

FIȘA DISCIPLINEI

Securitate Software
Anul universitar 2023-2024
Anul de studiu 2 / Semestrul 1

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea „1 Decembrie 1918” din Alba Iulia
1.2. Facultatea	de Informatică și Inginerie
1.3. Departamentul	Informatică, Matematică și Electronică
1.4. Domeniul de studii	Informatică
1.5. Ciclu de studii	Master
1.6. Programul de studii/calificarea*	Informatică / 251202 /251205 / 251206/

2. Date despre disciplină

2.1. Denumirea disciplinei	Securitate Software			2.2. Cod disciplină	MI201		
2.3. Titularul activității de curs	Lect. Dr. Incze Arpad						
2.4. Titularul activității de laborator	Lect. Dr. Incze Arpad						
2.5. Anul de studiu	2	2.6. Semestrul	1	2.7. Tipul de evaluare (E/C/VP)	E	2.8. Regimul disciplinei (O – obligatorie, Op – opțională, F – facultativă)	O

3. Timpul total estimat

3.1. Numar ore pe saptamana	3	din care: 3.2. curs	2	3.3. laborator	1
3.4. Total ore din planul de învățământ	42	din care: 3.5. curs	24	3.6. laborator	14
Distribuția fondului de timp					ore
Studiul după manual, suport de curs, bibliografie și notițe					40
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					30
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					60
Tutoriat					-
Examinări					3
Alte activități					-

3.7 Total ore studiu individual	133
3.9 Total ore pe semestru	175
3.10 Numărul de credite**	7

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	INFO 102 103 202 211 212
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	CB1 Analiza si proiectarea sistemelor informatice 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 rețelelor 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	<i>Cunoașterea și utilizarea adecvată a noțiunilor teoretice fundamentale legate de criptografie:</i> <ul style="list-style-type: none"> ●Capacitatea de a implementa algoritmi criptografici ●Capacitatea de a utiliza și modifica conform cerințelor algoritmi deja implementați ●Capacitatea de a proiecta și realiza aplicații complexe care utilizează algoritmi și tehnicile învățate
7.2 Obiectivele specifice	Competențe cognitive: dobândirea de cunoștințe fundamentale privind instrumentele criptografice și tipurile de vulnerabilități și atacuri bazate pe software în sistemele informatice Competențe tehnice/profesionale: deprinderea utilizării corecte a principiilor – modelelor – instrumentelor din domeniul securității informatice

8. Conținuturi*

8.1 Curs	Metode de predare	Observații
1 Scurt istoric al criptografiei. Concepte de baza.	Prelegere, discuții.	2
2 Tehnologii criptografice	Exemple practice.	4
3 Ascunderea informațiilor	<i>Predare fizică și/sau online</i>	2
4 Sisteme criptate prin chei secrete (simetrice).	<i>pe Microsoft Teams,</i>	4
5 Sisteme de criptare prin chei publice (asimetrice). Sisteme de certificare a cheilor publice.	<i>prezentări PowerPoint,</i>	4
6 Semnatura digitală.	<i>tutoriale video</i>	2
8 Infrastructura cheilor publice.		2
9 Atacuri informatice Cross Scripting SQL injection		4
Bibliografie⁴		
1) T.H. Cormen, C.E. Leiserson, R.R. Rivest, Introducere în algoritmi, Editia în limba română, Computer Libris AGORA, 2002		
2) B. Schneier - Applied Cryptography – Protocols, Algorithms and Source Code in C. Second Edition- John Wiley & Sons, 1996		
3) A. J. Menezes, Paul von Oorschot, S. A. Vanstone, Handbook of Applied Cryptography – CRC Press, 1997		
4) V. Patriciu, M. Pietrosanu, I. Bica, N. Voicu, C. Vaduva, - Securitatea în comerțul electronic-Ed. All, 2001		
5) M. Howard, D. LeBlanc, Writing Secure Code, Practical strategies and techniques for secure application coding in a networked world, Second Edition, Microsoft, 2002		
6) D. Oprea, Protecția și securitatea informațiilor, Ed. Polirom, Iași, 2003		
7) Introducere în Securitate Cibernetică – Ramon Nastase manual digital 2018 UVT		
8) R. Seacord, "CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems", Addison-Wesley, 2nd edition, 2014		
8.2. Seminar-laborator		Nr ore laborator
1. Introducere în criptografie. Cifrul Cezar. Cifrul Vigenere One time pad	Discuții, demonstrații,	2
2. Criptografia XOR. CBC EBC	exemple	2
3. DES, AES		2
4. Criptografia asimetrică. RSA, El Gamal.	Exerciții propuse, teme, proiecte	2
5. Semnatura digitală, funcții HASH		2
6. Atacuri software, SQL Injection		2
7. Atacuri software X Scripting		2
Bibliografie		
<i>Idem curs</i>		

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

Disciplina Securitate Software este o disciplină 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>Proiect final</i>	50%
10.5 Seminar/laborator	<i>Verificare pe parcurs</i>	<i>Teme de laborator</i>	50%
10.6 Standard minim de performanță: Promovarea examenului de certificare CISCO https://www.netacad.com/courses/cybersecurity/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 necesare securizării sistemului informatic studiat

Data completării

Semnătura titularului de curs

Semnătura titularului de laborator

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 – 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 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	Colocviu	Referat audit de securitate	60%
10.5 Seminar/laborator	Referate, eseuri, proiecte etc.	Prezentare la seminar	40%
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.