

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	CALCULATOARE si TEHNOLOGIA INFORMATIEI
1.5 Ciclu de studii	MASTER
1.6 Programul de studii/Calificarea	MANAGEMENT ÎN TEHNOLOGIA INFORMAȚIEI

2. Date despre disciplină

2.1 Denumirea disciplinei	Managementul securitatii informatiei						
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	I	2.5 Semestrul	1	2.6 Tipul de evaluare	Ex	2.7 Regimul disciplinei	I

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	0/2
3.4 Total ore din planul de învățământ	56	din care: 3.5 curs	28	3.6 laborator /proiect	0/28
Distribuția fondului de timp ore					ore
Studiul după manual, suport de curs, bibliografie și notițe					48
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					26
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					14
Tutoriat					2
Examinări					4
Alte activități.....					
3.7 Total ore studiu individual	94				
3.8 Total ore pe semestru	150				
3.9 Numărul de credite	6				

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	- Cursul se poate desfășura față în față sau on-line” - prezență la minim 50% din cursuri	- prezență la minim 50% din cursuri
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	- Prezența obligatorie la toate laboratoarele; - Studenții vin cu lucrările de laborator conspectate - Se pot recupera pe parcursul semestrului maxim 4 lucrări (30 %); - Frecvența la orele de laborator sub 70% conduce la refacerea disciplinei

6.1. Competențele specifice acumulate	
Competențe profesionale	CP3. Solutionarea problemelor folosind instrumentele științei și ingineriei calculatoarelor CP5. Proiectarea, gestionarea ciclului de viață, integrarea și integritatea sistemelor hardware, software și de comunicații
Competențe transversale	CT1. Aplicarea, în contextul respectării legislației, a drepturilor de proprietate intelectuală (inclusiv transfer tehnologic), a metodologiei de certificare a produselor, a principiilor, normelor și valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă și responsabilă CT2. Identificarea rolurilor și responsabilităților într-o echipă plurispecializată luarea deciziilor și atribuirea de sarcini, cu aplicarea de tehnici de relaționare și muncă eficientă în cadrul echipei

6.2. Rezultatele așteptate ale învățării

Cunoștințe	Studentul/absolventul descrie, identifică, sumarizează concepte și metode elementare privitoare la limbaje de programare, medii de programare, tehnici de programare, baze de date, inteligență artificială și inginerie software și modul lor de aplicare în probleme concrete.
Aptitudini	Studentul/absolventul alege și explică concepte proprii specifice proiectării algoritmilor, programării orientate pe obiecte, programării logice și funcționale. Studentul/absolventul specifică cerințe, analizează, elaborează, dezvoltă și testează programe în limbaje de programare de uz general (C, etc.) și /sau obiect-orientate (C++, Java, etc.), aplicând elementele specifice ingineriei software. Studentul/absolventul proiectează, implementează, dezvoltă și /sau gestionează aplicații ce includ diverse tipuri de baze de date.
Responsabilitate și autonomie	Studentul/absolventul are o comportare onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputația profesiei.

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

7.1 Obiectivul general al disciplinei	Disciplina are ca obiectiv familiarizarea 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.
7.2 Obiectivele specifice	- Cursul își propune să familiarizeze studenții cu probleme de securitate a informațiilor, cu înțelegerea și identificarea a ceea ce reprezintă vulnerabilitățile, cu modul în care se pune problema de protecție atât a sistemului neconectat, cât și a celor conectate într-o rețea internă / internet. Prin urmare, acesta propune să prezinte caracteristicile de bază ale problemelor de securitate a informațiilor și să dezvolte capacitățile de a dezvolta politici de securitate la nivel organizational în scopul protejării datelor. - Proiect: Urmărirea riscurilor și a vulnerabilităților la care se expun structurilor unei instituții considerate ca și studiu de caz cu identificare măsurilor de protecție care se impun

