



Anexa 2.

FIȘA DISCIPLINEI***1. Date despre program**

Instituția de învățământ superior	Universitatea Lucian Blaga din Sibiu
Facultatea	Facultatea de Științe
Departament	Departamentul de Matematică și Informatică
Domeniul de studiu	Informatică
Ciclul de studii	Master
Specializarea	Sisteme și tehnologii informatice avansate

2. Date despre disciplină

Denumirea disciplinei	Securitate Cibernetică			
Codul cursului	Tipul cursului	An de studiu	Semestrul	Număr de credite
38061004019	O	2	4	7
Tipul de evaluare	Categoría formativă a disciplinei (DA=aprofundare.; DS=sinteză)			
E	DS			
Titular activități curs	Conf. univ. dr. Nicolae CONSTANTINESCU			
Titular activități seminar / laborator/ proiect	Lect. Univ. Dr. Mircea NEAMTU			

3. Timpul total estimat

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

Distribuția fondului de timp pentru studiu individual		Nr.ore
Studiul după manual, suport de curs, bibliografie și notițe		35
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren		35
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri		35
Tutoriat:		32
Examinări:		2
Total ore alocate studiului individual (NOSI _{sem})		139
Total ore pe semestru (NOAD _{sem} + NOSI _{sem})		175

4. Preconții (acolo unde este cazul)

De curriculum (Discipline necesar a fi promovate anterior)	
De competențe	

5. Condiții (acolo unde este cazul)

De desfășurare a cursului	Sala cu tabla și videoproiector
De desfășurare a sem/lab/pr	Sala de laborator



6. Competențe specifice acumulate

Competențe profesionale	Dezvoltarea atitudinii pozitive față de muncă și responsabilitate pentru propria pregătire profesională. Dezvoltarea spiritului de munca în echipa.
Competențe transversale	Cunoașterea, înțelegerea și utilizarea noțiunilor fundamentale legate de securitatea sistemelor informatice. Capacitatea de a analiza un sistem informatic și a face o analiză a riscurilor existente: audit de securitate informatică. Cunoașterea politicilor de securitate într-o entitate ce conține informatizare. Capacitatea de adaptare a tehnicilor învățate la cazuri concrete

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

Obiectivul general al disciplinei	Însușirea noțiunilor și tehnicilor de securitate și securizare a sistemelor informatice. Identificarea și corecția erorilor respectiv a vulnerabilităților din cadrul aplicațiilor. Protecția împotriva atacurilor informatice.
Obiectivele specifice	Implementarea principiilor și politicilor de securitate cibernetică în intranet și internet. Înțelegerea metodelor de validare a tranzacțiilor. Instalarea și configurarea: firewall-urilor, a serverelor Proxy în cadrul sistemelor de operare Windows, Linux și MacOS. Realizarea tunelurilor de comunicație securizate, folosind tehnicile bazate pe VPN și VLAN. Configurare elemente de securizare a rețelelor compuse din device-uri eterogene

8. Conținuturi

Curs		Nr. ore
Curs 1-2	Vulnerabilități ale sistemelor hardware și software. BackDoor, TrapDoor	2
Curs 3-4	Securitatea la nivel de aplicație. Studiul tipurilor de informații și clasificarea lor. Acces ierarhizat la nivel aplicație.	2
Curs 5-6	Securitatea la nivel hardware. Modele de mecanisme la nivel fizic, de acces ierarhizat. Programarea embedded a procesoarelor criptografice. Studiul FPGA.	2
Curs 7-8	Securitatea la nivel de utilizator. Studiul principiilor limitării daunelor în cazul utilizatorului rău intenționat. Modele de ierarhizare a accesului într-o entitate IT.	2
Curs 9-10	Politici de securitate. Modele adaptive vs modele impuse.	2
Curs 11-12	Securitatea rețelelor de calculatoare. Strategii de atac cibernetic și metode de contracarare a acestora	2
Total ore curs:		12
Seminar/Laborator		Nr. ore
Lab 1-2	Instalarea și configurarea server-elor WEB Linux (cu accent pe securizarea device-urilor conectate și a serviciilor de baza).	4
Lab 3-4	Instalarea și configurarea server-elor WEB Windows (cu accent pe securizarea device-urilor conectate și a serviciilor de baza).	4
Lab 5-6	Instalarea și configurarea server-elor WEB MacOS (cu accent pe securizarea device-urilor conectate și a serviciilor de baza).	4



