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	**INGINERIA SISTEMELOR AUTOMATE ŞI MANAGEMENT**
1.4 Domeniul de studii	**INGINERIA SISTEMELOR**
1.5 Ciclul de studii	**MASTER**
1.6 Programul de studii/Calificarea	**SISTEME AUTOMATE AVANSATE /MASTER**

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	**DSI**

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	**2**
3.4 Total ore din planul de învăţământ	**56**	din care: 3.5 curs	**28**	3.6 laborator /proiect	**28**
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					28
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					32
Tutoriat					
Examinări					6
Alte activităţi.....					

3.7 Total ore studiu individual	**94**
3.9 Total ore pe semestru	**150**
3.10 Numărul de credite	**6**

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 desfăşura faţă în faţă sau on-line” - prezenţă la minim 50% din cursuri
5.2. de desfăşurare a laboratorului /proiectului	- Seminarul/laboratorul/proiectul se pot desfăşura faţă în faţă 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

6.1. Competenţele specifice acumulate

Competenţe profesionale	**C4.** Configurarea şi implementarea sistemelor de conducere aferente acţionărilor electrice, acţionările electrice avansate
Competenţe 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

6.2. Rezultatele aşteptate ale învățării

Cunoştinţe	1. Studentul/absolventul cunoaște instrumentele software şi hardware utilizate în modelarea, simularea şi implementarea sistemelor de automatizare. 2. Studentul/absolventul identifică, selectarea şi evaluarea în calitate de utilizator, de software dedicat tehnologii WEB pentru aplicaţii din ingineria sistemelor, tehnologia informaţiei şi comunicaţiilor.
Aptitudini	1. Studentul/absolventul implementează soluții de automatizare bazate pe tehnologii moderne, inclusiv control distribuit şi inteligență artificială. 2. Studentul/absolventul identifică tehnologiile de programare specifice dezvoltării de aplicaţii în sisteme automate avansate şi informatică industrială. Studentul/absolventul utilizeaza tehnologiile WEB în rezolvarea de probleme bine definite din ingineria sistemelor şi în aplicaţii ce impun utilizarea de software în sisteme industriale sau în sisteme informatice.
Responsabilitate și autonomie	1. Studentul/absolventul coordonează echipe interdisciplinare pentru dezvoltarea și implementarea proiectelor de automatizare. 2.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 prezentarea caracteristicilor de baza ale problemelor de securizare a informatiei. ▪ In final se doreste dezvoltarea capabilitatilor de devoltare a politici de securitate in ansamblu in vederea protejarii informatiei ▪ Laborator: Parcurgerea materialului de curs cuprin in Modulul 1 CISCO ▪ Proiect: Urmarirea riscurilor si a vulnerabilitatilor la care se expun structurile unei institutii considerate ca si studiu de caz cu identificarea masurilor de protectie care se impun

8. Conţinuturi

8.1.Curs	Metode de predare	Observaţii
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	• Expunerelibera curs cu videoproiector/ retroproiector si tabla intr-o maniera interactiva: punctate din cand in cand intrebari pentru studenti	28 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 şi obiecte • Modul de control al accesului (DAC, non-DAC, MAC şi RBAC) • Bell-LaPadula, Biba, Clark-Wilson, si arhitectura Zidul Chinezesc • Managementul identităților • Cloud computing 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 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 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 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 6. Cod şi 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	in scopul cresterii gradului de interactivitate • Indicarea unor teme pentru documentare si studiu individual	

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 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 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 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 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 12. Administrare si planificare securitate : • 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 • Locații alternative precum shot sites, cold sites, si warm sites • Organizații de securitate precum NIST și SUA – CERT 13. Prevederi legale: • Criminalistică computerizată (Computer forensics) • Trei faze ale unei anchete criminalistice pe calculator • Importanța protejării dovezilor • Cum să protejezi memoria		