8. Conținuturi

8.1 Curs (C)	Metode de predare	Obs.
1. Fundamentele managementului securității informației: informația ca activ organizațional; obiectivele de confidențialitate, integritate și disponibilitate; amenințări, vulnerabilități, riscuri și incidente; principiile apărării în profunzime, al privilegiului minim și al securității implicit configurate; tipuri de controale și responsabilități manageriale.	Prelegere, metode interactive, studii de caz	2 ore
2. Managementul identității, autentificarea și controlul accesului: identificarea utilizatorilor; autentificarea prin parole, chei criptografice, tokenuri și factori biometrici; autentificarea multifactor și autentificarea unică; reguli de securizare a parolelor; subiecte și obiecte de acces; modele DAC, MAC și RBAC; modelele Bell–LaPadula, Biba, Clark–Wilson și Chinese Wall; gestionarea identităților și accesului în mediile cloud.	Prelegere, metode interactive, studii de caz	2 ore
3. Fundamente de comunicații și rețele: modelele OSI și TCP/IP; protocoale și porturi uzuale; topologii și arhitecturi de rețea; Internet, intranet, extranet și zone demilitarizate; securitatea rețelelor fără fir prin WPA2 și WPA3; riscuri asociate tehnologiilor Bluetooth, RFID, NFC, dispozitivelor mobile și Internetului obiectelor.	Prelegere, metode interactive, studii de caz	2 ore
4. Securitatea comunicațiilor și a accesului la rețea: metode de conectare și acces la Internet; protejarea comunicațiilor VoIP; filtrarea traficului; firewall-uri de rețea, de gazdă și de aplicație; segmentarea și apărarea în profunzime; riscurile accesului la distanță; protocoale de tunelare și VPN; autentificarea utilizatorilor la distanță și controlul accesului la rețea.	Prelegere, metode interactive, studii de caz	2 ore
5. Actori de amenințare și tehnici de atac: categorii de actori și motivațiile acestora; amenințări interne și externe; atacuri DoS și DDoS; rețele botnet; interceptarea traficului; exploatarea vulnerabilităților zero-day; amenințări persistente avansate; inginerie socială; rolul conștientizării și instruirii utilizatorilor în reducerea riscurilor.	Prelegere, metode interactive, studii de caz	2 ore
6. Programe malițioase și protecția endpointurilor: virusuri, viermi, cai troieni, ransomware, rootkituri, backdoor-uri și spyware; metode de infectare și persistentă; detecție bazată pe semnaturi, euristică și comportament; soluții antivirus și EDR; filtrarea conținutului; actualizarea sistemelor; principiul privilegiului minim și practici sigure de utilizare.	Prelegere, metode interactive, studii de caz	2 ore
7. Managementul vulnerabilităților: identificarea vulnerabilităților și expunerilor comune; surse de informare și cicluri de publicare; evaluarea relevanței și severității; corelarea vulnerabilităților cu activele organizației; scanarea și validarea rezultatelor; gestionarea actualizărilor și a corecțiilor de securitate; prioritizarea remedierii și verificarea eficacității măsurilor aplicate.	Prelegere, metode interactive, studii de caz	2 ore
8. Managementul riscurilor și răspunsul la incidente: definirea riscului, amenințării, vulnerabilității, probabilității și impactului; identificarea și evaluarea activelor; analiză calitativă și cantitativă; tratarea riscurilor prin reducere, evitare, transfer și acceptare; risc rezidual; etapele răspunsului la incidente — pregătire, detectare, analiză, limitare, eradicare, recuperare și lecții învățate.	Prelegere, metode interactive, studii de caz	2 ore
9. Monitorizarea securității și evaluarea tehnică: gestionarea alertelor și a rezultatelor fals pozitive; sisteme IDS/IPS la nivel de rețea și gazdă; verificarea integrității fișierelor; honeypoturi și honeyneturi; colectarea și corelarea jurnalelor prin soluții SIEM; evaluarea vulnerabilităților; principii, limite și condiții de autorizare a testelor de penetrare.	Prelegere, metode interactive, studii de caz	2 ore
10. Controale de securitate și reziliență operațională: controale preventive, detective și corective; controale manageriale, tehnice și operaționale; întărirea configurațiilor; politici și proceduri; managementul configurației și al schimbării; redundanță, RAID și clustere de disponibilitate; strategii de backup complet, diferențial și incremental; testarea restaurării datelor.	Prelegere, metode interactive, studii de caz	2 ore
11. Auditul securității informației: rolul auditului în asigurarea responsabilității și conformității; definirea domeniului, obiectivelor și criteriilor de audit; piste de audit, jurnale și surse de dovezi; păstrarea și protejarea jurnalelor; auditarea conturilor,	Prelegere, metode interactive, studii de caz	2 ore

