FIŞA DISCIPLINEI
An universitar 2027 / 2028

1. Date despre program

Instituţia de învăţământ 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 in securitate cibernetica				
Titularul activităţilor de curs	Conf.univ.dr.ing. Raicu Gabriel				
Titularul activităţilor de seminar	Conf.univ.dr.ing. Raicu Gabriel				
Anul de studiu	VI	Semestrul	I	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DF – fundamentale, DS – de specializare, DC - complementare				DC
	Categoria de opţionalitate a disciplinei: DOB – obligatorii, DOP – opționale, DFA - facultative				DFA

3. Timpul total estimat (ore alocate activităţilor 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 învăţământ	56	Curs	28	Seminar		Laborator	28	Proiect	

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

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

4. Precondiţii (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 librarie electronica,Cunoașterea unei limbi străine

5. Condiţii necesare pentru desfăşurarea optimă a activităţilor didactice (acolo unde este cazul)

Desfăşurare a cursului		Material didactic disponibil pe platforma ECampus
Desfăşurare aplicaţii	Seminar	Nu este cazul
	Laborator	30 calculatore cu software specializat; Screen display – plasma; Aplicaţii software cu licentă 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 urmareste formarea unei baze conceptuale si metodologice solide in domeniul securitatii cibernetice, dezvoltand capacitatea masteranzilor de a intelege, analiza si gestiona amenintarile si riscurile cibernetice care afecteaza sistemele informatice, retelele si organizatiile moderne.
6.2. Obiective specifice ale disciplinei	Dezvoltarea abilităţii de a analiza si interpreta probleme de decizii manageriale în condiţiile unor atacuri cibernetice cu risc mare de expunere. Înţelegerea noţiunilor de bază privind estimarea riscului, tehnici aplicate în analiza de risc, principii general aplicate şi terminologie utilizată în domeniu, limitele metodelor curente de evaluare a riscului. Aplicarea metodelor şi tehnicilor de prevenire a atacurilor cibernetice care stau la baza conducerii, organizării şi funcţionării activităţilor specifice securitatii informatice dintr-o companie de transport maritim.

7. Rezultatele învăţării

Nr. crt.	Cunoştinţe	Abilități	Responsabilitate şi autonomie
1	Absolventul explica principiile fundamentale ale securitatii cibernetice, tipurile de atacuri si mecanismele de aparare	Aplica metode si instrumente pentru analiza si protejarea sistemelor informatice si a retelelor	Absolventul manifesta responsabilitate profesionala si etica in activitati de securitate cibernetica
2	Absolventul înțelege conceptele, principiile si mecanismele de baza ale securitatii cibernetice Cunoaste principalele amenintari, vulnerabilitati si masuri de protectie asociate sistemelor informatice si retelelor Intelege rolul criptografiei, autentificarii multifactor si controlului accesului in protejarea informatiei	Absolventul are capacitatea de a analiza riscurile cibernetice si de a propune solutii de securitate adecvata Utilizeza instrumente software specifice pentru monitorizarea, detectarea si prevenirea incidentelor Elaboreaza si implementeaza politici de securitate cibernetica	Absolventul participă într-o echipă multidisciplinară la realizarea unui proiect, demonstrând capacităţi de comunicare şi asumarea de roluri specifice în condiţiile colaborării cu specialişti din alte câmpuri ale cunoaşterii
3	Absolventul cunoaşte și înțelege conceptele, teoriile şi metodele de bază alesecuritatii cibernetice și le utilizează adecvat în comunicarea profesională.	Absolventul interpretează variate tipuri de concepte, situaţii, procese, proiecte asociate domeniului securitatii 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 activităţile 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 cibernetica si aplică competențe de comunicare în domeniul tehnic Aprobă proiecte inginerești si testează sisteme de analiza a traficului de date (Nmap, Metasploit, Zenmap, OpenVAS etc.)
Competențe transversale	Adoptă modalități de reducere a riscului de securitate cibernetica Gestionează resurse financiare și materiale folosite in managementul riscului Gândește rapid

