

FIȘA DISCIPLINEI

Anul universitar 2025 - 2026

1. Date despre program

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

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-6.5			
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			3	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
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					25
3.7. Număr de credite¹³					6

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 în domeniul construcțiilor optime a variantelor de implementare a principiilor de protecție a informației, analizei limitelor de securitate al funcțiilor criptografice și modalitatea de limitare a pierderilor informaționale 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. Rezultate ale învățării ¹⁷

Numărul de credite alocate disciplinei: 6				
Rezultatele învățării				Repartizare credite pe rezultatele învățării
Nr. crt.	Cunoștințe	Aptitudini	Responsabilitate și autonomie	
RÎ 1	Studentul explică modelele de analiză a riscului pentru sisteme software și conceptele fundamentale de criptanaliză.	Studentul aplică metode de analiză a riscului și identifică posibile vulnerabilități.	Studentul demonstrează responsabilitate în interpretarea rezultatelor și adoptă o atitudine critică.	1.5
RÎ 2	Studentul descrie metode de analiză criptografică a algoritmilor clasici, simetrici și asimetrici.	Studentul realizează evaluări practice asupra securității algoritmilor și compară nivelurile lor de rezistență.	Studentul manifestă autonomie în alegerea algoritmilor și respectă bune practici profesionale.	1.5
RÎ 3	Studentul înțelege analiza criptografică a semnăturilor digitale, protocoalelor criptografice și generatoarelor criptografice.	Studentul aplică tehnici de testare și evaluare a acestor mecanisme.	Studentul își asumă responsabilitatea utilizării instrumentelor și respectă normele legale și etice.	1.5
RÎ 4	Studentul explică modelele de audit și management al riscului pentru aplicații și cod sursă.	Studentul efectuează audituri de securitate și elaborează recomandări pentru reducerea riscurilor.	Studentul dovedește responsabilitate ridicată în documentarea rezultatelor și adoptă o conduită profesională.	1.5

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

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

8. Conținuturi

8.1. Curs ¹⁸	Metode de predare ¹⁹	Nr. ore
--------------------------------	--	----------------

Modele de analiză a gradului de risc al sistemelor software	<i>Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții</i>	1
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 riscului de pierderi informaționale 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 ²⁰ / 8.2.b. Laborator ²¹ / 8.2.c. Proiect ²² / 8.2.d. Alte act.practice ²³)	Metode de predare	Nr. ore
Aplicatii de analiza a nivelului de securitate al sistemelor software	<i>Demonstrație practică, exercițiu</i>	4
Software de analiza criptografică a algoritmilor clasici	<i>Demonstrație practică, exercițiu, implementare</i>	4
Software de analiza criptografică a algoritmilor simetrici	<i>Demonstrație practică, exercițiu, implementare</i>	2
Software de analiza criptografică a algoritmilor asimetrici	<i>Demonstrație practică, exercițiu, implementare</i>	2
Analiza experimentală: limitările semnăturii digitale	<i>Demonstrație practică, exercițiu, implementare</i>	2
Analiza experimentală: limitările 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 externă	<i>Demonstrație practică, exercițiu</i>	2
Analiza experimentală: managementul riscului pentru pierdere informațională	<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 Române, 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 programului²⁴

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. ²⁵
11.4a Examen / Colocviu	• Cunoștințe teoretice și practice însușite (cantitatea, corectitudinea, acuratețea)	Teste pe parcurs ²⁶ :	25%	50% (minim 5)	CPE
		Teme de casă:	20%		
		Alte activități ²⁷ :	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 aparaturii, a modului de utilizare a instrumentelor specifice; evaluarea unor instrumente sau realizări, prelucrarea și interpretarea unor rezultate	• 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	• Autoevaluarea, prezentarea și/sau susținerea proiectului • Evaluarea critică a unui proiect	25% (minim 5)	CPE
11.5 Standard minim de performanță ²⁸ : CP5. Cunoasterea tehnicilor clasice de analiza criptografică, a modelelor elementare de detectare și soluționare a breșelor de securitate.				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: |_0_|_8_| / |_0_|_9_| / |_2_|_0_|_2_|_5_|

Data avizării în Departament: |_1_|_0_| / |_0_|_9_| / |_2_|_0_|_2_|_5_|

	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	

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.

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)

$$\text{Nr. credite} = \frac{\text{NOCpSpD} \times C_C + \text{NOApSpD} \times C_A}{\text{TOCpSpD} \times C_C + \text{TOApSpD} \times C_A} \times 30 \text{ credite}$$

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
- TOCpSpD = Număr total ore curs/săptămână din plan
- TOApSpD = 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

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 Titluri de capitole și paragrafe

¹⁹ Expunere, prelegere, prezentare la tablă a problematicei studiate, utilizare videoproiector, discuții cu studenții (pentru fiecare capitol, dacă este cazul)

²⁰ Discuții, dezbateri, prezentare și/sau analiză de lucrări, rezolvare de exerciții și probleme etc.

²¹ Demonstrație practică, exercițiu, experiment etc.

²² Studiu de caz, demonstrație, exercițiu, analiza erorilor etc.

²³ Alte tipuri de activități practice specifice

²⁴ Legătura cu alte discipline, utilitatea disciplinei pe piața muncii

²⁵ CPE – condiționează participarea la examen; nCPE – nu condiționează participarea la examen; CEF - condiționează evaluarea finală; N/A – nu se aplică

²⁶ Se va preciza numărul de teste și săptămânile în care vor fi susținute.

²⁷ Cercuri științifice, concursuri profesionale etc.

²⁸ Se particularizează la specificul disciplinei standardul minim de performanță din grila de competențe a programului de studii, dacă este cazul.