configurațiilor și politicilor de securitate; constatări, neconformități, măsuri corective și urmărirea implementării acestora.		
12. Operațiuni de securitate și protecția datelor: clasificarea și ciclul de viață al informațiilor; date în repaus, în tranzit și în utilizare; politici de gestionare, păstrare și eliminare a datelor; protecția datelor cu caracter personal; gestionarea activelor; securitatea bazelor de date; riscuri de inferență și expunere; integrarea securității în ciclul de viață al sistemelor.	Prelegere, metode interactive, studii de caz	2 ore
13. Guvernanța și planificarea securității informației: sistemul de management al securității informației conform familiei ISO/IEC 27000; politici, standarde, proceduri, roluri și responsabilități; conștientizarea și instruirea personalului; analiza impactului asupra activității; continuitatea activității și recuperarea în caz de dezastru; relația dintre BCP și DRP; cerințe de conformitate relevante, inclusiv GDPR și NIS2.	Prelegere, metode interactive, studii de caz	2 ore
14. Securitatea perimetrului și evaluarea etică a sistemelor: rolul routerelor și firewall-urilor; definirea zonelor de încredere, segmentarea și regulile de filtrare; configurarea sigură și verificarea controalelor; etapele unei evaluări autorizate; recunoaștere, scanare activă și pasivă, identificarea și raportarea vulnerabilităților; demonstrații controlate cu Wireshark, Nmap și Nessus, inclusiv aplicații DigitalUO.	Prelegere, metode interactive, studii de caz	2 ore

Bibliografie:

1. Notitele de curs si inregistrările de pe platformele Microsoft 365 si Moodle ale Universitatii din Oradea: <https://e.uoradea.ro/course/view.php?id=54176>
2. Stallings W, Cryptography and Network Security Principles and Practice, Ththird Edition, Prentice Hall, 2003,
3. D.E.Popescu, Managementul securitatii informatiei, Editura Universitatii din Oradea, 2012
4. ITIL
1. https://cma.org.sa/en/RulesRegulations/Guides/Documents/Cyber_Security_en.pdf
2. Regulamentul nr. 6/2022 privind cadrul de desfășurare a testelor de reziliență cibernetică TIBER-RO
3. Directiva UE Digital Operational Resilience Act (DORA)
4. Directiva UE NIS
5. Directiva UE NIS2
6. Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice
7. OUG 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică
8. Hotărârea de Guvern nr. 1.321 din 30 decembrie 2021
9. <https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021>
10. <https://dnsc.ro/vezi/document/securitatea-serviciilor-internet-banking>
11. <https://www.europarl.europa.eu/news/ro/headlines/security/20221103STO48002/noile-norme-de-securitate-cibernetica-ale-ue-explicate>
12. <https://cybersecurity-romania.ro>
13. <https://www.consilium.europa.eu/ro/policies/cybersecurity/>
14. <https://www.mae.ro/node/28367>
15. <https://www.europarl.europa.eu/news/ro/headlines/security/20221103STO48002/noile-norme-de-securitate-cibernetica-ale-ue-explicate>

Bibliografie suplimentară DigitalUO*

1. <https://ro.safetydetectives.com/blog/o-que-e-um-firewall/>
2. <http://stud.usv.ro/RC/SetIII/router.html>
3. <https://ocw.cs.pub.ro/courses/rl/labs/02>
1. <https://nmap.org>
2. <https://ocw.cs.pub.ro/courses/rl/labs/11>
3. <https://ro.myservername.com/15-best-network-scanning-tools-network>
4. <https://nmap.org/man/ro/man-host-discovery.html>
5. <https://askit.ro/solutii/scanare-in-retea-nmap-precizarea-gazdelor-si-retelelor-tinta-si-descoperire-gazda/>
6. <https://www.gts.ro/ro/firewall-as-service>

