FIŞA DISCIPLINEI[1]

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Politehnica Timişoara
1.2 Facultatea[2] / Departamentul[3]	Automatică şi Calculatoare / Automatică şi Informatică Aplicată
1.3 Catedra	-
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	Licenţă
1.6 Programul de studii / Calificarea	Informatică / Informatician

2. Date despre disciplină

2.1 Denumirea disciplinei			**Securitatea informației**				
2.2 Titularul activităţilor de curs			Prof. dr. ing. Daniel Curiac				
2.3 Titularul activităţilor de seminar			Sl. dr. ing. Ovidiu Baniaş				
2.4 Anul de studiu	3	2.5 Semestrul	2	2.6 Tipul de evaluare	E	2.7 Regimul disciplinei	Obligatorie

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
Studiul după manual, suport de curs, bibliografie şi notiţe					10
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					10
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					10
Tutoriat					7
Examinări					3
Alte activităţi					

3.7 Total ore studiu individual	40
3.8 Total ore pe semestru	96
3.9 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	• Nu este cazul
4.2 de competenţe	• Cunoştinţe de matematică şi algoritmică elementară (la nivel de liceu)

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului	• Sală mare, Materiale suport: laptop, proiector, tablă.
5.2 de desfăşurare a seminarului/laboratorului	• Laborator cu 15-20 calculatoare – Mediu de programare pentru limbajul C, tablă

6. Competenţe specifice acumulate

Competenţe profesionale[4]	• Operarea cu concepte fundamentale din ştiinţa calculatoarelor, tehnologia informaţiei si comunicatiilor.

[1] Formularul corespunde Fişei Disciplinei promovată prin OMECTS 5703/18.12.2011 (Anexa3);

[2] Se înscrie numele facultăţii care gestionează programul de studiu căruia îi aparţine disciplina;

[3] Se înscrie numele departamentului căruia i-a fost încredinţată susţinerea disciplinei şi de care aparţine titularul cursului;

	Utilizarea fundamentelor automaticii, a metodelor de modelare, simulare, identificare şi analiză a proceselor, a tehnicilor de proiectare asistată de calculator. • Dezvoltarea de aplicaţii şi implementarea algoritmilor şi structurilor de conducere automata, utilizând principii de management de proiect, medii de programare şi tehnologii bazate pe microcontrolere, procesoare de semnal, automate programabile, sisteme încorporate.
Competenţe transversale	• 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. • Identificarea rolurilor şi responsabilităţilor într-o echipă plurispecializată luarea deciziilor si atribuirea de sarcini, cu aplicarea de tehnici de relaţionare şi muncă eficientă în cadrul echipei. • Identificarea oportunităţilor de formare continuă şi valorificarea eficientă a resurselor şi tehnicilor de învăţare pentru propria dezvoltare.

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

7.1 Obiectivul general al disciplinei	• Dobândirea noţiunilor de bază pentru securizarea informaţiei.
7.2 Obiectivele specifice	• însuşirea de către studenţi a tehnicilor moderne de securizare a datelor, cu precădere a securizării datelor prin criptare; • prezentarea principalelor breşe în securitatea sistemelor de calcul cuplate, precum şi a modului de realizare a protecţiei împotriva atacurilor asupra securităţii;

8. Conţinuturi

8.1 Curs	Număr de ore	Metode de predare
1. Introducere 1.1 Securitatea datelor; 1.2 Aspecte legate de securitatea informaţiei; 1.3 Servicii de securitate; 1.4 Modelul unei reţele sigure; 1.5 Atacuri; 1.6 Criptologia.	6	Prelegere susţinută de prezentări PPT, conversaţii, explicaţii, exemplificări
2. Criptarea convenţionala clasică 2.1 Modelul criptării convenţionale; 2.2 Algoritmi de criptare clasici	3	
3. Algoritmi moderni de criptare 3.1 Principiile codurilor bloc; 3.2 Structura codului Feistel; 3.3 DES (Data Encryption Standard); 3.4 AES (Advanced Encryption Standard). 3.5. Alti algoritmi cu utilizare larga (ex. RC6, Blowfish, etc.)	12	
4. Criptarea cu chei publice 4.1 Principii; 4.2 Algoritmul RSA; 4.3 Administrarea cheilor; 4.4 Algoritmul Diffie-Hellman; 4.5 Standardul pentru semnături digitale	5	
5. Studii de caz relativ la probleme de securitate in conducerea la distanta a proceselor industriale, retele de senzori, etc.	2	

Bibliografie

1. I.C. Mihai, *Securitatea informațiilor*, Editura Sitech, 2012
2. V.V. Patriciu, M. Ene Pietrosanu, I. Bica, J. Priescu, *Semnături electronice și securitate informatică*, Editura All, 2006
3. D.I. Curiac, *Tehnici de securizare a datelor si programelor*, Lito UPT, 2001
4. D.I. Curiac, *Algoritmi de criptare pentru securizarea datelor*, Editura Orizonturi Universitare, 2001
5. D.I. Curiac, *Securitatea informatiei*, Lito UPT, 2007
6. *Securitatea informatiei* (canalul media oficial al ARASEC - Asociația Română pentru Asigurarea Securității Informației), http://www.securitatea-informatiilor.ro/

