

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	CALCULATOARE si TEHNOLOGIA INFORMATIEI
1.4 Domeniul de studii	TEHNOLOGIA INFORMATIEI
1.5 Ciclu de studii	LICENȚĂ
1.6 Programul de studii/Calificarea	Tehnologia Informației

2. Date despre disciplină

2.1 Denumirea disciplinei	Securitatea datelor						
2.2 Titularul activităților de curs	Prof.univ.dr.habil. Daniela Elena POPESCU						
2.3 Titularul activităților de laborator/proiect	Prof.univ.dr.habil. Daniela Elena POPESCU						
2.4 Anul de studiu	III	2.5 Semestrul	6	2.6 Tipul de evaluare	Ex	2.7 Regimul disciplinei	DS

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

3.1 Număr de ore pe săptămână	4	din care: 3.2 curs	2	3.3 laborator /proiect	1/1
3.4 Total ore din planul de învățământ	56	din care: 3.5 curs	28	3.6 laborator /proiect	28
Distribuția fondului de timp ore					ore
Studiul după manual, suport de curs, bibliografie și notițe					28
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					8
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					14
Tutoriat					2
Examinări					4
Alte activități.....					
3.7 Total ore studiu individual	56				
3.9 Total ore pe semestru	112				
3.10 Numărul de credite	4				

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Sisteme de operare	
4.2 de competențe	Arhitecturi de sisteme de calcul	

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	- Cursul se poate desfășura față în față sau on-line” - prezență la minim 50% din cursuri	- prezen
5.2. de desfășurare a laboratorului /proiectului	- Seminarul/laboratorul/proiectul se pot desfășura față în față sau on-line - Prezența obligatorie la toate laboratoarele; - Studenții trebuie să fi parcurs partea teoretică a lucrării; - Se pot recupera pe parcursul semestrului maxim 4 lucrări (30 %); - Frecvența la orele de laborator sub 70% conduce la refacerea disciplinei	- Prezen - Studen - Se pot - Frecve

6.a. Competențele specifice acumulate

Competențe profesionale	CG1. Analizează, proiectează și dezvoltă sisteme informatice software și hardware. CG2. Asigură calitatea, securitatea și performanța sistemelor informatice. CG4. Se adaptează la noile tendințe tehnologice și dezvoltă soluții inovatoare Competențe ESCO C7. Aplică politici de securitate informatică
Competențe transversale	CT1. Gândește analitic CT2. Lucrează în echipe

6.b. Rezultatele așteptate ale învățării

Cunoștințe	Studentul/absolventul are cunoștințe solide despre securitatea informațională, criptografie și protecția datelor.
Aptitudini	Studentul/absolventul aplică algoritmi de criptografie, configurează politici de securitate/toleranță la defecte și implementează măsuri de protecție a informațiilor.
Responsabilitate și autonomie	Studentul/absolventul răspunde de securitatea sistemelor informatice și manifestă responsabilitate profesională, respectând standardele de protecție a datelor.

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

7.1 Obiectivul general al disciplinei	Familiarizarea studenților cu elementele definiției pentru implementarea și creșterea nivelului de securitate a informațiilor la nivel organizațional precum și identificarea strategiilor sănătoase de dezvoltare instituțională sub acest aspect
7.2 Obiectivele specifice	- Disciplina are ca obiectiv familiarizarea studenților cu problemele de securitate a informației, cu ceea ce reprezintă vulnerabilitățile datelor, cu modul în care se pune problema protecției sistemelor atât neconectate în rețea cât și a celor conectate în rețea. - Cursul își propune prezentarea caracteristicilor de bază ale problemelor de securizare a informației, având ca scop dezvoltarea capacităților de dezvoltare a politici de securitate în ansamblu în vederea protejării informației - Laboratoarele sunt orientate spre prezentarea în prima fază a problemelor de Securitate la nivelul sistemelor de calcul, după care accentul cade asupra dezvoltării abilităților de utilizarea a tool-urilor utile pentru scanarea și identificarea vulnerabilităților, pe prezentarea etapelor și a modului în care se realizează testele de penetrării a sisteme, precum și protecțiilor ce se pot lua în acest sens

8. Conținuturi

8.1.Curs	Metode de predare	Observații
1. Introducere în securitatea datelor ○ Definiții și concepte de bază ○ Importanța securității datelor 2. Principii fundamentale ale securității informațiilor ○ Confidențialitate, integritate și disponibilitate ○ Managementul riscurilor 3. Reglementări și standarde de securitate ○ GDPR, HIPAA, ISO/IEC 27001 ○ Alte reglementări relevante 4. Amenințări și vulnerabilități ○ Tipuri de amenințări (malware, phishing, etc.) ○ Identificarea și analiza vulnerabilităților 5. Măsuri de protecție a datelor ○ Controlul accesului și autentificarea ○ Criptografie și protecția datelor în tranzit și în repaus 6. Politici și proceduri de securitate ○ Crearea și implementarea politicilor de securitate ○ Proceduri de gestionare a incidentelor 7. Securitatea rețelelor ○ Protecția rețelelor locale și globale ○ Firewall-uri, IDS/IPS 8. Securitatea aplicațiilor ○ Securitatea dezvoltării software-ului ○ Testarea și evaluarea securității aplicațiilor 9. Backup și recuperare în caz de dezastru ○ Strategii de backup ○ Planuri de recuperare și continuitate 10. Audit și monitorizare ○ Tehnici de auditare a securității ○ Monitorizarea activităților și detectarea anomaliilor 11. Securitatea fizică și a infrastructurii ○ Protecția echipamentelor fizice ○ Măsuri de securitate a infrastructurii IT 12. Aspecte legale și etice în securitatea datelor ○ Drepturile și responsabilitățile legale ○ Dilemele etice și gestionarea acestora 13. Tendențe emergente și viitorul securității datelor ○ Tehnologii emergente (blockchain, AI, etc.)	• Expunere liberă curs cu videoproiector/ retroproiector și tabla într-o manieră interactivă: punctate din când în când întrebări pentru studenți în scopul creșterii gradului de interactivitate • Indicarea unor teme pentru documentare și studiu individual	28 ore

