FIŞA DISCIPLINEI

Denumirea disciplinei :		Compresia,Criptarea şi Securitatea Datelor			
Codul disciplinei:					
Domeniul:		Calculatoare şi Tehnologia Informaţiei			
Specializarea:		Calculatoare			
Catedra:		Calculatoare şi Automatizări			
Facultatea:		Facultatea de Inginerie „Hermann Oberth”			
Universitatea:		Universitatea „Lucian Blaga” din Sibiu			
Anul de studiu**:**	4	Semestrul	7	Tipul de evaluare finală	**Examen**
Regimul disciplinei (DI=obligatorie/ DO=opţională/DF=liber aleasă):			**DF**	Numărul de credite:	**4**
Categoria formativă a disciplinei (DF=fundamentală.; DI=ingineresti; DS=specialitate; DC=complementară)					**DS**
Total ore din planul de învăţământ		**4**		Total ore pe semestru:	56
Titularul disciplinei: conf. dr. ing. Macarie BREAZU					

Numărul total de ore (pe semestru) din planul de învăţământ					
Total ore/ semestru	**C**	**S**	**L**	**P**	**Total**
	28	**0**	**28**	**0**	**56**

Obiective:	Cunoaşterea de către studenţi a metodelor consacrate de compresie, criptare şi securitate a datelor şi a soluţiilor impuse recent în domeniu, domeniu care a cunoscut o creştere explozivă odată cu dezvoltarea Internetului
Competenţe specifice disciplinei	**1. Cunoaştere şi înţelegere:** • cunoaşterea şi înţelegerea principiilor generale ale disciplinei • cunoaşterea şi operarea adecvată cu noţiunile specifice disciplinei • dobândirea capacităţii de a integra cunoştinţe dobândite la alte cursuri • identificarea principalelor surse de informare
	2. Explicare şi interpretare: • analiza critică a modelelor teoretice, ideilor şi a abordărilor consacrate • aptitudini de realizare a unui proiect şi a unui raport aferent • familiarizarea cu munca în echipă
	3. Instrumental – aplicative: • cunoaşterea şi stăpânirea mediilor de dezvoltare consacrate • proiectarea pe diverse niveluri ale aplicaţiilor • utilizarea unei game variate de strategii, metode, tehnici de proiectare, implementare şi evaluare

	4. Atitudinale: • renunţarea la atitudinea de dezinteres faţă de şcoală • dobândirea unei atitudini pozitive faţă de activitatea de cercetare • aprecierea muncii în echipă, responsabilizarea faţă de rezultatele echipei • dobândirea unei atitudini pozitive faţă de (necesitatea validării aspectelor teoretice prin) aplicaţia practică • conştientizarea necesităţii participării la propria dezvoltare profesională.

Conţinutul tematic (descriptori)	**TEMATICA CURSURILOR**		
	Nr. crt.	Denumirea temei	Nr. ore
	1	Introducere, modele generale, clasificări.	2
	2	Elemente de teoria transmiterii informaţiei şi codării.	2
	3	Compresie bazată pe modelare statistică: codare Shannon-Fano, codare Huffman statică şi dinamică, codare aritmetică.	4
	4	Compresie bazată pe modelare lingvistică: LZ77, LZ78, LZW	2
	5	Codare bazată pe transformate, DCT, standarde de compresie a imaginilor JPEG şi a secvenţelor video MPEG.	4
	6	Codare predictivă, DPCM, compresie cu pierderi controlate (near-lossless).	2
	7	Criptografia computaţională convenţională (simetrică).	2
	8	Criptografia computaţională cu chei publice (asimetrică).	2
	9	Securitatea transferului de date.Gestiunea cheilor de cifrare.	2
	10	Autentificare, semnătură digitală,	2
	11	Protectie şi securitate la nivelul sistemului de operare	2
	12	Aplicaţii: securitatea în Internet	2
	TEMATICA LABORATOARELOR		
	1	Introducere, codificare RLE, Formatul BinHex.	2
	2	Codificare Shannon-Fano şi Huffman static.	2
	3	Codificare Huffman dinamic.	2
	4	Codificare LZ77, LZ78, LZW.	2
	5	Compresie de imagini bazată pe DCT - JPEG.	4
	6	Compresie predictivă lossless şi near-lossless.	4
	7	Implementarea unui algoritm de criptare simetric.	2
	8	Implementarea unui algoritm de criptare asimetric.	2
	9	Implementarea unei scheme de criptare hibridă.	2
	10	Implementarea semnaturii digitale folosind funcţii hash şi criptare cu cheie publică.	2
	11	Instalarea protocolului SSL.	2
	12	Configurarea unei aplicaţii de tip firewall.	2

Metode de predare / seminarizare	Prelegeri, explicaţii, conversaţii, problematizări, demonstraţii, studii de caz, exerciţii, dezbateri

Stabilirea notei finale (procentaje)	- răspunsurile la examen/colocviu(evaluare finală)	60%
	- teste pe parcursul semestrului	
	- răspunsurile finale la lucrările practice de laborator	20%
	- activitaţi gen teme/referate/eseuri/traduceri/proiecte etc.	20%

	- teme de control	
	- alte activităţi*(precizaţi)*……..	
	- TOTAL	100%

Evaluarea finală va cuprinde examen scris (subiecte descriptive şi probleme).	
Cerinţe minime pentru nota 5 minim nota 5.00 la laborator/proiecte minim nota 4.50 la examen	**Cerinţe pentru nota 10** medie ponderată note minim 9.50
TOTAL ore studiu individual (pe semestru) = 40	

Bibliografia	**Minimală obligatorie**: 1. Alexandru Spătaru - *Teoria transmisiunii informaţiei* - Editura Didactică şi Pedagogică, Bucureşti, 1983 2. David Salomon, "*Data Compression: The Complete Referen*ce", Fourth Edition, ISBN 978-1846286025, Springer, 2006 3. Bruce Schneier, "*Applied Cryptography*", Second Edition, ISBN 0-471-11709-9, John Wiley & Sons, 1996 **Complementară:** 1. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, "*Operating System Concepts*", ISBN 0-471-25060-0, John Wiley & Sons, 2003 2. Khalid Sayood, "*Introduction to Data Compression*", Third Edition, ISBN: 978-0126208627, Morgan Kaufmann, 2005
Lista materialelor didactice utilizate în procesul de predare: note de curs, lista bibliografică, videoproiector, acces Internet	

	Grad didactic, titlul, prenume, numele	Semnătura
Coordonator de Disciplină	Conf. dr. ing. Macarie BREAZU	