Lab 7-8	Configurarea Firewall-ului.	4
Lab 9-10	Instalare, configurare, optimizare pe un caz concret: SNIFFER.	4
Lab 11-12	Folosire API de generare certificate criptografice.	4
Total ore seminar/laborator		24

Metode de predare

Expunerea sistematică a cunoștințelor (deductivă, inductivă și formalizată, expuneri beamer/prezi); conversația frontală; conversația euristică, problematizare, studii de caz, modelarea

Bibliografie

Referințe bibliografice recomandate	<ol style="list-style-type: none"> Nicolae Constantinescu, Criptografie, Editura Academiei Romane, 2009. 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 si strategii de securitate cibernetica, Editura: Sitech, 2015, Pag: 230, ISBN: 9786061149513.
Referințe bibliografice suplimentare	<ol style="list-style-type: none"> 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. Davis D. – "The Problems Catch Up With The Solution", in Card Technology, April 2003. 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. S. C. Coutinho, The Mathematics of Ciphers: Number Theory and RSA Cryptography. Eli Biham and Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard. Abraham Sinkov, Elementary Cryptanalysis: A Mathematical Approach. Helen F Gaines, Cryptanalysis: A Study of Ciphers and Their Solutions.

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

Disciplina Securitate Cibernetica își găsește aplicabilitatea în majoritatea companiilor IT dar și pentru utilizatori particulari ai sistemelor informatice, atât în formarea de baza în ceea ce privește protecția informației cât și în optimizări ale metodelor existente prin adaptări la cazuri particulare. Materia, prin titularul de curs, este în contact direct cu firmele de profil, pentru evidențierea necesităților acestora și coordonarea unui schimb de informații care să dinamizeze și adapteze programa. Există un contact permanent și cu lumea științifică din domeniu, prin articolele științifice și contractele de cercetare în care este implicat titularul de curs.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Ponderea în nota finală	Obs.**
----------------	----------------------	--------------------	-------------------------	--------



ULBS

Universitatea "Lucian Blaga" din Sibiu

Curs	Înțelegerea noțiunilor. Nivelul la care cursanții le pot explica și fundamenta afirmațiile Nivelul tehnic al expunerii termenilor Claritatea și percepția ansamblului problematicii din cadrul materiei	Evaluare Continua Proiect Aplicativ / Studiu fundamental sau Combinat Examen practic și teoretic	50%	nCPE CEF
Laborator	Capacitatea de sinteză a cunoștințelor dobândite Capacitatea de a adapta exemple făcute pentru probleme similare Capacitatea de generalizare Nivelul tehnic al implementării Claritatea și percepția ansamblului proiectului în lucru	Întocmirea și susținerea unui referat Teme pentru acasă Participare activă la laboratoare Realizarea unui proiect final	50%	nCPE CEF
Standard minim de performanță				
<ul style="list-style-type: none">• Cunoașterea noțiunilor de baza din domeniul Securității Cibernetice: Definiții, Diferențe între securitate fizică și logică• Cunoașterea principalelor sisteme de protecție cibernetică, din punct de vedere hardware și software.• Cunoașterea politicilor de securitate.• Toate aceste cerințe se reflectă în modul de notare pentru a obține nota minimă 5				

(*) Fișa disciplinei cuprinde componente adaptate persoanelor cu dizabilități, în funcție de tipul și gradul acestora.

(**) CPE – condiționează participarea la examen; nCPE – nu condiționează participarea la examen; CEF - condiționează evaluarea finală;

Data completării: 26.09.2019

Data avizării în Departament: 30.09.2019

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