○ Provocări și oportunități viitoare 14. Managementul securității informației – privire globală, suita de protocoale ISO 27000, GDPR		
Bibliografie 1. Notițe de curs (slide-uri) puse la dispoziție studenților în format electronic pe platforma Office 365 2. Stallings W, Cryptography and Network Security Principles and Practice, Third Edition, Prentice Hall, 2003, 3. D.E.Popescu, Managementul securității informației, Editura Universității din Oradea, 2012 4. Computer Hacking, Security testing, Penetration testing and basic Security, Author: Cary hall & Erin Watson, Kindle edition, free, https://www.amazon.com/Hacking-Computer-Security-Testing-Penetration-ebook/dp/B01N1UPX8D 5. ITIL 6. https://portswigger.net		
8.2. Laborator	Metode de predare	Observații
1. 1. Prezentarea activitatilor de laborator, laboratoare, reguli de protecția muncii și semne convenționale specifice domeniului sistemelor informatice - informații generale, generale privind protecția și monitorizarea datelor 2. Anonimat și confidențialitate, Darknet, darkweb. Studii de caz 4. Comparatie între instrumentele de scanare în rețea și instrumentele de scanare a vulnerabilităților. 5. Utilizarea NMAP pentru scanarea porturilor și scanarea vulnerabilităților (sau alternativă Nessus). Case de studiu 6-7. Utilizarea facilităților Metasploit. Case de studiu 8 programe SetUid. Exemple 9-13 Utilizarea platformei Portswigger pentru exploatarea vulnerabilităților aplicațiilor web. Cazuri selectate 14. Laboratorul didactic lucrează cu verificarea cunoștințelor	Discuții și recomandări legate de temele primite spre rezolvare prin temele de proiect abordate	Se alocă 2 ore pentru fiecare dintre cele 14 puncte detaliate ale activității de laborator.
Bibliografie 1. D.E.Popescu, Managementul securității informației, Editura Universitatii din Oradea, 2012 2. Modulul Moodle cu lucrările de laborator 3. Webografie recomandată în cadrul orelor de proiect 4. Platforma Portswigger - https://portswigger.net 5. Metasploit: The Penetration Tester's Guide, Authors: David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni, https://www.amazon.com/Metasploit-Penetration-Testers-David-Kennedy/dp/159327288X		

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

▪ Conținutul disciplinei se regăsește în curricula specializărilor de Calculatoare și Tehnologia Informației și din alte centre universitare care au acreditate aceste specializări, iar cunoașterea problemelor legate de Cloud Computing precum și a modului de funcționare și proiectare a acestora este o cerință stringentă a angajatorilor din domeniu (Rds&Rcs, Plexus, Neologic, Celestica, Keysys etc).
--

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	- pentru nota 5 este necesară cunoașterea noțiunilor fundamentale cerute în subiecte, fără a prezenta detalii asupra acestora - pentru nota 10, este necesară cunoașterea	Evaluarea se poate face față în față sau on-line în funcție de situația impusă	70 %

	amănunțită a tuturor subiectelor		
10.5 Laborator	- pentru nota 5, cunoașterea în linii mari a alternativelor de soluționare a temei de proiect primită Concret: Pentru nota 5: răspuns corect la minim 1/3 din întrebările primite legate de tema proiectului - pentru nota 10, cunoașterea detaliată a soluției propuse cu prezentarea unor analize comparative pentru demonstrarea eficienței acesteia. Concret: Pentru nota 10: răspuns corect la toate întrebările legate	Test + aplicație practică La fiecare laborator studenții primesc un test și o notă. De asemenea, fiecare student primește o notă pentru activitatea la laborator în timpul semestrului și pentru dosarul cu lucrările de laborator. Astfel rezultă o medie pentru laborator. Întrebările sunt puse pe baza referatelor întocmite la lucrările de laborator.	30%
10.7 Standard minim de performanță			
Asimilarea unor cunoștințe detaliate despre vulnerabilități, riscuri și soluții de securitate în gestionarea și vehicularea informației într-o companie Soluționarea la termen, în activități individuale și activități desfășurate în grup, în condiții de asistență calificată, a problemelor care necesită aplicarea de principii și reguli respectând normele deontologiei profesionale. Asumarea responsabilă de sarcini specifice în echipe pluri-specializate și comunicarea eficientă la nivel instituțional. Dezvoltare a spiritului de echipă, spiritului de ajutorare reciprocă, conștientizarea importanței pregătirii pe parcursul semestrului pentru obținerea rezultatelor bune și durabile, conștientizarea importanței căutării, cercetării proprii legate de învățare (bibliotecă, internet), cultivarea unei discipline a muncii, efectuate corect și la timp			

Data completării
08.09.2026

Semnătura titularului de curs
Prof.dr.habil.D.E.Popescu

Semnătura titularului de laborator
ing. D.L.Lucaciu

e-mail : depopescu@uoradea.ro e-mail : lucaciu.daianalarisa@didactic.uoradea.ro

Data avizării în departament
____.09.2026

Semnătura directorului de departament,
Conf.univ.dr.ing.Elisa Valentina Moisi
emoisi@uoradea.ro

Data avizării în Consiliul Facultății
____.09.2026

Semnătură Decan
Prof. dr.ing. Eugen Gergely
egergely@uoradea.ro