

SECURITATEA INFORMAȚIONALĂ

1. Date despre unitatea de curs/modul

Facultatea	Calculatoare, Informatică și Microelectronică				
Catedra/departamentul	Informatică și Ingineria Sistemelor				
Ciclul de studii	Studii superioare de licență, ciclul I				
Programul de studiu	0612.2 Managementul Informației				
Anul de studiu	Semestrul	Tip de evaluare	Categoria formativă	Categoria de opționalitate	Credite ECTS
I (învățământ cu frecvență);	4	E	S – unitate de curs de specialitate	A - unitate de curs la alegere	4

2. Timpul total estimat

Total ore în planul de învățământ	Din care				
	Ore auditoriale		Lucrul individual		
	Curs	Laborator/seminar	Proiect de an	Studiul materialului teoretic	Pregătire aplicații
120	30	15/15		30	30

3. Precondiții de acces la unitatea de curs/modul

Conform planului de învățământ	Matematici speciale și matematica computațională, Programarea calculatoarelor, Structuri de date și algoritmi, Programare procedurală, Programare interactivă
Conform competențelor	Informarea studenților cu cele mai noi probleme privind securitatea și protecția informației cât și cu utilizarea celor mai noi metode de protecție

4. Condiții de desfășurare a procesului educațional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector și calculator. Nu vor fi tolerate întârzierile studenților, precum și convorbirile telefonice în timpul cursului.
Laborator/seminar	Studenții vor perfecta rapoarte conform condițiilor impuse de indicațiile metodice. Termenul de predare a lucrării de laborator – o săptămână după finalizarea acesteia. Pentru predarea cu întârziere a lucrării aceasta se depunceață cu 1pct./săptămână de întârziere.

5. Competențe specifice acumulate

Competențe profesionale	<p>CP1. Utilizarea adecvată a fundamentelor teoretice ale științelor exacte și științelor inginerești aplicate</p> <ul style="list-style-type: none"> ✓ Cunoștințe teoretice și experimentale de bază proprii informaticii aplicate și științelor inginerești aplicate. ✓ Explicarea structurii și funcționării componentelor diferitelor tipuri de modelele de gestiune a informației, utilizând teorii și instrumente specifice. ✓ Aplicarea principiilor, tehnicilor și metodelor de bază din disciplinele fundamentale
-------------------------	--

ale științelor exacte necesare în procesul de prelucrare și tratare a informațiilor specifice domeniului și specializării.

- ✓ Utilizarea metodelor de validare a soluțiilor constructive pentru componentele și structurile proiectate.
- ✓ Aplicarea cunoștințelor teoretice la identificarea și analiza tendințelor de dezvoltare, a metodelor de modelare și de utilizare a aplicațiilor din domeniul managementului informațional.

CP2. Utilizarea sistemelor informatice de prelucrare și gestiune a datelor

- ✓ Descrierea structurii și a modului de funcționare a sistemelor informatice în general.
- ✓ Explicarea rolului, funcționalității și utilității sistemelor informatice în general și a sistemelor de prelucrare și gestiune a datelor în domeniul specializării.
- ✓ Utilizarea componentelor software ale sistemelor informatice, folosind algoritmi, protocoale, limbaje, structuri de date.
- ✓ Utilizarea adecvată de criterii și metode standard de apreciere a caracteristicilor și a calităților sistemelor informațional.
- ✓ Prelucrarea și gestionarea datelor utilizând sisteme informatice dedicate.

CP4. Rezolvarea problemelor economice și ingineresti folosind metode matematice, metode statistice și tehnici informatice

- ✓ Identificarea problemelor economice și ingineresti care se pretează la modelare matematică și statistică precum și a metodelor utilizabile din informatica aplicată.
- ✓ Însușirea cunoștințelor teoretice și a deprinderilor de actualizare a acestora, necesare în procesul de interpretare a rezultatelor experimentale.
- ✓ Abilitatea de a utiliza și adapta șabloane de soluții specifice matematicii și informaticii aplicate pentru rezolvarea problemelor economice și ingineresti.
- ✓ Utilizarea criteriilor și metodelor de evaluare pentru adoptarea procedurilor, tehnicilor și metodelor de bază, necesare creșterii performanțelor.
- ✓ Analiza cerințelor pieței și tendințelor contemporane privind dezvoltarea unor soluții la problemele economice și ingineresti folosind principii și metode ale matematicii, statisticii și informaticii aplicate.

CP5. Proiectarea și integrarea sistemelor informatice utilizând tehnologii și medii de programare

- ✓ Identificarea și descrierea de tehnologii informatice și medii de programare.
- ✓ Explicarea și argumentarea manierei de conducere a organizațiilor sau a unor elemente structurale ale acestora având ca obiect de activitate managementul informațional.
- ✓ Elaborarea specificațiilor și proiectarea unor sisteme informatice folosind metode și instrumente specifice.
- ✓ Evaluarea performanțelor sistemelor software și gestionarea pe această bază a ciclului de viață a sistemelor software.
- ✓ Dezvoltarea, implementarea și integrarea sistemelor informatice.

