FIŞA DISCIPLINEI
An universitar 2025 / 2026

1. Date despre program

Instituţia de învăţământ superior	Universitatea Maritimă din Constanța
Facultatea	Navigaţie şi Transport Naval
Departamentul	Management în transporturi
Domeniul de studii	Inginerie şi Management
Ciclul de studii	Master
Programul de studii/calificarea	Managementul Sistemelor Integrate de Transport

2. Date despre disciplină

Denumirea disciplinei	Introducere în securitatea cibernetică					
Titularul activităţilor de curs	conf. univ. Raicu Gabriel					
Titularul activităţilor de seminar	conf. univ. Raicu Gabriel					
Anul de studiu	V	Semestrul	I	Tipul de evaluare	V	
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	32
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	13
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	24
III Tutoriat	2
IV Examinări	2
V Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c)	69
Total ore pe semestru (Ib+II+III+IV+V)	129
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 De curriculum	• Notiuni generale legate de despre operare și programarea calculatoarelor
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 • Masteranzii trebuie să respecte normele de conduită academică • Data susținerii examenului se va stabili de titular de comun acord cu masteranzii.
Desfăşurare aplicaţii	Seminar	• Nu e cazul
	Laborator	• 30 calculatore cu software specializat; • Screen display – plasma; • Aplicaţii software cu licentă specializate; • Campusul Virtual al UMC – materiale didactice • Prezentări multimedia • Acces Internet

		• Trebuie să respecte normele de conduită academică; • Termenele de predare și susținere a lucrărilor de seminar sunt stabilite de titular de comun acord cu masteranzii.
	Proiect	• Nu e cazul

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

6.1. Obiectivul general al disciplinei	Disciplina urmărește dezvoltarea unei fundații conceptuale și metodologice solide în domeniul securității cibernetice, facilitând înțelegerea, analiza și gestionarea amenințărilor și riscurilor cibernetice care vizează sistemele informatice, rețelele și infrastructurile organizaționale moderne.
6.2. Obiective specifice ale disciplinei	• Dezvoltarea capacității de a analiza, interpreta și fundamenta decizii manageriale în contextul unor atacuri cibernetice cu nivel ridicat de risc, impact și expunere operațională. • Înțelegerea conceptelor esențiale privind evaluarea riscului cibernetic, a tehnicilor utilizate în analiza de risc, a principiilor și terminologiei specifice domeniului, precum și a limitelor metodelor actuale de evaluare. • Aplicarea metodelor, tehnicilor și bunelor practici de prevenire, detectare și răspuns la atacuri cibernetice, necesare conducerii, organizării și funcționării eficiente a activităților specifice securității informatice la nivel operațional și organizațional.

7. Rezultatele învățării

Nr. crt.	Cunoştinţe	Abilități	Responsabilitate şi autonomie
1.	Studentul înțelege principiile de integrare a tehnologiilor digitale în logistică	Studentul folosește aplicații informatice pentru analiza datelor privind transportul și depozitarea	Studentul participă la implementarea soluțiilor digitale și își asumă sarcini de integrare în echipe de proiect
2.	Studentul are cunoștințe despre legislația europeană și internațională în transport și comerț	Studentul interpretează reglementările și le integrează în scenarii operaționale practice	Studentul aplică cunoștințele juridice cu autonomie parțială pentru asigurarea conformității logistice
3.	Studentul deține cunoștințe privind instrumentele de evaluare a riscurilor operaționale	Studentul evaluează riscurile din lanțul de aprovizionare și propune soluții de reducere	Studentul își asumă responsabilitatea participării la planuri de management al riscului logistic
4.	Studentul înțelege arhitectura rețelelor de distribuție și strategiile de localizare	Studentul elaborează modele de configurare și optimizare a rețelelor logistice	Studentul răspunde, cu autonomie crescută, de realizarea planurilor de proiectare logistică
5.	Studentul cunoaște metode de management cross-cultural în echipe internaționale	Studentul aplică strategii de comunicare interculturală în contexte logistice	Studentul coordonează, cu autonomie graduală, sarcini în echipe multiculturale și gestionează interacțiuni eficiente

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

Competențe profesionale	• Asigura îndeplinirea cerintelor legale • Tine legatura cu managerii • Supravegheaza personal • Asigura conformitatea cu legislatia în materie de securitate • Sintetizeaza informatii • Recomanda masuri de îmbunatatire a sigurantei • Monitorizeaza tendintele tehnologiei • Asigură managementul logisticii
Competențe transversale	• Comunică observatii analitice • Realizeaza analize de date • Evalueaza factorii de risc

9. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
• Concepte generale privind securitatea informației	2	Prelegere explicativă Expunere interactivă și discuții dirijate	
• Securitatea informatiei în medii heterogene	2	Prelegere explicativă	
• Arhitecturi de retea reziliente	6	Expunere interactivă și discuții dirijate	3 ședințe x 2hrs

