FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	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	Licență
1.6 Programul de studii / Calificarea	Calculatoare
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	59.00

2. Date despre disciplină

2.1 Denumirea disciplinei	Criptografie și securitate informațională						
2.2 Aria de conţinut							
2.3 Responsabil de curs	Șef lucr.dr.ing. Adrian Petrovan, adrian.petrovan@ieec.utcluj.ro						
2.4 Titularul activităţilor de seminar / laborator / proiect	Șef lucr.dr.ing. Adrian Petrovan, adrian.petrovan@ieec.utcluj.ro						
2.5 Anul de studiu	4	2.6 Semestrul	2	2.7 Tipul de evaluare	E	2.8 Regimul disciplinei	DS/DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	2	din care: 3.2 curs	2	3.3 proiect	2
3.4 Total ore din planul de învăţământ	56	din care: 3.5 curs	28	3.6 proiect	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					10
Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri					12
Tutoriat					3
Examinări					4
Alte activităţi.……					

3.7 Total ore studiu individual	69
3.8 Total ore pe semestru	125
3.9 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Rețele de calculatoare
4.2 de competenţe	Cunoștințe ale disciplinei rețele de calculatoare

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Calculator și access la Internet
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Acces internet, Software specific

6. Competenţele specifice acumulate

Competenţe profesionale	**C5 -Întreţinerea şi exploatarea sistemelor hardware, software şi de comunicaţii** C5.1 -Identificarea şi descrierea instrumentelor de modelare, simulare şi evaluare a performanţelor sistemelor hardware, software şi de comunicaţii C5.2 -Utilizarea unor cunoştinţe interdisciplinare pentru asigurarea exploatării sistemelor hardware, software şi de comunicaţiiîn raport cu cerinţele domeniului de aplicaţii C5.3 -Utilizarea unor principii şi metode de bază pentru asigurarea securităţii, siguranţei şi uşurinţei în exploatare a sistemelor hardware, software şi de comunicaţii C5.4 -Testarea şi evaluareacalitativă a caracteristicilor funcţionale şi nefuncţionale ale sistemelor informatice, pe baza unor criterii specifice C5.5 -Dezvoltarea de sisteme şi aplicaţii pentru întreţinerea şi utilizarea desisteme hardware, software şi de comunicații
Competenţe transversale	**N/A**

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

7.1 Obiectivul general al disciplinei	Cunoașterea conceptelor, aplicațiilor și tehnologiilor pentru securitatea sistemelor și a software. Dobândirea abilității de a contribui constructiv la analiza, evaluarea și proiectarea sistemelor sigure.
7.2 Obiectivele specifice	Înțelegerea componentelor fundamentale legate de securitatea sistemelor, a riscurilor legate de utilizarea lor, a vulnerabilităților și amenințărilor importante. Participarea activă la identificarea și analiza problemelor de securitate informatică.Folosirea criptografiei in protecția informației. Aplicarea tehnicilorpotrivite pentru rezolvarea unor probleme de securitate. Înțelegerea construcției mecanismelor de securitate și aplicarea lor

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
Concepte de securitate generale	Exponere online pe platforma **kb.cunbm.utcluj.ro**	2 ore
Scrierea programelor cu grad ridicat de securitate. Șirurile în C/C++. Gestiunea memoriei		2 ore
Introducere în criptografie. Transpoziție și substituție. Criptografia simetrică		2 ore
Introducere în criptografie. Criptografia asimetrică.		4 ore
Securitatea programelor. Codul rău intenționat		4 ore
Securitatea în sistemele de operare.Protecția în SO. Controlul accesului. Arhitectura de securitate. Securitatea accesului:parolele Securitatea SO Windows		2 ore
Securitatea reţelelor de calculatoare. Conexiuni securizate –SSL/TLS, IPSEC		4 ore

