FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Facultatea de Electronică, Telecomunicaţii şi Tehnologia Informaţiei
1.3 Departamentul	Comunicații
1.4 Domeniul de studii	Inginerie electronică, telecomunicații şi tehnologii informaţionale
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Inteligență artificială și prelucrări de semnale în electronică și telecomunicații (în limba engleză) / Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	IAPSET-E 14.00

2. Date despre disciplină

2.1 Denumirea disciplinei	Securitatea Cibernetică bazată pe inteligența artificială						
2.2 Aria de conţinut	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 activităţilor 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 învăţământ	42	din care: 3.5 curs	14	3.6 seminar / laborator	28

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie şi notiţe	20
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	12
Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri	20
Tutoriat	3
Examinări	3
Alte activităţi:	

3.7 Total ore studiu individual	58
3.8 Total ore pe semestru	100
3.9 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	N/A
4.2 de competenţe	N/A

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Cluj-Napoca
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Cluj-Napoca

6. Competenţele specifice acumulate

Competenţe profesionale	C1. Utilizarea elementelor fundamentale referitoare la dispozitivele, circuitele, sistemele, instrumentaţia şi tehnologia electronică C2. Aplicarea metodelor de bază pentru achiziţia şi prelucrarea semnalelor C3. Aplicarea cunoştinţelor, conceptelor şi metodelor de bază privitoare la arhitectura sistemelor de calcul, microprocesoare, microcontrolere, limbaje şi tehnici de programare C4. Conceperea, implementarea si operarea serviciilor de date, voce, video, multimedia, bazate pe întelegerea si aplicarea notiunilor fundamentale din domeniul comunicatiilor si transmisiunii informatiei C5. Selectarea, instalarea, configurarea si exploatarea echipamentelor de telecomunicatii fixe sau mobile si echiparea unui amplasament cu retele uzuale de telecomunicatii C6. Rezolvarea problemelor specifice pentru retele de comunicatii de banda larga: propagare în diferite medii de transmisiune, circuite si echipamente pentru frecvente înalte (microunde si optice) 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
Competenţe transversale	N/A

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Dezvoltarea de competențe profesionale în domeniul Securității Cibernetice bazată pe Inteligența Artificială
7.2 Obiectivele specifice	1. Intelegerea conceptelor de baza privind funcționarea sistemelor de securitate cibernetică 2. Dezvoltarea de deprinderi si abilitati necesare pentru proiectarea de sisteme de securitate cibernetică ce se bazează pe Inteligența Artificială

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1. Introducere în domeniul Securității Cibernetice	Expunere la tablă, prezentare cu videoproiector, discuţii.	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.(în engleză)
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(în engleză)
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(în engleză)

8.2 Laborator	Metode de predare	Observaţii
1. Platforma Google Colab și biblioteci utilizate	Experimente practice pe echipamente fizice precum și în cloud.	Și
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.(în engleză)
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(în engleză)
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(în engleză)

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

Competentele dobandite vor fi folosite in urmatoarele ocupatii conform COR (Clasificarea Ocupațiilor din România): Inginer emisie; Inginer electronist, transporturi, telecomunicatii; Inginer imagine; Inginer sunet; Proiectant inginer electronist; Proiectant inginer de sisteme si calculatoare; Inginer sef car reportaj; Inginer sef schimb emisie; Inginer proiectant comunicatii; Inginer sisteme de securitate; Inginer suport vânzari; Dezvoltator de aplicatii multimedia; Inginer operare retea; Inginer testare sisteme de comunicatii; Manager proiect; Inginer de trafic; Consultant pentru sisteme comunicatii.

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 şi răspunsuri la un set de întrebări din teorie	Probă scrisă	75%
10.5 Laborator	Verificarea deprinderilor şi abilităţilor dobândite în urma activităţilor de laborator	Verificare pe parcurs prin teste de laborator	25%
10.6 Standard minim de performanţă			

Nivel calitativ:

Cunoştinţe minimale:

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

Competenţe 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 şi laborator să fie minim 5.
- ✓ Nota la disciplină se calculează cu relaţia: 0,75*Nota_examen+0,25*Nota_laborator

Data completării:	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
21.06.2024	Curs	Conf.dr.ing. Daniel ZINCA	
	Aplicații	Conf.dr.ing. Daniel ZINCA	

Data avizării în Consiliul Departamentului Comunicatii 10.07.2024	Director Departament Comunicatii Prof.dr.ing. Virgil DOBROTA
Data aprobării în Consiliul Facultății ETTI 11.07.2024	Decan Prof.dr.ing. Ovidiu POP