Universitatea Ştefan cel Mare Suceava

FIŞA DISCIPLINEI

1. Date despre program

Facultatea	Facultatea de Inginerie Alimentară
Departamentul	Tehnologii Alimentare, Siguranța Producției Alimentare și a Mediului
Domeniul de studii	**Ingineria Produselor Alimentare**
Ciclul de studii	**Licenţă**
Programul de studii	**Ingineria produselor alimentare**

2. Date despre disciplină

Denumirea disciplinei	**Inteligență artificială și securitate cibernetică**				
Anul de studiu	II	Semestrul	3	Tipul de evaluare	V
Regimul disciplinei	Categoria formativă a disciplinei DF - fundamentală, DS - de specializare, DC – complementară				DC
	Categoria de opționalitate a disciplinei: DOB – obligatorie, DOP – opțională, DFA – facultativă				DOB

3. Timpul total estimat (ore alocate activităților didactice)

I a) Număr de ore pe săptămână	2	Curs	1	Seminar	1	Laborator/ Lucrări practice	0	Proiect	0
I b) Totalul de ore pe semestru din planul de învățământ	28	Curs	14	Seminar	14	Laborator/ Lucrări practice	0	Proiect	0

Distribuția fondului de timp pe semestru	ore
II.Studiu individual	20
III. Examinări	2
IV. Alte activități (precizați):	0

Total ore studiu individual (II+III)	22
Total ore pe semestru (I.b+II+III+IV)	50
Numărul de credite	2

4. Competențe specifice acumulate

Competențe transversale	C.T. 6. Gândește în mod inovator C.T. 7. Gândește holistic
Competențe profesionale	-

5. Rezultatele învățării

Cunoștințe	Aptitudini	Responsabilitate și autonomie
Studentul/absolventul operează cu concepte, principii metode de de bază din matematică, fizică, chimie, desen tehnic, economie și informatică.	• Studentul/absolventul operează cu concepte, principii metode de de bază din matematică, fizică, chimie, desen tehnic, economie și informatică. • Studentul/absolventul rezolvă probleme de matematică, fizică şi chimie cu aplicabilitate în inginerie şi validează soluţia obţinută. • Studentul/absolventul efectuează calcule inginereşti şi economice de complexitate medie şi le asociază cu reprezentări grafice letrice sau specifice proiectării asistate de calculator. • Studentul/absolventul descrie fenomene şi procese fizico-chimice şi economice. • Studentul/absolventul măsoară, evaluează performanţele, diagnostichează şi analizează fenomenele şi sistemele de complexitate mică/medie.	• Studentul/absolventul aplică valorile eticii și deontologiei profesiei de inginer. • Studentul/absolventul practică raționamentul logic, evaluarea și autoevaluarea în luarea deciziilor. • Studentul/absolventul comunică eficient despre activitățile de inginerie cu o gamă largă de public. • Studentul/absolventul este angajat în învățarea pe tot parcursul vieții pentru dobândirea și implementarea cunoștințelor, după cum este necesar, folosind strategii de învățare adecvate. • Studentul/absolventul promovează dialogul, cooperarea, respectul față de ceilalți și interculturalitatea. • Studentul/absolventul lucrează eficient ca membru în echipă sau lider al acesteia. • Studentul/absolventul folosește în comunicare limba străină (engleză, franceză) tehnică.

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

Obiectivul general al disciplinei	Formarea unei culturi tehnologice și digitale avansate prin asimilarea fundamentelor teoretice ale Inteligenței Artificiale și Securității Cibernetice specifice domeniului ingineriei alimentare.

