

FIȘA DISCIPLINEI
Anul universitar 2024-2025
Anul de studiu 3 / Semestrul 2

1. Date despre program

1.1. Instituția de învățămînt superior	Universitatea „1 Decembrie 1918” din Alba Iulia
1.2. Facultatea	de Informatică și Inginerie
1.3. Departamentul	Departamentul de Informatică, Matematică și Electronică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Licență
1.6. Programul de studii/calificarea*	Informatică/ ESCO-08: 2511/ Systems Analyst, 2512/ Software developers COR: Analist/251201, Programator de sistem informatic/251204, Inginer de sistem în informatică/251203

2. Date despre disciplină

2.1. Denumirea disciplinei	Securitatea Sistemelor Informaticice			2.2. Cod disciplină	INFO315
2.3. Titularul activității de curs	Lect. Dr. Incze Arpad				
2.4. Titularul activității de seminar / laborator	Matei Căpînaș				
2.5. Anul de studiu	3	2.6. Semestrul	2	2.7. Tipul de evaluare (E/C/VP)	C
				2.8. Regimul disciplinei (O – obligatorie, Op – opțională, F – facultativă)	Op

3. Timpul total estimat

3.1. Numar ore pe saptamana	4	din care: 3.2. curs	2	3.3. seminar/laborator	2
3.4. Total ore din planul de învățămînt	48	din care: 3.5. curs	24	3.6. seminar/laborator	24
Distribuția fondului de timp					ore
Studiul după manual, suport de curs, bibliografie și notițe					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					30
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					36
Tutoriat					-
Examinări					6
Alte activități					-

3.7 Total ore studiu individual	102
3.8 Total ore din planul de invatamant	48
3.9 Total ore pe semestru	150
3.10 Numărul de credite**	6

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	INFO 110 Sisteme de Operare INFO 203 Rețele de calculatoare
4.2. de competențe	C2 Dezvoltarea și întreținerea aplicațiilor informatice C6 Proiectarea și administrarea rețelor de calculatoare

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Sală de curs dotat cu videoproiector
5.2. de desfășurarea a seminarului/laboratorului	Labrator dotat cu PC-uri, videoproiector SO Windows / Linux cu acces de admin

6. Competențe specifice acumulate

Competențe profesionale	C6 Proiectarea și administrarea rețelor de calculatoare C6.1. Identificarea conceptelor și modelelor de bază pentru sisteme de calcul și rețele de calculatoare C6.3. Utilizarea tehnicilor pentru instalarea, configurarea și administrarea sistemelor și rețelor C6.4. Efectuarea de măsurători de performanță pentru timpi de răspuns. Consum, Resurse, stabilirea drepturilor de acces
Competențe transversale	Nu e cazul

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

7.1 Obiectivul general al disciplinei	<p>În cadrul disciplinei "Securitatea sistemelor informatice" studenții trebuie să-și însușească conceptele de bază privind tipurile de vulnerabilități ale sistemelor informatice. Disciplina are un rol important în instruirea studenților prin atingerea a două obiective importante:</p> <ol style="list-style-type: none"> 1. În primul rând oferă studenților elementele teoretice necesare pentru înțelegerea și aprofundarea conceptelor de bază privind securitatea în sistemel informatice.Vulnerabilități, atacuri, metode de detecție și apărare 2. În al doilea rând, prin modul de desfășurare al orelor de seminar și laborator se urmărește formarea unor deprinderi practice care să permită studentului identificarea vulnerabilităților sistemului informatic al unei organizații și îmbunătățirea securității sistemului informatic . <p>În conformitate cu planul de învățământ, activitatea didactică la această disciplină se finalizează prin colocviu practic. Pentru aprecierea activității de laborator, la care frecvența este obligatorie, fiecare student va fi apreciat cu o notă</p>
7.2 Obiectivele specifice	<p>Competențe cognitive: dobândirea de cunoștințe fundamentale privind vulnerabilitățile și tipurile de atacuri în sistemele informatice-rețele de calculatoare.</p> <p>Competențe tehnice/profesionale: deprinderea utilizării corecte a principiilor – modelelor – instrumentelor din domeniul securității informatice</p>

