

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	De Inginerie
1.3 Departamentul	Inginerie Electrică, Electronică și Calculatoare
1.4 Domeniul de studii	Calculatoare și Tehnologia Informației
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Sisteme inteligente în Internetul lucrurilor
1.7 Forma de învățământ	IF – învățământ cu frecvență
1.8 Codul disciplinei	15.00

2. Date despre disciplină

2.1 Denumirea disciplinei	Securitate IoT				
2.2 Titularul de curs	Șef lucr. dr.ing. Adrian Petrovan – adrian.petrovan@ieec.utcluj.ro				
2.3 Titularul activităților de seminar / laborator / proiect	Șef lucr. dr.ing. Adrian Petrovan – adrian.petrovan@ieec.utcluj.ro				
2.4 Anul de studiu	2	2.5 Semestrul	1	2.6 Tipul de evaluare	E
2.7 Regimul disciplinei	Categorია formativă				DS
	Opționalitate				DI

3. Timpul total estimate

3.1 Număr de ore pe săptămână	3	din care:	3.2 Curs	2	3.3 Seminar	0	3.3 Laborator	1	3.3 Proiect	0
3.4 Număr de ore pe semestru	42	din care:	3.5 Curs	28	3.6 Seminar	0	3.6 Laborator	14	3.6 Proiect	0
3.7 Distribuția fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie și notițe										28
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren										28
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri										14
(d) Tutoriat										7
(e) Examinări										6
(f) Alte activități:										
3.8 Total ore studiu individual (suma (3.7(a))...3.7(f)))						83				
3.9 Total ore pe semestru (3.4+3.8)						125				
3.10 Numărul de credite						5				

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	Videoproiector, acces la Internet	
5.2. de desfășurare a seminarului / laboratorului / proiectului	Laborator calculatoare, acces Internet, software specific	

6. Competențele specifice acumulate

Competențe profesionale	- Abilitatea de a proiecta, dezvolta, gestiona și evalua mecanisme de asigurare a securității pentru procesarea și accesul la informații în dispozitive limitate din punct de vedere computațional și rețele IoT. - Abilitatea de a integra diferite sisteme de percepție și control al proceselor atât din punct de vedere hardware cât și software. - Abilitatea de a aplica legislația, reglementările și standardizările în IoT.
Competențe transversale	- Studentii sunt capabili să integreze cunoștințele și să facă față complexității emiterii de judecăți bazate pe informații care sunt incomplete sau limitate, inclusiv reflecții asupra responsabilităților sociale și etice asociate cu aplicarea cunoștințelor și judecăților lor. - Studentii sunt capabili să comunice concluziile lor, cunoștințele și motivele din spatele lor, unui public specializat și nespecialist, într-o manieră clară și lipsită de ambiguitate.

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

7.1 Obiectivul general al disciplinei	Acest curs este conceput pentru ca studenții să se familiarizeze cu securitatea IoT. Aceștia vor putea înțelege sau administra securitatea în cadrul dispozitivelor IoT, din perspectiva hardware, sistem și/sau rețea.
7.2 Obiectivele specifice	- Cunoașterea și aplicarea legislației și a aspectelor legale ale IoT. - Cunoașterea modelelor și structurilor de referință ale IoT. - Abilitatea de a analiza, proiecta și controla sisteme și servicii - Cunoașterea riscurilor de securitate inerente unui mediu IoT.

8. Conținuturi

8.1 Curs	Nr. ore	Metode de predare	Observații
Introducere în securitate cibernetică	4	Expunere orală. Discuții.	
Arhitecturi de comunicații IoT	4		
Vulnerabilități ale dispozitivelor IoT	4		
Atacuri de securitate în IoT	4		
Analiza securității în IoT	4		
Protocoale criptografice specifice IoT	4		
Criptanaliza datelor în IoT	4		
Bibliografie			
1. Aaron Guzman, Aditya Gupta. IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices. Packt Publishing. 2017			
2. D. Uckelmann, M. Harrison and F. Michahelles. Architecting the Internet of Things. Springer-Verlag Berlin Heidelberg. 2011			
3. Dimitrios Serpanos, Marilyn Wolf . Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies. Springer. 2018			
4. FTC Staff Report. Internet of Things: Privacy & Security in a Connected World. FTC. 2015			
8.2 Seminar / laborator / proiect	Nr. ore	Metode de predare	Observații
Criptografie. Sisteme de criptare în IoT.	2	Lucrări practice de laborator	
Arhitecturi de comunicații IoT	2		
Vulnerabilități ale dispozitivelor IoT	2		
Atacuri de securitate în IoT	2		
Analiza securității în IoT	2		
Criptanaliza	2		
Evaluare laborator	2		
Bibliografie			
5. Aaron Guzman, Aditya Gupta. IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices. Packt Publishing. 2017			

6. D. Uckelmann, M. Harrison and F. Michahelles. Architecting the Internet of Things. Springer-Verlag Berlin Heidelberg. 2011
 7. Dimitrios Serpanos, Marilyn Wolf . Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies. Springer. 2018
- FTC Staff Report. Internet of Things: Privacy & Security in a Connected World. FTC. 2015

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

Scenariile prezentate sunt practice. Cursul face legătura între cunoștințele de securitate cibernetică și cele specifice echipamentelor IoT. Dinamica actuală în domeniul IoT implică ca cei aflați în prima linie a luptei vor trebui să înțeleagă mediul în care evoluează organizația lor și să abordeze riscul crescând de amenințări cibernetice ca un efort comun între furnizor, profesioniști în domeniul securității și IT.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Abilitatea de rezolvare a unor probleme specifice domeniului. Capacitatea de a argumenta și susține opinii în timpul orelor de curs	Examen scris	60%
10.5 Laborator	Respectarea termenelor. Capacitatea de a identifica avantajele și dezavantajele soluției propuse.	Evaluarea temelor rezolvate	40%
10.6 Standard minim de performanță Cunoașterea principalelor vulnerabilități ale sistemelor IoT. Capacitatea de a modela scenarii realiste. Capacitatea de a propune soluții la problemele identificate. Capacitatea de a respecta termenele limita. Calcul nota disciplina: 0.2 Partial+0.3 laborator + 0.5 examen Condiții de participare la examenul final: Laborator ≥ 5 Condiții de promovare: Nota ≥ 5			

Data completării:	Titulari	Titlu Prenume NUME	Semnătura
09.09.2023	Curs	Şef lucr. dr.ing. Adrian PETROVAN	
	Aplicații	Şef lucr. dr.ing. Adrian PETROVAN	

Data avizării în Consiliul Departamentului de Inginerie
Electrică, Electronică și Calculatoare

_____15.09.2023_____

Director Departament de Inginerie
Electrică, Electronică și Calculatoare

Sl.dr.ing. Claudiu LUNG

Data aprobării în Consiliul Facultății de Inginerie

_____20.09.2023_____

Decan

Conf.dr.ing. ec. Dinu DARABĂ