

FIȘA DISCIPLINEI

Anul universitar 2023 - 2024

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Lucian Blaga din Sibiu
1.2. Facultatea	Științe
1.3. Departament	Matematică și Informatică
1.4. Domeniul de studiu	Informatică
1.5. Ciclul de studii ¹	Master
1.6. Specializarea	Informatică

2. Date despre disciplină

2.1. Denumirea disciplinei	Criptologie. Auditarea sistemelor informatice și managementul securității riscurilor	Cod	FSTI.MAI.STIA.M.SO.3.1020.E-6.14		
2.2. Titular activități de curs	Conf. univ. dr. Nicolae CONSTANTINESCU				
2.3. Titular activități practice	Conf. univ. dr. Nicolae CONSTANTINESCU				
2.4. An de studiu ²	2	2.5. Semestrul ³	1	2.6. Tipul de evaluare ⁴	E
2.7. Regimul disciplinei ⁵	O	2.8. Categoria formativă a disciplinei ⁶	S		

3. Timpul total estimat

3.1. Extinderea disciplinei în planul de învățământ – număr de ore pe săptămână					
3.1.a.Curs	3.1.b. Seminar	3.1.c. Laborator	3.1.d. Proiect	3.1.e Alte	Total
1	-	2	-	-	3
3.2. Extinderea disciplinei în planul de învățământ – total ore din planul de învățământ					
3.2.a.Curs	3.2.b. Seminar	3.2.c. Laborator	3.2.d. Proiect	3.2.e Alte	Total ⁷
14	-	28	-	-	42
Distribuția fondului de timp pentru studiu individual⁸					Nr. ore
Studiul după manual, suport de curs, bibliografie și notițe					43
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					31

¹ Licență / Master

² 1-4 pentru licență, 1-2 pentru master

³ 1-8 pentru licență, 1-3 pentru master

⁴ Examen, colocviu sau VP A/R – din planul de învățământ

⁵ Regim disciplină: O=Disciplină obligatorie; A=Disciplină opțională; U=Facultativă

⁶ Categoria formativă: S=Specialitate; F=Fundamentală; C=Complementară; I=Asistată integral; P=Asistată parțial; N=Neasistată

⁷ Este egal cu 14 săptămâni x numărul de ore de la punctul 3.1 (similar pentru 3.2.a.b.c.d.e.)

⁸ Liniile de mai jos se referă la studiul individual; totalul se completează la punctul 3.37.



Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	23
Tutoriat ⁹	7
Examinări ¹⁰	4
3.3. Total ore alocate studiului individual¹¹ (NOSI_{sem})	108
3.4. Total ore din Planul de învățământ (NOAD_{sem})	42
3.5. Total ore pe semestru¹² (NOAD_{sem} + NOSI_{sem})	150
3.6. Nr ore / ECTS	150
3.7. Număr de credite¹³	6

⁹ Între 7 și 14 ore

¹⁰ Între 2 și 6 ore

¹¹ Suma valorilor de pe liniile anterioare, care se referă la studiul individual.

¹² Suma (3.5.) dintre numărul de ore de activitate didactică directă (NOAD) și numărul de ore de studiu individual (NOSI) trebuie să fie egală cu numărul de credite alocate disciplinei (punctul 3.7) x nr. ore pe credit (3.6.)

¹³ Numărul de credit se calculează după formula următoare și se rotunjește la valori vecine întregi (fie prin micșorare fie prin majorare)

Unde:

- NOCpSpD = Număr ore curs/săptămână/disciplina pentru care se calculează creditele
- NOApSpD = Număr ore aplicații (sem./lab./pro.)/săptămână/disciplina pentru care se calculează creditele
- TOCpSdP = Număr total ore curs/săptămână din plan
- TOApSdP = Număr total ore aplicații (sem./lab./pro.)/săptămână din plan
- C_C/C_A = Coeficienți curs/aplicații calculate conform tabelului

Coeficienți

Curs

Aplicații (S/L/P)

Licență

2

1

Master

2,5

1,5

Licență lb. străină

2,5

1,25

4. Precondiții (acolo unde este cazul)

4.1. Discipline necesar a fi promovate anterior (de curriculum) ¹⁴	Fundamentele Programării, Algoritmi și Structuri de Date. Criptografie
4.2. Competențe	Întelegerea notiunilor de baza in domeniul constructiilor optime a variantelor de implementare a principiilor de protectie a informatiei, analizei limitelor de securitate al functiilor criptografice si modalitatea de limitare a pierderilor informationale datorate atacurilor informatice.

