Anexa 2.

FIŞA DISCIPLINEI*

1. Date despre program

Instituţia de învăţământ superior	Universitatea Lucian Blaga din Sibiu
Facultatea	Stiinte
Departament	Matematica si Informatica
Domeniul de studiu	Informatica
Ciclul de studii	Master / STIA / 2 ani
Specializarea	Informatica

2. Date despre disciplină

Denumirea disciplinei	**SECURITATE CIBERNETICA**			
Codul cursului	Tipul cursului	An de studiu	Semestrul	Număr de credite
38061004019	O	2	2	7
Tipul de evaluare	Categoria formativă a disciplinei *(DF=fundamentală.; DD=domeniu; DS=specialitate; DC=complementară)*			
Examen	Examen scris+Proiect			
Titular activităţi curs	Conf. univ. dr. Nicolae CONSTANTINESCU			
Titular activităţi seminar / laborator/ proiect	Conf. univ. dr. Nicolae CONSTANTINESCU			

3. Timpul total estimat

Extinderea disciplinei în planul de învăţământ – număr de ore pe săptămână				
Curs	Seminar	Laborator	Proiect	Total
1	-	2	-	**3**
Extinderea disciplinei în planul de învăţământ – Total ore din planul de învăţământ				
Curs	Seminar	Laborator	Proiect	Total ($NOAD_{sem}$)
12	-	24	-	**36**

Distribuţia fondului de timp pentru studiu individual	Nr.ore
Studiul după manual, suport de curs, bibliografie şi notiţe	28
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	28
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	88
Tutoriat:	5
Examinări:	5
Total ore alocate studiului individual ($NOSI_{sem}$)	154
Total ore pe semestru ($NOAD_{sem}$ + $NOSI_{sem}$)	**196**

4. Precondiţii (acolo unde este cazul)

De curriculum	Fundamentele Programarii, Retele de Calculatoare, Algoritmi si Structuri de Date, Sisteme de Operare
De competenţe	

5. Condiţii (acolo unde este cazul)

De desfăşurare a cursului	
De desfăşurare a sem/lab/pr	

6. Competenţe specifice acumulate

Competenţe profesionale	• Dezvoltarea atitudinii pozitive faţă de muncă şi responsabilitate pentru propria pregătire profesională. • Dezvoltarea spiritului de munca in echipa.
Competenţe transversale	• Cunoaşterea şi utilizarea noţiunilor fundamentale legate de securitatea sistemelor informatice. • Capacitatea de formare privind accesul personalului în sistemele informatice, cu tipuri de control al accesului, metode de autentificare şi identificare a utilizatorilor. • Capacitatea de a intelege si folosi sistemul de "Modele şi programe de securitate"; sisteme de securitate multinivel şi multilateral precum şi programe, politici, norme şi standarde de securitate. • Capacitatea de a folosi tehnici, servicii şi soluţii de securitate pentru Intranet-uri şi portaluri, cu detalierea unor aspecte prinvind tehnicile de criptare şi a funcţiilor folosite pentru transmiterea securizată a cheilor de criptare, autentificarea Kerberis 5, SSL/TTL, NTLM, SSH, S/MIME şi prezentarea firewall-urilor. • Capacitatea de a adaptare in timp real la strategiile de securitate ale războiului informaţional.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	• Insusirea si verificarea notiunilor si tehnicilor de securitate si securizare a sistemelor informatice. Identificarea si corectia erorilor respectiv a vulnerabilitatilor aplicatiilor Web. Protectia impotriva atacurilor informatice.
Obiectivele specifice	• Implementarea principalilor algoritmi de criptare, codare si stenografie. Validarea tranzacţiilor, securitatea si securizarea acestora. Instalarea şi configurarea: firewall-urilor, a serverelor proxy sub Windows/Linux. • Realizarea unei reţele VPN printr-un tunel OpenVPN. • Obiectivul principal al acestui program pentru protecţia informaţiilor îl reprezintă asigurarea încrederii in grupul partenerilor de afaceri, avantajul competitiv, conformitatea cu cerinţele legale şi maximizarea investiţiilor.

8. Conţinuturi

Curs		Nr. ore
Curs 1-2	Securitatea la nivel de aplicatie. Notiuni privind securitatea informatiei. Clasificarea informatiilor. Definirea notiunii de securitate. Standarde de securitate. Mecanisme de control si protectie date. Politici de securitate ISO/IEC. Dezvoltarea si intretinerea sistemului. Controlul accesului.	2
Curs 3-4	Clasificarea informatiilor, criterii si proceduri. Determinarea nivelurilor clasificarii. Durata, si degradarea informatiilor clasificate. Principiile protejarii informatiilor	2

