F I Ş A D I S C I P L I N E I

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	Automatică, informatică aplicată și sisteme inteligente
1.5. Ciclul de studii universitare	Licență
1.6. Programul de studii universitare	Automatică și Informatică Aplicată

2. Date despre disciplină

2.1. Denumirea disciplinei	Tehnologii digitale și securitate în mediul online
2.2. Titularul activităților de curs	Conf. dr. ing. PRICOP Emil
2.3. Titularul activităților laborator	Asist. ing. drd. POTECĂ Luiza-Alexandra
2.4. Titularul activității proiect	-
2.5. Anul de studiu	II
2.6. Semestrul *	1
2.7. Tipul de evaluare	Examen
2.8. Categoria formativă** / regimul*** disciplinei	DF/DOB

* numărul semestrului este conform planului de învățământ;

** DF - Discipline fundamentale; DS - discipline de specializare; DC - discipline complementare

*** obligatorie/impusă = DOB; opțională = DOP; facultativă = DFA

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. Laborator	2	3.4. Proiect	-
3.5. Total ore din planul de învățământ	56	din care: 3.6. curs	28	3.7. Laborator	28	3.8. Proiect	-
3. 9. Total ore studiu individual (studiu după suport de curs, bibliografie și notițe, documentare suplimentară în bibliotecă, pe platformele electronice de specialitate, pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri)							94
3.10. Total ore pe semestru							150
3.11. Numărul de credite							5

4. Condiții (acolo unde este cazul)

4.1. de curriculum	➢ Programarea calculatoarelor și limbaje de programare ➢ Introducere în automatică și calculatoare
4.2. de desfășurare a cursului	➢ Sala de curs dotată cu videoproiector / tablă inteligentă și conexiune la Internet
4.3. de desfășurare a laboratorului	➢ Laborator dotat cu sisteme PC cu sisteme de operare de clasă Windows sau Linux, browsere Web, software pentru analiza traficului de rețea (ex. Wireshark) și instrumente pentru aplicații IoT (ex. Node-RED, broker MQTT). ➢ Acces la platforma cloud Amazon Web Services (AWS), pentru lucrările de laborator dedicate serviciilor cloud. ➢ Conexiune la Internet pentru accesarea resurselor de pe platforma de e-learning și/sau tutoriale on-line.

5. Competențe specifice acumulate și rezultatele învățării* care stau la baza acestora

Competențe profesionale	Rezultatele învățării*
Cp2. Operarea cu concepte fundamentale din știința calculatoarelor, tehnologia informației și comunicațiilor.	**C1** - Studentul/absolventul descrie și identifică concepte fundamentale referitoare la transformarea digitală, la funcționarea serviciilor Web, la cloud computing și la IoT/IIoT, precum și principalele amenințări la adresa securității informației în mediul online (phishing, malware, inginerie socială). **A1** - Studentul/absolventul utilizează argumentat serviciile și tehnologiile digitale (servicii Web, platforme cloud, aplicații IoT) în rezolvarea de probleme bine definite, inclusiv din ingineria sistemelor. **A2** – Studentul/absolventul utilizează instrumente și tehnici specifice (platforma AWS, Node-RED, manager de parole, autentificare multi-factor, VPN) pentru dezvoltarea unor aplicații simple și pentru protejarea conturilor, a datelor și a comunicațiilor. **RA1** - Studentul/absolventul arată spirit de inițiativă și acțiune pentru actualizarea cunoștințelor privind tehnologiile digitale și amenințările la adresa securității în mediul online.
Competențe transversale	**Rezultatele învățării***
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 dezvoltare.	**C1** - Studentul/absolventul descrie, identifică și sumarizează principiile, normele și valorile codului de etică profesională și aspectele legislative referitoare la securitatea informației și la protecția datelor cu caracter personal în mediul online **A1** - Studentul/absolventul aplică normele de etică profesională și respectă legislația referitoare la confidențialitatea și protecția datelor cu caracter personal. **RA1** - Studentul/absolventul are o comportare onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputația profesiei, în utilizarea tehnologiilor digitale și a serviciilor online.
Ct3. Identificarea oportunităților de formare continuă și valorificarea eficientă a resurselor și tehnicilor de învățare pentru propria dezvoltare.	**C1** - Studentul/absolventul descrie, identifică și sumarizează oportunitățile de formare continuă și resursele digitale (cursuri online, portaluri, documentația platformelor cloud) utile pentru actualizarea competențelor digitale și de securitate. **A1** - Studentul/absolventul valorifică eficient resursele digitale și tehnicile de învățare pentru propria dezvoltare și evaluează critic sursele de informare online. **RA1** - Studentul/absolventul arată spirit de inițiativă și acțiune pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.