8.2 Seminar (S)	Metode de predare	Obs.
8.3 Proiect: Tema: Strategie de securitate pentru o firma mica/medie Definirea studiului de caz și planificarea proiectului – selectarea unei firme mici/mijlocii, descrierea domeniului de activitate, a dimensiunii și a cerințelor de securitate; stabilirea scopului, obiectivelor, livrabilelor și responsabilităților echipei. Inventarierea activelor și descrierea infrastructurii IT – identificarea datelor, aplicațiilor, echipamentelor, conturilor, serviciilor cloud și conexiunilor de rețea; elaborarea inventarului activelor și a unei reprezentări a infrastructurii analizate. Identificarea amenințărilor și vulnerabilităților – analiza expunerii activelor la atacuri cibernetice, erori umane, defecțiuni tehnice, pierderi de echipamente și incidente fizice; documentarea vulnerabilităților relevante pentru studiul de caz. Evaluarea și prioritizarea riscurilor – estimarea probabilității și impactului, construirea matricei de risc, stabilirea nivelurilor de risc și selectarea riscurilor care necesită tratament prioritar. Proiectarea strategiei și a măsurilor de securitate – definirea măsurilor tehnice, organizaționale și fizice privind protecția datelor, controlul accesului, securitatea rețelei și a echipamentelor, backupul, instruirea personalului și continuitatea activității, cu raportare la ISO/IEC 27001, GDPR și cerințele aplicabile. Elaborarea planului de implementare, monitorizare și îmbunătățire – ordonarea măsurilor pe priorități, alocarea responsabililor, termenelor și resurselor; stabilirea indicatorilor de monitorizare, a auditului periodic, a testării și a mecanismului de revizuire continuă. Finalizarea, prezentarea și evaluarea proiectului – integrarea rezultatelor în raportul final, formularea concluziilor și recomandărilor, pregătirea anexelor și a prezentării, susținerea proiectului și valorificarea observațiilor primite.	Învățare bazată pe proiect; studiu de caz; problematizare; lucru individual și în echipă; demonstrații și exerciții aplicative; consultații și feedback formativ pe etape; prezentarea și susținerea proiectului; evaluare colegială	4 ore 4 ore 4 ore 4 ore 4 ore 4 ore 4 ore
Bibliografie: Bibliografie - ISO/IEC 27001:2022, <i>Information security, cybersecurity and privacy protection — Information security management systems — Requirements</i>. - ISO/IEC 27002:2022, <i>Information security, cybersecurity and privacy protection — Information security controls</i>. - ISO/IEC 27005:2022, <i>Information security, cybersecurity and privacy protection — Guidance on managing information security risks</i>. - ISO, <i>ISO/IEC 27001:2022 — Information Security Management Systems: A Practical Guide for SMEs</i>, 2024. - National Institute of Standards and Technology, <i>The NIST Cybersecurity Framework (CSF) 2.0</i>, NIST CSWP 29, 2024, sursa oficială NIST. - Center for Internet Security, <i>CIS Critical Security Controls, Version 8.1</i>, 2024, sursa oficială CIS. - European Union Agency for Cybersecurity (ENISA), <i>Cybersecurity Guide for SMEs — 12 Steps to Securing Your Business</i>, 2021, sursa oficială ENISA.		

12. European Union Agency for Cybersecurity (ENISA), *Cybersecurity for SMEs — Challenges and Recommendations*, 2021, [sursa oficială ENISA](#).
13. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția datelor cu caracter personal (GDPR), [EUR-Lex](#).
14. Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS2), [EUR-Lex](#).
15. Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, [Portal Legislativ](#).

Bibliografie suplimentară DigitalUO*

1. <https://docplayer.ro/142739635-Laborator-configurarea-setărilor-de-bază-ale-router-ului-cu-ccp-topologie-tabela-de-adresare-echipament-interfață-adresă-ip-masca-de-subrețea-default.html>
1. <https://ro.safetydetectives.com/blog/o-que-e-um-firewall/>
2. <http://stud.usv.ro/RC/SetIII/router.html>
3. <https://ocw.cs.pub.ro/courses/rl/labs/02>
4. https://staff.fmi.uvt.ro/~stelian.mihalas/sec_cib/cursuri/eBook_-_Introducere_in_Securitate_Cibernetica20190802-105063-owh8vu.pdf
5. https://learn.ramonnastase.ro/ebook-securitate-cibernetica?utm_campaign=redirect&utm_medium=page&utm_source=ramonnastase.ro
6. <https://www.gmb.ro/securitate-cibernetica/servicii-de-securitate-cibernetica/>
7. <https://www.gts.ro/ro/firewall-as-service>

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

Conținutul disciplinei este în concordanță cu cele ale disciplinelor similare predate la programe de studii de licență de la facultăți de profil din țară și străinătate și cu cerințele angajatorilor consultați cu diferite ocazii formale și non-formale

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
10.1 Curs	Înțelegerea conceptelor de management al securității informației, standarde și politici de securitate, managementul riscurilor, continuitatea afaceri	Examen scris / test grilă și întrebări deschise	60%
10.2 Seminar			
10.3 Laborator			
10.4 Proiect	Elaborarea unui plan de management al securității informației pentru o organizație / analiză de risc / plan de continuitate	Susținere proiect și raport scris	40%
10.5 Standard minim de performanță*			
Cunoașterea conceptelor fundamentale privind managementul securității informației, promovarea examenului final și realizarea minimă a activităților practice și a proiectului Obținerea notei minime 5 la fiecare componentă evaluată			

* Se va detalia modalitatea în care rezultatele declarate ale învățării sunt evaluate / cuantificate prin componentele de evaluare /examinare.

Data completării
08.09.2026

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

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

Data avizării în departament
17.09.2026

e-mail : depopescu@uoradea.ro

e-mail : depopescu@uoradea.ro

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

Data avizării în Consiliul Facultății
18.09.2026

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