F I Ş A D I S C I P L I N E I [1)]

1. Date despre program

1.1. Instituţia de învăţământ superior	Universitatea Petrol-Gaze din Ploiești
1.2. Facultatea	Litere și Științe
1.3. Departamentul	Informatică, Tehnologia Informaţiei, Matematică şi Fizică
1.4. Domeniul de studii universitare	Informatică
1.5. Ciclul de studii universitare	Master
1.6. Programul de studii universitare	Tehnologii Avansate pentru Prelucrarea Informaţiei

2. Date despre disciplină

2.1. Denumirea disciplinei	Securitatea informației
2.2. Titularul activităţilor de curs	Conferenţiar dr. Moise Gabriela
2.3. Titularul activităţilor aplicative	Conferenţiar dr. Constantinescu Zoran
2.4. Anul de studiu	I
2.5. Semestrul *	2
2.6. Tipul de evaluare	E
2.7. Categoria formativă** / regimul*** disciplinei	O

* numărul semestrului este conform planului de învăţământ; ** fundamentală = F0; de domeniu = D1; de specialitate = S2; complementară = C3 *** obligatorie = O; opţională = A; facultativă = L

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1. Număr de ore pe săptămână	4	din care: 3.2. curs	2	3.3. Seminar/laborator	2
3.4. Total ore din planul de învăţământ	56	din care: 3.5. curs	28	3.6. Seminar/laborator	28

3.7. Distribuţia fondului de timp	ore
Studiu după manual, suport de curs, bibliografie şi notiţe	30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	45
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	50
Tutoriat	0
Examinări	19
Alte activităţi	0

3.7. Total ore studiu individual	144
3.8. Total ore pe semestru	200
3.9. Numărul de credite	8

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	➢ Programare procedurala avansata, Algoritmi şi structuri de date, Algebră
4.2. de competenţe	➢ Limbaje de programare, elemente de teoria numerelor

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• sală de curs multimedia necesară pentru realizare de expuneri, studii de caz, conversații, dezbateri
5.2. de desfăşurare a	• sală de laborator echipată cu rețea de calculatoare

seminarului/laboratorului	

6. Competenţe specifice acumulate

Competenţe profesionale	➢ Dobândirea cunoştinţelor fundamentale, teoretice şi practice, despre dezvoltarea de aplicaţii specifice şi infrastructurile performante pentru prelucrarea acestora; ➢ Dobândirea cunoştinţelor fundamentale, teoretice şi practice în domeniul securităţii informaţiei (algoritmi de criptare, sisteme şi protocoale criptografice); ➢ Capacitatea de a participa la proiecte de dezvoltare de aplicaţii şi instrumente informatice/software, respectiv de proiecte care implică folosirea acestora în cadrul unor sisteme complexe, tehnice sau socio-tehnice.
Competenţe transversale	➢ Folosirea eficientă a vocabularului profesional şi a limbajului specific în domeniul securitatii informatice pentru prezentarea convingătoare a cunoştinţelor, abilităţilor şi valorilor proprii; ➢ Respectarea unei etici profesionale solide, adecvate societăţii moderne, ca bază a dezvoltării profesionale și personale în concordanță cu cerinţele societăţii noastre dinamice; ➢ Capacitatea de a desfăşura activităţi profesionale într-un cadru organizat, în mod eficient, cu responsabilitate, în conformitate cu codul de etică şi practică profesională, pentru a rezolva probleme concrete prin transpunerea în practică a cunoştinţelor, abilităţilor şi valorilor dobândite pe parcursul programului de master; ➢ Dezvoltarea capacităţilor de integrarea cunoştinţelor, abilităţilor şi valorilor dobândite pe parcursul programului de masterat pentru o inserţie rapidă pe piaţa muncii din domeniu, dar şi pentru construirea unei cariere solide şi care să ofere împlinire profesională; ➢ Conştientizarea impactului social, economic şi moral al informaticii în societatea noastră bazată pe informaţie şi cunoaştere, precum şi a implicaţiilor etice ale dezvoltarii şi utilizării sistemelor, aplicaţiilor şi instrumentelor informatice.