Securitatea reţelelor de calculatoare. Ziduri antifoc. Detecția intruziunilor		4 ore
Securitatea stocării. Testarea penetrării. Securitatea WLAN. Botnets		4 ore
Bibliografie 1.Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, 3rd edition, Prentice Hall PTR; 3 edition (December 2, 2003), ISBN: 0130355488,în limba engleză 2.Matt Bishop, Introduction to Computer Security, Addison-Wesley Professional (October 26, 2004), ISBN: 0321247442, în limba engleză 3.Robert C. Seacord, Secure Coding in C and C++, Addison Wesley Professional (September 09, 2005), ISBN: 978-0-7686-8592-3, în limba engleză		
8.2 Lucrări de laborator	Metode de predare	Observaţii
Algoritmicriptograficiclasici –aplicații, partea 1	Exponere online pe platforma **kb.cunbm.utcluj.ro**	
Algoritmi criptografici clasici –aplicații, partea 2		
Metode și utilitare de analiză a numerelor aleatoare și a pattern-urilor în fluxuri de date pentru analiza criptografică, partea 1		
Metode și utilitare de analiză a numerelor aleatoare și a pattern-urilor în fluxuri de date pentru analiza criptografică, partea 2		
Implementarea unor cifruri de tip stream și bloc în C		
Implementarea unor funcții hash în C		
Prezentarea unor cazuri recente de atacuri criptografice. Discuții		
Topic-uri și metode noi de criptografie		
Crearea tunelurilor securizate cu SSH		
Aplicații de tip firewall		
Configurarea și monitorizarea unui firewall în Windows		
Configurarea și monitorizarea unui firewall în Linux		
Atacuri împotriva DNS și serverelor de Web		
Verificarea activității de laborator		
Bibliografie 1. Understanding Cryptography: A Textbook for Students and Practitioners,(Paar, Pelzl-2010,Springer-Verlag New York Inc .) 2. Cryptography Engineering: Design Principles and Practical Applications (Ferguson, Niels -2010-Willey) 3. Cryptography and Network Security. Principles and Practice (Stallings, William –2013 –Prentice Hall) 4. Cryptography: A Very Short Introduction (Piper, Fred –2002 –Oxford University Press) 5. Ogletree, T.W., Firewalls – Protecția rețelelor conectate la Internet, Teora, 2001. 6. Barrett, D., Silverman, R., SSH, The Secure Shell. TheDefinitive Guide, O'Reilly, 2001.		

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

Este o disciplină a domeniului "Calculatoare și Tehnologia Informației". În cadrul acestei discipline studenții au posibilitatea însușiirii unor cunoștințe esențiale privind securitatea informatică. Totodată vor putea experimenta în cadrul lucrărilor de laborator diferite mecanisme de asigurare a securității sistemelor informatice, sistemelor software și rețelelor de calculatoare.

10. Evaluare (prezenta fizica / online)

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Abilități de utilizare a conceptelor din domeniul securității informatice Abilități de documentare a unor problematici specifice din cadrul domeniul securității informatice	Evaluare online pe baza de chestionar	60%

10.5 Seminar/Laborator	Abilități de rezolvare a problemelor utilizând tehnici de configurare a mecanismelor de securitate din cadrul diferitelor sisteme informatice Prezență, Activitate	Evaluare practică prin verificarea resurselor studenților	40%
10.6 Standard minim de performanţă			
Demonstrarea înțelegerii noțiunilor de bază, a principiilor și a metodelor uzuale din criptografie, cum ar fi: numere aleatoare, importanța problemelor fundamentale de matematică care stau la baza primitivelor de criptografie (cum ar fi problema de factorizării a două numere prime), proprietățile esențiale ale funcțiilor criptografice de hash, proprietățile criptografiei simetrice, noțiuni de criptanaliză, noțiuni și metode de atac criptografic, atacuri tip side-channel. Să poată specifica principalele vulnerabilități care pot afecta sistemele informatice; Să poată prezenta principalele politici, soluții și tehnici de securitate Să poată selecta și aplica politici de securitate în anumite cazuri specifice.			

Data completării:	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
	Curs	Șef lucr.dr.ing. Adrian Petrovan	
	Aplicații	Șef lucr.dr.ing. Adrian Petrovan	

Data avizării în Consiliul Departamentului Inginerie Electrică, Electronică și Calculatoare

_____

Director Departament Inginerie Electrică, Electronică și Calculatoare
Șef lucr..dr.ing. Claudiu Lung

Data aprobării în Consiliul Facultății de Inginerie

_____

Decan
Conf.dr.ing.,ec. Dinu Daraba