

FIȘA DISCIPLINEI ¹⁾

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Petrol-Gaze din Ploiești
1.2. Facultatea	Litere și Științe
1.3. Departamentul	Informatică, Tehnologia Informației, Matematică și 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 Informației

2. Date despre disciplină

2.1. Denumirea disciplinei	Securitatea informației
2.2. Titularul activităților de curs	Conferențiar dr. Moise Gabriela
2.3. Titularul activităților aplicative	Conferențiar dr. Moise Gabriela
2.4. Titularul activității proiect	-
2.5. Anul de studiu	I
2.6. Semestrul *	2
2.7. Tipul de evaluare	E
2.8. Categoria formativă** / regimul*** disciplinei	DS/O

*numărul semestrului este conform planului de învățământ; **DF - Discipline fundamentale; DD - discipline de domeniu; DS - discipline de specialitate; DC - discipline complementare, DA - disciplina de aprofundare, DSI - disciplina de sinteză. ***obligatorie = O; opțională = A; facultativă = L

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

3.1. Număr de ore pe săptămână	4	din care:	2	3.3. Seminar/laborator	2	3.4. Proiect	-
		3.2. curs					
3.5. Total ore din planul de învățământ	56	din care:	28	3.7. Seminar/laborator	28	3.8. Proiect	-
		3.6. curs					
3.9. Distribuția fondului de timp							ore
Studiu după manual, suport de curs, bibliografie și notițe							30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren							45
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri							50
Tutoriat							0
Examinări							19
Alte activități							0
3.10. 3.7. Total ore studiu individual	144						
3.11. 3.8. Total ore pe semestru	200						
3.12. 3.9. Numărul de credite	8						

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	➤ Programare procedurală avansată, Algoritmi și structuri de date, Algebră
4.2. de competențe	➤ Limbaje de programare, elemente de teoria numerelor

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	<ul style="list-style-type: none"> sală de curs multimedia necesară pentru realizare de expuneri, studii de caz, conversații, dezbateri
5.2. de desfășurare a seminarului/laboratorului	<ul style="list-style-type: none"> sală de laborator echipată cu rețea de calculatoare

6. Competențe specifice acumulate

Competențe profesionale	<ul style="list-style-type: none"> ➤ Cunoașterea, înțelegerea, analizarea și utilizarea adecvată a conceptelor, metodelor științifice și tehnicilor din domeniul prelucrării avansate a informației pentru a dezvolta inovativ, întreține, utiliza și administra adecvat sisteme software și aplicații informatice complexe din domeniul securității informației; ➤ Utilizarea fundamentelor teoretice și practice ale informaticii pentru interpretarea unor situații și contexte noi, pentru găsirea de soluții pentru probleme specifice acestora, precum și utilizarea nuanțată și pertinentă de modele, metode și tehnici de evaluare pentru a putea formula judecăți de valoare și a fundamenta decizii constructive în domeniul securității informației; ➤
--------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Competențe transversale	<ul style="list-style-type: none"> ➤ Folosirea eficientă a vocabularului profesional și a limbajului specific în domeniul securității informației pentru prezentarea convingătoare a cunoștințelor, abilităților și valorilor proprii; ➤ Respectarea unei etici profesionale solide, adecvate societății moderne, ca bază a dezvoltării profesionale și personale în concordanță cu cerințele societății noastre dinamice; ➤ Capacitatea de a desfășura activități profesionale într-un cadru organizat, în mod eficient, cu responsabilitate, în conformitate cu codul de etică și practică profesională, pentru a rezolva probleme concrete prin transpunerea în practică a cunoștințelor, abilităților și valorilor dobândite pe parcursul programului de master; ➤ Conștientizarea impactului social, economic și moral al informaticii în societatea noastră bazată pe informație și cunoaștere, precum și a implicațiilor etice ale dezvoltării și utilizării sistemelor, aplicațiilor și instrumentelor informatice.
--------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

7.1. Obiectivul general al disciplinei	Formarea de competențe profesionale și transversale necesare obținerii calificării. Obiectivul principal al disciplinei constă în însușirea și înțelegerea principiilor, tehnicilor securității informației; principalelor protocoale de securitate; a modurilor de identificarea a diverselor vulnerabilități și de combatere a amenințărilor informatice.
7.2. Obiectivele specifice	Formarea competențelor profesionale și transversale specificate. După parcurgerea disciplinei studenții vor putea să: <ul style="list-style-type: none"> • Utilizeze tehnici de criptare în comunicația pe canale nesigure; • Dezbata și să propună strategii de securitate informatică; • Analizeze și să implementeze protocoale criptografice; • Analizeze critic aplicații web din punctul de vedere al securității și să ofere soluții pentru securizarea acestora.