5. Condiții (acolo unde este cazul)

5.1. De desfășurare a cursului ¹⁵	Sală de curs, dotată cu tablă, calculator, videoproiector și software/Predare Oline
5.2. De desfășurare a activităților practice (lab/sem/pr/alte) ¹⁶	Sală de laborator dotată cu calculatoare desktop/Predare Online

6. Competențe specifice acumulate¹⁷

		Număr de credite alocate disciplinei ¹⁸	6	Repartizare credite pe competențe ¹⁹
6.1. Competențe profesionale	CP1	Cunoașterea și utilizarea adecvată a noțiunilor teoretice fundamentale legate de analiza limitărilor funcțiilor criptografice		1
	CP2	Capacitatea de a analiza rezistența la atacuri informatice a unui model criptografic și de analiza a gradului de risc al categoriilor de pierderi informaționale		2
	CP3	Capacitatea de a interpreta rezultatele obținute		1
6.2. Competențe transversale	CT1	Dezvoltarea atitudinii pozitive față de muncă și responsabilitate pentru propria pregătire profesională		1
	CT2	Dezvoltarea spiritului de muncă în echipă		1

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

7.1. Obiectivul general	Însușirea algoritmilor criptografici și a modului în care aceștia pot fi folosiți în diverse situații reale
7.2. Obiectivele specifice	Însușirea tehnicilor de criptare, codare, identificare respectiv corecție a erorilor și vulnerabilităților Protecția împotriva atacurilor informatice

8. Conținuturi

8.1. Curs ²⁰	Metode de predare ²¹	Nr. ore
Modele de analiză a gradului de risc al sistemelor software	Expunere, prelegere, prezentare la tablă a problematicei studiate, utilizare videoproiector, discuții cu studenții	1

¹⁴ Se menționează disciplinele obligatoriu a fi promovate anterior sau echivalente

¹⁵ Tablă, videoproiector, flipchart, materiale didactice specifice, platforme on-line etc.

¹⁶ Tehnică de calcul, pachete software, standuri experimentale, platforme on-line etc.

¹⁷ Competențele din Grilele aferente descrierii programului de studii, adaptate la specificul disciplinei

¹⁸ Din planul de învățământ

¹⁹ Creditele alocate disciplinei se distribuie pe competențe profesionale și transversale în funcție de specificul disciplinei

²⁰ Titluri de capitole și paragrafe

²¹ Expunere, prelegere, prezentare la tablă a problematicei studiate, utilizare videoproiector, discuții cu studenții (pentru fiecare capitol, dacă este cazul)



Analiza criptografică a algoritmilor clasici	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	1
Analiza criptografică a algoritmilor de criptare simetrici	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	1
Analiza criptografică a algoritmilor de criptare asimetrici	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	1
Analiza criptografică a sistemelor de semnătură digitală	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	1
Analiza criptografică a protocoalelor criptografice	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	2
Analiza criptografică a generatoarelor criptografice	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	1
Modele de analiză a riscului de pierdere informațională datorate atacurilor informatice	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	1
Audit asupra nivelului de securitate a aplicațiilor	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	1
Audit asupra codului sursă al aplicațiilor	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	2
Managementul riscurilor datorate pierderilor informaționale	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	2
Total ore curs:		14

8.2. Activități practice (8.2.a. Seminar ²² / 8.2.b. Laborator ²³ / 8.2.c. Proiect ²⁴ / 8.2.d. Alte act.practice ²⁵)	Metode de predare	Nr. ore
Aplicatii de analiza a nivelului de securitate al sistemelor software	<i>Demonstrație practică, exercițiu</i>	4
Softare de analiza criptografica a algoritmilor clasici	<i>Demonstrație practică, exercițiu, implementare</i>	4
Software de analiza criptografica a algoritmilor simetrici	<i>Demonstrație practică, exercițiu, implementare</i>	2
Software de analiza criptografica a algoritmilor asimetrici	<i>Demonstrație practică, exercițiu, implementare</i>	2
Analiza experimentală: limitarile semnăturii digitale	<i>Demonstrație practică, exercițiu, implementare</i>	2
Analiza experimentală: limitarile protocoalelor criptografice	<i>Demonstrație practică, exercițiu, implementare</i>	2
Analiza experimentală: auditul SO	<i>Demonstrație practică, exercițiu, implementare</i>	4
Analiza experimentală: auditul sistemelor de autentificare	<i>Demonstrație practică, exercițiu, implementare</i>	2
Analiza experimentală: auditul software-ului de stocare externa	<i>Demonstrație practică, exercițiu</i>	2
Analiza experimentală: managementul riscului pentru pierdere informatională	<i>Demonstrație practică, exercițiu</i>	4
Total ore seminar/laborator		28

