

FIȘA DISCIPLINEI

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea „Tibiscus” din Timișoara
1.2. Facultatea	Calculatoare și Informatică Aplicată
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Licență
1.6. Programul de studii/Calificarea	Informatică / Asistent de cercetare în informatică - 214918; Proiectant sisteme informatice - 25110; Analist - 251201; Administrator baze de date - 252101; Administrator de rețea de calculatoare - 252301; Profesor în învățământul gimnazial - 233002; Programator - 251202

2. Date despre disciplină

2.1. Denumirea/codul disciplinei	ALGORITMI DE SECURITATE INFORMATICĂ (ASI) - LIN221						
2.2. Titularul activității de curs	Lect.univ.drd. Lucian Valentin Ciorba						
2.3. Titularul activității de laborator	Lect.univ.drd. Lucian Valentin Ciorba						
2.4. Anul de studiu	2	2.5. Semestrul	2	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	DF

3. Timpul total estimat

3.1. Numărul de ore pe săptămână	4	din care 3.2. curs	2	3.3. laborator+proiect	1+1
3.4. Total ore din planul de învățământ	56	din care 3.5. curs	28	3.6. laborator+proiect	14+14
Distribuția fondului de timp					Ore
Studiul după manual, suport de curs, bibliografie și notițe					24
Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate					20
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					25
Tutoriat					4
Examinări					4
Alte activități					
3.7. Total ore studiu individual					69
3.8. Total ore pe semestru					125
3.9. Numărul de credite					5

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	-
4.2. de competențe	Bune cunoștințe de programare într-un limbaj de nivel înalt

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Online: Google Classroom, Zoom
5.2. de desfășurare a seminarului/laboratorului	Online: Google Classroom, Zoom

6. Competențe specifice acumulate

6.1. Competențe profesionale	C1. Descrierea de concepte, teorii și modele folosite în domeniul de aplicare. C2. Identificarea și explicarea modelelor informatice de baza adecvate domeniului de aplicare. C3. Analiza datelor și a modelelor. C4. Elaborarea componentelor informatice ale unor proiecte interdisciplinare.
------------------------------	--

6.2. Competențe transversale	CT1. Desfășurarea eficientă a activităților organizate într-un grup inter-disciplinar CT2. Dezvoltarea capacităților empatice de comunicare inter-personală, de relaționare și colaborare cu grupuri diverse.
------------------------------	--

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

7.1. Obiectivul general al disciplinei	Cunoașterea diferitelor sisteme de numerație și a regulilor de bază ale operațiilor aritmetice, înțelegerea metodelor de reprezentare a datelor
7.2. Obiectivele specifice	Explicarea diferitelor tehnici de transformare a numerelor între bazele de numerație, explicarea tehnicilor de implementare a formulelor logice, prezentarea algoritmilor specifici de reducere a formulelor logice

8. Conținuturi

8.1. Curs	Metode de predare	Observații
Probleme ale protecției și securității datelor -Noțiuni generale -Vulnerabilitatea informației și calculatoarelor -Modele de securitate a informației	Expunerea interactivă, problematizarea, conversația euristică, documentarea pe web, exemplificarea	Materialele de curs vor fi postate pe Google Classroom Întâlnirile online vor fi pe ZOOM
Evoluția sistemelor criptografice -Structura unui sistem criptografic -Evoluția istorică a criptografiei		
Bazele matematice ale criptografiei -Noțiuni generale. Informație și entropie -Modelul matematic al unui sistem criptografic	Expunerea interactivă, problematizarea, conversația euristică, documentarea pe web, exemplificarea	Materialele de curs vor fi postate pe Google Classroom Întâlnirile online vor fi pe ZOOM
Metode criptografice clasice -Metoda substituției -Metoda transpoziției -Metode computaționale: sisteme simetrice, sisteme cu chei publice -Metode cu coduri redundante		
Arhitecturi de securitate la calculatoare și sisteme distribuite -Protecția informațiilor -Protocoale de identificare și autentificare -Protocoale pentru transferul de date -Integrarea securității în arhitectura rețelelor de calculatoare	Expunerea interactivă, problematizarea, conversația euristică, documentarea pe web, exemplificarea	Materialele de curs vor fi postate pe Google Classroom Întâlnirile online vor fi pe ZOOM

