

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	UNIVERSITATEA DIN ORADEA
1.2 Facultatea	Facultatea de Inginerie Electrică și Tehnologia Informației
1.3 Departamentul	Departamentul de Electronică și Telecomunicații
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicații și Tehnologii Informaționale
1.5 Ciclul de studii	Licență (ciclul I)
1.6 Programul de studii/Calificarea	Rețele și Software de Telecomunicații / Inginer

2. Date despre disciplină

2.1 Denumirea disciplinei	Securitatea comunicațiilor de date						
2.2 Titularul activităților de curs	Ș.I. dr. ing. TEPELEA LAVINIU						
2.3 Titularul activităților de laborator	Ș.I. dr. ing. TEPELEA LAVINIU						
2.4 Anul de studiu	IV	2.5 Semestrul	VIII	2.6 Tipul de evaluare	VP	2.7 Regimul disciplinei	O

(I) Impusă; (O) Opțională; (F) Facultativă

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	3	din care: 3.2 curs	2	3.3 Seminar/laborator/proiect	-/1/-
3.4 Total ore din planul de învățământ	42	din care: 3.5 curs	28	3.6 laborator	14
Distribuția fondului de timp					33
Studiul după manual, suport de curs, bibliografie și notițe					9
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					9
Pregătire laboratoare, teme, referate, portofolii și eseuri					7
Tutoriat					-
Examinări					8
Alte activități.....					-
3.7 Total ore studiu individual	33				
3.9 Total ore pe semestru	75				
3.10 Numărul de credite	3				

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	
4.2 de competențe	

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Sală de curs dotată cu calculator, software adecvat și video proiector, dar și online pe platforma e.uoradea.ro si programul Microsoft Teams, în funcție de situația pandemiei Covid
5.2. de desfășurare a laboratorului	Sală de laborator dotată cu calculatoare și software dedicat, dar și online pe platforma e.uoradea.ro si programul Microsoft Teams, în funcție de situația pandemiei Covid

6a. Competențele specifice acumulate	
Competențe profesionale	C7. Dezvoltă software cu sursă deschisă C8. Estimează costurile instalării de dispozitive de telecomunicații; C9. Sprijină utilizatorii sistemelor TIC
Competențe transversale	

6b. Rezultatele așteptate ale învățării	
Cunoștințe	Studentul/absolventul trebuie să descrie, să analizeze și să aplice principiile fundamentale, metodele și algoritmi de criptare (simetrică și asimetrică), de autentificare și de asigurare a integrității datelor în scopul securizării comunicațiilor în diverse arhitecturi de rețea.
Aptitudini	Studentul/absolventul selectează, configurează și implementează algoritmi criptografici (e.g., AES, RSA, funcții hash, semnături digitale) pentru a asigura confidențialitatea, integritatea și autentificarea datelor transmise în rețele. Studentul/absolventul operează și configurează instrumente și protocoale criptografice standard (e.g., SSL/TLS, IPsec, SSH, PGP) și utilizează medii de programare (e.g., Python, C++) pentru simularea și testarea mecanismelor de securitate. Studentul/absolventul evaluează performanța și rezistența schemelor criptografice implementate la atacuri comune și proiectează soluții de securitate adaptate cerințelor specifice ale arhitecturilor de rețea.
Responsabilitate și autonomie	Studentul/absolventul manifestă responsabilitate în gestionarea și protecția datelor sensibile, acționând autonom pentru a se menține la curent cu cele mai noi vulnerabilități și standarde criptografice din domeniul securității cibernetice.

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Familiarizarea studenților cu cele mai uzuale tehnici de securizare a rețelelor de calculatoare.
7.2 Obiectivele specifice	Cunoașterea tipurilor de atacuri informatice. Capacitatea de auditare a rețelelor de calculatoare. Cunoașterea principalelor protocoale de securitate web și pentru rețele de calculatoare. Cunoașterea modalităților de atac asupra aplicațiilor web și protejarea aplicațiilor. Cunoașterea metodelor de securizare a rețelelor wireless. Cunoașterea metodelor de securizare a comerțului electronic.

8. Conținut

8.1 Curs	Metode de predare	Nr. Ore / Observații
1. Introducere. Ce înseamnă securitate în domeniul rețelelor de calculatoare.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
2. Tipuri de atacuri informatice. Complexitatea atacurilor.	Prelegerea. Explicația.	2

