

FIȘA DISCIPLINEI¹⁾

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Petrol-Gaze din Ploiești
1.2. Facultatea	Inginerie Mecanică și Electrică
1.3. Departamentul	Automatică, Calculatoare și Electronică
1.4. Domeniul de studii universitare	Ingineria Sistemelor
1.5. Ciclu de studii universitare	Licență
1.6. Programul de studii universitare	Automatică și Informatică Aplicată

2. Date despre disciplină

2.1. Denumirea disciplinei	Securitatea sistemelor de calcul
2.2. Titularul activităților de curs	Prof.univ.dr.ing. Otilia Cangea
2.3. Titularul activităților seminar/laborator	Prof.univ.dr.ing. Otilia Cangea
2.4. Titularul activității proiect	-
2.5. Anul de studiu	IV
2.6. Semestrul *	8
2.7. Tipul de evaluare	Examen
2.8. Categoria formativă** / regimul*** disciplinei	DS

* 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 sinteza.

*** 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: 3.2. curs	2	3.3. Seminar/laborator	2	3.4. Proiect	-
3.5. Total ore din planul de învățământ	56	din care: 3.6. curs	28	3.7. Seminar/laborator	28	3.8. Proiect	-
3.9. Distribuția fondului de timp							ore
Studiu după manual, suport de curs, bibliografie și notițe							15
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren							15
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri							10
Tutoriat							
Examinări							4
Alte activități							
3.10 Total ore studiu individual	44						
3.11. Total ore pe semestru	100						
3.12. Numărul de credite	4						

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	➤ Introducere în automatică și calculatoare ➤ Transmisia datelor
--------------------	---

¹⁾ Adaptare după Ordinul Ministrului educației, cercetării, tineretului și sportului nr. 5 703/2011 privind implementarea Codului național al calificărilor din învățământul superior, publicat în Monitorul Oficial al României, partea I, nr.880 bis / 13.XII.2011

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	➤ Modalitate de predare convențională folosind suport de curs, cu interacțiune profesor-student și tehnici moderne multimedia ➤ Desfășurare prin videoconferință folosind platforme dedicate (Google Meet sau echivalentă) - în condiții speciale
5.2. de desfășurare a seminarului/laboratorului	➤ Laborator dotat cu tehnică de calcul și medii de programare specifice

6. Competențe specifice acumulate

Competențe profesionale	➤ Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul ➤ Operarea cu metode și concepte moderne din știința sistemelor, a calculatoarelor, tehnologia informației și comunicațiilor (C2) ➤ Analiza și evaluarea securității unui sistem de calcul, identificarea vulnerabilităților software (C2) ➤ Analiza și evaluarea vulnerabilităților sistemelor de calcul simulate prin tehnici software ➤ Proiectarea și dezvoltarea de soluții și instrumente software de securitate (C5)
Competențe transversale	➤ Manifestarea unei atitudini onorabile, responsabile, în concordanță cu statutul de student al specializării AIA, față de importanța științifică a domeniului profesional ➤ Demonstrarea spiritului de integrare, de inițiativă și de identificare a problemelor și responsabilităților în cadrul unei echipe de lucru ➤ Capacitatea de a sesiza, înțelege și promova calitatea și creativitatea, pe baza informării și perfecționării continue

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

7.1. Obiectivul general al disciplinei	➤ La sfârșitul cursului, studentul va fi capabil să înțeleagă conceptele, aplicațiile și tehnologiile specifice securității sistemelor, precum și să aibă abilitatea de a analiza, evalua și proiecta sisteme sigure.
7.2. Obiectivele specifice	La sfârșitul cursului, studentul va fi capabil să: - aibă cunoștințe fundamentale privind vulnerabilitățile din sistemele de calcul și modul în care acestea pot fi exploatate cu intenții malițioase; - folosească criptografia în protecția informației specifice; - aplice tehnici corespunzătoare pentru rezolvarea problemelor de securitate prin dezvoltarea, instalarea și configurarea unor aplicații dedicate; - proiecteze și dezvolte aplicații de tip soluții și instrumente software de securitate (tema de casă, proiect de licență)

8. Conținuturi

8.1. Curs	Nr. ore	Metode de predare	Observații
1. Concepte generale de securitate a sistemelor informatice	3	Interactivă și convențională, centrata pe student	Suport de curs în format tipărit și în format electronic, suport multimedia

