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	**CALCULATOARE si TEHNOLOGIA INFORMATIEI**
1.4 Domeniul de studii	**CALCULATOARE si TEHNOLOGIA INFORMATIEI**
1.5 Ciclul de studii	**MASTER**
1.6 Programul de studii/Calificarea	**Management in Tehnologia Informatiei**

2. Date despre disciplină

2.1 Denumirea disciplinei	**Managementul securitatii informatiei**						
2.2 Titularul activităţilor de curs	**Prof.univ.dr.habil. Daniela Elena POPESCU**						
2.3 Titularul activităţilor 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	**DD**

3. Timpul total estimat (ore pe semestru al activităţilor 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 învăţământ	**56**	din care: 3.5 curs	**28**	3.6 laborator /proiect	**14/14**
Distribuţia fondului de timp ore					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					28
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					8
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					**14**
Tutoriat					2
Examinări					4
Alte activităţi.....					

3.7 Total ore studiu individual	**56**
3.9 Total ore pe semestru	**112**
3.10 Numărul de credite	**4**

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

6.a. Competenţele specifice acumulate

Competențe profesionale	**CP3.** Solutionarea problemelor folosind instrumentele stiintei si ingineriei calculatoarelor **CP5.** Proiectarea, gestionarea ciclului de viata, integrarea si integritatea sistemelor hardware, software si de comunicatii
Competențe transversale	**CT1.** Aplicarea, în contextul respectării legislaţiei, a drepturilor de proprietate intelectuala (inclusiv transfer tehnologic), a metodologiei de certificare a produselor, a principiilor, normelor şi valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă şi responsabilă **CT2.** Identificarea rolurilor şi responsabilităţilor într-o echipă plurispecializată luarea deciziilor si atribuirea de sarcini, cu aplicarea de tehnici de relaţionare şi muncă eficientă în cadrul echipei

6.b. Rezultatele aşteptate ale învăţării

Cunoştiinţe	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 şi 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 (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	• Disciplina are ca obiectiv familiarizarea cu problemele de securitate a informatiei, cu ceea ce reprezinta vulnerabilitatile datelor, cu modul in care se pune problema protectiei sistemelor atat neconectate in retea cat si a celor conectate in retea.
7.2 Obiectivele specifice	▪ Cursul isi propune să familiarizeze studenții cu probleme de securitate a informațiilor, cu intelegerea si identificarea a ceea ce reprezintă vulnerabilitățile, cu modul în care se pune problema de protecție atât a sistemului neconectat, cât și a celor conectate intr-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 in scopul protejarii datelor. ▪ Proiect: Urmarirea riscurilor si a vulnerabilitatilor la care se expun structurilor unei institutii considerate ca si studiu de caz cu identificare masurilor de protectie care se impun