	speciale.	
Curs 5-6	Securitatea la nivelul utilizatorilor. Controlul accesului/modele de control al accesului in sistemele informatice.	2
Curs 7-8	Studiul securitatii sistemelor de calcul individual. Criptografia vs Criptanaliza, stenografia, filigramarea. Sisteme si tehnici de criptare. 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.	2
Curs 9-10	Modele criptografice folosite in securizarea structurilor de retea. Securitatea retelelor de calculatoare. Rolul unui si utilizarea unui firewall. Serverele proxy. Retele VPN. Protocoale de comunicatii. Tipuri de tuneluri. Tehnici, servicii şi soluţii de securitate pentru Intranet-uri şi portaluri. Semnatura si certificarea digitala. Mesaje de securitate MIME/SMIME.	2
Curs 11-12	Securitatea in retele de calculatoare. WAN. Strategii de securitate ale războiului informaţional. Vulnerabilitatile sistemelor informatice. Atacuri informatice. Testarea serviciilor si aplicatiilor WEB folosind unelte specifice.	2
	Total ore curs:	**12**
Seminar/Laborator		Nr. ore
Sem 1-2	Implementari ale modelelor clasice in sisteme distribuite. Servere de Web. Servere de date.	4
Sem 3-4	Limbaje de programare si tehnologii folosite: Oracle, PhP, Pyton, JavaScript, VB, Joomla, Apache, Mysql, MariaDB, XAMPP, WAMPP.	4
Sem 5-6	Criptarea, stenografia ca metodă de securitate a informaţiilor. Ascunderea si descoperirea unui fisier ascuns. Configurarea, înţelegerea funcţionării şi rolul unui firewall în securitatea sistemelor informatice.	4
Sem 7-8	Păcălirea Firewall/IDSurilor şi ascunderea identităţii. Servere Proxy pe diferite SO (configurare). Interfaţa Modem / Router – Internet. Open VPN (configurare sistem client/server).	4
Sem 9-10	Semnatura digitala. Atacuri informatice. Atacuri criptografice (forta bruta; text clar: cunoscut, ales, selectat,…; atac zi de nastere, intalnire la mijloc, om la mijloc, …).	4
Sem 11-12	Validarea tranzacţiilor, securitatea si securizarea acestora. Erorile sistemelor.	4
	Total ore seminar/laborator	24

Metode de predare

La curs se va folosi expunerea, explicatia, exem-plificarea si conversatia fron-tala.	La orele de laborator se va folosi explicatia, exemplificarea, invatarea prin descoperire.	

Bibliografie

Referinţe bibliografice recomandate	1. Nicolae Constantinescu, Criptografie, Editura Academiei Romane, 2009 2. M.I. Neamtu, Vulnerabilitati ale sistemelor informatice. Securitatea si securizarea acestora. Ed. Univ. Lucian Blaga di Sibiu, 2013; 3. Ioan Cosmin-Mihai, Laurentiu Giurea, Costel Ciuchi, Gabriel Petrica; Provocari si strategii de securitate cibernetica, Editura: Sitech, 2015, Pag: 230, ISBN: 9786061149513;
Referinţe bibliografice	1. Anderson R. – Security Engineering : A Guide to Building Dependable Distributed Systems, NY 2001;

suplimentare	2. Andress, M. – Surviving Security: How to Integrate People, Process and Technology, SAMS, Indianapolis, 2002, pp. 59-63. 3. Davis D. – "The Problems Catch Up With The Solution", in Card Technology, April 2003; 4. Denning D.E. – Information Warfare and Security, Addison-Wesley, Reading, Massachusetts, 1999; 5. N. Ferguson and B. Schneier,A Cryptographic Evaluation of IPsec, Chapman&Hall/CRC 2002 6. S. C. Coutinho,The Mathematics of Ciphers: Number Theory and RSA Cryptography, 7. Eli Biham and Adi Shamir,Differential Cryptanalysis of the Data Encryption Standard, 8. Abraham Sinkov, Elementary Cryptanalysis: A Mathematical Approach, 9. Helen F Gaines,Cryptanalysis: A Study of Ciphers and Their Solutions,

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

Se realizeaza prin contacte periodice cu acestia in vederea analizei problemei.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Ponderea în nota finală	Obs.**
Curs	Proiect	Condiţionează participarea la examen	40.00%	
	Examen	Condiţionează evaluarea finală	50.00%	
Laborator	Activitati aplicative	1.Teme/pondere = 5 % 2.Referate/pondere= 10% 3.Lucrări practice = 10%	10.00%	
	Examen partial			
Standard minim de performanţă: Capacitatea de invatare si adaptare la aplicarea strategiilor de securitate ale războiului informaţional.				

(*) **Fişa disciplinei cuprinde componente adaptate persoanelor cu dizabilităţi, în funcţie de tipul şi gradul acestora.**
(**) CPE – condiţionează participarea la examen; nCPE – nu condiţionează participarea la examen; CEF - condiţionează evaluarea finală;

Data completării: 24.09.2020
Data avizării în Departament: 25.09.2020

	Grad didactic, titlul, prenume, numele	Semnătura
Titular disciplină	Conf. univ. dr. Nicolae CONSTANTINESCU	
Director de departament	Prof. Univ. Dr. Mugur ACU	