.dr.ing. Raicu Gabriel				
Titularul activităților de seminar	Conf.univ.dr.ing. Raicu Gabriel				
Anul de studiu	V	Semestrul	I	Tipul de evaluare	C
Regimul disciplinei	Categorია formativă a disciplinei DF – fundamentale, DS – de specializare, DC - complementare				DC
	Categorია de opționalitate a disciplinei: DOB – obligatorii, DOP – opționale, DFA - facultative				DFA

3. Timpul total estimat (ore alocate activităților didactice)

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

II Distribuția fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie și notițe	11
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren	5
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	3
III Tutoriat	2
IV Examinări	2
V Alte activități (precizați):	

Total ore studiu individual II (a+b+c)	19
Total ore pe semestru (Ib+II+III+IV+V)	79
Numărul de credite	3

4. Precondiții (acolo unde este cazul)

4.1 De curriculum	Notiuni generale legate de despre operare, programare calculatoare
4.2 De rezultate ale învățării	Operare computer (desktop/laptop, terminal mobil), operare platforme educationale si librerie electronica, Cunoașterea unei limbi străine

5. Condiții necesare pentru desfășurarea optimă a activităților didactice (acolo unde este cazul)

Desfășurare a cursului	Material didactic disponibil pe platforma ECampus	
Desfășurare aplicații	Seminar	Nu este cazul
	Laborator	30 calculatoare cu software specializat; Screen display – plasma; Aplicații software cu licență specializate; Campusul Virtual al UMC – materiale didactice Prezentări multimedia Tutoriale video Acces Internet

	Proiect	Nu este cazul
--	---------	---------------

6. Obiectivele disciplinei (în corelație cu rezultatele învățării specifice acumulate – pct 7)

6.1. Obiectivul general al disciplinei	Disciplina urmarește formarea unei baze conceptuale și metodologice solide în domeniul securității cibernetice, dezvoltând capacitatea masteranzilor de a înțelege, analiza și gestiona amenințările și riscurile cibernetice care afectează sistemele informatice, rețelele și organizațiile moderne.
6.2. Obiective specifice ale disciplinei	Dezvoltarea abilității de a analiza și interpreta probleme de decizii manageriale în condițiile unor atacuri cibernetice cu risc mare de expunere. Înțelegerea noțiunilor de bază privind estimarea riscului, tehnici aplicate în analiza de risc, principii general aplicate și terminologie utilizată în domeniu, limitele metodelor curente de evaluare a riscului. Aplicarea metodelor și tehnicilor de prevenire a atacurilor cibernetice care stau la baza conducerii, organizării și funcționării activităților specifice securității informatice dintr-o companie de transport maritim.

7. Rezultatele învățării

Nr. crt.	Cunoștințe	Abilități	Responsabilitate și autonomie
1	Absolventul explică principiile fundamentale ale securității cibernetice, tipurile de atacuri și mecanismele de apărare	Aplica metode și instrumente pentru analiza și protejarea sistemelor informatice și a rețelelor	Absolventul manifestă responsabilitate profesională și etică în activități de securitate cibernetică
2	Absolventul înțelege conceptele, principiile și mecanismele de bază ale securității cibernetice Cunoaște principalele amenințări, vulnerabilități și măsuri de protecție asociate sistemelor informatice și rețelelor Înțelege rolul criptografiei, autentificării multifactor și controlului accesului în protejarea informației	Absolventul are capacitatea de a analiza riscurile cibernetice și de a propune soluții de securitate adecvate Utilizează instrumente software specifice pentru monitorizarea, detectarea și prevenirea incidentelor Elaborează și implementează politici de securitate cibernetică	Absolventul participă într-o echipă multidisciplinară la realizarea unui proiect, demonstrând capacități de comunicare și asumarea de roluri specifice în condițiile colaborării cu specialiști din alte câmpuri ale cunoașterii
3	Absolventul cunoaște și înțelege conceptele, teoriile și metodele de bază ale securității cibernetice și le utilizează adecvat în comunicarea profesională.	Absolventul interpretează variate tipuri de concepte, situații, procese, proiecte asociate domeniului securității cibernetice Absolventul este capabil să comunice rezultatele cercetării și proiectelor în contexte științifice și industriale, naționale și internaționale.	Absolventul conduce echipe multidisciplinare în activități de cercetare, inovare și dezvoltare industrială. Este familiarizat cu rolurile și activitățile specifice muncii în echipă și distribuirea de sarcini pentru nivelurile subordonate.