8. Conţinuturi

8.1 Curs (C)	Metode de predare	Obs.
1. Securitatea prelucrarii informatiei, protecţia valorilor, Caracteristici ale intruziunii prin computere, Atacuri, Semnificaţia securităţii computerelor, Scopurile securităţii, Confidenţialitatea, Integritatea, Disponibilitatea, Vulnerabilităţi - ale hardware-ului, ale software-ului, Vulnerabilităţi ale datelor, Infractorii computerelor, Metode de apărare, Controale, Viitorul în domeniu	Prelegere, metode interactive, studii de caz	2 ore
2. Protecţia calculatoarelor neconectate în reţea, Autentificarea utilizatorului, Sisteme cu parole, Avantajele sistemelor cu parole, Dezavantaje, Reguli pentru creşterea securităţii asigurate de sistemele cu parole, Protecţia prin criptare, Autentificarea bazată pe chei cifrate, Autentificarea bazată pe ceva ce utilizatorul este, Sisteme de autentificare biometrice, Utilizarea amprentelor în autentificare 1. Controlul acces: • Identificare • Autentificare Trei factori • O singură logare • Condamnare unică • Control acces cu subiecte și obiecte • Modul de control al accesului (DAC, non-DAC, MAC și RBAC) • Bell-LaPadula, Biba, Clark-Wilson, si arhitectura Zidul Chinezesc • Managementul identităților • Cloud computing	Prelegere, metode interactive, studii de caz	2 ore
2. Elemente avansate de comunicatie si de retea: Modelele de interconectare a sistemelor deschise (OSI) și a protocolului de control al transmisiei / protocolului de internet (TCP / IP) • Configurații de rețea pentru autobuz, stea și token ring • Protocoale comune în suita TCP / IP • Porturi utilizate cu protocoale comune • Diferite arhitecturi de rețea precum Internet, intranet, extranet și • zone demilitarizate (DMZ) • Protocoale de securitate wireless, cum ar fi Confidențialitate echivalentă cu fir (WEP), Acces protejat Wi-Fi (WPA) și WPA2 • Tehnologii fără fir precum Bluetooth, RFID, 802.11, WiMax, GSM, 3G și NFC	Prelegere, metode interactive, studii de caz	2 ore
3. Elemente de comunicatie si de retea: • Metode de telecomunicații utilizate pentru a accesa internetul • Securizarea protocolului Voice over Internet (VoIP) cu Secure Real-Time • Protocol de transport (SRTP) • Filtrarea pachetelor, firewall-urile și firewall-urile de aplicație • Apără diversitatea cu firewall-uri • Diferențele dintre firewall-urile bazate pe rețea și gazdă • Riscuri și vulnerabilități legate de soluțiile de acces la distanță • Diferite protocoale de tunelare utilizate cu acces la distanță • Metode de autentificare utilizate cu acces la distanță • Controlul accesului la rețea	Prelegere, metode interactive, studii de caz	2 ore
4. Diferențe între hackeri și crackeri • Diferențe între whitehats, blackhats, and grayhats • Atacuri de refuz de serviciu și atacuri de refuz de serviciu distribuite (Denial-of-service and distributed denial-ofservice attacks) • Botnets și zombi • Sniffers și sniffing atacuri • Exploatări zero-day • Amenințări persistente avansate • Tacticile de inginerie socială • Importanța instruirii pentru a reduce atacurile de inginerie socială	Prelegere, metode interactive, studii de caz	2 ore
5. Cod si Activitate malitioasa: Diferite tipuri de virusuri • Diferențe între viruși, viermi, cai troieni și bombe logice • Seturi de rădăcini, trape, uși din spate și programe spion • Diferențe între detectare pe bază de semnătură și detectare pe bază de euristică • pentru software antivirus • Importanța păstrării la zi a definițiilor semnăturii antivirus • Utilizarea filtrelor de spam și a dispozitivului de filtrare a conținutului • Principiul celui mai mic privilegiu și cum poate ajuta la prevenirea infecțiilor • Educarea utilizatorilor despre practicile	Prelegere, metode interactive, studii de caz	2 ore
6. Cod și activitate rău intenționată: • Diferite tipuri de virusuri • Diferențe între viruși, viermi, cai troieni și bombe logice • Seturi de rădăcini, trape, uși din spate și programe spion • Diferențe între detectare pe bază de semnătură și detectare pe bază de euristică pentru antivirusuri • Importanța păstrării actualizării definițiilor semnăturilor antivirus • Utilizarea filtrelor de spam și a dispozitivului de filtrare a conținutului • Principiul celui mai mic privilegiu și cum poate ajuta la prevenirea infecțiilor • Educarea utilizatorilor despre practicile informatice sigure • Lista de vulnerabilități și expuneri comune	Prelegere, metode interactive, studii de caz	2 ore
7. Risc, raspuns si recuperare: • Definirea riscului, amenințărilor, vulnerabilităților și impactului • Patru metode principale de gestionare a riscului: atenuarea (mitigate), evitarea, transferul și acceptarea • Definiția riscului rezidual • Pașii folosiți în evaluarea riscurilor • Diferențele dintre analiza cantitativă și cea calitativă • Pași în răspuns la	Prelegere, metode interactive, studii de caz	2 ore