8.2 Laborator/proiect	Număr de ore	Metode de predare
1. Codul Caesar, Roata alfabetica, Codificarea cu ceasul spiral,	2	Expunere temă, discuţii, întrebări, rezolvare pe
2. Corelaţia alfabet&cuvint, Codificarea busola, Codificarea Pig Latin	2	

[4] Aspectul competenţelor profesionale va fi tratat cf. Metodologiei OMECTS 5703/18.12.2011. Se vor prelua competenţele care sunt precizate în Registrul Naţional al Calificărilor din Învăţământul Superior RNCIS (http://www.rncis.ro/portal/page?_pageid=117,70218&_dad=portal&_schema=PORTAL) pentru domeniul de studiu de la pct. 1.4, programul de studii de la pct. 1.6 din această fişă şi materia în cauză

3. Tabela Viginere, Tabela Porta, Codificări matrice	2	calculator a 1-2 probleme.
4. Coduri monoalfabetice, Maşini rotative, Codificare Pig Pen	2	
5. Codificare tip harta, Diagraphic substitution.	2	
6. Realizarea si susținerea orala a unui referat asupra unui topic ce intervine in securizarea sistemelor (Firewalls, viruşi informatici, Programe antivirus, Sistemul Kerberos, Sistemul SESAME, PGP/PEM, securitatea sistemelor incorporate, criptarea pe curbe eliptice, criptarea cuantica, etc.)	6	
7. Proiectarea si implementarea intr-unul din limbajele cunoscute (de preferința C, pentru a satisface necesitatile de viteza) a unui algoritm modern de criptare destinat unor sisteme precizate prin tema de proiectare: un exemplu – securizarea informației prin criptare in rețele de senzori: alegerea tipului de algoritm (cheie secreta/cheie publica); alegerea algoritmului in funcție de lungimea mesajelor schimbate de senzori, de durata de viața a mesajelor, etc.; implementarea in C; testarea.	10	
8. Recuperări	2	

Bibliografie

1. I.C. Mihai, *Securitatea informațiilor*, Editura Sitech, 2012
2. V.V. Patriciu, M. Ene Pietrosanu, I. Bica, J. Priescu, *Semnături electronice și securitate informatică*, Editura All, 2006
3. D.I. Curiac, *Tehnici de securizare a datelor si programelor*, Lito UPT, 2001
4. D.I. Curiac, *Algoritmi de criptare pentru securizarea datelor*, Editura Orizonturi Universitare, 2001
5. D.I. Curiac, *Securitatea informatiei*, Lito UPT, 2007
6. *Securitatea informatiei* (canalul media oficial al ARASEC - Asociația Română pentru Asigurarea Securității Informației), http://www.securitatea-informatiilor.ro/

9. Corelarea conţinutului disciplinei cu cerinţele specialiştilor din domeniu şi cu aşteptările angajatorilor reprezentativi

- Cunoştinţele de securizare a informației sunt importante pentru toate componentele (software sau hardware) din domeniile IT&C si conducerea proceselor.
- Majoritatea angajatorilor reprezentativi din domeniul aferent programului solicită cunoştinţe specifice securizării informației.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Rezolvarea unui subiect conținând patru problematici teoretice si aplicative	Examinare scrisă	66 %
10.5 Laborator/proiect	Rezolvarea problemelor corespunzătore lucrărilor de laborator	Prezentarea rezolvărilor, răspunsuri la întrebări	9 %
	Teme de casă	Prezentarea rezolvărilor, răspunsuri la întrebări	8 %
	Test laborator	Examinare scrisă	16 %
10.6 Standard minim de performanţă (volumul de cunoştinţe minim necesar pentru promovarea disciplinei şi modul în care se verifică stăpânirea lui)			
• Efectuarea tuturor aplicaţiilor practice de laborator si a temelor de laborator si realizarea a 50% răspunsuri corecte la partea scrisa (corespunzătoare cursului)			

11. Compatibilitate internaţională

- Stanford University http://crypto.stanford.edu/cs155/
- University of California - Berkeley http://inst.eecs.berkeley.edu/~cs161/fa08/
- Massachusetts Institute of Technology http://courses.csail.mit.edu/6.857/2013/

Data completării

Semnătura titularului de curs

Prof. dr. Ing. Daniel CURIAC

……..

Semnătura titularilor de laborator/proiect

Sl. dr. ing. Ovidiu BANIAS

……

Data avizării în departament

Semnătura directorului de departament

Prof. dr. Ing. Ioan SILEA

……