7. Conținutul predării și învățării

Curs	Nr. ore	Metode de predare	Observații
CURS I. FUNDAMENTE TEORETICE ȘI CONCEPTUALE ALE INTELIGENȚEI ARTIFICIALE ȘI SECURITĂȚII CIBERNETICE ÎN INDUSTRIA ALIMENTARĂ **I.1** Repere terminologice și taxonomii în IA: *Machine Learning*, *Deep Learning*, IA Generativă, IA Slabă vs. IA Generală **I.2** Paradigmele securității cibernetice: definirea spațiului cibernetic, Triada C-I-A (Confidențialitate, Integritate, Disponibilitate) **I.3** Cadrul conceptual al tranziției digitale în ingineria alimentară (Industria 4.0/5.0) în industria alimentară	2	• Prelegerea • Explicația • Demonstrația • Dezbaterea conceptuală • Conversație euristică	Material necesar: - sală cu videoproiector, - laptop/PC cu conexiune la Internet pentru profesor.
CURS II. VIZIUNE COMPUTERIZATĂ ȘI MACHINE LEARNING ÎN INSPECȚIA CALITĂȚII ALIMENTELOR **II.1** Principii de achiziție și procesare a imaginilor prin spectroscopie hiperspectrală **II.2** Aplicații ale învățării automate (*Machine Learning*) în identificarea defectelor morfologice, sortare automată și detecția adulterării alimentelor	2	• Prelegerea interactivă • Analiza critică a studiilor de caz	
CURS III. GEMENI DIGITALI, MENTENANȚĂ PREDICTIVĂ ȘI REȚELE IOT INDUSTRIALE **III.1** Arhitectura rețelelor de senzori industriali IoT în monitorizarea parametrilor microclimatici și ai lanțului frigorific (*Cold Chain*) **III.2** Paradigma *Digital Twins* și modelarea matematică a proceselor pentru optimizarea producției și prevenirea avariilor	2	• Prelegerea teoretică • Demonstrația pe modele funcționale	
CURS IV. TRASABILITATE AVANSATĂ ȘI TEHNOLOGII EMERGENTE: SINERGIA BLOCKCHAIN-IA **IV.1** Arhitectura registrelor distribuite (Blockchain) aplicată pe filiera *Farm-to-Fork* **IV.2** Integrararea algoritmilor de IA cu tehnologia Blockchain pentru validarea autenticității datelor și prevenirea fraudei alimentare	2	• Prelegerea • Prezentarea de arhitecturi de sistem	
CURS V. TAXONOMIA AMENINȚĂRILOR CIBERNETICE ÎN INFRASTRUCTURILE INDUSTRIALE DIN SECTORUL ALIMENTAR **V.1** Analiza vulnerabilităților din cadrul sistemelor de conducere a proceselor (SCADA/ICS) și al interfețelor om-mașină (HMI) **V.2** Vectori de atac avansați: Ransomware industrial, DoS/DDoS și manipularea neautorizată a datelor senzoriale/rețetarelor	2	• Prelegerea interactivă • Analiza tipologică a atacurilor	
CURS VI. FACTORUL UMAN, INGINERIE SOCIALĂ ȘI IGIENĂ CIBERNETICĂ ORGANIZAȚIONALĂ **VI.1** Atacuri bazate pe factorul uman: *Phishing*, *Spear-Phishing*, *Business Email Compromise* (BEC) pe lanțul de aprovizionare **VI.2** Protocolul de securizare a activelor digitale: criptografie, autentificare multifactorială (MFA) și protecția secretelor de fabricație	2	• Prelegerea • Dezbaterea pe studii de caz din industrie	
CURS VII. CADRUL DE REGLEMENTARE, ETICĂ ȘI GUVERNANȚĂ DIGITALĂ **VII.**1 Reglementarea europeană privind IA (*EU AI Act* - Regulamentul UE 2024/1689) și clasificarea riscurilor în sectorul agroalimentar **VII.2** Cadrul de conformitate Directiva NIS2 și GDPR în gestionarea datelor industriale	2	• Prelegerea • Analiza comparativă a legislației	

Bibliografie minimală recomandată

Cursuri

1. **Stroe S.-G.** *Inteligență artificială și securitate cibernetică - Note de curs. Format digital,* Universitatea „Ștefan cel Mare” din Suceava, Facultatea de Inginerie Alimentară, 2026.

