

TEHNOLOGII INFORMAȚIONALE ȘI SECURITATE CIBERNETICĂ
1. Date despre disciplină/modul

Facultatea	Construcții, Geodezie și Cadastru				
Departamentul	Inginerie Civilă și Geodezie				
Ciclul de studii	Studii superioare de licență, ciclul I				
Programul de studiu	0710.1 Inginerie și management în construcții 0732.1 Construcții industriale și civile 0732.5 Inginerie antiincendii și protecție civilă 0731.2 Inginerie geodezică și cadastru 0731.4 Evaluarea și dezvoltarea imobilului 0421.1 Drept				
Anul de studiu	Semestrul	Tip de evaluare	Categoria formativă	Categoria de opționalitate	Credite ECTS
I (învățământ cu frecvență); I (învățământ cu frecvență redusă)	I I	E E, Iv	S -disciplină de specialitate.	O - disciplină obligatorie	3

2. Timpul total estimat

Total ore în planul de învățământ	Din care				
	Ore auditoriale		Lucrul individual		
	Curs	Laborator/seminar	Proiect de an	Studiul materialului teoretic	Pregătire aplicații
90	30	0/15	-	45	-
90	12	0/6	-	72	-

3. Precondiții de acces la disciplină/modul

Conform planului de învățământ	Științe inginerești, tehnologice, economice și informatice
Conform competențelor	Cunoștințe dobândite la disciplinele matematică, fizică și informatică. Încadrarea în domeniul IT, organizarea activităților în condiții de securitate cibernetică, evaluarea riscurilor de natură tehnologică și cibernetică

4. Condiții de desfășurare a procesului educațional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector și calculator, tablă, cretă, marker, internet
Laborator/seminar	Studentii vor aplica materialul teoretic în rezolvarea problemelor, sala de computere cu sisteme suficiente pentru o clasă de studenți.

5. Competente specifice acumulate

CG1. Utilizarea în activitatea profesională a legităților de bază definite de științele fundamentale	1. Aplica mecanismele și conceptele fundamentale în procesul evaluării tendințelor și oportunităților în care activează entitățile economice, utilizând tehnologiile informaționale 2. Aplica în mod creativ și critic metodele și instrumentele manageriale în diverse studii de caz în vederea interpretării rezultatelor
---	--

6. Obiectivele disciplinei/modulului

Obiectivul general	Însușirea și aplicarea în practică a cunoștințelor în domeniul sistemelor informaționale și comunicațiilor, cit și a cunoștințelor legate de securitatea cibernetică.
Obiectivele specifice	Dobândirea cunoștințelor teoretice privind arhitectura sistemelor informatice, dimensionarea și validarea componentelor hardware și software, precum și integrarea mecanismelor de securitate cibernetică în infrastructurile digitale.

7. Conținutul disciplinei

Tematica activităților didactice	Numărul de ore	
	învățământ cu frecvență	învățământ cu frecvență redusă
Tematica prelegerilor		
T1. Introducere în rețele de calculatoare.	2	1
T2. Modele și protocoale de rețea.	2	1
T3. Nivelul Fizic. Rolul nivelului fizic.	2	1
T4. Sisteme de numerație.	2	1
T5. Rețeaua Ethernet.	2	1
T6. Nivelul Rețea.	2	1
T7. Nivelul Transport și Nivelul Aplicație.	2	1
T8. Conceptele de bază în domeniul securității cibernetic.	2	1
T9. Tehnici și tipuri de atac cibernetic.	2	1
T10. Protejarea datelor online și a confidențialității.	2	1
T11. Strategii de securizare a rețelelor, echipamentelor și datelor.	2	1
T12. Programarea modernă cu Web 2.0 și Web 3.0.	2	1
T13. Tehnologia de Cloud.	2	1
T14. Inteligența Artificială și Învățarea Automată (Machine Learning).	2	1
T15. Automatizarea și rolul acesteia în domeniul securității cibernetic.	2	1
Total prelegeri:	30	12

Tematica activităților didactice	Numărul de ore	
	învățământ cu frecvență	învățământ cu frecvență redusă
Tematica lucrărilor de laborator		
LL1 Packet Tracer. Simularea rețelelor.	2	1
LL2 Explorarea nivelului fizic.	2	1
LL3 Adresarea IP.	1	0,5

