FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**UNIVERSITATEA DIN ORADEA**
1.2 Facultatea	**Facultatea de Inginerie Electrică şi Tehnologia Informaţiei**
1.3 Departamentul	**Departamentul de Electronică şi Telecomunicaţii**
1.4 Domeniul de studii	**Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale**
1.5 Ciclul de studii	**Licenţă (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 activităţilor de curs				**Ș.l. dr. ing. ȚEPELEA LAVINIU**			
2.3 Titularul activităţilor de laborator				**Ș.l. dr. ing. ȚEPELEA 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) Opţională; (F) Facultativă

3. Timpul total estimat (ore pe semestru al activităţilor 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 învăţământ	42	din care: 3.5 curs	28	3.6 laborator	14
Distribuţia fondului de timp					33
Studiul după manual, suport de curs, bibliografie şi notiţe					9
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					9
Pregătire laboratoare, teme, referate, portofolii şi eseuri					7
Tutoriat					-
Examinări					8
Alte activităţi.....					-

3.7 Total ore studiu individual	**33**
3.9 Total ore pe semestru	**75**
3.10 Numărul de credite	**3**

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	
4.2 de competenţe	

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare 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 desfăşurare 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. Competenţele specifice acumulate	
Competenţe profesionale	**C4. Selectarea, instalarea şi exploatarea echipamentelor de comunicaţii, fixe şi mobile, precum şi planificarea, configurarea şi integrarea serviciilor de telecomunicaţii şi elemente de securitatea informaţiei** **C5. Analiza şi adaptarea arhitecturilor, tehnologiilor şi protocoalelor de comunicaţii pentru aplicaţii suport de reţele locale, metropolitane, de arie mare şi integrate:** **C6. Utilizarea unor limbaje şi instrumente specializate pentru inginerie software, cu orientare către sistemele de telecomunicaţii integrate:**
Competenţe transversale	

6b. Rezultatele aşteptate ale învăţării	
Cunoştiinţe	Studentul/absolventul trebuie să descrie, să analizeze și să aplice principiile fundamentale, metodele și algoritmii 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 (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Familiarizarea studenţilor cu cele mai uzuale tehnici de securizare a retelelor de calculatoare.
7.2 Obiectivele specifice	Cunoaşterea tipurilor de atacuri informatice. Capacitatea de auditare a retelelor de calculatoare. Cunoaşterea principalelor protocoale de securitate web si pentru reţele de calculatoare. Cunoaşterea modalităţilor de atac asupra aplicaţiilor web si protejarea aplicaţiilor. Cunoaşterea metodelor de securizare a retelelor wireless. Cunoaşterea metodelor de securizare a comerţului electronic.

8. Conţinut

8.1 Curs	Metode de predare	Nr. Ore / Observaţii
1. Introducere. Ce înseamnă securitate in domeniul retelelor de calculatoare.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
2. Tipuri de atacuri informatice. Complexitatea atacurilor.	Prelegerea. Explicaţia.	2

	Descrierea. Exemplificarea.	
3. Tipuri de auditări in privința securității: Security audit, Vulnerability scanning, Penetration testing.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
4. Securitatea retelelor de calculatoare la nivel IP. Firewall, VPN.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
5. Securitatea retelelor de calculatoare la nivel IP. SSL, Remote Access.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
6. Rolul criptografiei in securitatea retelelor. Algoritmi de criptare utilizaţi. Funcţii Hash, integritatea datelor.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
7. Autentificare si autorizare. Securitatea retelelor wireless.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
8. Metode de autentificare. Kerberos, Biometrie, PKI, Single Sign On.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
9. Protocoale si servere de securitate. IPSEC, Kerberos, Sesame, Radius.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
10. Securitatea poștei electronice. Autentificarea prin DKIM. Mecanisme antispam. PGP	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
11. Vulnerabilități de tipul social engineering. Asigurarea intimității utilizatorului.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
12. Securitatea aplicaţiilor web. Exploit, SQL injection.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
13. Securitatea aplicațiilor web. Cross Site Scripting (XSS), Depasiri de zone tampon (buffer overflows).	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2
14. Securitatea comerţului electronic. Semnătura digitala, certificatul digital.	Prelegerea. Explicaţia. Descrierea. Exemplificarea.	2

Bibliografie:

1. A. Medvinsky, *Addition to Kerberos Cipher Suites to Transport Layer Security (TLS)* (RFC 2712), Excite, 1999
2. ***, *Encyclopedia of Cryptography and Security*, 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, *Handbook of Applied Cryptography*, CRC Press, 1997
4. Alan O. Freier, Philip Karlton, Paul C. Kocher, *The SSL Protocol*, Version 3.0 (Internet Draft), Transport Layer Security Working Group, 1996
5. Tanenbaum, A.S., *Computer Networks*, 4 th edition, Prentice-Hall, New Jersey, 2003.
6. V. Patriciu, *Criptografia si securitatea retelelor de calculatoare*, Ed. Tehnica, 1994
7. P. Reid, *Biometrics for Network Security*, Prentice Hall PTR, 2003
8. Roy H. Campbell, M. Dennis Mickusas, Monika Chandak, *Sesame Authentication protocol*, University of Illinois at Urbana-Champaign, 1999
9. Rhodes-Ousley, M., Bragg, R., Strassberg, K., *Network security: The complete reference*, McGraw-Hill, 2003.
10. V. Stalling, *Cryptography and Network Security*, Prentice Hall, 1999
11. Ogletree, T.W., *Firewalls – Protecţia reţelelor conectate la Internet*, Teora, 2001.

