ANEXA 1

FIŞA DISCIPLINEI

Anul universitar 2020-2021

Anul de studiu 3 / Semestrul 2

1. Date despre program

1.1. Instituţia de învăţământ superior	**Universitatea „1 Decembrie 1918" din Alba Iulia**
1.2. Facultatea	**de Ştiinţe Exacte şi Ingineresti**
1.3. Departamentul	**Departamentul de Informatică, Matematică şi Electronică**
1.4. Domeniul de studii	**Informatică**
1.5. Ciclul de studii	**Licență**
1.6. Programul de studii/calificarea*	**Informatică / 251201, 251203, 251204**

2. Date despre disciplină

2.1. Denumirea disciplinei	**Securitatea Sistemelo Informatice**			2.2. Cod disciplină		**315**	
2.3. Titularul activităţii de curs	Lect. Dr. Incze Arpad						
2.4. Titularul activităţii de seminar / laborator	Lect. Dr. Incze Arpad						
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** – opţională, **F** – facultativă)	**Op**

3. Timpul total estimat

3.1. Numar ore pe saptamana	6	din care: 3.2. curs	**2**	3.3. seminar/laborator	**4**
3.4. Total ore din planul de învăţământ	72	din care: 3.5. curs	**24**	3.6. seminar/laborator	**48**

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie şi notiţe	**20**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	**20**
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	**32**
Tutoriat	**-**
Examinări	**6**
Alte activităţi …….	**-**

3.7 Total ore studiu individual	78
3.9 Total ore pe semestru	150
3.10 Numărul de credite**	6

* 3.9. = 3.4. + 3.7.; numărul total de ore pe semestru trebuie calculat în funcție de nr. de credite (3.9.) și de volumul de muncă aferent unui credit (1 credit = 25 ore conform Ghidului de aplicare a ECTS).
** 3.10. = numărul de credite prevăzut a fi atribuit disciplinei prin planul de învățământ.

4. **Precondiţii** (acolo unde este cazul)

4.1. de curriculum	*INFO 110 Sisteme de Operare* *INFO 203 Reţele de calculatoare*
4.2. de competenţe	*C2 Dezvoltarea şi întreţinerea aplicaţiilor informatice* *C6 Proiectarea şi administrarea reţelor de calculatoare*

5. **Condiţii** (acolo unde este cazul)

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

6. Competenţe specifice acumulate

Competenţe profesionale	*C6 Proiectarea şi administrarea reţelor de calculatoare* *C6.1.Identificarea conceptelor şi modelelor de bază pentru sisteme de calcul şi reţele de calculatoare* *C6.3.Utilizarea tehnicilor pentru instalarea, configurarea şi administrarea sistemelor şi reţelelor* *C6.4.Efectuarea de măsurători de performanţă pentru timpi de răspuns. Consum,. Resurse, stabilirea drepturilor de acces*	
Competenţe transversale	*Nu e cazul*	

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

7.1 Obiectivul general al disciplinei	*În cadrul disciplinei "Securitatea sistemlor informatice" studenţii trebuie să-şi însuşească conceptele de bază privind tipurile de vulnerabilităţi ale sistemelor informatice. Disciplina are un rol important în instruirea studenţilor prin atingerea a două obiective importante:* **1.** *În primul rând oferă studenţilor elementele teoretice necesare pentru înţelegerea şi aprofundarea conceptelor de bază privind securitatea in sistemel informatice.Vulnerabilităţi, atacuri, metode de detecţe şi apărare* **2.** *În al doilea rând, prin modul de desfăşurare al orelor de seminar şi laborator se urmăreşte formarea unor deprinderi practice care să permită studentului identificarea vulnerabilităţilor sistemului informatic al unei organizaţii şi imbunătăţirea securităţii sistemului informatic .* *În conformitate cu planul de învăţământ, activitatea didactică la această disciplină se finalizează prin colocviu practic. Pentru aprecierea activităţii de laborator, la care frecvenţa este obligatorie, fiecare student va fi apreciat cu o notă*	
7.2 Obiectivele specifice	**Competenţe cognitive:** dobândirea de cunoştinţe fundamentale privind vulnerabilităţile ţi tipurile de atacuri în sistemele informatice-reţele de calculatoare. **Competenţe tehnice/profesionale:** deprinderea utilizării corecte a principiilor – modelelor – instrumentelor din domeniul securităţii informatice	