8. Competențe la care participă disciplină, conform suplimentului la diplomă

Competențe profesionale	Utilizează software de securitatea cibernetică și aplică competențe de comunicare în domeniul tehnic Aprobă proiecte inginerești și testează sisteme de analiza a traficului de date (Nmap, Metasploit, Zenmap, OpenVAS etc.)
Competențe transversale	Adoptă modalități de reducere a riscului de securitate cibernetică Gestionează resurse financiare și materiale folosite în managementul riscului Gândește rapid

9. Conținuturi

Curs	Nr. ore	Metode de predare	Obs.
C1. Principii de bază ale securității cibernetice. Triada CIA	2	Expunerea interactivă și discuția dirijată, Prelegerea, Explicația	

C2+C3. Gestionarea Riscurilor de Securitate. Definitie si exemple. Metode de estimare/calcul. Bune practici. Relatia intre risc si alte elemente de cybersecurity	4	Expunerea sistematica – Explicația Prelegerea, Exemplificarea, Studiu de caz	
C4. Securitatea datelor. Modele si arhitecturi de securitate.	2	Expunerea interactiva si discutia dirijata, Prelegerea	
C5. Mecanisme de apărare în cybersecurity. Apararea in-depth. Arhitectura PKI.	2	Expunerea sistematica, Prelegerea, Explicația	
C6+C7. Noțiuni Fundamentale de Rețea în Cybersecurity. Scurta introducere in Rețele de Calculatoare. Notiuni si principii de baza despre Rețele. Modelul OSI si modelul TCP/IP.	4	Expunerea sistematica – Explicația Prelegerea, Exemplificarea Studiu de caz	
C8 8. Tipuri de atacuri cibernetice. Procesul de Hacking.	2	Expunerea sistematica. Prelegere	
C9. Evaluarea securitatii si Managementul vulnerabilitatilor. Penetration testing.	2	Expunerea sistematica, Prelegerea, Explicația	
C 10. Operațiuni de securitate cibernetică (SOC)	2	Expunerea sistematica. Prelegerea	
C 11. Identificarea vulnerabilitatilor si a nevoilor de securitate cibernetica la nivel național. Functiile rețelei Internet.	2	Expunerea sistematica Prelegerea, Explicații	
C 12. Masuri de sporire a nivelului de securitate cibernetica in plan national. Politici, standarde, norme si proceduri de de securitate	2	Expunerea interactiva si discutia dirijata, Prelegerea	
C 13. Vectori de propagare a amenintarilor cibernetice. Securitatea sistemelor de calcul și a rețelelor de calculatoare	2	Expunerea sistematica Prelegerea, Explicația	
C 14. Criptografie generala	2	Expunerea interactiva si discutia dirijata, Prelegerea	