8. Conținuturi*

8.1 Curs	Metode de predare	Observații
<ol style="list-style-type: none"> 1. Probleme de securitate IT. Principii, definiții exemple 2. Securitatea sitemelor de operare. Controlul accesului 3. Securitatea rețelelor de calculatoare. Vulnerabilități, tipuri de atac 4. Securitatea în rețele wireless 5. Securitatea rețelelor de calculatoare. Metode de protecție Firewall & IDS 6. Viruși, malware, backdoor 7. Securitate software. Exploitari . Programare defensiva 8. Securitatea aplicațiilor WEB 9. Tehnici Penetration testing 10. Auditul de securitate, politici de securitate. Modele 11. Introducere in criptografie. 12. Examen/colocviu 	Prelegere, discutii. Exemple practice.	
<p>Bibliografie</p> <ol style="list-style-type: none"> 1. Dieter Gollmann. Computer Security. ed. 3, Wiley, 2011 2. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography, CRC Press, 2001 3. Ross J. Anderson. Security Engineering. ed. 2, Wiley, 2008 4. M. Down, J. McDonald, J. Schuh, „ The Art of Software Security Assessment. Identifying and Preventing Software Vulnerabilities ”, AddisonWesley, 2007 5. M. Howard, D. LeBlanc, J. Viega, „ 24 Deadly Sins of Software Security. Programming Flows and How to Fix Them ”, McGraw Hill, 2010 6. M. Howard, D. LeBlanc, „ Writing Secure Code for Windows Vista ”, Microsoft Press, 2007 7. G. McGraw, „ Software Security:Building Security In ”, AddisonWesley, 2006 8. R. Seacord, „CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems”, AddisonWesley, 2 nd edition, 2014 9. , „ Common Weaknesses Enumeration (WCE)”, online: http://cwe.mitre.org/data/index.html 10. , Rețele de calculatoare ed. A patra A Andrew S. Tanenbaum Universitatea Vrije Amsterdam, Olanda ©2003 Byblos 11. https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials 		
8.2. Seminar-laborator		Nr ore sem + laborator
<ol style="list-style-type: none"> 1. Studiu de caz implementarea unui atac folosind Inginerie socială. 2. Utilizatori, drepturi de acces în SO windows & linux 3. Controlul accesului la fișiere în SO Windows & Linux. 4. Securitatea în rețele. Controlul accesului la resurse în rețea, 5. Configurații routere, servere etc. 6. Atacuri asupra rețelelor de calculatoare. Man in the midle, DoS, desincronizare etc. 7. Instalarea și configurarea unui firewall si NIDS 8. Antivirusi, antimalware. Soluți integrate 9. Programare defensiva. Cross-site scripting, cross-site request forgery SQL injection 10. Evaluarea riscurilor, auditul de securitate, politici de securitate 11.Elemente de criptografie Funcții de criptare predefinite in limbajele de programare 12. Proiect final / evaluare 	<p>Discutii, demonstrații, exemple</p> <p>Exerciții propuse, teme, proiecte</p>	<p>2+2</p> <p>2+2</p> <p>2+2</p> <p>2+2</p> <p>2+2</p> <p>2+2</p> <p>2+2</p> <p>2+2</p> <p>2+2</p> <p>2+2</p> <p>2+2</p> <p>2+2</p>
<p>Bibliografie Idem Curs</p>		

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

Disciplina Securitatea sistemelor informatice este o disciplină opțională care pregătește viitori specialiști administratori de sistem/administratori de rețele punând accent pe componenta de securitate IT, domeniu foarte cautat și apreciat. Conținutul disciplinei este conceput în scopul formării de bază a oricărui informatician.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	<i>Evaluare finală/</i>	<i>Final exam Cybersecurity Essentials</i>	60%
10.5 Seminar/laborator	<i>Verificare pe parcurs</i>	<i>Teme de laborator Cybersecurity Essentials</i>	40%
10.6 Standard minim de performanță: Promovarea examenului de certificare CISCO Cybersecurity Essentials Realizarea unui audit de securitate pentru un sistem informatic (calculator propriu, sau la locul de munca). Auditul trebuie să conțină toate etapele: - Testarea sistemului pentru identificarea vulnerabilităților - Eliminarea/diminuarea impactului vulnerabilităților găsite Întocmirea politicii de securitate impuse sistemului studiat			

Data completării

Semnătura titularului de curs

Semnătura titularului de seminar

Data avizării în departament

Semnătura directorului de departament

Data aprobării în Consiliul Facultății

Semnătura Decanul Facultății

.....

Anexă la Fișa disciplinei (facultativă)

ANEXĂ LA FIȘA DISCIPLINEI

b. Evaluare – mărirea de notă

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs			
10.5 Seminar/laborator			
10.6 Standard minim de performanță			
Participarea la 50% din activitățile didactice și însușirea conceptelor de bază.*			
Data completării	Semnătura titularului de curs		Semnătura titularului de seminar

c. Evaluare – restanță

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Examen	Lucrare scrisă	50%
10.5 Seminar/laborator	Referate, eseuri, proiecte etc.	Prezentare la seminar	50%
10.6 Standard minim de performanță			
Participarea la 50% din activitățile didactice și însușirea conceptelor de bază.*,**			
Data completării	Semnătura titularului de curs		Semnătura titularului de seminar

*Formulare orientativă

**Dacă disciplina are prevăzute ore de laborator trebuie prevăzute modalitățile de recuperare a acestora.