MD-2004, CHIŞINĂU, STR. ŞTEFAN CEL MARE 168, TEL: 022 23-54-41 | www.utm.md

S.05.O.038 SECURITATEA INFORMAȚIONALĂ

1. Date despre disciplină/modul

Facultatea	Electronică și Telecomunicații				
Departamentul	Telecomunicații și Sisteme Electronice				
Ciclul de studii	Studii superioare de licență, ciclul I				
Programul de studii	**0714.2 REȚELE ȘI SOFTWARE DE TELECOMUNICAȚII**				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opționalitate**	**Credite ECTS**
III - învățământ cu frecvență IV - învățământ cu frecvență redusă	V VII	E	S – unitate de curs de specialitate	O – disciplină obligatorie	5

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
180	45	15/15	-	45	45
180	16	12/8	-	70	74

3. Precondiții de acces la disciplină/modul

Conform planului de învățământ	Pentru a atinge obiectivele cursului studenții trebuie să posede cunoștințe generale despre sisteme electronice digitale, despre Internet, despre arhitectura calculatorului (software și hardware), despre tehnologii și dispozitive de comunicații wireless (fără fir). În plus, studentul trebuie să fie capabil să utilizeze instrumente software pentru modelarea și simularea circuitelor și dispozitivelor electronice.
Conform competențelor	Abilitățile obținute în cadrul studierii disciplinei „Securitatea Informației” includ capacitatea de a analiza și identifica vulnerabilitățile și amenințările cibernetice, de a implementa măsuri de protecție în rețele și sisteme informatice și de a utiliza soluții software și hardware avansate pentru asigurarea securității datelor și dispozitivelor endpoint. Studenții vor dezvolta competențe practice în configurarea și administrarea rețelelor, în utilizarea instrumentelor de securitate, precum firewall-uri, sisteme de detecție a intruziunilor (IDS) și soluții antivirus, și vor învăța să aplice metode de criptare și autentificare pentru protecția informațiilor. Totodată, aceștia vor fi capabili să monitorizeze activitatea sistemelor pentru a identifica și remedia atacurile cibernetice, contribuind astfel la prevenirea riscurilor și la menținerea integrității infrastructurilor informatice.

4. Condiții de desfășurare a procesului educațional pentru

Curs	Pentru prezentarea materialului în sala de curs sunt necesare tabla interactivă/ proiector și calculator.
Laborator/ Seminar	Laboratoarele vor avea loc digital în platforma de e-learning netacad.com.

5. Competențe specifice acumulate

Competențe profesionale	**C4. Orgartizarea eficientă a activității și operarea serviciilor multimedia, bazate pe înțelegerea si aplicarea noțiunilor fundamentale din domeniul comunicațiilor si transmisiunii informației și conceperea implementării metodelor de estimare al eficienței economice de dezvoltare a domeniului de comunicații electronice.** C4.1. Identificarea conceptelor fundamentale referitoare la transmisiunea informației și la comunicațiile analogice si digitale. C4.2. Explicarea si interpretarea principalelor cerințe și tehnici specifice de abordare pentru transmisiile.de date, voce, video, multimedia. C.4.3. Rezolvarea de probleme practice utilizând cunoștințe generale privind tehnicile multimedia. C.4.4. Utilizarea principalilor parametri specifici în evaluări bazate pe conceptul de calitate a serviciilor în comunicații.

