

SECURITATE AVANSATĂ A REȚELELOR INFORMATICE

1. Date despre disciplină/modul

Facultatea	Calculatoare, Informatică și Microelectronică				
Departamentul	Inginerie Software și Automatică				
Ciclul de studii	Ciclul II, Studii superioare de master				
Programul de studii	Securitate informațională				
Anul de studii	Semestrul	Tip de evaluare	Categoria formativă	Categoria de opționalitate	Credite ECTS
Anul I (<i>învățământ cu frecvență</i>)	II	E	F – uniate de curs fundamentală	O - unitate de curs obligatorie	5

2. Timpul total estimat

Total ore în planul de învățământ		Din care				
		Ore auditoriale		Lucrul individual		
		Curs	Practice	Proiect de an	Studiul materialului teoretic	Pregătire aplicații
Învățământ cu frecvență	150	20	20	-	60	50

3. Precondiții de acces la disciplină/modul

Conform planului de învățământ	Programarea în limbajul C, Sisteme de operare și limbaje de asamblare, Bazele transmiterii de date, Rețele de calculatoare, administrarea și securitatea rețelor.
Conform competențelor	Inițiere în modelul de referință ISO/OSI, cunoștințe în domeniul transmisiunilor de date, noțiuni de protocoale de rețea, securitatea sistemelor și a rețelor de calculatoare.

4. Condiții de desfășurare a procesului educațional pentru

Curs	Prezentarea materialului teoretic în sala de curs cu ajutorul unui proiector și a unui calculator. Materialele didactice vor fi puse la dispoziția studenților pe pagina de curs de pe serverul pedagogic al catedrei.
Practice	Studenții vor perfecta rapoarte conform condițiilor enunțate în indicațiile metodice. Termenul de predare a lucrării de laborator – doua săptămâni după finalizarea acesteia. Pentru predarea cu întârziere a lucrării aceasta se depunțează cu 0,25 pct./zi de întârziere.

5. Competențe specifice acumulate

Competențe profesionale	Proiectarea sistemelor hardware, software și de comunicații ✓ Descrierea structurală și funcțională a componentelor hardware, software și de comunicații. ✓ Explicarea și înțelegerea destinației, interacțiunii și funcționării componentelor hardware și software de comunicații. ✓ Elaborarea unor componente de comunicații folosind metode de proiectare, limbaje de programare și descriere hardware, algoritmi, structuri de date, protocoale și tehnologii. ✓ Evaluarea caracteristicilor comportamentale și structurale ale rețelor de calculatoare în baza unor metrici. ✓ Proiectarea și implementarea componentelor rețelor de calculatoare. Îmbunătățirea performanțelor sistemelor de comunicații. ✓ Identificarea și descrierea parametrilor de bază ale performanțelor echipamentelor din rețelele de calculatoare. ✓ Explicarea interacțiunii factorilor care determină parametrii de performanță ai rețelor de calculatoare. ✓ Aplicarea de principii și metode de bază pentru determinarea, calcularea și optimizarea parametrilor de performanță ai rețelor de calculatoare. ✓ Dezvoltarea de aplicații pentru monitorizarea și controlul parametrilor de bază ai rețelor de comunicații. Implementarea, testarea, administrarea și mentenanța sistemelor de comunicații ✓ Descrierea instrumentelor de modelare, simulare, verificare și evaluare a performanțelor rețelor de comunicații.
--------------------------------	--

	✓ Utilizarea unor cunoștințe interdisciplinare pentru asigurarea exploatării rețelelor în conformitate cu cerințele domeniului de aplicații. ✓ Utilizarea de principii și metode de bază pentru asigurarea fiabilității, siguranței și securității de funcționare a rețelelor de comunicații. ✓ Testarea, validarea și evaluarea calitativă a caracteristicilor comportamentale și structurale ale rețelelor de calculatoare. Dezvoltarea de sisteme și aplicații pentru întreținerea și exploatarea rețelelor de calculatoare.
Competențe transversale	CT1. Comportarea onorabilă, responsabilă, etică în spiritul legii pentru a asigura îndeplinirea sarcinilor profesionale. CT2. <i>Demonstrarea capacității de lucru în echipă, identificarea rolurilor și responsabilităților individuale și comune, luarea deciziilor și atribuirea de sarcini, cu aplicarea de tehnici de relaționare și muncă eficientă în cadrul echipei</i> CT3. Demonstrarea spiritului de inițiativă și acțiune pentru dezvoltarea profesională și personală prin formare continuă utilizând surse de documentare în limba română și în limbile de circulație internațională.

