S.07.O.047 SECURITATEA REȚELELOR DE COMUNICAȚII

1. Date despre disciplină

Facultatea	Electronică şi Telecomunicaţii				
Departamentul	Telecomunicații și Sisteme Electronice				
Ciclul de studii	Studii superioare de licenţă, ciclul I				
Programul de studiu	0714.2 Rețele și Software de Telecomunicații				
Anul de studiu	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
IV (învăţământ cu frecvenţă); IV (învățământ cu frecvență redusă)	VII VIII	E	S – unitate de curs de specialitate	O - unitate de curs obligatorie	5

2. Timpul total estimat

Total ore în planul de învățământ	Din care					Tipul formei de învățământ
	Ore în auditoriu			Lucrul individual		
	Curs	Lucr. practice	Laborator	Studiul materialului teoretic	Pregătire aplicații	
150	30	15	30	50	25	cu frecvență
150	14	4	12	80	40	frecvență redusă

3. Precondiţii de acces la disciplină

Conform planului de învăţământ	Programarea calculatoarelor și limbaje de programare I,II, Limba engleză, Tehnologii Informaționale Aplicate, Securitatea Informației în Sistemele de Telecomunicații, Aplicații în baza Protocoalelor de Rețea.
Conform competenţelor	Abilități de programare în limbajul C și C++, cunoștințe și abilități de operare cu sistemele informaționale.

4. Condiţii de desfăşurare a procesului educaţional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector, calculator și acces la Internet. Nu vor fi tolerate întârzierile studenţilor, precum şi convorbirile telefonice în timpul cursului.
Laborator	Studenţii vor realiza și perfecta rapoartele conform condiţiilor impuse de indicaţiile metodice. Termenul de predare a lucrării de laborator – 2 săptămâni după finalizarea acesteia. Pentru prezentarea cu întârziere a lucrării, aceasta se depunctează cu 1pct./săptămână de întârziere.

5. Competenţe specifice acumulate

Competențe profesionale	**C4. Elaborarea specificațiilor tehnice, selectarea și achiziționarea, dar și exploatarea echipamentelor de comunicații și integrarea pe acestea a diferitor servicii ale comunicațiilor ce respectă elementele securității cibernetice**

	C4.1. Definirea principiilor şi metodelor de transmisie a mesajelor de voce, audio, video şi de date, precum şi a principiilor de integrare a serviciilor în reţelele cu comutaţie de pachete; C4.2. Explicarea si interpretarea principalelor cerinţe şi tehnici specifice de abordare pentru transmisiile de date, voce, video, multimedia; C4.3. Elaborarea specificaţiilor tehnice, achiziţia, instalarea şi exploatarea echipamentelor de comunicaţii fixe şi mobile; C4.4. Utilizarea criteriilor de performanţă adecvate pentru aprecierea calităţii serviciilor oferite de echipamentele de comunicaţii şi evidenţierea parametrilor care influenţează calitatea; C4.5. Elaborarea de proiecte privind instalarea, punerea în funcţiune şi configurarea unor echipamente de comunicaţii. **C5. Proiectarea infrastructurii de comunicații, selectarea protocoalelor de diferit nivel pentru funcționarea rețelelor LAN, MAN, WAN, WMN, WLAN, VLAN** C5.1. Definirea conceptelor, principiilor şi metodelor folosite în reţelele de Telecomunicaţii integrate referitor la arhitecturile şi protocoalelor de comunicaţii; C5.2. Explicarea şi interpretarea diferitelor protocoale de acces şi de comunicaţii precum şi a tehnologiile utilizate în reţelele locale, metropolitane, de arie mare şi integrate; C5.3. Elaborarea, instalarea, punerea în funcţiune şi exploatarea reţelelor de capacitate mică/medie; C5.4. Utilizarea criteriilor de performanţă adecvate pentru aprecierea calităţii serviciilor oferite în diversele tipuri de reţele şi remedierea unor deranjamente; C5.5. Elaborarea de proiecte privind dimensionarea, instalarea, punerea în funcţiune şi configurarea unor reţele de capacitate mică/medie. **C6. Utilizarea limbajelor şi instrumentelor specializate pentru inginerie software, cu orientare către sistemele de telecomunicaţii integrate** C6.1. Definirea de metodologii, limbaje şi instrumente software implicate în dezvoltarea sistematică a sistemelor software de comunicaţii; C6.2. Explicarea şi interpretarea elementelor limbajului unificat de modelare (UML), necesar în dezvoltarea asistată a sistemelor software de comunicaţii integrate; C6.3. Aplicarea cunoştinţelor generale privind metodologiile şi limbajul de modelare UML; C6.4. Utilizarea tehnicilor orientate pe obiecte pentru analiza si modelarea sistemelor SW; C6.5. Modelarea şi programarea elementelor pentru aplicatii functionand în reţea şi WEB.

6. Obiectivele disciplinei

Obiectivul general	Asimilarea tehnicilor de securizare a resurselor transmise prin rețelele de comunicație.
Obiectivele specifice	Înţelegerea metodologiilor de securizare - fizice și logice - a resurselor:. Formarea capacității de extragere, identificare şi specificare a cerinţelor.