Bibliografie

- Gabriel Raicu –Unități de învățare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentație gratuită accesibilă online, 2025
- ENISA, Cybersecurity Guidelines and Framework, 2024
- ISO/IEC 27001:2022 – Information Security management Systems.
- Legea nr.362/2028 privind asigurarea unui nivel comun ridicat de securitate a rețelelor si sistemelor informatice
- Stallings, W., *Computer Security: Principles and practice*, 5th edition, Pearson, 2023.
- Daneci Patrau D., Material de studiu in format digital disponibil pe platforma ECampus
- Nastase, R., *Introducere in Securitate cibernetica si Hacking*, Bucuresti, 2024.
- Nastase, R., *Introducere in retele de calculatoare*, Bucuresti, 2018.
- Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of CyberSecurity". *Journal of Digital Forensics, Security and Law*. 12 (2). ISSN 1558-7215.
- Mares D.M., Mihai G., *Informatică generală*, Editura Fundatiei România de Măine, Bucuresti, 2018
- Grama, A.(coord.), *Sisteme integrate colaborative pentru afaceri mici și mijlocii*, Ed. Universității Al. I. Cuza, Iași, 2017.
- "Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian Stevens, Tim (2018-06-11). "Global Cybersecurity: New Directions in Theory and Methods". *Politics and Governance*. 6 (2): 1–4. doi:10.17645/pag.v6i2.1569
- LINCH, Michael Patrick, *Internetul nostru. Știm mai mult, înțelegem mai puțin*, traducere de Silvia Palade, București, Editura Niculescu, 2017;
- Thurlow, Crispin; Lengel, Laura; Tomic, Alice (2024). *Computer Mediated Communication*. SAGE. ISBN 978-0-7619-4954-1.
- Colonati., C., *Radiocomunicatii digitale. Note, Aplicatii si Software*, Editura: N'Ergo Galați, 2014.
- Nicolae URS, „Comunicarea mediată de calculator. Internetul și schimbările în peisajul mediatic”, în *Studia Ephemerides*, LVI, nr. 2, 2021.
- <https://vredu.cysec.center> - Portal educațional de tip VirtualRange dezvoltat în cadrul Centrului de Securitate Cibernetică al UMC
- <https://www.cybersecuritychallenge.ro> - Campionatul European de Securitate Cibernetică
- <https://www.cyberedu.ro> – Exercițiile din cadrul etapelor nationale si finale ale ECSC din anii anteriori, precum si alte exercitii de la alte competitii internationale

- <http://ocw.cs.pub.ro/courses/cns> - Computer and Network Security
- <https://www.netacad.com/>

Bibliografie minimală

- Gabriel Raicu – Unități de învățare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentație gratuită accesibilă online, 2025
- Schneider, B., *Applied Cryptography*, 2th edition, Wiley, 2015
- Nastase, R., *Introducere in retele de calculatoare*, Bucuresti, 2018. Introducere în securitate cibernetică,

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Obs.
L1: Introducere in securitatea cibernetica. Protejarea datelor personale. Atacatori ciberneticici.	2	Conversatia. Exemple teste grila	
L2: Analiza unui atac cibernetic. Metode de infiltrare.Vulnerabilitati de securitate si exploit-uri.	2	Expunere. Exemple. Test grila	
L3: Protejarea datelor si a confidentialitatii. Mentenanta datelor. Instructiuni practice privind parolele.	2	Studiu de caz, dezbateri, problematizare. Test grila	
L4: Dispozitive si tehnologii in securitate cibernetica de protejare a organizatiei. Sisteme de detectare și prevenire a intruziunilor. Scanarea porturilor si protejarea împotriva programelor malware.	2	Studiu de caz, demonstratii practice, problematizare. Test grila	
L5: Abordarea comportamentala a securitatii ciberneticice. Aspecte legale si etice in securitatea ciberneticica.	2	Expunere. Calcule. Interpretări. Exemple	
L6: Securitatea sistemului de gestiune a bazelor de date.	2	Conversatia. Exemple; teste grila	
L7: Adresarea riscurilor si paradigme legislative.	1	Conversatia. Exemple; teste grila	
L8: Adresarea riscurilor si paradigme legislative asociate	3	Conversatia. demonstratii practice teste grila	
L9: Securitatea informatiei, exemple si aplicatii	2	Studiu de caz, dezbateri, problematizare	
L10: Schimbul de date in medii eterogene	2	Conversatia. Exemple	
L11: Arhitecturi de retea si elemente de propagare a riscurilor	2	Studiu de caz, dezbateri, problematizare	
L12: Sisteme criptografice, algoritmi si viteza de calcul	2	Studiu de caz, dezbateri, problematizare. Test grila	
L13: Pentesting. Exemple si aplicatii	2	Studiu de caz, dezbateri, problematizare	
L14: Recapitulare si pregatirea examenului final	2	Conversatia. Exemple	