8. Conținuturi

8.1. Curs	Nr.ore	Metode de predare	Observații
Introducere în securitatea informațiilor, scurt istoric, importanță, spectrul atacurilor	2	Prelegerea, dezbateri, cercetarea documentelor	
Principii și standarde – standardul ISO/IEC 27001	2		
Criptografie: obiective și aplicații criptografice, criptare simetrică vs. criptare cu cheie publică	2		
Algoritmi asimetrice. RSA	2		
Problema logaritmilor discreți	2		
Funcții Hash. Birthday attack	2		
Criptarea bazată pe curbe eliptice	4		
Aplicații criptografice și protocoale de securitate	4		
Securitate cibernetică, înțelegerea unui atac, identificare vulnerabilități, strategii de apărare	4		
Securitatea aplicațiilor web, vulnerabilități, instrumente software pentru identificare vulnerabilităților	2		
Recapitulare			
Bibliografie Yuri Diogenes (Author), Erdal Ozkaya, Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition, 2019. Trappe W., Washington L.C., Introduction to Cryptography with Coding Theory, Pearson Education, 2006. Paar, Christof and Pelzl, Jan, Understanding Cryptography, A Textbook for Students and Practitioners, Springer-Verlag Berlin Heidelberg 2010. Constantinescu Zoran, Moise Gabriela, Criptarea informației - ghid practic, Ed. Universității Petrol-Gaze din Ploiești, 2013. Dr. Erdal Ozkaya, Cybersecurity: The Beginner's Guide, Packt Publishing, 2019 ENISA Threat Landscape 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 Practical cryptography for developers, Svetlin Nakov, https://cryptobook.nakov.com/ https://cve.mitre.org/cve/ https://www.thevintagenews.com/2018/08/26/cyberattacks-in-the-1830s/?chrome=1			

https://www.isaca.de/sites/default/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf

<https://portswigger.net/burp>

8.2. Seminar / laborator/proiect	Nr. ore	Metode de predare	Observații
Studiu – vulnerabilități și amenințări	4	Explicații, exerciții, rezolvare teme de securitate informatică	
Criptare cu Python	14		
Securitatea aplicațiilor web	8		
Evaluări, prezentare teme	2		

Bibliografie

Yuri Diogenes (Author), Erdal Ozkaya, Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition, 2019.

Trappe W., Washington L.C., Introduction to Cryptography with Coding Theory, Pearson Education, 2006.

Paar, Christof and Pelzl, Jan, Understanding Cryptography, A Textbook for Students and Practitioners, Springer-Verlag Berlin Heidelberg 2010.

Constantinescu Zoran, Moise Gabriela, Criptarea informației - ghid practic, Ed. Universității Petrol-Gaze din Ploiești, 2013.

Dr. Erdal Ozkaya, Cybersecurity: The Beginner's Guide, Packt Publishing, 2019

ENISA Threat Landscape 2021, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>

Practical cryptography for developers, Svetlin Nakov, <https://cryptobook.nakov.com/>

<https://cve.mitre.org/cve/>

<https://www.thevintagenews.com/2018/08/26/cyberattacks-in-the-1830s/?chrome=1>

https://www.isaca.de/sites/default/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf

<https://portswigger.net/burp>

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

- Conținuturile disciplinei corespund cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului.
- Disciplina respectă recomandările IEEE și ACM legate de conținuturile programelor de studii de master din domeniul 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. Se urmărește completitudinea și corectitudinea cunoștințelor acumulate, capacitatea de sinteză a cunoștințelor, grad de asimilarea a limbajului de specialitate	Proba orală – prezentare proiect	70% (1 pct din oficiu)
10.5. Seminar/laborator/proiect	Se urmărește capacitatea de aplicare în practică a cunoștințelor predate, capacitatea de a explica și compara diferite tehnici de securitate.	Realizare teme de laborator	30% (1 pct din oficiu)
Pentru promovarea examenului este necesară obținerea notei 5 pentru fiecare probă (curs și laborator).			
10.6. Standard minim de performanță			
➤ Propunerea unei strategii de securitate informatică			

Data completării

Semnătura titularului de curs

Semnătura titularului de seminar/laborator

13.09.2021

Conf. dr. Gabriela Moise

Conf. dr. Gabriela Moise

Data avizării în departament

Semnătura directorului de departament

16.09.2021

Conf. dr. Gabriela Moise