

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Facultatea de Electronică, Telecomunicații și Tehnologia Informației
1.3 Departamentul	Comunicații
1.4 Domeniul de studii	Inginerie electronică, telecomunicații și tehnologii informaționale
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Telecomunicații / Master
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	TC17.40

2. Date despre disciplină

2.1 Denumirea disciplinei	Securitatea cibernetică bazată pe inteligența artificială						
2.2 Aria de conținut	Arie teoretică Arie metodologică Arie de analiză						
2.3 Responsabil de curs	Conf.dr.ing. Daniel ZINCA – Daniel.Zinca@com.utcluj.ro						
2.4 Titularul activităților de laborator	Conf.dr.ing. Daniel ZINCA – Daniel.Zinca@com.utcluj.ro						
2.5 Anul de studiu	2	2.6 Semestrul	1	2.7 Tipul de evaluare	E	2.8 Regimul disciplinei	DA/DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	3	din care: 3.2 curs	1	3.3 seminar / laborator	2
3.4 Total ore din planul de învățământ	42	din care: 3.5 curs	14	3.6 seminar / laborator	28
Distribuția fondului de timp					ore
Studiul după manual, suport de curs, bibliografie și notițe					20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					12
Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri					20
Tutoriat					3
Examinări					3
Alte activități:					
3.7 Total ore studiu individual			58		
3.8 Total ore pe semestru			100		
3.9 Numărul de credite			4		

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	N/A
4.2 de competențe	N/A

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Cluj-Napoca
--------------------------------	-------------

5.2. de desfășurare a seminarului / laboratorului / proiectului	Cluj-Napoca
---	-------------

6. Competențele specifice acumulate

Competențe profesionale	<p>C1. Utilizarea elementelor fundamentale referitoare la dispozitivele, circuitele, sistemele, instrumentația și tehnologia electronica</p> <p>C2. Aplicarea metodelor de bază pentru achiziția și prelucrarea semnalelor</p> <p>C3. Aplicarea cunoștințelor, conceptelor și metodelor de bază privitoare la arhitectura sistemelor de calcul, microprocesoare, microcontrolere, limbaje și tehnici de programare</p> <p>C4. Conceperea, implementarea și operarea serviciilor de date, voce, video, multimedia, bazate pe înțelegerea și aplicarea notiunilor fundamentale din domeniul comunicațiilor și transmisiunii informației</p> <p>C5. Selectarea, instalarea, configurarea și exploatarea echipamentelor de telecomunicații fixe sau mobile și echiparea unui amplasament cu rețele uzuale de telecomunicații</p> <p>C6. Rezolvarea problemelor specifice pentru rețele de comunicații de banda largă: propagare în diferite medii de transmisiune, circuite și echipamente pentru frecvențe înalte (microunde și optice)</p> <p>C7. Conceperea, implementarea și testarea de sisteme și de diverse tipuri de aplicații (prelucrări de semnale, clasificare, regresie, detecție, procesarea limbajului natural, recunoaștere de forme) care se bazează pe tehnici de învățare automată sau de învățare profundă</p>
Competențe transversale	N/A

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

7.1 Obiectivul general al disciplinei	Dezvoltarea de competențe profesionale în domeniul securității cibernetice bazată pe Inteligența Artificială
7.2 Obiectivele specifice	<ol style="list-style-type: none"> 1. Înțelegerea conceptelor de baza privind funcționarea sistemelor de securitate cibernetică 2. Dezvoltarea de deprinderi și abilități necesare pentru proiectarea de sisteme de securitate cibernetică ce se bazează pe Inteligența Artificială

8. Conținuturi

8.1 Curs	Metode de predare	Observații
1. Introducere în domeniul Securității Cibernetice	Expunere la tablă, prezentare cu videoproiector, discuții.	Nu este cazul.
2. Aplicații ale Inteligenței Artificiale în Domeniul Securității Cibernetice		
3. Algoritmi de Inteligență Artificială pentru detecție emailuri spam și phishing		
4. Sisteme de Detecție a Intruziunilor folosind algoritmi de Inteligență Artificială		
5. Rețele Generative Adversariale GAN și aplicații în domeniul securității cibernetice		