incident: pregătirea, detectarea, analiza, reținerea, eradicarea, • recuperare și activități post incidente		
8. Monitorizare si analiza: • Alerte de securitate și fals pozitiv • Sisteme de detectare a intruziunilor bazate pe rețea și bazate pe gazdă • Sisteme de prevenire a intruziunilor • Metode de detectare și prevenire a atacurilor • Verificatoare de integritate a fișierelor • Honeypots, plase de miere și celule căptușite • Managerii de evenimente și incidente (Event And Incident Managers), cu ar fi SIM-urile, managerii de evenimente de sistem (System Event Managers - SEMs) și SIEMs • tipuri de teste pentru evaluări de vulnerabilitate • Instrumente de evaluare a vulnerabilități (Instrumente de evaluare a vulnerabilității) • Testele de penetrare	Prelegere, metode interactive, studii de caz	2 ore
9. Controale si contramasuri: • Obiectivele contraalelor și contramăsurilor • Diferența dintre controale preventive, detective și corective • Diferența dintre management, și controale tehnice și operaționale • Utilizarea întăririi unui sistem pentru control • Diferențe între politici și proceduri • Controale de bază, cum ar fi controlul modificărilor și gestionării configurației • Utilizarea discurilor RAID pentru a asigura toleranța la erori • Utilizarea eșecului la nivelul clusterelor (fail over of clusters) pentru a vă proteja împotriva pierderilor unui server • Diferite tipuri de copii de rezervă (backups), cum ar fi complet, diferențial și incremental	Prelegere, metode interactive, studii de caz	2 ore
10. Audit: • Valoarea auditului pentru fortarea răspunderii • Niveluri de tăiere • Trasee de audit • Diferite tipuri de jurnale de audit utilizate pentru a crea trasee de audiție • Audituri de securitate, cum sunt fi auditori de parole și auditori de politici de securitate • Controlul configurației • Managementul schimbării	Prelegere, metode interactive, studii de caz	2 ore
11. Operatiuni de securitate : • Clasificări de dată, cum ar fi confidențial, Sensibil, Privat și Public • Diferența dintre date în repaus și date în mișcare • Diferite elemente ale politicilor de gestionare a datelor • Componente ale unei baze de date, cum ar fi rânduri, chei primare și chei străine • Riscuri legat de inferență date • Cerințe de reglementare legat de PII, PHI și companii deținute public • Componenta de gestionare a activelor • Diferențele dintre certificare și acreditare • Criteriile comune și nivelurile sale de evaluare • Utilizarea unui cadru de gestionare a riscurilor cu un proces de certificare și acreditare • Diferite faze ale unui ciclu de viață la dezvoltarea sistemului	Prelegere, metode interactive, studii de caz	2 ore
12. Administrare si planificare securitate; Managementul securitatii informatiei, suita de protocoale ISO 27000 • Conținutul și caracteristicile politice de securitate • Creșterea gradului de conștientizare a politicilor de securitate • Planuri de continuitate a afacerilor • Analiza impactului asupra afacerilor • Planuri de recuperare în caz de catastrofă • Diferență între un BCP și DRP • Prevederi legale; GDPR	Prelegere, metode interactive, studii de caz	2 ore
14. Curs nou: Protectia retelelor prin utilizarea si configurarea corecta a ruterelor si a firewall-urilor - DigitalUO*	Prelegere, metode interactive, studii de caz	2 ore
14. Curs nou: Ethical hacking: Procesul de hacking, Reconnaissance, Scanarea resurselor IT la nivelul organizatiei si identificarea vulnerabilitatilor: Scanare activa si scanare pasiva, prezentare Tool-uri de lucru: Wireshark, NMAP, Nessus*	Prelegere, metode interactive, studii de caz	2 ore

Bibliografie:

1. Notitele de curs si inregistrarile 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, Thhird 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 desfăşurare 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 reţelelor şi 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 Laborator 1Prezentarea activităților de laborator, a laboratoarelor, a normelor de protecție a muncii și a semnelor convenționale specifice domeniului sistemelor informatice - informații generale, generale privind protecția și monitorizarea datelor 2. Analiza vulnerabilitatilor si a riscurilor existente pentru studiul de caz luat in considerare 3. Clasificarea informatiei, Identificarea solutiilor pentru cresterea securitatii cu stabilirea politicilor de securitate concrete pentru cazul considerat 4. Trasarea tehnicilor de auditare pentru mentinerea securitatii la nivelul obiectivului analizat 5. Laborator nou : Operarea si configurarea ruterelor si a firewall-urilor* 6. Laborator nou : Scanarea porturilor, si vulnerabilitatilor cu NMAP* 7. Predarea lucrărilor de laborator cu verificarea cunoștințelor	Prezentarea cu ajutorul videoproiectorului; discuții libere;	

Bibliografie:

Bibliografie

5. D.E Notitele de curs si inregistrarile de pe platformele Microsoft 365 si Moodle ale Universitatii din Oradea: https://e.uoradea.ro/course/view.php?id=54176
6. Stallings W, Cryptography and Network Security Principles and Practice, Thhird Edition, Prentice Hall, 2003,
7. D.E.Popescu, Managementul securitatii informatiei, Editura Universitatii din Oradea, 2012
8. OUG 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică
9. Hotărârea de Guvern nr. 1.321 din 30 decembrie 2021
10. https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021
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://docplayer.ro/142739635-Laborator-configurarea-setărilor-de-bază-ale-router-ului-cu-ccp-topologie-tabela-de-adresare-echipament-interfață-adresă-ip-masca-de-subreţea-defaul.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 conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

Conţinutul disciplinei este în concordanţă cu cele ale disciplinelor similare predate la programe de studii de licenţă de la facultăţi de profil din ţară şi străinătate și cu cerințele angajatorilor consultați cu diferite ocazii formale și non-formale

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs (C)	Examen scris	- pentru nota 5 este necesară cunoaşterea noţiunilor fundamentale cerute în subiecte, fără a prezenta detalii asupra acestora - pentru nota 10, este necesară cunoaşterea amănunţită a tuturor subiectelor	70%
10.5 Seminar (S)	-		
10.6 Laborator (L)	Test practic	- pentru nota 5, cunoasterea in linii mari a alternativelor de solutionare a temei de proiect primita Concret: Pentru nota 5: răspuns corect la minim 1/3 din intrebarile primite legate de tema laboratorului - pentru nota 10, cunoasterea detaliata a solutiei propuse cu prezentarea unor analize comparative pentru demonstrarea eficientei acesteia. Concret: Pentru nota 10: răspuns corect la toate întrebările legate	30%
10.6 Proiect (P)			
10.8 Lucrări practice (P)			

10.9 Standard minim de performanţă

Asimilarea unor cunoştinţe detaliate despre vulnerabilitati, riscuri si solutii de securitate in gestionarea si vehicularea informatiei intr-o companie

Soluţionarea la termen, în activităţi individuale şi activităţi desfăşurate în grup, în condiţii de asistenţă calificată, a problemelor care necesită aplicarea de principii şi reguli respectând normele deontologiei profesionale.

Asumarea responsabilă de sarcini specifice în echipe plurispecializate şi comunicarea eficientă la nivel instituţional.

- Dezvoltare a spiritului de echipă, spiritului de ajutorare reciprocă, conştientizarea importanţei pregătirii pe parcursul semestrului pentru obţinerea rezultatelor bune şi durabile, conştientizarea importanţei căutării, cercetării proprie legate de învăţare (bibliotecă, internet), cultivarea unei discipline a muncii, efectuate corect şi la timp

Data completării
02.09.2024

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

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

e-mail : depopescu@uoradea.ro **e-mail : depopescu@uoradea.ro**

Data avizării în departament
25.09.2024

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

Data avizării în Consiliul Facultății
16.09.2024

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