***** C – cunoștințe; A – aptitudini; RA – responsabilitate și autonomie.

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

6.1. Obiectivul general al disciplinei	➢ La sfârșitul cursului studentul va fi familiarizat, prin cunoștințele dobândite, cu bazele transformării digitale, ale serviciilor Web, ale cloud computing-ului și ale IoT, precum și cu bunele practici de securitate și de protecție a datelor în mediul online
6.2. Obiectivele specifice	La sfârșitul cursului, studentul va fi capabil: ➢ să înțeleagă conceptele de digitizare, digitalizare și transformare digitală și rolul tehnologiilor digitale în modernizarea proceselor, inclusiv a celor industriale; ➢ să explice principiile de acces la serviciile Web (adresare, DNS, HTTP/HTTPS);

	➢ să descrie modelele și serviciile de cloud computing și să utilizeze servicii de bază ale platformei AWS; ➢ să descrie arhitectura unui sistem IoT/IIoT și să colecteze și să vizualizeze date de la dispozitive; ➢ să recunoască principalele amenințări online și să aplice măsuri practice de protecție a conturilor, a dispozitivelor, a datelor și a comunicațiilor, respectând cadrul legal privind protecția datelor.

7. Conținuturi

7.1. Curs	Nr. ore	Metode de predare	Observații
Introducere în transformarea digitală: digitizare, digitalizare, transformare digitală. Tehnologii suport și exemple din industrie	2	Interactivă și convențională, centrată pe student, folosind prezentări PowerPoint, demonstrații și exemple on-line.	
Internet și Web: adrese IP, DNS, protocoalele HTTP/HTTPS, browsere și servere Web	4		
Cloud computing: concepte, modele de servicii (IaaS, PaaS, SaaS) și modele de utilizare	4		
Servicii cloud în practică (exemplu: Amazon Web Services): calcul, stocare, rețea. Identități și acces, responsabilitate partajată, costuri	2		
Internet of Things (IoT) și Industrial IoT: arhitectură, senzori și elemente de execuție, protocoale de comunicație (MQTT)	4		
IoT și cloud. Conceptul Industry 4.0. Securitatea dispozitivelor IoT	2		
Securitatea online: principii, amenințări și incidente reprezentative. Ingineria socială și phishing	4		
Protecția conturilor și a dispozitivelor: parole, autentificare multi-factor, malware, actualizări, copii de rezervă	4		
Comunicații sigure (HTTPS, VPN) și protecția datelor cu caracter personal (GDPR)	2		

Bibliografie

1. Vogel-Heuser B., Wimmer M. (eds.), Digital Transformation: Core Technologies and Emerging Topics from a Computer Science Perspective, Springer, 2023
2. Ziegler S. et al. (eds.), Springer Handbook of Internet of Things, Springer, 2024
3. Wittig A., Wittig M., Amazon Web Services in Action, Third Edition, Manning Publications, 2023
4. Schneier B., Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, W. W. Norton, 2018
5. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 (GDPR)
6. ***, Directoratul Național de Securitate Cibernetică (DNSC) – materiale de conștientizare, https://dnsc.ro
7. Pricop E., Tehnologii digitale și securitate în mediul online, suport de curs, platforma e-learning F-IME, 2026

7.2. Laborator	Nr. ore	Metode de predare	Observații
Servicii Web: analiza comunicațiilor HTTP/HTTPS și DNS	2	Activitate interactivă și convențională, centrată pe student, bazată pe demonstrații aplicative și exerciții practice ghidate.	
Introducere în Amazon Web Services: consola, utilizatori și permisiuni (IAM), autentificare multi-factor	2		
Publicarea unui site Web static utilizând Amazon S3	4		
Crearea și securizarea unei instanțe Amazon EC2: configurarea regulilor de acces și conectarea la instanță	4		
Internet of Things (IoT): colectarea și vizualizarea datelor de la un senzor simulat utilizând Node-RED și MQTT	4		
Identificarea mesajelor și a site-urilor de tip phishing	4		
Protecția conturilor: parole, manager de parole, autentificare multi-factor și verificarea conturilor compromise. Actualizări și copii de rezervă	4		
Comunicații sigure și protecția vieții private: analiza traficului nesecurizat și traficul HTTPS, utilizarea VPN și configurarea setărilor de confidențialitate. Recapitulare și evaluare finală	4		