	Obținerea cunoştinţelor referitoare la identificarea vunerabilităților și a riscurilor într-o rețea de comunicație. Aplicarea corectă a procedeelor și metodelor de implementare a soluțiilor de combatere a riscurilor depistate într-o rețea de comunicație. Obținerea cunoştinţelor şi abilităţilor de utilizare în detectarea vulnerabilităților într-o rețea. Aplicarea corectă a procedeelor de planificare și gestiune a activităților, îmbunătăţire a procesului de securizare a resurselor fizice și logice dintr-o rețea de comunicație.

7. Conţinutul disciplinei

Tematica activităţilor didactice	**Numărul de ore, învăţământ cu frecvenţă**
T1. Fundamentele securității informației. Modelul CIA (*Confidentiality*, *Integrity*, *Availability*)	2
T2. Criptografie: algoritmi de criptare simetrică și asimetrică. Funcții hash și semnături digitale. Protocoale de schimb de chei (ex. Diffie-Hellman)	4
T3. Parole de acces și securizarea parolelor	2
T4. Protocoale de securitate în rețele	2
T5. Autentificare și controlul accesului. Studii de caz asupra managementului identităților și implementării controalelor de acces	2
T6. Securitatea rețelelor wireless	2
T7. Securitatea aplicațiilor web și mobile	4
T8. Detectarea și prevenirea intruziunilor	2
T9. Securitatea în cloud computing	2
T10. Atacuri cibernetice și metode de apărare	4
T11. Politici și standarde de securitate	2
T12. Analiza riscurilor și managementul incidentelor	2
Total prelegeri:	**30**

Tematica activităţilor didactice	**Numărul de ore, învăţământ cu frecvenţă**
LP1. Studiu de caz. Analiza unui atac informatic și stabilirea componentelor din modelul CIA care au fost afectate	2
LL1. Funcții Hash. Exemple de utilizare	4
LL2. Aplicații pentru generarea și păstrarea sigură a parolelor	4
LL3. Protocoale de securitate: *SSL/TLS* și *Ipsec*, utilizate pentru protecția datelor în tranzit	4
LL4. Autentificarea și autorizarea utilizatorilor în aplicațiile web. Diverse metode de autentificare. Diferența dintre autentificare și autorizarea utilizatorului. Exemple	4
LL5. Identificarea vulnerabilităților specifice rețelelor wireless. Evaluarea riscurilor aferente și propunerea măsurilor de prevenire a riscurilor	4
LL6. Explorarea amenințărilor și a atacurilor asupra aplicațiilor web și ale celor mobile. SQL-injection și XSS	4
LP2. Analiza unui scenariu real de intruziune într-o rețea și aplicarea unor metode de detectare și prevenire	4
LP3. Analizarea unui scenariu real de securitate compromisă în cloud și identificarea măsurilor de prevenire	4

LL7. Realizarea și prezentarea unui referat la tema ”*Prezentarea a trei forme de atac, specifice rețelelor de comunicații*”	4
LP4. Analiza unui incident real pentru a evidenția rolul politicilor/standardelor (ISO/IEC 27001, NIST, OWASP). Aplicarea unor reguli și politici în cadrul unui scenariu simulat	5
LL8. Realizarea unui plan cu potențiale incidente și răspunsuri/ reacții de combatere ale lor	2
Total lucrări de laborator	**45**

8. Referinţe bibliografice

Principale	1. William Stallings, "Network Security Essentials: Applications and Standards", 2011 Pearson Education, Inc., publishing as [Prentice Hall, 1 Lake Street, Upper Saddle River, NJ 07458] 2. William Stallings, "Cryptography and Network Security: Principles and Practice", © Pearson Education Limited 2017 3. Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, "Security in Computing", Copyright © 2015 Pearson Education, Inc. 4. Standarde din domeniu, RFC (Request for Comments) Documents (RFC 5246 (Transport Layer Security - TLS) și RFC 4301 (Security Architecture for IP)) 5. OWASP (Open Web Application Security Project), https://owasp.org/www-project-top-ten/ (accesat 05. 06.2024) 6. NIST Application Security Framework: https://csrc.nist.gov/publications/detail/sp/800-218/final (accesat 05.06.2025) 7. OWASP Mobile Security Testing Guide: https://owasp.org/www-project-mobile-security-testing-guide/ (accesat 05.06.2025) 8. Android Developers Security: https://developer.android.com/topic/security (accesat 05.06.2025)
Suplimentare	9. Coursera - "Computer and Network Security", University of Colorado (Coursera | Degrees, Certificates, & Free Online Courses, accesat 05. 06.2024) 10. edX - "Cybersecurity Fundamentals", Rochester Institute of Technology (Build new skills. Advance your career. | edX, accesat 05. 06.2024)

9. Evaluare

Forma de învățământ	Periodică		Curentă	Lucrul individual	Examen final
	Atestarea 1	Atestarea 2			
Cu frecvenţă	15%	15%	15%	15%	40%
Cu frecvență redusă	25%			25%	50%
Standard minim de performanţă					
Prezenţa şi activitatea la prelegeri, lucrări de laborator; Obţinerea notei minime de „5” la ambele atestări, activitatea curentă, lucrul individual; Obţinerea notei minime de „5” la examenul final.					