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

7.1. Obiectivul general al disciplinei	Formarea de competențe prefesionale și transverale necesare obținerii calificării. Obiectivul principal al disciplinei constă în însușirea și înțelegerea tehnicilor și algoritmilor de criptare, primitivelor criptografice, protocoalelor criptografice, identificarea vulnerabilităților sistemelor de securitate, realizarea de comparații între diferite cifruri.
7.2. Obiectivele specifice	Formarea următoarelor competențelor profesionale și transversale. După parcurgerea disciplinei studenţii vor putea să: • definească criptarea, criptografia, algoritmi de criptare, protocoale criptografice, identifice problemele din sistemele de securitate • descrie tehnici de criptare • clasifice algoritmi de criptare • clasifice și compare tehnici de criptare • modifice algoritmi de criptare

8. Conţinuturi

8.1. Curs	Nr.ore	Metode de predare	Observaţii
1. Introducere în criptografie si securitatea datelor 2. Criptografie simetrica 3. Functii Hash	1. 2 2. 2 3. 2 4. 2 5. 4	Prelegerea, dezbatere, cercetarea documentelor	

4. Cifruri de tip stream 5. Cifruri de tip bloc 6. Cifrul DES 7. Cifrul AES 8. Criptarea cu chei publice 9. Criptosistemul RSA 10. Managementul cheilor de criptare 11. Semnaturi digitale	6. 3 7. 2 8. 1 9. 2 10. 2 11. 2		
Bibliografie Atanasiu, A., Cursul de criptografie, www.galaxzng.com/adrian_atanasiu/cript.htm Kessler G., C., An overview of Cryptography, 2018, www.garykessler.net/library/crypto.html Paar, Christof and Pelzl, Jan, Understanding Cryptography, A Textbook for Students and Practitioners, Springer-Verlag Berlin Heidelberg 2010. Menezes, Alfred, van Oorchot, Paul and Vanstone, Scott - Handbook of Applied Cryptography, 2001. Constantinescu Zoran, Moise Gabriela, Criptarea informaţiei - ghid practic, Ed. Universităţii Petrol-Gaze din Ploieşti, 2013.			
8.2. Seminar / laborator/proiect	Nr. ore	Metode de predare	Observaţii
1. Sistemul Cezar, Vigenere – aplicaţii 2. Sisteme de criptare de tip stream (RC4) – aplicaţii 3. Sistemul de criptare DES, AES - aplicaţii	8 8 8	Prelegere, expunere, exemplificare, exerciţii.	
Bibliografie Atanasiu, A., Cursul de criptografie, www.galaxzng.com/adrian_atanasiu/cript.htm Kessler G., C., An overview of Cryptography, 2018, www.garykessler.net/library/crypto.html Paar, Christof and Pelzl, Jan, Understanding Cryptography, A Textbook for Students and Practitioners, Springer-Verlag Berlin Heidelberg 2010. Menezes, Alfred, van Oorchot, Paul and Vanstone, Scott - Handbook of Applied Cryptography, 2001. Constantinescu Zoran, Moise Gabriela, Criptarea informaţiei - ghid practic, Ed. Universităţii Petrol-Gaze din Ploieşti, 2013.			

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

- Cursul și seminarul sunt astfel concepute încât, prin competențele formate, să răspundă cerințelor pieței muncii. Ocupațiile absolvenților sunt cele din COR.
- Cursul respecta recomandările IEEE şi ACM legate de Curiculla pentru specializarea Informatică.

10. Evaluare

Tip activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Calitatea răspunsurilor, coerența argumentării, calitatea corelațiilor, etc.	Proba scrisa	45%

	Se urmăreşte completitudinea și corectitudinea cunoștințelor acumulate, capacitatea de sinteză a cunoștințelor, grad de asimilarea a limbajului de specialitate		
10.5. Seminar/laborator/ proiect	Participarea la activitățile de laborator prin realizarea temelor propuse. Se urmăreşte capacitatea de aplicare în practică a cunoștințelor predate, capacitatea de a implementa tehnici de criptare.	Realizarea temelor de laborator	45%
			Din oficiu 10%
Pentru promovarea examenului este necesară obţinerea notei 5 pentru fiecare probă (curs şi laborator).			
10.6. Standard minim de performanţă			
➢ Definirea corectă a termenilor din domeniul criptării, explicarea schemelor de criptare simetrică şi asimetrică. ➢ Realizarea temelor de laborator.			

Data completării

Semnătura titularului de curs
Conf. dr. Gabriela Moise

Semnătura titularului de seminar/laborator

Conf. dr. Zoran Constantinescu

Data avizării în departament

Semnătura directorului de departament

Conf. dr. Gabriela Moise