Competențe transversale	<p>CT1. Aplicarea, în contextul respectării legislației, a drepturilor de proprietate intelectuală (inclusiv transfer tehnologic), a metodologiei de certificare a produselor, a principiilor, normelor și valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă și responsabilă.</p> <p>CT2. Identificarea rolurilor și responsabilităților într-o echipă și aplicarea de tehnici de relaționare și muncă eficientă în cadrul echipei.</p> <p>CT3. Identificarea oportunităților de formare continuă și valorificarea eficientă a resurselor și tehnicilor de învățare pentru propria dezvoltare.</p>
-------------------------	---

6. Obiectivele unității de curs/modulului

Obiectivul general	Studierea problemelor privind securitatea și protecția informației cât și obținerea abilități de utiliza celor mai noi metode de protecție.
Obiectivele specifice	<p>Să înțeleagă și să descrie metodele și tehnici de securitate.</p> <p>Să cunoască sisteme și algoritmi de criptare/decriptare</p> <p>Să selecteze procedee adecvate pentru elaborarea și analiza a modelului de securitate.</p>

7. Conținutul unității de curs/modulului

Tematica activităților didactice	Numărul de ore	
	învățământ cu frecvență	învățământ cu frecvență redusă
Tematica prelegerilor		
T1. Securitatea informației și criptografia. Criptarea cu chei simetrice. Criptarea cu chei simetrice. Criptografie cu chei publice.	6	
T2. Elemente de steganografie.	2	
T3. Protocoale și mecanisme. Stabilirea cheilor, management și certificare. Clase de atacuri și modele de securitate.	4	
T4. Utilizarea cvasigrupurilor în criptografie.	2	
T5. Autentificare și identificare. Semnături digitale.	2	
T6. Metode de protecție: firewall, programe antivirus, detectarea software-ului malițios, detectarea punctelor vulnerabile. Troieni. Spyware. Adware. Dialer. Exploit.	2	
T7. Tipuri de atac: buffer overflow, denial of services, phishing.	2	
T8. Viruși, microviruși. Viruși polimorfi. Viruși metamorfi. Viermi, mailer, mass mailer. Viruși de telefonie mobilă.	4	
T9. Servere Proxy. Rețele VPN	4	
T10. Clasificarea pericolelor securitatii informationale. Clasificarea crimelor informationale.	2	
Total prelegeri:	30	

Tematica activităților didactice	Numărul de ore	
	învățământ cu frecvență	învățământ cu frecvență redusă
Tematica lucrărilor practice		
LP1. Steganografia ca metodă de securitate a informațiilor.	4	

LP2. Algoritmii de criptare IDEA și AES	6	
LP3. Servere Proxy	5	
Total lucrări de laborator:	15	

Tematica activităților didactice	Numărul de ore	
	învățământ cu frecvență	învățământ cu frecvență redușă
Tematica lucrărilor de laborator		
LL1. Criptarea ca metodă de securitate a informațiilor	4	
LL2. Algoritmii de criptare RSA și DES	5	
LL3. Paravanul de protecție Firewall.	2	
LL4. Rețele VPN	4	
Total lucrări de laborator:	15	

8. Referințe bibliografice

Principale	<ol style="list-style-type: none"> Gutmann, P., Cryptography and Data Security, http://www.cs.auckland.ac.nz/apgut001. Bellovin, S.M., Security Problems in the TCP/IP Protocol Suite, AT&T Bell Lab. Murray Hill, New Jersey, 07974, 2002. Fergusson, N., Schneier, B., A Cryptografic Evaluation of IP sec., http://www.counterpane.com, 2000. Gligorovski, D., Markovski, S., Kocarev, L., New Directions in Coding: From Statistical Physics to Quasigroup String Transformation, NOLTA 2004, Japan, Nov 29-Dec 3, 2004
Suplimentare	<ol style="list-style-type: none"> Dimovski, A., Gligorovski, D., Attacks on the Polyalphabetic Substitution Cipher Using a Parallel Genetic Algorithm, Tech. Rep. SCOPES project, March 2003, Ohoid, Macedonia Dimovski, A., Gligorovski, D., Attacks on the Transposition Cipher Using Optimization Heuristics, Proc. Of ICEST 2003, Oct 2003, Sofia, Bulgaria

9. Evaluare

Forma de învățământ	Periodică		Curentă	Lucrul individual	Examen final
	Atestarea 1	Atestarea 2			
Cu frecvență	15%	15%	15%	15%	40%
Standard minim de performanță					
Prezența la lecții; activitatea și calitatea pregătirii la / pentru prelegeri și lucrări de laborator; Obținerea notei minime de „5” la fiecare dintre atestări și lucrări de laborator.					