6. Obiectivele disciplinei/modulului

Obiectivul general	Studierea principiilor de proiectare, administrare și de securizare a unei de rețele de calculatoare, căpătarea deprinderilor practice în administrarea unei rețele în baza sistemului de operare GNU/Linux, a routerelor Cisco, cunoașterea principiilor de și a metodelor de securizare a rețelelor informaționale, căpătarea aptitudinilor practice în configurarea rețelelor cu scopul de a reduce vulnerabilitățile lor,
Obiectivele specifice	Ca rezultat al studiului cursului studentul va cunoaște: • principiile de administrare și de securizare a unei de rețele de calculatoare • metodele de asigurare a confidențialității și a integrității informației transmise prin rețea • principiile de autentificare în rețele; • protocoalele criptografice din Internet • administrarea și utilizarea sistemelor de operare GNU/Linux și Cisco IOS

7. Conținutul disciplinei/modulului

Tematica activităților didactice	Numărul de ore
	învățământ cu frecvență
Tematica cursurilor	
T1. Rețelele informatice ca obiect de securizare	2
T2. Tehnici de proiectare securizată a infrastructurii rețelelor	2
T3. Securizarea perimetrică. Firewall-uri: principii, funcționalități, strategii, tipuri.	2
T4. Metodele criptografice de protecția a informației	2
T5. Metode și protocoale de autentificare	2
T6. Infrastructura cu chei publice (PKI) : servicii, actori, funcționare.	2
T7. Sistemul de criptare PGP (Pretty Good Privacy).	2
T8. Rețele private virtuale (VPN): arhitecturi și tehnologii.	2
T9. Securizarea rețelelor fără fir, a aplicațiilor cloud computing și a Internetului lucrurilor (IoT)	4
Total curs:	20
Tematica lucrărilor practice	
LL1. Comunicația securizată în rețelele informatice: studierea protocolului SSH pentru securizarea comunicațiilor.	4
LL2. Structurarea unei rețele IP securizate, studierea funcționării, configurarea și testarea unui firewall	4
LL3. Studierea structurilor cu chei publice (PKI), configurarea unei CA în baza OpenSSL	4
LL4. Rețele private virtuale.	4
Total lucrări practice:	20

8. Referințe bibliografice

Principale	1. Moise Gabriela; Constantinescu Zoran; Vlădoiu Monica; Dumitru Marius Networking și securitate , Ed. Ploiești Editura Universității Petrol-Gaze din Ploiești 2. Nicolaescu Ștefan Victor Securitatea în rețele Wi-Fi, Ed. AGIR, București, 2008
Suplimentare	3. Oprea Dumitru, Protecția și securitatea informațiilor, Ed, POLIROM, Iasi, 2003

9. Utilizarea IA generativă

Permise de utilizare	Utilizarea IA generative în cadrul temelor și proiectelor este permisă, cu condiția ca studenții să respecte următoarele reguli: - IA generativă poate fi utilizată pentru generarea de idei, structuri de text sau cod, dar toate materialele generate trebuie să fie revizuite și ajustate de către student pentru a se asigura că acestea corespund cerințelor academice. - Orice utilizare a IA generative trebuie să fie declarată în secțiunea de apendice a fiecărei lucrări, folosind fraza: "În timpul pregătirii acestei lucrări, autorul a utilizat [NUME INSTRUMENT / SERVICIU] în scopul [MOTIV]. După utilizarea acestui instrument/serviciu, autorul a revizuit și editat conținutul după cum a fost necesar și își asumă întreaga responsabilitate pentru conținutul lucrării."
Restricții de utilizare	Studenții nu trebuie să considere IA generativă ca o sursă de încredere pentru informații, deoarece nu oferă referințe clare sau surse documentate. - Nu este permisă citarea directă a conținutului generat de IA în lucrările academice ca și cum ar fi sursă primară. - Activitățile în care este interzis utilizarea IA generativă sunt specificare de profesor și sunt de regulă evaluări intermediare și finale sau care nu presupun activități de dezvoltare a competențelor profesionale.

10. Evaluare

Periodică		Curentă	Studiu individual	Proiect/teză	Examen
EP 1	EP 2				
Învățământ cu frecvență					
15%	15%	15%	15%		40%
Standard minim de performanță					
Prezența și activitatea la prelegeri și lucrări practice.					
Obținerea notei minime de „5” la fiecare dintre atestări și lucrări practice.					

11. Criterii de evaluare

Activitate	Componente evaluare	Metodă de evaluare, criterii de evaluare	Pondere în nota finală a activității	Ponderea în evaluarea disciplinei
Evaluare periodică I	Conținut teoretic Teme 1-4	Test electronic pe platforma else.fcim.utm.md	100%	15%
Evaluare periodică II	Conținut teoretic Teme 5-8	Test electronic pe platforma else.fcim.utm.md	100%	15%
Evaluare curentă	Participare, lucrări practice, rapoarte	Participarea la activități, calitatea și acuratețea realizării lucrărilor practice, pregătirea și susținerea rapoartelor	100%	15%
Studiul individual	Prezentarea unui articol științific	Prezentare orală/discurs la tema articolului în fața colegilor; evaluarea coerenței, clarității și documentării	100%	15%
Evaluarea finală	Conținut teoretic și practic	Test electronic pe platforma else.fcim.utm.md	100%	40%