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 informaţiei
2.2. Titularul activităţilor de curs	Conferenţiar dr. Moise Gabriela
2.3. Titularul activităţilor aplicative	Conferenţiar dr. Moise Gabriela
2.4. Titularul activităţii 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 învăţământ; **DF - Discipline fundamentale; DD - discipline de domeniu; DS - discipline de specialitate; DC - discipline complementare, DA - disciplina de aprofundare, DSI- disciplina de sinteza. ***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. Proiect	-
3.5. Total ore din planul de învăţământ	56	din care: 3.6. curs	28	3.7. Seminar/laborator	28	3.8. Proiect	-
3.9. 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

3.10. 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. Precondiţii (acolo unde este cazul)

4.1. de curriculum	➢ Programare
4.2. de competenţe	➢ Programare în Python

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 seminarului/laboratorului	• sală de laborator echipată cu reţea de calculatoare

6. Competenţe specifice acumulate

Competențe profesionale	➢ Cunoaşterea, înţelegerea, analizarea şi utilizarea adecvată a conceptelor, metodelor ştiinţifice şi tehnicilor din domeniul prelucrării avansate a informației pentru a dezvolta inovativ, întreține, utiliza și administra adecvat sisteme software și aplicaţii informatice complexe din domeniul securității informației. ➢ Utilizarea fundamentelor teoretice şi practice ale informaticii pentru interpretarea unor situaţii şi contexte noi, pentru găsirea de soluţii pentru probleme specifice acestora, precum şi utilizarea nuanţată şi pertinentă de modele, metode şi tehnici de evaluare pentru a putea formula judecăţi de valoare şi a fundamenta decizii constructive în domeniul securității informației.

Competenţe transversale	➢ Folosirea eficientă a vocabularului profesional şi a limbajului specific în domeniul securitatii informației 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 cunoștințelor, abilităților şi valorilor dobândite pe parcursul programului de master. ➢ 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 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: • Utilizeze tehnici de criptare în comunicația pe canale nesigure; • Dezbată și să propună strategii de securitate informatică; • Analizeze și să implementeze protocoale criptografice; • Analizeze critic aplicații din punctul de vedere al securității și să ofere soluții pentru securizarea acestora.

8. Conţinuturi

8.1. Curs	Nr.ore	Metode de predare	Observaţii
Prezentarea obiectivelor cursului. Istoricul scurgerii de informații, atacurilor cibernetice.	2	Prelegerea, dezbatere, cercetarea documentelor	
Spectrul atacurilor, vulnerabilități, vectori de atac, tipuri de atac. Vulnerabilități și amenințări.	2		
Termeni – securitatea informației. Obiectivele generale ale securității: confidenţialitatea, integritatea şi disponibilitatea.	2		
Standarde ISO/IEC familia 27000			
Generalități despre criptografie și aplicații.	2		
Criptosisteme clasice.	2		
Criptosisteme moderne.	2		
Aplicații criptografice și protocoale de securitate.	4		
Strategii de securitate cibernetică.	4		
Securitatea aplicațiilor, vulnerabilități, instrumente software pentru identificarea vulnerabilităților.	2 4		
Recapitulare. Discutarea problemelor din securitate.	2		

Bibliografie

Documente curs, https://timf.upg-ploiesti.ro/cursuri/

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

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

ENISA Threat Landscape, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

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

CVE program, https://cve.mitre.org/cve/.

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

https://www.sans.org/security-resources/glossary-of-terms/.

https://csrc.nist.gov/glossary/term/infosec.

ISO/IEC 27000 - ISO/IEC 27002:2013, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005

https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-27001.

https://www.ogcio.gov.hk/en/our_work/information_cyber_security/collaboration/doc/overview_of_iso_27000_family.pdf.

https://www.isaca.de/sites/default/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf.
PortSwigger, https://portswigger.net/burp.
Strategia de securitate cibernetică a României pe perioada 2022-2027
https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235.
Ghiduri Directoratul Național de Securitate Cibernetică, https://dnsc.ro/doc/ghid.
https://dnsc.ro/vezi/document/ghid-pentru-asigurarea-securitatii-cibernetice-pentru-imm-uri.
https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021.

8.2. Seminar / laborator/proiect	Nr. ore	Metode de predare	Observaţii
Introducere în securitatea informației. Vulnerabilități și amenințări. Termeni – securitatea informației. Obiectivele generale ale securității: confidențialitatea, integritatea și disponibilitatea. Standarde ISO/IEC familia 27000 Dezvoltarea aplicații criptografice în Python	2 4 2 16	Explicații, exerciții, rezolvare teme de securitate informatică	

Bibliografie
Documente curs, https://timf.upg-ploiesti.ro/cursuri/
Svetlin Nakov, Practical cryptography for developers, Svetlin Nakov, https://cryptobook.nakov.com/.
ENISA Threat Landscape, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
CVE program, https://cve.mitre.org/cve/.
https://www.isaca.de/sites/default/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf.
https://www.sans.org/security-resources/glossary-of-terms/.
https://csrc.nist.gov/glossary/term/infosec.
ISO/IEC 27000 - ISO/IEC 27002:2013, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-27001.
https://www.ogcio.gov.hk/en/our_work/information_cyber_security/collaboration/doc/overview_of_iso_27000_family.pdf.
https://www.isaca.de/sites/default/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf.

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

- Conţinuturile disciplinei corespund cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului.
- Disciplina respectă recomandările IEEE şi 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 – sesiune de întrebări și răspunsuri pe baza unui 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)
10.6. Standard minim de performanţă			
Pentru promovarea examenului este necesară cunoașterea termenilor din securitatea informației, a vulnerabilităților, a obiectivelor securității informației, realizare teme laborator.			

	Semnătura titularului de curs	Semnătura titularului de seminar/laborator
Data completării 23 septembrie 2024	Conf. dr. Gabriela Moise	Conf. dr. Gabriela Moise
Data avizării în departament 24 septembrie 2024	Semnătura directorului de departament Lector dr, Anca Baciu	Decan Prof. univ. dr. Mihaela Suditu