	Descrierea. Exemplificarea.	
3. Tipuri de auditări în privința securității: Security audit, Vulnerability scanning, Penetration testing.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
4. Securitatea rețelelor de calculatoare la nivel IP. Firewall, VPN.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
5. Securitatea rețelelor de calculatoare la nivel IP. SSL, Remote Access.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
6. Rolul criptografiei în securitatea rețelelor. Algoritmi de criptare utilizați. Funcții Hash, integritatea datelor.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
7. Autentificare și autorizare. Securitatea rețelelor wireless.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
8. Metode de autentificare. Kerberos, Biometrie, PKI, Single Sign On.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
9. Protocoale și servere de securitate. IPSEC, Kerberos, Sesame, Radius.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
10. Securitatea poștei electronice. Autentificarea prin DKIM. Mecanisme antispam. PGP	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
11. Vulnerabilități de tipul social engineering. Asigurarea intimității utilizatorului.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
12. Securitatea aplicațiilor web. Exploit, SQL injection.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
13. Securitatea aplicațiilor web. Cross Site Scripting (XSS), Depasiri de zone tampon (buffer overflows).	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
14. Securitatea comerțului electronic. Semnătura digitală, certificatul digital.	Prelegerea. Explicația. Descrierea. Exemplificarea.	2
Bibliografie: 1. A. Medvinsky, <i>Addition to Kerberos Cipher Suites to Transport Layer Security (TLS)</i> (RFC 2712), Excite, 1999 2. ***, <i>Encyclopedia of Cryptography and Security</i> , Editor-in-chief Henk C.A. van Tilborg, Eindhoven University of Technology The Netherlands, Springer, ISBN-13: (e-book) 978-0387-23483-0, 2005 3. A. Menezes, P. van Oorschot and S. Vanstone, <i>Handbook of Applied Cryptography</i> , CRC Press, 1997 4. Alan O. Freier, Philip Karlton, Paul C. Kocher, <i>The SSL Protocol</i> , Version 3.0 (Internet Draft), Transport Layer Security Working Group, 1996 5. Tanenbaum, A.S., <i>Computer Networks</i> , 4 th edition, Prentice-Hall, New Jersey, 2003. 6. V. Patriciu, <i>Criptografia și securitatea rețelelor de calculatoare</i> , Ed. Tehnica, 1994 7. P. Reid, <i>Biometrics for Network Security</i> , Prentice Hall PTR, 2003 8. Roy H. Campbell, M. Dennis Mickusas, Monika Chandak, <i>Sesame Authentication protocol</i> , University of Illinois at Urbana-Champaign, 1999 9. Rhodes-Ousley, M., Bragg, R., Strassberg, K., <i>Network security: The complete reference</i> , McGraw-Hill, 2003. 10. V. Stallings, <i>Cryptography and Network Security</i> , Prentice Hall, 1999 11. Ogletree, T.W., <i>Firewalls – Protecția rețelelor conectate la Internet</i> , Teora, 2001.		

8.2 Seminar	Metode de predare	Nr. Ore / Observații
8.3 Laborator		
1. Configurarea unui firewall, software VPN, software remote access.	Descrierea. Explicația. Exemplificarea. Verificarea.	2
2. Verificarea securității rețelei. Software: NMAP, ZENMAP, NESSUS.	Descrierea. Explicația. Exemplificarea. Verificarea.	2
3. Descoperirea vulnerabilităților. Software: Nikto, Nessus, OpenVAS, WebScarab	Descrierea. Explicația. Exemplificarea. Verificarea.	2
4. Atacuri MITM (man-in-the-middle) în rețeaua locală. Software: BackTrack, Wireshark.	Descrierea. Explicația. Exemplificarea. Verificarea.	2
5. Atacuri online și offline wireless. Software: BackTrack, Aircrack.	Descrierea. Explicația. Exemplificarea. Verificarea.	2
6. Studii de caz privind utilizarea protocoalelor de securitate web. Software: Wireshark.	Descrierea. Explicația. Exemplificarea. Verificarea.	2
7. Exploatarea vulnerabilităților aplicațiilor web. Software: METASPLOIT.	Descrierea. Explicația. Exemplificarea. Verificarea.	2
8.4 Proiect	-	-
Bibliografie: 1. A. Medvinsky, <i>Addition to Kerberos Cipher Suites to Transport Layer Security (TLS)</i> (RFC 2712), Excite, 1999 2. Alan O. Freier, Philip Karlton, Paul C. Kocher, <i>The SSL Protocol</i> , Version 3.0 (Internet Draft), Transport Layer Security Working Group, 1996 3. Tanenbaum, A.S., <i>Computer Networks</i> , 4 th edition, Prentice-Hall, New Jersey, 2003. 4. V. Patriciu, <i>Criptografia și securitatea rețelelor de calculatoare</i> , Ed. Tehnica, 1994 5. P. Reid, <i>Biometrics for Network Security</i> , Prentice Hall PTR, 2003 6. Roy H. Campbell, M. Dennis Mickus, Monika Chandak, <i>Sesame Authentication protocol</i> , University of Illinois at Urbana-Champaign, 1999 7. Rhodes-Ousley, M., Bragg, R., Strassberg, K., <i>Network security: The complete reference</i> , McGraw-Hill, 2003. 8. Ogletree, T.W., <i>Firewalls – Protecția rețelelor conectate la Internet</i> , Teora, 2001.		

9. Coroborarea conținutului disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Cunoașterea tipurilor de atacuri informatice și a modalităților de auditare a rețelelor de calculatoare.	Verificare pe parcurs prin două teste scrise sau două teste grilă în cazul evaluării online	70%
10.5 Seminar	-	-	-
10.6 Laborator	Acumularea cunoștințelor din partea teoretică și utilizarea practică a aplicațiilor.	Un procent de 10% din nota finală de la laborator, se acordă pentru finalizarea cu succes a tematicii de studiu individual. Verificarea acumulării cunoștințelor și a abilității de utilizare a aplicațiilor practice.	30%
10.7 Proiect	-	-	-
10.8 Standard minim de performanță: Cunoașterea tipurilor de atacuri informatice. Capacitatea de auditare a rețelelor de calculatoare. Capacitatea de configurare a unui firewall și a unui software VPN. Cunoștințe pentru nota 5: Cunoașterea tipurilor de atacuri informatice. Capacitatea de configurare a unui firewall și a unui software VPN.			

Data completării:

09.09.2026

Data avizării în

Departament:

10.09.2026

Data aprobării în
Consiliul Facultății:
.09.2026

Semnătura titularului de curs:

Ș.l. dr. ing. Țepelea Laviniu

ltepelea@uoradea.ro

<https://prof.uoradea.ro/ltepelea/>

Semnătura titularului de
seminar/laborator:

Ș.l. dr. ing. Țepelea Laviniu

ltepelea@uoradea.ro

<https://prof.uoradea.ro/ltepelea/>

Director de Departament,

Ș.l. dr. ing. Adrian-Traian Burcă

aburca@uoradea.ro

Decan,

Conf. univ. dr. ing. Eugen Ioan Gergely

egergely@uoradea.ro