LL4 Schimbul de date prin TCP și UDP.	2	0,5
LL5 Identificarea unui loc de muncă în securitate cibernetică.	1	0,5
LL6 Explorarea criptării și verificarea integrității fișierelor.	1	0,5
LL7 Detectarea vulnerabilităților și amenințărilor.	1	0,5
LL8 Utilizarea stenografiei.	1	0,5
LL9 Configurarea Modulului de Transport VPN.	2	0,5
LL10 Configurarea Modulului Tunel VPN.	2	0,5
Total lucrări de laborator:	15	6

Tematica lucrărilor de laborator (15 ore / 6 ore)

8. Referințe bibliografice

Principale	Hotărârea Parlamentului Nr. HP391/2023 din 15.12.2023 privind aprobarea Strategiei securității naționale a Republicii Moldova Ludmila PECA, Dinu ȚURCANU. Network security: Practical examples solved. ISBN 978-9975-45-941-9. Chișinău: Tehnica-UTM, 2023 Cisco Networking Academy. Introducere în Securitatea Cibernetică. 2022 Cisco Networking Academy. Curs CCNA Routing & Switching. 2023 Palo Alto Networks Academy - Cursuri de Securitate NIST Cybersecurity Framework - Versiunea 2.0. National Institute of Standards and Technology. Ghid de implementare a standardelor de securitate cibernetică pentru organizații. Disponibil: https://www.nist.gov/cyberframework ISO/IEC 27001:2022 - Information Security Management Systems. Standard internațional privind managementul sistemelor de securitate informatică. Ediția a doua actualizată. 2022 OWASP Top 10 - 2021. Open Web Application Security Project. Cele mai critice zece vulnerabilități ale aplicațiilor web și modalități de prevenire. Disponibil: https://owasp.org/www-project-top-ten/ CompTIA Security+ Study Guide (SY0-601). Kaplan IT Training. Ghid cuprinzător pentru certificări în domeniul securității IT și gestionarea amenințărilor cibernetice. 2021
Suplimentare	PECA, ȚURCANU. Computer networks: Practical examples. ISBN 978-9975-45-812-2. 2022 Ghid de bune practici securitate rețele sociale - STISC Ghid de bune practici securitate cibernetică - SRI ALECU et al. Ghid de securitate cibernetică. ISBN 978-973-0-33645-0. 2021 CIS Controls v8 - Center for Internet Security. Măsuri esențiale de control pentru prevenirea atacurilor cibernetice și gestionarea riscurilor de securitate. Disponibil: https://www.cisecurity.org/cis-controls/ Azure Security Best Practices - Microsoft Documentation. Ghid oficial pentru implementarea securității în infrastructura cloud Microsoft Azure. Actualizat periodic. Disponibil: https://docs.microsoft.com/azure/security/ MITRE ATT&CK Framework. Bază de cunoștințe cu tactici și tehnici adversare bazate pe observații din lumea reală. Utilizată pentru evaluarea amenințărilor și vulnerabilităților. Disponibil: https://attack.mitre.org/ Rapport Anual asupra Amenințărilor Cibernetice - Kaspersky Securelist. Analiză detaliată a tendințelor în atacuri cibernetice, malware și vulnerabilități din anul anterior. Publicat anual RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax și RFC 7230-7235 - HTTP/2 Protocol Specification. Standarde tehnice IETF pentru protocoale de rețea și comunicație pe internet

9. Evaluare

Forma de învățământ	Periodică		Curentă	Lucrul individual	Examen final
	Evaluarea 1	Evaluarea 2			
Cu frecvență	15%	15%	15 %	15 %	40%
Cu frecvență redusă	25 %			25 %	50 %
Standard minim de performanta					
▪ Prezența și activitatea la prelegeri și lucrări de laborator ▪ Obținerea notei minime de "5" la fiecare evaluare periodică și la lucrul individual ▪ Demonstrarea în lucrarea de examinare finală a cunoașterii materialului studiat referitor la: • Conceptele fundamentale de rețele de calculatoare și securitate cibernetică • Aplicații practice și tendințe viitoare în domeniu • Capacitatea de a aplica cunoștințele în context real					