Cărți și monografii de specialitate:

2. **Yadav, S., Gehlot, A., & Singh, R. (2025/2026).** A*rtificial intelligence and innovation in the food industry*. New Delhi: Wisdom Leaf Press / ICAPSR [Carte integrală Open Access / CC BY 4.0 PDF].
   Disponibil la: https://www.researchgate.net/publication/399495377
3. **IIP International Series. (2023).** *Futuristic trends in artificial intelligence (Vol. 3, Ch. 4: Artificial Intelligence in Food Industry)*. Chikkamagaluru: Iterative International Publishers (IIP) [Carte / Capitol Open Access PDF].
   Disponibil la: https://iipseries.org/assets/docupload/rsl2024DA8F4C05ADA9E56.pdf
4. **Food and Agriculture Sector ISAC & IT-ISAC. (2025).** *Farm-to-table ransomware realities: exploring the ransomware landscape and cyber threat report for agriculture and food sector*. Global cyber threat monograph Series [Raport / Monografie de securitate Open Access].
   Disponibil la: https://industrialcyber.co/reports/food-and-ag-isac-cyber-threat-report-provides-actionable-intelligence-on-cyber-threats-ransomware-tactics/
5. **Yerinde, M., Öztürk, B., & Hürriyetoglu, A. (2025).** *Cybersecurity and food safety in the digital era: bridging the gap for data-driven platforms*. Wageningen academic publications / EFRA Project [Ghid monografic PDF Free].
   Disponibil la: https://research.wur.nl/en/publications/white-paper-cybersecurity-and-food-safety-in-the-digital-era-brid/

Review-uri ştiințifice și articole de sinteză:

1. **Hassoun, A., Jagtap, S., & Garcia-Garcia, G. (2026).** *Artificial intelligence in the food industry: transforming safety, efficiency, and sustainability from farm to fork*. MDPI Foods, 15(2), 101–124. [Open Access PDF].
   Disponibil la: https://www.researchgate.net/publication/404963472
2. **Al-Hasan, M., & Rahman, A. (2024).** *Cybersecurity threats in agriculture supply chains: A comprehensive review*. World Journal of Advanced Research and Reviews, 23(1), 1205–1218. [Open Access PDF].
   Disponibil la: https://www.researchgate.net/publication/384049365
3. **Pratt, M., & Gupta, A. (2025).** *Designing a cybersecurity curriculum for the food and agriculture sector*. Cornell University / arXiv.org, arXiv:2503.16292. [PDF Free Open Access].
   Disponibil la: https://arxiv.org/pdf/2503.16292
4. **Marcu, D., & Popescu, C. (2024).** *Inteligența artificială și securitatea cibernetică: Active IA care se pot constitui în amenințări*. Reviste de specialitate / ResearchGate. [Open Access PDF].
   Disponibil la: https://www.researchgate.net/publication/370579140

Ghiduri instituționale și cadrul normativ (România și UE):

1. **Directoratul Național de Securitate Cibernetică (DNSC). (2023–2026).** *Ghiduri practice de securitate cibernetică și igienă digitală pentru IMM-uri și infrastructuri industriale*. București: DNSC.ro [Colecție online gratuită].
   Disponibil la: https://dnsc.ro/vezi/ghiduri
2. **Comisia Europeană. (2024/2025).** *Regulamentul (UE) 2024/1689 privind Inteligența Artificială (EU AI Act)*. Jurnalul Oficial al Uniunii Europene, L/2024/1689. [Text integral acces gratuit].
   Disponibil la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R1689