Bibliografie

1. ***, Tehnologii digitale și securitate în mediul online – lucrări de laborator. Disponibil pe platforma de e-learning F-IME.
2. ***, Amazon Web Services – AWS Documentation. Disponibil on-line: https://docs.aws.amazon.com/
3. ***, Node-RED – documentație. Disponibil on-line: https://nodered.org/docs/
4. ***, Wireshark Foundation, Wireshark User's Guide. Disponibil on-line: https://www.wireshark.org/docs/wsug_html/
5. OASIS, MQTT Version 5.0, OASIS Standard, 2019.
6. NIST, Digital Identity Guidelines: Authentication and Authenticator Management, NIST SP 800-63B-4, 2025.

7.3. Proiect	Nr. ore	Metode de predare	Observații
Nu este cazul			

Bibliografie

Nu este cazul

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

- Conținuturile disciplinei sunt coroborate cu așteptările angajatorilor ce activează în acest domeniu.
- Prin studiul disciplinei se asigură cunoștințele necesare pentru utilizarea în siguranță a tehnologiilor digitale, înțelegerea bazelor serviciilor Web, ale cloud computing-ului și ale IoT și aplicarea bunelor practici de securitate și de protecție a datelor în mediul online.

9. Evaluare

Tip activitate	9.1. Criterii de evaluare	9.2. Metode de evaluare	9.3. Pondere din nota finală
9.4. Curs	Cunoașterea noțiunilor fundamentale teoretice și practice referitoare la tehnologiile digitale și securitatea în mediul online	Lucrare scrisă cu două subiecte - Subiectul 1, notat de la 1 la 10, constă în 15 întrebări cu răspuns rapid sau grilă (0,6 pct. / răspuns corect + 1 pct. din oficiu). - Subiect 2, notat de la 1 la 10, care constă în rezolvarea unor subiecte aplicative referitoare la analiza unui scenariu de securitate (recunoașterea unei tentative de phishing, alegerea măsurilor de protecție adecvate). Nota finală la examen se calculează dacă la fiecare dintre cele două subiecte se obțin minim 5 puncte.	60%
	Evaluarea implicării active la activitatea de curs	Cuantificarea numărului de prezențe la curs, participarea activă – răspunsuri la întrebări / rezolvarea de probleme la curs, etc.	10%
9.5. Laborator	Activitatea desfășurată la lucrările de laborator	Evaluarea activității de laborator are două componente: -Componenta 1 constă în media notelor obținute pe parcursul semestrului pentru realizarea lucrărilor de laborator. -Componenta 2 constă într-un test grilă final, alcătuit din 15 întrebări (0,6 pct. / răspuns corect + 1 pct. din oficiu). Nota finală la laborator se calculează pe baza celor două componente.	30%
9.6. Proiect	*Nu este cazul*		
9.7. Standard minim de performanță			
➢ Realizarea tuturor lucrărilor de laborator ➢ Studentul trebuie să demonstreze cunoașterea terminologiei de bază (digitalizare, transformare digitală, cloud computing, IoT/IIoT) și a principiilor de funcționare a serviciilor Web, precum și capacitatea de a exemplifica utilizarea acestor tehnologii în aplicații din automatică și industrie. ➢ Recunoașterea principalelor amenințări online (phishing, malware, inginerie socială) și aplicarea măsurilor elementare de protecție: parole și autentificare multi-factor, actualizări, copii de rezervă, comunicații sigure, respectarea principiilor privind protecția datelor personale. ➢ Obținerea a cel puțin 5 puncte (din 10) la fiecare dintre subiectele lucrării scrise finale.			

Data completării	Semnătura titularului de curs	Semnătura titularului de laborator	Semnătura titularului de proiect
18.09.2026	*Conf. dr. ing. Pricop Emil*	*Asist. drd. ing. Potecă Luiza-Alexandra*	

Data avizării în departament	Director de departament	Decan
25.09.2026	*Conf. dr. ing. Pricop Emil*	*Conf. dr. ing. Bădicioiu Marius*