Bibliografie

- [1] I. Angheloiu, E. Gyorfi, V. V. Patriciu, *Securitatea și protecția informației în sistemele electronice de calcul*, Editura Militară, București, 1986
- [2] T. Băjenescu, M. Borda, *Securitatea în informatică și telecomunicații*, Editura Dacia, Cluj Napoca, 2001
- [3] D. Ionescu, *Codificare și coduri*, Editura Tehnică, București, 1981
- [4] T. M. Karnyanszky, *Coduri și criptografie*, Timișoara, 2015 – sub tipar
- [5] V. V. Patriciu, *Criptografia și securitatea rețelelor de calculatoare cu aplicații în C și Pascal*, Editura Tehnică, București, 1994
- [6] V. V. Patriciu, M. Pietroșanu-Ene, I. Bica, C. Cristea, *Securitatea informatică în Unix și Internet*, Editura Tehnică, București, 1998
- [7] D. Tărniceriu, *Prelucrarea Digitală a Semnalelor*, Universitatea Tehnică “Gh. Asachi” Iași, 2018, disponibil pe: http://telecom.etc.tuiasi.ro/pns/cc/curs_cc/criptare_curs_an6.pdf
- [8] Harold F. Tipton, Micki Krause – *Information Security Management Handbook*, Auerbach Publications, CRC Press LLC, 2000

8.2. Laborator/proiect	Metode de predare/învățare	Observații
1. Pătratul lui Polibiu	Exercițiul, discuțiile și dezbaterile, modelarea, proiectul, lucrul în grup organizat	Laboratoarele și temele vor fi postate pe Google Classroom
2. Coduri Shannon-Fano		
3. Coduri cu substituție monoalfabetică		
4. Coduri de tip Vigenere		
5. Coduri omofonice		
6. Coduri cu transpoziție pe blocuri de caractere		

7. Coduri cu transpoziție cu cheie literală	Exercițiul, discuțiile și dezbaterile, modelarea, proiectul, lucrul în grup organizat	Laboratoarele și temele vor fi postate pe Google Classroom
8. Cifruri bloc cu transpoziții și deplasări		
9. Cifruri bloc cu operații complexe		
10. Cifruri cu chei publice		
11. Mecanism de semnătură electronică		
12. Mecanism de identificare și autentificare a utilizatorului		
13. Mecanism de verificare a posibilităților de acces		
14. Cifruri hardware		

Bibliografie

- [1] T. Băjenescu, M. Borda, *Securitatea în informatică și telecomunicații*, Editura Dacia, Cluj Napoca, 2001
 [2] M. Joldoș, *Securitatea sistemelor și a aplicațiilor*, Universitatea Tehnică din Cluj-Napoca, 2015, disponibil pe: <http://users.utcluj.ro/~jim/SSA/Resources/Laboratory/>
 [3] T. M. Karnyanszky, *Coduri și criptografie*, Timișoara, 2015
 [4] V. V. Patriciu, *Criptografia și securitatea rețelelor de calculatoare cu aplicații în C și Pascal*, Editura Tehnică, București, 1994
 [5] V. V. Patriciu, M. Pietroșanu-Ene, I. Bica, C. Cristea, *Securitatea informatică în Unix și Internet*, Editura Tehnică, București, 1998

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

Conținutul disciplinei corespunde curriculei din alte centre universitare, din țară sau Uniunea Europeană.
 Conținuturile practice (lucrări de laborator) corespund cerințelor de pe piața muncii locală.

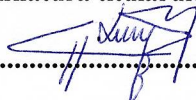
10. Evaluare

Tip de activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Examen	Probă scrisă online	25%
10.5. Laborator/proiect	Teme de laborator	Activitate de laborator online	25%
	Proiect individual	Prezentare online	50%
10.6. Standard minim de performanță			
Examinare scrisă: <i>Aspecte minimale teoretice ale securității informației</i> Probe practice și activitate de laborator: <i>Realizarea unor programe folosind metode de cifrare/descifrare și aplicații practice folosind noțiuni de bază ale sistemelor de operare</i>			

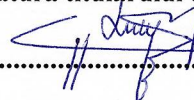
Data completării

28.09.2020

Semnătura titularului de curs



Semnătura titularului de laborator/proiect



Data avizării în departament

05.10.2020

Semnătura directorului de departament