Aplicații (seminar)	Nr. ore	Metode de predare	Observații
I. CADRUL METODOLOGIC DE ELABORARE A LUCRĂRILOR APLICATIVE ȘI STABILIREA TEMATICILOR DE LUCRU I.1 Prezentarea ghidului aplicativ și a șablonului integrat de lucru (*Project Canvas*) I.2 Alocarea tematicilor pe filiere specifice din industria alimentară (lactate, carne, panificație, fermentative)	2	• Expunerea • Dezbaterea	Lista materialelor didactice necesare: - note de curs IASC, - alte suporturi bibliografice de specialitate. - PC/laptop profesor, - PC/laptop student, - ecran de proiecție, - videoproiector.
II. CARTOGRAFIEREA FLUXULUI TEHNOLOGIC ȘI IDENTIFICAREA OPORTUNITĂȚILOR IA II.1 Elaborarea schemei tehnologice a procesului ales II.2 Identificarea punctelor critice de proces (PCP-IA) unde se justifică integrarea sistemelor de viziune computerizată sau sortare automată	2		
III. CONCEPEREA ȘI PROIECTAREA SOLUȚIEI IA/IOT ȘI OPTIMIZAREA PRIN PROMPT ENGINEERING III.1 Configurarea conceptuală a sistemului de senzori IoT / Gemene Digital pentru monitorizarea parametrilor III.2 Aplicarea tehnicilor de *Prompt Engineering* pentru generarea documentației tehnice și optimizarea fluxului	2		
IV. MODELAREA TRASABILITĂȚII DIGITALE ȘI A INTEGRITĂȚII DATELOR IV.1 Definirea arhitecturii de trasabilitate pe filieră (materii prime – procesare – distribuție frigorifică) IV.2 Integrararea punctelor de verificare a integrității datelor prin ledger distribuit (Blockchain) și senzori IA	2		
V. EVALUAREA RISCURILOR CIBERNETICE ȘI MATRICEA DE VULNERABILITĂȚI V.1 Construirea matricei de riscuri cibernetice pe fluxul tehnologic (SCADA/ICS, senzori IoT, interfețe HMI) V.2 Analiza scenariilor de atac: Ransomware industrial,	2		

Phishing pe lanțul de aprovizionare și alterarea rețetarelor			
VI. PLANUL DE IGIENĂ CIBERNETICĂ ȘI FIȘA DE CONFORMITATE NORMATIVĂ VI.1 Formularea măsurilor tehnice de prevenție (MFA, politici de acces, copii de siguranță) V.2 Evaluarea conformității aplicațiilor proiectate cu cerințele *EU AI Act*, *NIS2* și *GDPR*	2		
VII. DEFINITIVAREA, SUSȚINEREA ȘI EVALUAREA PROIECTULUI INTEGRAT VII.1 Sintetizarea și integrarea tuturor modulelor în documentul final (Project Canvas) VII.2 Susținerea orală publică a temelor elaborate, dezbaterea critică și evaluarea lor	2		

Bibliografie minimală recomandată

Cursuri

1. **Stroe S.-G.** *Inteligență artificială şi securitate cibernetică - Note de curs. Format digital,* Universitatea „Ştefan cel Mare" din Suceava, Facultatea de Inginerie Alimentară, 2026.

Cărți și monografii de specialitate:

1. **Yadav, S., Gehlot, A., & Singh, R. (2025/2026).** A*rtificial intelligence and innovation in the food industry*. New Delhi: Wisdom Leaf Press / ICAPSR [Carte integrală Open Access / CC BY 4.0 PDF].
   Disponibil la: https://www.researchgate.net/publication/399495377
2. **IIP International Series. (2023).** *Futuristic trends in artificial intelligence (Vol. 3, Ch. 4: Artificial Intelligence in Food Industry)*. Chikkamagaluru: Iterative International Publishers (IIP) [Carte / Capitol Open Access PDF].
   Disponibil la: https://iipseries.org/assets/docupload/rsl2024DA8F4C05ADA9E56.pdf
3. **Food and Agriculture Sector ISAC & IT-ISAC. (2025).** *Farm-to-table ransomware realities: exploring the ransomware landscape and cyber threat report for agriculture and food sector*. Global cyber threat monograph Series [Raport / Monografie de securitate Open Access].
   Disponibil la: https://industrialcyber.co/reports/food-and-ag-isac-cyber-threat-report-provides-actionable-intelligence-on-cyber-threats-ransomware-tactics/
4. **Yerinde, M., Öztürk, B., & Hürriyetoglu, A. (2025).** *Cybersecurity and food safety in the digital era: bridging the gap for data-driven platforms*. Wageningen academic publications / EFRA Project [Ghid monografic PDF Free].
   Disponibil la: https://research.wur.nl/en/publications/white-paper-cybersecurity-and-food-safety-in-the-digital-era-brid/

