FIŞA DISCIPLINEI

Anul universitar 2026 - 2027

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	Securitate Cibernetică			Cod	FSTI.MAI.STIA.M.SO.4.1020.E-7.3	
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]		4	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 individual[8]	**Nr. ore**
Studiul după manual, suport de curs, bibliografie și notițe	26
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren	26
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	69
Tutoriat[9]	7
Examinări[10]	5
3.3. Total ore alocate studiului individual[11] ***(NOSI$_{sem}$)***	**133**
3.4. Total ore din Planul de învățământ (*NOAD$_{sem}$*)	**42**
3.5. Total ore pe semestru[12] **(*NOAD$_{sem}$* + *NOSI$_{sem}$*)**	**175**
3.6. Nr ore / ECTS	**25**
3.7. Număr de credite[13]	**7**

4. Precondiții (acolo unde este cazul)

4.1. Discipline necesar a fi promovate anterior (de curriculum) [14]	Criptografie, Fundamentele Programării, Rețele de Calculatoare, Algoritmi și Structuri de Date, Sisteme de Operare
4.2. Competențe	Intelegerea notiunilor necesare pentru gestionarea si ameliorarea vulnerabilitatilor din sistemele de calcul si ale conexiunilor dintre acestea. Impolementarea si gestionarea politicilor de securitate. Elemente primare de audit de securitate cibernetica.

5. Condiții (acolo unde este cazul)

5.1. De desfășurare a cursului[15]	Tablă, Videoproiector
5.2. De desfășurare a activităților practice (lab/sem/pr/alte) [16]	Rețea de calculatoare conectată la internet

6. Rezultate ale învățării [17]

Numărul de credite alocat disciplinei: 7				
Rezultatele învățării				Repartizare credite pe rezultatele învățării
Nr. crt.	Cunoștințe	Aptitudini	Responsabilitate și autonomie	
RÎ 1	Studentul explică noțiunile fundamentale de securitate a informației, clasificarea informațiilor și standardele de securitate.	Studentul aplică criterii și proceduri de clasificare și stabilește niveluri de protecție.	Studentul demonstrează responsabilitate în respectarea standardelor și adoptă o conduită etică.	1.5
RÎ 2	Studentul descrie mecanismele de control al accesului și modelele teoretice de securitate (Bell-LaPadula, Biba, modelul zidului chinezesc, BMA).	Studentul configurează și utilizează modele de control al accesului și implementează politici de securitate.	Studentul manifestă autonomie în alegerea modelelor adecvate și respectă bune practici profesionale.	1.5
RÎ 3	Studentul înțelege conceptele de securitate la nivel de utilizator și sistem individual.	Studentul implementează soluții de protecție pentru calculatoare individuale și servicii de e-mail securizat.	Studentul își asumă responsabilitatea protejării datelor personale și organizaționale.	1.5
RÎ 4	Studentul explică rolul firewall-urilor, VPN-urilor, serverelor proxy și protocoalelor de comunicații în securizarea rețelelor.	Studentul configurează și optimizează soluții de protecție pentru intranet-uri, portaluri și rețele WAN.	Studentul dovedește autonomie în gestionarea infrastructurilor și respectă normele legale.	1.5
RÎ 5	Studentul descrie vulnerabilitățile sistemelor informatice, atacurile cibernetice și strategiile de securitate în contextul războiului informațional.	Studentul utilizează unelte pentru testarea securității aplicațiilor web și identifică vulnerabilități.	Studentul își asumă responsabilitatea raportării vulnerabilităților și adoptă o conduită profesională.	1

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

7.1. Obiectivul general	Insusirea si verificarea notiunilor si tehnicilor de securitate și securizare a sistemelor informatice. Identificarea si corecția erorilor respectiv a vulnerabilităților aplicațiilor Web. Protecția împotriva atacurilor informatice

7.2. Obiectivele specifice	Studiul rezistenței la atacuri a principalilor algoritmi de criptare, codare si stenografie. Validarea tranzacțiilor, securitatea și securizarea acestora. Instalarea și configurarea: firewall-urilor, a serverelor proxy sub Windows/Linux Realizarea unei rețele VPN printr-un tunel OpenVPN Asigurarea încrederii în grupul partenerilor de afaceri, avantajul competitiv, conformitatea cu cerințele legale și minimizarea riscurilor de atacuri asupra sistemelor informatice