Bibliografie

1. Gabriel Raicu – Unități de învățare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentație gratuită accesibilă online, 2025
2. ENISA, Cybersecurity Guidelines and Framework, 2024
3. ISO/IEC 27001:2022 – InformationSecurity management Systems.
4. Legea nr.362/2028 privind asigurarea unui nivel comun ridicat de securitate a rețelilor si sistemelor informatice
5. Stallings, W., *Computer Security:Principles and practice*, 5th edition, Pearson, 2023.
- 6.
7. Bibliografie in format e-Book disponibilă în UMC eCampus
8. Nastase, R., *Introducere in Securitate ciberneticica si Hacking*, Bucuresti, 2024
9. Nastase, R., *Introducere in retele de calculatoare*,Bucuresti, 2018,
10. Wireless mouse leave billions at risk of computer hack: cyber security firm Archived 3 April 2016 at the WaybackMachine "Multi-Vector Attacks Demand Multi-Vector Protection". MSSP Alert. July 24, 2018

Bibliografie minimală

Material de studiu in format electronic- disponibil pe platforma Ecampus.

Gabriel Raicu – Unități de învățare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentație gratuită accesibilă online, 2025

ENISA, Cybersecurity Guidelines and Framework, 2024

ISO/IEC 27001:2022 – InformationSecurity management Systems.

Introducere în securitate cibernetică, Materiale www.cmu-edu.eu

Mențiuni suplimentare

- ✓ Studenții pot realiza fotografii sau înregistrări audio-video în sălile în care se desfășoară activități didactice numai cu acordul cadrului didactic și în condițiile stabilite de către acesta;
- ✓ La intrarea în sala în care se desfășoară activitățile didactice, studenții sunt rugați să comute telefoanele mobile pe modul silențios și să nu le folosească în timpul orelor;

Toate materialele primite de către studenți în mod direct sau prin postare pe platforma campus.cmu-edu.eu sunt supuse legislației naționale și internaționale privind drepturile de autor; acestea pot fi utilizate de către studenți numai în scop didactic; orice altă utilizare sau postare pe site-uri cu acces deschis fără acordul deținătorului drepturilor de autor poate fi pedepsită în conformitate cu legea nr.8/1996 privind drepturile de autor și drepturile conexe și cu Convenția de la Berna

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

Disciplina conține noțiuni teoretice și aplicative care sunt în acord cu solicitările angajatorilor din domeniul ingineriei marine și care vor facilita studierea disciplinelor de specialitate în studiilor doctorale. De asemenea, în vederea schițării conținuturilor, titularul disciplinei a consultat continutul unor discipline similare predate la universități din țară și străinătate.

11. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- Claritatea și coerența exprimării cunoștințelor; - cunoasterea termenilor de specialitate și înțelegerea conceptelor privind securitatea cibernetică și a interacțiunilor individului în spațiul virtual; - originalitate și capacitatea de analiza - respectarea normelor de etica și desecuritate	Examinare – test scris grila 18 itemi, 0,5pct/item și 1 pct din oficiu.	70%
Seminar	-	-	-
Laborator	- Folosirea terminologiei specifice disciplinei ISC; - Responsabilitatea studentilor față de rezolvarea sarcinilor de lucru primite; - Realizarea temelor de laborator	-Aprecierea activității experimentale a studentului în timpul orelor de laborator -Evaluare continua, activitate și implicare	30%
Proiect			

10.5 Condiții de promovare: minimum 50 de puncte obținute; 50,...54p ► nota 5; 55,...64p ► nota 6; 65,...74. ► nota 7; 75,...84p ► nota 8; 85...94p ► nota 9; 95,...100 p ► nota 10

Mențiuni suplimentare:

- în timpul semestrului se poate organiza examen parțial;
- în cazul în care studentul participă la conferințe (studentești, locale, naționale, internaționale) sau concursuri (naționale, internaționale) care au ca tematică această disciplină, acesta va putea beneficia de puncte suplimentare sau de echivalarea unor teme de casa și/sau lucrări și/sau prezență, în funcție de rezultatele obținute;
- la lucrările scrise studenții nu au voie să folosească telefoanele mobile și nici alte echipamente electronice cu excepția calculatoarelor științifice simple.

Standard minim de performanță

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
22.09.2025	Conf.univ.dr.ing. Raicu Gabriel	Conf.univ.dr.ing. Raicu Gabriel

Data avizării în departament	Semnătura directorului de departament
25.09.2025	Ș.l.univ.dr.ing. Cătălin Faităr

Data avizării în Consiliul Facultății	Semnătura decanului
29.09.2025	Conf.univ.dr-habil.ing. Liviu Stan