• Retele wireless si modele de securitate	2	Prelegere explicativă Expunere interactivă și discuții dirijate	
• Arhitectura retelei Internet	2	Prelegere explicativă Expunere interactivă și discuții dirijate	
• Sisteme distribuite si concepte generale de securitate	2	Prelegere explicativă Expunere interactivă și discuții dirijate	
• Securitatea sistemelor izolate	2	Prelegere explicativă Expunere interactivă și discuții dirijate	
• Criptografie generala	4	Prelegere explicativă Expunere interactivă și discuții dirijate	2 ședințe x 2hrs
• Testarea securității și identificarea vulnerabilităților (Introducere în PenTesting)	2	Prelegere explicativă Expunere interactivă și discuții dirijate	
• Raspunsul la incidentele de securitate cibernetica	2	Prelegere explicativă Expunere interactivă și discuții dirijate	
• Politici, standarde si managementul riscului	2	Prelegere explicativă Expunere interactivă și discuții dirijate	

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.362/2018 privind asigurarea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice
- Stallings, W., *Computer Security:Principles and practice*, 5th edition, Pearson, 2023.
- 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

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.
- Legea nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice

Aplicaţii (laborator)	Nr. ore	Metode de predare	Observaţii
• Securitatea informatiei, exemple si aplicatii	4	Demonstrații și exemplificări practice, problematizare, exercitiu.	
• Schimbul de date in medii eterogene	4	Demonstrații și exemplificări practice, problematizare, exercitiu.	
• Arhitecturi de retea si elemente de propagare a riscurilor	4	Demonstrații și exemplificări practice, problematizare, exercitiu.	
• Sisteme criptografice, algortimi si viteza de calcul	4	Demonstrații și exemplificări practice, problematizare, exercitiu.	
• Securitatea informatiei, tehnici de obfuscare si steganografie	4	Demonstrații și exemplificări practice, problematizare, exercitiu.	

• Pentesting. Exemple si aplicatii live	4	Demonstrații și exemplificări practice, problematizare, exercitiu.	
• Adresarea riscurilor si paradigme legislative asociate	4	Demonstrații și exemplificări practice, problematizare, exercitiu.	

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.362/2018 privind asigurarea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice
- Stallings, W., Computer Security:Principles and practice, 5th edition, Pearson, 2023.
- Nastase, R., Introducere in Securitate cibernetica si Hacking, Bucuresti, 2024.
- NIST – National Institute of Standards and Technology (USA) , NIST Cybersecurity Framework (CSF), https://www.nist.gov/cyberframework
- ENISA – European Union Agency for Cybersecurity, Cybersecurity Threat Landscape 2024, https://www.enisa.europa.eu/publications
- MITRE, MITRE ATT&CK Framework, https://attack.mitre.org/, MITRE D3FEND (defensive techniques), https://d3fend.mitre.org/, MITRE CVE Database (vulnerabilități publice), https://www.cve.org/

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.
- Legea nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice

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 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 conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

Elaborarea fişei disciplinei a avut loc în urma discutării conţinutului disciplinei şi a cerinţelor practice cu specialişti şi practicieni din domeniu care îşi desfăşoară activitatea în sectorul public și privat (manageri publici, funcţionari publici de conducere şi de execuţie, personal contractual etc.), dar şi pornind de la competenţele profesionale cerute de piaţa muncii (prin însuşirea noţiunilor teoretico-metodologice şi a aspectelor practice din cadrul disciplinei, masteranzii dobândesc cunoştinţe, în concordanţă cu competenţele parţiale cerute pentru ocupaţiile posibile prevăzute în Grila RNCIS).

11. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	• Cunoașterea termenilor de specialitate și a conceptelor de bază în securitate cibernetică. • Explicarea clară a principiilor și proceselor din operațiile informaționale. • Identificarea și justificarea abordărilor decizionale în situații de securitate. • Utilizarea corectă a spațiului virtual pentru comunicare profesională. • Claritate, coerență și acuratețe în exprimare. • Originalitate, analiză critică și respectarea normelor de etică și securitate.	Examen scris	70%

Laborator	• Folosirea corectă a terminologiei de specialitate în analiza și rezolvarea exercițiilor. • Înțelegerea și aplicarea practică a conceptelor fundamentale de securitate cibernetică. • Responsabilitatea și implicarea în îndeplinirea sarcinilor și exercițiilor de laborator. • Realizarea completă și corectă a temelor și lucrărilor de laborator. • Utilizarea adecvată a spațiului virtual și a instrumentelor tehnice pentru activitățile practice	Evaluare continua, activitate și implicare	30%
Condiţii de promovare: minimum 50 de puncte obţinute **Menţiuni suplimentare:** 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 și/sau lucrări și/sau prezenţă, în funcţie de rezultatele obţinute;			
Standard minim de performanţă • Însușirea minimală a conceptelor și termenilor folosiți în domeniul securității cibernetice • Corelarea minimală între două sau mai multe prevederi legislative • Utilizarea primară a instrumentelor tehnice specializate de evaluare a securității sistemelor informatice			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
25.09.2025	conf. univ. Raicu Gabriel	conf. univ. Raicu Gabriel

Data avizării în departament	Semnătura directorului de departament
26.09.2025	Lector univ.dr. Ana-Cornelia Olteanu

Data avizării în Consiliul Facultății	Semnătura decanului
29.09.2025	Conf.univ.dr.ing. Nicoleta Acomi