	C.4.5. Organizarea și monitorizarea activităților entităților economice în conformitate cu cadrul normativ și exigențele mediului de afaceri. C4.6. Dezvoltarea relațiilor productive de colaborare în cadrul echipelor; aplicarea și raționalizarea instrumentelor de motivare a participanților acestora; **C5. Integrarea, exploatarea și managementul comunicațiilor electronice în diferite domenii ale economiei naționale.** C5.1. Definirea principiilor ce stau la baza principalelor tehnologii de telecomunicații, fixe și mobile, prin diverse.medii de transmisiune. C5.2. Explicarea si interpretarea tehnologiilor si protocoalelor fundamentale pentru sistemele integrate de comunicații fixe si mobile. C.5.3. Instalarea, configurarea și exploatarea rețelelor de comunicații. C.5.4. Utilizarea tehnicilor de evaluare și diagnoza a sistemelor și echipamentelor de comunicații. C.5.5. Asigurarea cu mijloace de comunicații a unei locații cu grad de complexitate mic/mediu. C.5.6. Aplicarea instrumentelor manageriale de evaluare a eficacității și eficienței activităților, de intentificare și mobilizare optimă a rezervelor și măsurilor de sporire a eficacității și eficienții. **C6. Utilizatea tehnologiilor informalionale specifice domeniului în scopul organizării soluționării problemelor tipice rețelelor de comunicații de banda largă și realizarea lucrărilor de evidență contabilă, financiară în domeniul cominicațiilor electronice.** C6.1. Identificarea/ Definirea/Prezentarea legilor câmpului electromagnetic în abordarea problemelor specifice propagării și transmisiei, precum și a circuitelor specifice. C6.2. Explicarea metodelor specifice de implementare a tehnicilor de comunicații. C.6.3. Rezolvarea de probleme practice utilizând metode de proiectare a circuitelor de microunde, planificare, acoperire, selecție și amplasareaechipamentelor de emisie-recepție C.6.4. Utilizarea principalilor parametri de calitate și a tehnicilor de măsură specifice mediilor de propagare și transmisie. C.6.5. Elaborarea de proiecte de complexitate mica/medie privind echipamentele de emisie/recepție. C. 6.6. Elaborarea și coordonarea proiectelor aferente administrării afacerilor prin utilizarea eficientă a resurselor organizaționale

6. Obiectivele disciplinei/modulului

Obiectivul general	Cunoașterea, configurarea, mentenanța și depanarea rețelelor, sistemelor de operare și dispozitivelor endpoint, cu scopul asigurării securității informației.
Obiectivele specifice	• Cunoașterea tipurilor de amenințări și vulnerabilități asociate securității dispozitivelor endpoint; • Familiarizarea cu metodele de configurare și protejare a sistemelor de operare Windows și Linux pentru securitate; • Folosirea simulatoarelor și instrumentelor de analiză pentru formarea deprinderilor practice necesare protejării dispozitivelor endpoint.

7. Conţinutul disciplinei/modulului

Tematica activităţilor didactice	**Numărul de ore** **învăţământ cu frecvenţă/ frecvenţă redusă**
Tematica prelegerilor	
T1. Amenințări și vulnerabilități cibernetice – tipuri și caracteristici. Tipurile principale de amenințări (phishing, ransomware, spyware) și vulnerabilități comune (software neactualizat, configurări greșite). Caracteristici și impact asupra dispozitivelor endpoint.	**4/1**
T2. Metode de atac asupra sistemelor endpoint și tehnici de protecție. Identificarea atacurilor asupra endpoint-urilor (exploatare vulnerabilități, brute-force, injectare cod). Tehnici pentru detectarea și protejarea dispozitivelor împotriva acestor atacuri.	**6/2**
T3. Securitatea fizică și informațională a dispozitivelor endpoint. Măsuri de securitate fizică (acces controlat, protecția hardware) și protecția datelor stocate (criptare, parole). Importanța politicilor de securitate pentru prevenirea accesului neautorizat.	**5/1**
T4. Principii de autentificare și control al accesului în rețele endpoint. Metode de autentificare (parole, 2FA, biometrie) și rolul lor în securizarea endpoint-urilor. Principii de control al accesului bazate pe roluri și politici.	**6/2**