6. Extragerea de caracteristici pentru Sisteme de Detecție a Intruziunilor		
7. Detecția Exfiltrării DNS și a tunelării DNS folosind algoritmi de Inteligență Artificială		
Bibliografie 1. E. Tsukerman, “Machine Learning for Cybersecurity Cookbook”, Packtpub, 2019. 2. A. Parisi. Hands-on Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies, Packtpub, 2019. 3. A-G.Mari, D. Zinca, V.Dobrota. Development of a Machine-Learning Intrusion Detection System and Testing of Its Performance Using a Generative Adversarial Network, Sensors, Volume 23, issue 3, 2023.		
8.2 Laborator	Metode de predare	Observații
1. Platforma Google Colab și biblioteci utilizate	Experimente pe echipamente fizice și în cloud.	
2. Detecția emailurilor de tip spam utilizând algoritmi de învățare automată		
3. Detecția emailurilor de tip phishing folosind algoritmi de Inteligență Artificială		
4. Implementarea de reguli snort pentru realizarea de sisteme de detecție a intruziunilor IDS		
5. Setul de date NSL-KDD pentru aplicații de învățare automată		
6. Implementarea de sisteme de detecție a intruziunilor folosind algoritmi de învățare automată		
7. Rețele Generative Adversariale GAN în sisteme de detecție a intruziunilor		
8. Detecția atacurilor DDoS folosind algoritmi de învățare automată și setul de date CICDDoS2019		
9. Extragerea de caracteristici pentru sisteme de detecție a intruziunilor cu învățare automată utilizând Wireshark și Python		
10. Detecția traficului VPN și setul de date ISCXVPN2016		
11. Detecția atacurilor de tip DNS Exfiltration folosind algoritmi de învățare automata și setul de date CIC-Bell-DNS-EXF-2021		
12. Algoritmi de învățare automată pentru securitate cibernetică în cloud Azure/AWS		
13. Aplicații de învățare automată pentru detecția anomaliilor în Event log din Microsoft Windows		
14. Sisteme complete de inteligență artificială în sisteme de securitate cibernetică		
Bibliografie 1. E. Tsukerman, “Machine Learning for Cybersecurity Cookbook”, Packtpub, 2019.		

2. A. Parisi. Hands-on Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies, Packtpub, 2019.
3. A-G.Mari, D. Zinca, V.Dobrota. Development of a Machine-Learning Intrusion Detection System and Testing of Its Performance Using a Generative Adversarial Network, Sensors, Volume 23, issue 3, 2023.

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

Competențele dobândite vor fi folosite în următoarele ocupații conform COR (Clasificarea Ocupațiilor din România): Inginer emisie; Inginer electronist, transporturi, telecomunicații; Inginer imagine; Inginer sunet; Proiectant inginer electronist; Proiectant inginer de sisteme și calculatoare; Inginer șef car reportaj; Inginer șef schimb emisie; Inginer proiectant comunicații; Inginer sisteme de securitate; Inginer suport vânzări; Dezvoltator de aplicații multimedia; Inginer operare rețea; Inginer testare sisteme de comunicații; Manager proiect; Inginer de trafic; Consultant pentru sisteme de comunicații.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Rezolvarea unei probleme și răspunsuri la un set de întrebări din teorie	Probă scrisă	75%
10.5 Laborator	Verificarea deprinderilor și abilităților dobândite în urma activităților de laborator	Verificare pe parcurs prin teste de laborator	25%

10.6 Standard minim de performanță

Nivel calitativ:

Cunoștințe minimale:

- ✓ Înțelegerea arhitecturii, funcționalităților și componentelor unui sistem de Securitate cibernetică
- ✓ Cunoașterea principalilor algoritmi de inteligență artificială ce se utilizează în securitatea cibernetică

Competențe minimale:

- ✓ Să poată implementa algoritmi de inteligență artificială pentru a detecta un anumit tip de atac cibernetic.
- ✓ Să poată analiza și îmbunătăți performanțele unui sistem de Securitate cibernetică bazat pe inteligența artificială.

Nivel cantitativ:

- ✓ Efectuarea tuturor lucrărilor de laborator
- ✓ Notele la examen și laborator să fie minim 5.
- ✓ Nota la disciplină se calculează cu relația: $0,75 * \text{Nota_examen} + 0,25 * \text{Nota_laborator}$

Data completării:	Titulari	Titlu Prenume NUME	Semnătura
01.07.2024	Curs	Conf.dr.ing. Daniel ZINCA	
	Aplicații	Conf.dr.ing. Daniel ZINCA	

Data avizării în Consiliul Departamentului COM
10.07.2024

Director Departament Comunicații
Prof.dr.ing. Virgil DOBROTĂ

Data aprobării în Consiliul Facultății ETTI
11.07.2024

Decan
Prof.dr.ing. Ovidiu POP