RAM volatilă şi datele de pe unităţile de disc • Diferenţa dintre abuzul de calculator şi criminalitatea computerizată • Cum contribuie vacanţele obligatorii şi rotirea locurilor de muncă la prevenirea fraudei Unele dintre legile destinate protejării datelor personale 14. Managementul securitatii informatiei, suita de protocoale ISO 27000, GDPR		
Bibliografie 1. Notite de curs (slide-uri) puse la dispozitie studentilor in format electronic pe platforma Office 365 2. Deborah Russel and . mul 1 CISCOmaterialului de curs cuprin in Mprotectie care se impuncareamilor de cautare specifici IA notiunilor generale legaG.T. Gangemi Sr, Computer security basics, Editura O'Reilly & Assoc, ISBN:0-937175-71-4, 1993 3. Stallings W, Cryptography and Network Security Principles and Practice, Thhird Edition, Prentice Hall, 2003, 4. K.Hwang, F.A.Briggs, Computer Architecture and Parallel processing, Mc Graw - Hill Book company 1987 5. Artech House, Fundamentals of Network Security, Artech House 6. D.E.Popescu, Managementul securitatii informatiei, Editura Universitatii din Oradea, 2012 7. ITIL		
8.3. Proiect	Metode de predare	Observaţii
1. Prezentarea specificarilor de proiectare 2. Analiza vulnerabilitatilor existente pentru studiul de caz luat in considerare 3. Analiza riscurilor existente pentru studiul de caz luat in considerare 4. Clasificarea informatiei cu stabilirea politicilor de securitate pentru cazul considerat 5. Identificarea solutiilor pentru cresterea securitatii cu stabilirea politicilor de securitate concrete pentru cazul considerat 6. Trasarea tehnicilor de auditare pentru mentinerea securitatii la nivelul obiectivului analizat 7. Predarea proiectului	Discutii si recomandari legate de temele primite spre rezolvare prin temele de proiect abordate	Rezultatele activitatilor de proiect sunt prezentate in plen la nivel de grupa 28 ore
Bibliografie 1. D.E.Popescu, Managementul securitatii informatiei, Editura Universitatii din Oradea, 2012 2. Modulul Moodle cu lucrarile de proiect 3. Webografie recomandata in cadrul orelor de proiect		

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

- Conţinutul disciplinei se regăseşte în curricula specializărilor de Calculatoare si Tehnologia Informatiei şi din alte centre universitare care au acreditate aceste specializări (Universitatea Tehnică din Cluj-Napoca, Universitatea din Craiova, Universitatea „Politehnica"din Timişoara, Universitatea Gh. Asachi Iaşi, etc), iar cunoaşterea arhitecturii si organizarii sistemelor de calcul precum şi a modului de funcţionare şi proiectare a acestora este o cerinţă 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 cunoaşterea noţiunilor fundamentale cerute în subiecte, fără a prezenta detalii asupra acestora - pentru nota 10, este necesară cunoaşterea amănunţită a tuturor subiectelor	Evaluarea se poate face faţă în faţă sau on-line in functie de situatia impusa	50 %

10.5 Proiect	- 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 proiectului - 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	**Testare cunostiinte + aplicaţie practică** Întrebările sunt puse pe baza referatelor întocmite in cadrul activitatilor de cercetare cuprinse in orele de proiect	50%
10.7 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
15.09.2025

Semnătura titularului de curs
Prof.dr.habil.D.E.Popescu
e-mail : depopescu@uoradea.ro

Semnătura titularului de proiect
Conf. dr. ing. Gergely Eugen Ioan
e-mail : egergely@uoradea.ro

Data avizării în departament
18.09.2025

Semnătura directorului de departament
Prof.univ.dr.ing. Helga Silaghi
E-mail: hsilaghi@uoradea.ro
http://hsilaghi.webhost.uoradea.ro/

Data avizării în Consiliul facultăţii
25.09.2025

Semnătură Decan
Conf. dr. ing. Gergely Eugen Ioan
e-mail : egergely@uoradea.ro