Review-uri ştiințifice și articole de sinteză:

1. **Hassoun, A., Jagtap, S., & Garcia-Garcia, G. (2026).** *Artificial intelligence in the food industry: transforming safety, efficiency, and sustainability from farm to fork*. MDPI Foods, 15(2), 101–124. [Open Access PDF].
   Disponibil la: https://www.researchgate.net/publication/404963472
2. **Al-Hasan, M., & Rahman, A. (2024).** *Cybersecurity threats in agriculture supply chains: A comprehensive review*. World Journal of Advanced Research and Reviews, 23(1), 1205–1218. [Open Access PDF].
   Disponibil la: https://www.researchgate.net/publication/384049365
3. **Pratt, M., & Gupta, A. (2025).** *Designing a cybersecurity curriculum for the food and agriculture sector*. Cornell University / arXiv.org, arXiv:2503.16292. [PDF Free Open Access].
   Disponibil la: https://arxiv.org/pdf/2503.16292
4. **Marcu, D., & Popescu, C. (2024).** *Inteligența artificială și securitatea cibernetică: Active IA care se pot constitui în amenințări*. Reviste de specialitate / ResearchGate. [Open Access PDF].
   Disponibil la: https://www.researchgate.net/publication/370579140

Ghiduri instituționale și cadrul normativ (România și UE):

1. **Directoratul Național de Securitate Cibernetică (DNSC). (2023–2026).** *Ghiduri practice de securitate cibernetică și igienă digitală pentru IMM-uri și infrastructuri industriale*. București: DNSC.ro [Colecție online gratuită].
   Disponibil la: https://dnsc.ro/vezi/ghiduri
2. **Comisia Europeană. (2024/2025).** *Regulamentul (UE) 2024/1689 privind Inteligența Artificială (EU AI Act)*. Jurnalul Oficial al Uniunii Europene, L/2024/1689. [Text integral acces gratuit].
   Disponibil la: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R1689

8. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Evaluare finală	Însușirea și operarea riguroasă cu noțiunile teoretice privind inteligența artificială, securitatea cibernetică și cadrul legislativ conex.	Evaluare sumativă scrisă (test grilă)	40%
Evaluare pe parcurs	Calitatea soluțiilor tehnice identificate și calitatea redactării finale a lucrărilor conform cerințelor impuse pentru fiecare temă.	- Observația sistematică; - Evaluarea continuă a activității din timpul orelor de seminar; - Verificarea și evaluarea temelor aplicative elaborate individual și prin susținere orală.	60%

Fișa disciplinei include, dacă este cazul, elemente adaptate persoanelor cu dizabilități, în funcție de tipul și gradul acestora.

Data completării	Grad didactic, nume, prenume, semnătura titularului de curs	Grad didactic, nume, prenume, semnătura titularului de aplicație
15 septembrie 2026	Șef lucrări dr. ing. Silviu-Gabriel STROE 	Șef lucrări dr. ing. Silviu-Gabriel STROE 

Data avizării	Grad didactic, nume, prenume, semnătura responsabilului de program
17 septembrie 2026	Conf. univ. dr. bioing. Maria POROCH – SERIȚAN 

Data avizării în departament	Grad didactic, nume, prenume, semnătura directorului de departament
17 septembrie 2026	Șef lucrări dr. ing. Amelia BUCULEI 

Data aprobării în consiliul facultății	Grad didactic, nume, prenume, semnătura decanului
17 septembrie 2026	Prof. univ. dr. ing. Mircea-Adrian OROIAN 