Tematica activităţilor didactice	Numărul de ore învăţământ cu frecvenţă/ frecvenţă redusă
T5. Aplicații software pentru monitorizarea și securizarea dispozitivelor endpoint. Utilizarea aplicațiilor software (antivirus, EDR, firewall) pentru monitorizarea activităților suspecte și implementarea securității la nivel endpoint.	**6/2**
T6. Mecanisme de criptare și integritatea datelor în sisteme endpoint. Metode de criptare (simetrică și asimetrică) pentru protejarea datelor. Tehnici pentru asigurarea integrității datelor utilizând hashing și semnături digitale.	**5/1**
T7. Securitatea sistemelor de operare Windows și Linux. Configurarea și securizarea sistemelor Windows și Linux. Utilizarea actualizărilor, permisiunilor și politicilor pentru reducerea riscurilor.	**2/1**
T8. Detectarea și protejarea împotriva malware-ului pe dispozitive endpoint. Metode de identificare a malware-ului (viruși, troieni, ransomware) și implementarea soluțiilor antimalware pentru eliminare și prevenire.	**3/2**
T9. Implementarea soluțiilor de protecție endpoint: Antivirus, HIDS, NIDS. Configurarea și utilizarea soluțiilor precum antivirus, sisteme de detecție a intruziunilor (HIDS, NIDS) pentru protejarea dispozitivelor endpoint.	**4/2**
T10. Evaluarea riscurilor și măsurile de prevenire în securitatea endpoint. Metode pentru evaluarea riscurilor de securitate (analiza vulnerabilităților, scanare). Implementarea măsurilor preventive pentru protejarea dispozitivelor și rețelelor endpoint.	**4/2**
Total curs:	**45/16**
Tematica lucrărilor practice	
L.P1. Configurarea și utilizarea instrumentelor pentru detectarea amenințărilor endpoint.	**2/1**
L.P2. Implementarea soluțiilor antivirus și antimalware pe sistemele endpoint.	**2/1**
L.P3. Analiza și remedierea vulnerabilităților dintr-un sistem Windows/Linux.	**2/1**
L.P4. Configurarea autentificării și controlului accesului pe dispozitive endpoint.	**2/1**
L.P5. Utilizarea log-urilor pentru identificarea atacurilor asupra sistemelor endpoint.	**2/1**
L.P6. Instalarea și configurarea firewall-urilor pentru protecția endpoint.	**2/1**
L.P7. Simularea atacurilor cibernetice și aplicarea măsurilor de protecție.	**2/1**
L.P8. Aplicarea metodelor de criptare pentru protejarea datelor pe endpoint-uri.	**1/1**
Total lucrări practice:	**15/8**
Tematica lucrărilor de laborator	
L.L1. Configurarea și utilizarea instrumentelor de monitorizare a securității endpoint.	**4/2**
L.L2. Instalarea și configurarea unui sistem de detecție a intruziunilor (IDS).	**4/2**
L.L3. Detectarea și izolarea malware-ului folosind aplicații specifice.	**4/1,5**
L.L4. Implementarea mecanismelor de backup și restaurare a datelor endpoint.	**8/2**
L.L5. Configurarea protocoalelor de securitate pentru accesarea resurselor în rețele endpoint.	**2/1,5**
L.L6. Analiza traficului de rețea și identificarea activităților suspecte.	**2/1,5**
L.L7. Simularea atacurilor de tip phishing și măsuri de prevenire pe endpoint-uri.	**6/1,5**
Total lucrărări de laborator:	**30/12**

8. Referinţe bibliografice

Principale	1. CISCO Networking Academy, Endpoint Security www.netacad.com
Suplimentare	1. Leitner Achim, "Reţele WLAN sigure, cu un tunel OpenVPN criptat", Linux Magazin, nr. 22, iunie 2005; 2. Lachi A., Securitatea Sistemelor Informaționale, Partea I, Îndrumar de laborator, UTM, Chișinău, 2015;

9. Evaluare

Periodică		Curentă	Studiul individual	Examen
EP 1	**EP 2**			
15%	**15%**	**15%**	**15%**	**40%**

Standard minim de performanţă:
Prezența și activitatea la prelegeri, lucrările practice și lucrările de laborator;
Obținerea notei minime de ”5” la evaluările periodice (EP1 și EP2), curentă și studiul individual al studentului privind temele la prelegeri, lucrările practice și lucrările de laborator;
Obținerea notei minime de ”5” la evaluarea finală.