8.2 Seminar	Metode de predare	Nr. Ore / Observaţii
8.3 Laborator		
1. Configurarea unui firewall, software VPN, software remote access.	Descrierea. Explicaţia. Exemplificarea. Verificarea.	2
2. Verificarea securităţii reţelei. Software: NMAP, ZENMAP, NESSUS.	Descrierea. Explicaţia. Exemplificarea. Verificarea.	2
3. Descoperirea vulnerabilităților. Software: Nikto, Nessus, OpenVAS, WebScarab	Descrierea. Explicaţia. Exemplificarea. Verificarea.	2
4. Atacuri MITM (man-in-the-middle) in reţeaua locala. Software: BackTrack, Wireshark.	Descrierea. Explicaţia. Exemplificarea. Verificarea.	2
5. Atacuri online si offline wireless. Software: BackTrack, Aircrack.	Descrierea. Explicaţia. Exemplificarea. Verificarea.	2
6. Studii de caz privind utilizarea protocoalelor de securitate web. Software: Wireshark.	Descrierea. Explicaţia. Exemplificarea. Verificarea.	2
7. Exploatarea vulnerabilităţilor aplicaţiilor web. Software: METASPLOIT.	Descrierea. Explicaţia. Exemplificarea. Verificarea.	2
8.4 Proiect	-	-

Bibliografie:

1. A. Medvinsky, *Addition to Kerberos Cipher Suites to Transport Layer Security (TLS)* (RFC 2712), Excite, 1999
2. Alan O. Freier, Philip Karlton, Paul C. Kocher, *The SSL Protocol*, Version 3.0 (Internet Draft), Transport Layer Security Working Group, 1996
3. Tanenbaum, A.S., *Computer Networks*, 4 th edition, Prentice-Hall, New Jersey, 2003.
4. V. Patriciu, *Criptografia si securitatea retelelor de calculatoare*, Ed. Tehnica, 1994
5. P. Reid, *Biometrics for Network Security*, Prentice Hall PTR, 2003
6. Roy H. Campbell, M. Dennis Mickusas, Monika Chandak, *Sesame Authentication protocol*, University of Illinois at Urbana-Champaign, 1999
7. Rhodes-Ousley, M., Bragg, R., Strassberg, K., *Network security: The complete reference*, McGraw-Hill, 2003.
8. Ogletree, T.W., *Firewalls – Protecţia reţelelor conectate la Internet*, Teora, 2001.

9. Coroborarea conţinutului disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi 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	Cunoasterea tipurilor de atacuri informatice si a modalitatilor de auditare a retelelor de calculatoare.	Verificare pe parcurs prin doua teste scrise sau două teste grilă în cazul evaluarii online	70%
10.5 Seminar	-	-	-
10.6 Laborator	Acumularea cunostintelor din partea teoretica si utilizarea practica a aplicatiilor.	Un procent de 10% din nota finala de la laborator, se acorda pentru finalizarea cu succes a tematicii de studiu individual. Verificarea acumularii cunostintelor si a abilitatii de utilizare a aplicatiilor practice.	30%
10.7 Proiect	-	-	-

10.8 Standard minim de performanţă:

Cunoaşterea tipurilor de atacuri informatice. Capacitatea de auditare a retelelor de calculatoare. Capacitatea de configurare a unui firewall si a unui software VPN.

Cunostinte pentru nota 5:

Cunoaşterea tipurilor de atacuri informatice. Capacitatea de configurare a unui firewall si a unui software VPN.

Data completării:	Semnătura titularului de curs:	Semnătura titularului de seminar/laborator:
08.09.2025	Ș.l. dr. ing. Țepelea Laviniu ltepelea@uoradea.ro https://prof.uoradea.ro/ltepelea/	Ș.l. dr. ing. Țepelea Laviniu ltepelea@uoradea.ro https://prof.uoradea.ro/ltepelea/

Data avizării în Departament:
24.09.2025

Director de Departament,
Ș.l. dr. ing. Adrian-Traian Burcă
aburca@uoradea.ro

Data aprobării în Consiliul Facultăţii:
25.09.2025

Decan,
Conf. univ. dr. ing. Eugen Ioan Gergely
egergely@uoradea.ro