9. Bibliografie

9.1. Referințe bibliografice recomandate	R. Pompon, IT Security Risk Control Management, An Audit Preparation Plan, Apress 2016
	S. Parkinson, A. Crampton, R. Hill, Guide to Vulnerability Analysis for Computer Networks and Systems, Springer 2021
9.2. Referințe bibliografice suplimentare	Nicolae Constantinescu, Criptografie, Editura Academiei Romane, 2009
	An Introduction to Computer Security, NIST 2017

10. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului²⁶

Se realizează prin contacte periodice cu aceștia în vederea analizei problemei. Conținutul disciplinei a fost stabilit ținând cont de interacțiunile constructive ale cadrelor didactice, studenților și a reprezentanților din mediul economic, științific, în cadrul manifestărilor științifice, întâlnirilor de lucru și activităților de practică și dezvoltare de proiecte a studenților.

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală	Obs. ²⁷	
		Teste pe parcurs ²⁸ :	25%	50% (minim 5)	CPE

²² *Discuții, dezbateri, prezentare și/sau analiză de lucrări, rezolvare de exerciții și probleme etc.*

²³ *Demonstrație practică, exercițiu, experiment etc.*

²⁴ *Studiu de caz, demonstrație, exercițiu, analiza erorilor etc.*

²⁵ *Alte tipuri de activități practice specifice*

²⁶ *Legătura cu alte discipline, utilitatea disciplinei pe piața muncii*

²⁷ *CPE – condiționează participarea la examen; nCPE – nu condiționează participarea la examen; CEF - condiționează evaluarea finală; N/A – nu se aplică*

²⁸ *Se va preciza numărul de teste și săptămânile în care vor fi susținute.*



11.4a Examen / Colocviu	● Cunoștințe teoretice și practice însușite (cantitatea, corectitudinea, acuratețea)	Teme de casă:	20%		
		Alte activități ²⁹ :	5%		
		Evaluare finală:	50% (min. 5)		
11.4b Seminar	● Frecvența/relevanța intervențiilor sau răspunsurilor	Evidența intervențiilor, portofoliu de lucrări (referate, sinteze științifice)		% (minim 5)	N/A
11.4c Laborator	● Cunoașterea aparatului, a modului de utilizare a instrumentelor specifice; evaluarea unor instrumente sau realizări, prelucrarea și interpretarea unor rezultate	<ul style="list-style-type: none"> ● Chestionar scris ● Răspuns oral ● Caiet de laborator, lucrări experimentale, referate etc. ● Demonstrație practică 		25% (minim 5)	nCPE
11.4d Proiect	● Calitatea proiectului realizat, corectitudinea documentației proiectului, justificarea soluțiilor alese	<ul style="list-style-type: none"> ● Autoevaluarea, prezentarea și/sau susținerea proiectului ● Evaluarea critică a unui proiect 		25% (minim 5)	CPE
11.5 Standard minim de performanță ³⁰ : CP5					CEF

Fișa disciplinei cuprinde componente adaptate persoanelor cu CES (persoane cu dizabilități și persoane cu potențial înalt), în funcție de tipul și gradul acestora, la nivelul tuturor elementelor curriculare (competențe, obiective, conținuturi, metode de predare, evaluare alternativă), pentru a asigura șanse echitabile în pregătirea academică a tuturor studenților, acordând atenție sporită nevoilor individuale de învățare.

Data completării: | 2 | _ | 5 | _ | / | 0 | _ | 9 | _ | / | 2 | _ | 0 | _ | 2 | _ | 3 | _ |

Data avizării în Departament: | 2 | _ | 8 | _ | / | 0 | _ | 9 | _ | / | 2 | _ | 0 | _ | 2 | _ | 3 | _ |

	Grad didactic, titlul, prenume, numele	Semnătura
Titular disciplină	Conf. Univ. Dr. Nicolae CONSTANTINESCU	
Responsabil program de studii	Conf. Univ. Dr. Florin STOICA	
Director Departament	Prof. Univ. Dr. Mugur ACU	

²⁹ Cercuri științifice, concursuri profesionale etc.

³⁰ Se particularizează la specificul disciplinei standardul minim de performanță din grila de competențe a programului de studii, dacă este cazul.