8. Conținuturi

8.1. Curs[18]	**Metode de predare**[19]	**Nr. ore**
Securitatea la nivel de aplicatie. Notiuni privind securitatea informatiei. Clasificarea informatiilor. Definirea notiunii de securitate. Standarde de securitate	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	1
Mecanisme de control si protectie date. Politici de securitate ISO/IEC. Dezvoltarea si intretinerea sistemului. Controlul accesului.	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	1
Clasificarea informatiilor, criterii si proceduri. Determinarea nivelurilor clasificarii. Durata, si degradarea informatiilor clasificate	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	1
Principiile protejarii informatiilor speciale.	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	1
Securitatea la nivelul utilizatorilor	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	1
Controlul accesului/modele de control al accesului in sistemele informatice.	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	1
Studiul securitatii sistemelor de calcul individual	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	1
Ascunderea informatiilor. Modele, sisteme si programe de securitate: multinivel (Bell-LaPadula, modelul matricei de control al accesului, Biba); multilateral (modelul zidului chinezesc, Modelul BMA (British Medical Association)). Politica accesului la distanta. Posta electronica.	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	1
Modele criptografice folosite in securizarea structurilor de retea	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	1
Rolul unui firewall si modul de optimizare in functie de specificul sistemului in care este integrat. Serverele proxy. Retele VPN. Protocoale de comunicatii. Tipuri de tuneluri. Tehnici, servicii și soluții de securitate pentru Intranet-uri și portaluri. Semnatura si certificarea digitala. Mesaje de securitate MIME/SMIME.	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	2

Securitatea in modele de tip WAN	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	1
Strategii de securitate ale războiului informaţional. Vulnerabilitatile sistemelor informatice. Atacuri informatice. Testarea serviciilor si aplicatiilor WEB folosind unelte specifice.	*Expunere, prelegere, prezentare la tablă a problematicii studiate, utilizare videoproiector, discuții cu studenții*	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**
Implementări ale modelelor clasice în sisteme distribuite. Servere de Web	*Demonstrație practică, exercițiu*	4
Servere de date	*Demonstrație practică, exercițiu*	2
Limbaje de programare și tehnologii folosite: Oracle, PhP, Pyton, JavaScript, VB, Joomla, Apache, Mysql, MariaDB, XAMPP, WAMPP.	*Demonstrație practică, exercițiu*	4
Politici de securitate. Aplicabilitate. Adaptabilitate	*Demonstrație practică, exercițiu*	2
Ascunderea și descoperirea unui fișier ascuns	*Demonstrație practică, exercițiu*	2
Configurarea, înțelegerea funcționarii şi rolul unui firewall în securitatea sistemelor informatice	*Demonstrație practică, exercițiu*	2
Păcălirea Firewall/IDSurilor şi ascunderea identității	*Demonstrație practică, exercițiu*	2
Servere Proxy pe diferite SO (configurare). Interfață Modem / Router – Internet. Open VPN (configurare sistem client/server).	*Demonstrație practică, exercițiu*	2
Risk Management	*Demonstrație practică, exercițiu*	2
Minimizarea pierderilor in cazul unei penetrari de securitate	*Demonstrație practică, exercițiu*	2
Modele de analiza a claselor de riscuri	*Demonstrație practică, exercițiu*	2
Cazul utilizatorului rau intentionat	*Demonstrație practică, exercițiu*	2
	Total ore seminar/laborator	28

9. Bibliografie

9.1. Referințe bibliografice recomandate	Anand Shinde, Introduction to Cyber Security, WCS Notion Press, 2021
	M.I. Neamtu, Vulnerabilitati ale sistemelor informatice. Securitatea si securizarea acestora. Ed. Univ. Lucian Blaga din Sibiu, 2013
	Ioan Cosmin-Mihai, Laurentiu Giurea, Costel Ciuchi, Gabriel Petrica; Provocari și strategii de securitate cibernetica, Editura: Sitech, 2015
9.2. Referințe bibliografice suplimentare	Anderson R., Security Engineering : A Guide to Building Dependable Distributed Systems, NY 2001
	Andress M., Surviving Security: How to Integrate People, Process and Technology, SAMS, Indianapolis, 2002, pp. 59-63
	Denning D.E., Information Warfare and Security, Addison-Wesley, Reading, Massachusetts, 1999
	N. Ferguson and B. Schneier, A Cryptographic Evaluation of IPsec, Chapman&Hall/CRC 2002
	Eli Biham and Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard
	Abraham Sinkov, Elementary Cryptanalysis: A Mathematical Approach

10. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului[24]

Se realizează prin contacte periodice cu aceștia în vederea analizei problemei
Conținutul disciplinei a fost stabilit ţinând cont de interacţiunile constructive ale cadrelor didactice, studenţilor şi a reprezentanţilor din mediul economic, ştiinţific, în cadrul manifestărilor ştiinţifice, întâlnirilor de lucru şi activităţilor de practică şi dezvoltare de proiecte a studenţilor.

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]: CP2. Cunoasterea					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: |_0_|_9_| / |_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 alocat 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*

$$Nr.credite = \frac{NOCpSpD \times C_C + NOApSpD \times C_A}{TOCpSdP \times C_C + TOApSdP \times C_A} \times 30\ credite$$

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
- 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

[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 problematicii 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.*