2. Viruși informatici	4	Interactivă și convențională, centrată pe student	Suport de curs in format tiparit si in format electronic, suport multimedia
3. Firewall	3	Interactivă și convențională, centrată pe student	
4. Securitate web. Securitate e-mail	4		
4. Criptografie pentru protecția informației	4	Interactivă și convențională, centrată pe student.	
5. Primitive de autentificare. Funcții hash	4	Interactivă și convențională, centrată pe student	
6. Studii de caz - Securitatea sistemelor SCADA - Securizarea unei infrastructuri de rețele informatice - Sistem informatic de tip honeypot pentru securizarea informației	6	Interactivă și convențională, centrată pe student	
Bibliografie 1. Cangea, O., <i>Algoritmi de criptare pentru securitatea sistemelor informatice</i> , Editura Universității Petrol-Gaze din Ploiești, 2012 2. Muniz, J., <i>Web Penetration Testing with Kali Linux</i> , Packt Publishing, 2013 3. Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Josang, A., Pereira, T., Stavrou, E., <i>Global perspectives on cybersecurity education for 2030: a case for a meta-discipline</i> , a 23-a Conferință Anuală pentru Inovație și Tehnologie în Știința Calculatoarelor, Cipru, 2018. 4. Stuttard, D., <i>The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws</i> , Wiley (2nd ed), 2011 5. Engebretson, P., <i>The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy</i> , Syngress, 2013 6. Mihai, I. C., Ciuchi, C., Petrică, G., <i>Securitatea cibernetică, provocări și perspective în educație</i> , Editura Sitech, Craiova, 2021 7. Dumitrescu, M., Simionovici, D., <i>Securitatea rețelelor și a sistemelor informatice. Implementarea directivei NIS în România</i> , Volumul 2, Editura Universitară, București, 2022.			
8.2. Seminar / laborator	Nr. ore	Metode de predare	Observații
Firewall	2	Clasica, centrata pe student si pe rezultatele invatarii	
Criptografie cu cheie privată	2	Clasica, centrata pe student si pe rezultatele invatarii	
Criptografie cu cheie publică și infrastructuri de chei publice	4	Clasica, centrata pe student si pe rezultatele invatarii	
Funcții hash – SHA-1, SHA-2, MD5, Bcrypt, Tiger, Whirlpool	4	Clasica, centrata pe student si pe rezultatele invatarii	
Protocoale criptografice TLS, SSL	4	Clasica, centrata pe student si pe rezultatele invatarii	
Ethical hacking. Teste de penetrare	4	Clasica, centrata pe student si pe rezultatele invatarii	
Programe antivirus	4	Clasica, centrata pe student si pe rezultatele invatarii	
Securitatea Web și a bazelor de date	4	Clasica, centrata pe student si pe rezultatele invatarii	

Bibliografie			
1. Cangea, O., <i>Algoritmi de criptare pentru securitatea sistemelor informatice</i> , Editura Universității Petrol-Gaze din Ploiești, 2012			
2. Rescorla, E., <i>The Transport Layer Security (TLS) Protocol Version 1.3</i> . RFC 8446. Internet Engineering Task Force (IETF), 2018.			
3. Rescorla, E., Tschofenig, H., Modadugu, N., <i>The Datagram Transport Layer Security (DTLS) Protocol Version 1.3</i> . RFC 9147. Internet Engineering Task Force (IETF), 2022			
8.3. Proiect	Nr. ore	Metode de predare	Observații
-	-	-	-
Bibliografie			
-			

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

➤ Conținuturile disciplinei sunt specifice domeniului securității informației, fiind coroborate cu așteptările comunității epistemice, ale asociațiilor profesionale și ale angajatorilor care activează în domeniu

10. Evaluare

Tip activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Examinare finală	Lucrare scrisă cu subiecte teoretice și aplicații	50%
	Teste la curs	Teme de casa, referate	10%
10.5. Seminar/laborator	Activitate laborator și verificări periodice	Verificare la încheierea activității de laborator. Efectuarea tuturor lucrărilor de laborator este obligatorie.	40%
10.6. Proiect	-	-	-
10.7. Standard minim de performanță			
➤ Prezența la laborator 100%, cu funcționalitate integrală a lucrărilor			
➤ Capacitatea de a defini și explica conceptele și tehnologiile specifice de securitate ale sistemelor de calcul			

Data
completării
20.09.2024

Semnătura titularului de curs
Prof. dr. ing. CANGEA Otilia

Semnătura titularului de laborator
Prof. dr. ing. CANGEA Otilia

Semnătura titularului
de proiect

Data avizării în
departament

27.09.2024

Director de departament
Conf. dr. ing. Pricop Emil

Decan
Conf. dr. ing. Bădicioiu Marius