9. Conţinuturi

Curs	Nr. ore	Metode de predare	Obs
C1. Principii de baza ale securitatii cibernetice. Triada CIA	**2**	Expunerea interactiva si discutia dirijata; 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 Retele de Calculatoare. Notiuni si principii de baza despre Retele. 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 retelei 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 –Unităţi de învăţare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentaţie gratuită accesibilă online, 2025
- ENISA, Cybersecurity Guidelines and Framework, 2024
- ISO/IEC 27001:2022 – InformationSecurity management Systems.
- Legea nr.362/2028 privind asigurarea unui nivel comun ridicat de securitate a retelelor 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 Mâine, Bucuresti, 2018
- Grama, A.(coord.), *Sisteme integrate colaborative pentru afaceri mici şi mijlocii*, Ed. Universităţii Al. I. Cuza, Iaşi, 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 andGovernance. 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 dezvoltatîn cadrul Centrului de Securitate Cibernetică al UMC
- https://www.cybersecuritychallenge.ro - Campionatul European de Securitate Cibernetică
- **https://www.cyberedu.ro** – Exercitiile 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 – Unităţi de învăţare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentaţie gratuită accesibilă online, 2025 Schneider, B., *Applied Cryptografy*, 2th edition, Wiley, 2015 Nastase, R., *Introducere in retele de calculatoare,* Bucuresti, 2018. Introducere în securitate cibernetică, Materiale www.cmu-edu.eu

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
L1: Introducere in securitatea cibernetica. Protejarea datelor personale. Atacatori cibernetici.	**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, dezbatere, 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 cibernetice. Aspecte legale si etice in securitatea cibernetica.	**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, dezbatere, 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, dezbatere, problematizare	
L12: Sisteme criptografice, algortimi si viteza de calcul	**2**	Studiu de caz, dezbatere, problematizare. Test grila	
L13: Pentesting. Exemple si aplicatii	**2**	Studiu de caz, dezbatere, problematizare	
L14: Recapitulare si pregatirea examenului final	**2**	Conversatia. Exemple	

Bibliografie

1. Gabriel Raicu – Unităţi de învăţare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentaţie 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 retelelor si sistemelor informatice
5. Stallings, W., *Computer Security:Principles and practice*, 5th edition, Pearson, 2023.
6. Bibliografie in format e-Book disponibilă în UMC eCampus
7. Nastase, R., *Introducere in Securitate cibernetica si Hacking*, Bucuresti, 2024
8. Nastase, R., *Introducere in retele de calculatoare,*Bucuresti, 2018,
9. 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

Gabriel Raicu – Unităţi de învăţare, prezentări multimedia CMU Campus, campus.cmu-edu.eu, documentaţie 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

Menţiuni suplimentare

- ✓ Studenţii pot realiza fotografii sau înregistrări audio-video în sălile în care se desfăşoară activităţi didactice numai cu acordul cadrului didactic şi în condiţiile stabilite de către acesta;
- ✓ La intrarea în sala în care se desfăşoară activităţile didactice, studenţii sunt rugaţi să comute telefoanele mobile pe modul silenţios şi 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 conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi 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 in 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 şi înţelegerea conceptelor privind securitatea cibernetică și a interacțiunilor individului în spațiul virtual; - originalitate si capacitatea de analiza - respectarea normelor de etica si desecuritate	Examinare – test scris grila 18 itemi, 0,5pct/item si 1 pct din oficiu.	**70%**
Seminar	-	-	**-**
Laborator	- Folosirea terminologiei specifice disciplinei ISC; - Responsabilitatea studentilor faţă 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 Condiţii de promovare: minimum 50 de puncte obţinute; 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

Menţiuni suplimentare:

- în timpul semestrului se poate organiza examen parțial;
- în cazul în care studentul participă la conferinţe (studenţeşti, locale, naţionale, internaţionale) sau concursuri (naţionale, internaționale) care au ca tematică această disciplină, acesta va putea beneficia de puncte suplimentare sau de echivalarea unor teme de casa şi/sau lucrări şi/sau prezenţă, în funcţie de rezultatele obţinute;
- la lucrările scrise studenții nu au voie să folosească telefoanele mobile și nici alte echipamente electronice cu excepţia calculatoarelor științifice simple.

Standard minim de performanţă

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
20.09.2025	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 Faitar

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