8. Conţinuturi*

8.1 Curs	**Metode de predare**	**Observaţii**
1. *Probleme de securitate IT. Principii, definiţii exemple* 2. *Securitatea sitemelor de operare. Controlul accesului* 3. *Securitatea reţelelor de calculatore. Vulnerabilităţi, tipuri de atac* 4. *Securitatea în reţele wireless* 5. *Securitatea reţelelor de calculatore. Metode de protecţie Firewall & IDS* 6. *Viruşi, malware, backdoor* 7. *Securitate software. Exploituri . Programare defensiva* 8. *Securitatea aplicaţiilor WEB* 9. *Tehnici Penetration testing* 10. *Auditul de securitate, politici de securitate. Modele* 11. *Introducere in criptografie.* 12. *Examen/colocviu*	Prelegere,discutii. Exemple practice.	

Bibliografie

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. , Reţele de calculatoare ed. A patra A Andrew S. Tanenbaum Universitatea Vrijie Amsterdam, Olanda ©2003 Byblos
11. https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials

8.2. Seminar-laborator		**Nr ore sem + laborator**
1. *Studiu de caz implementarea unui atac folosind Inginerie socială.*	*Discutii, demonstrații,*	2+2
2. *Utilizatori, drepturi de acces în SO windows & linux*	*exemple*	2+2
3. *Controlul accesului la fişiere în SO Windows & Linux.*	*Exerciții propuse, teme, proiecte*	2+2
4. *Securitatea în reţele. Controlul accesului la resurse în reţea,*		2+2
5. *Configuraţii routere, servere etc.*		2+2
6. *Atacuri asupra reţelelor de calculatoare. Man in the midle, DoS, desincronizare etc.*		2+2
7. *Instalarea şi configurarea unui firewall si NIDS*		2+2
8. *Antiviruşi, antimalware. Soluţi integrate*		2+2
9. *Programare defensiva. Cross-site scripting, cross-site request forgery SQL injection*		2+2
10. *Evaluarea riscurilor, auditul de securitate, politici de securitate*		2+2
11. *Elemente de criptografie Funcţii de criptare predefinite in limbajele de programare*		2+2
12. *Proiect final / evaluare*		
Bibliografie *Idem Curs*		

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

Disciplina Securitatea sistemelor informatice este o disciplina opţinală care pregăteşti viitori specialişti administratori de sistem/administratori de reţele punând accent pe componenta de securitate IT, domeniu foarte cautat şi apreciat. Conţinutul disciplinei este conceput in scopul formarii 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	*Evaluare finală/*	*Final exam Cybersecurity Essentials*	60%
10.5 Seminar/laborator	*Verificare pe parcurs*	*Teme de laborator Cybersecurity Essentials*	40%
10.6 Standard minim de performanţă: Promovarea examenului de certificare CISCO Cybersecurity Essentials Realizarea unui audit de securitate pentru un sistem informatic (calculator propriu, sau la locul de munca). Auditul trebuei să conţină toate etapele: - Testarea sistemului pentru identificarea vulnerabilităţilor - Eliminarea/diminuarea impactului vulnerabilităţilor 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
23.09.2019

Data aprobării în Consiliul Facultăţii Semnătura Decanul Facultăţii

…….

Anexă la Fișa disciplinei (facultativă)

ANEXĂ LA FIŞA DISCIPLINEI

b. Evaluare – mărire 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 performanţă			
Participarea la 50% din activităţile didactice şi însuşirea conceptelor de bază.*			
Data completării	Semnătura titularului de curs		Semnătura titularului de seminar

c. Evaluare – restanţă

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 performanţă			
Participarea la 50% din activităţile didactice şi însuşirea 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.