

PLAN DE ÎNVĂȚĂMÂNT

Pentru seria de studenți 2025-2027

Programul de studii univ. de master:	SECURITATEA INFORMAȚIILOR ȘI A SISTEMELOR CIBERNETICE
Tipul de masterat:	profesional
Domeniul fundamental (DFI):	ȘTIINȚE INGINEREȘTI
Ramura de știința (RSI):	INGINERIA SISTEMELOR, CALCULATOARE ȘI TEHNOLOGIA INFORMAȚIEI
Domeniul de licență (DL):	INGINERIA SISTEMELOR
Durata studiilor / Numărul de credite:	2 ani / 120 credite
Forma de învățământ:	IF - Învățământ cu frecvență
Domeniul de studii universitare de master (DSU_M):	INGINERIA SISTEMELOR

RECTOR,
Conf.univ.dr.ing. Florin DRĂGAN

DECAN,
Prof.univ.dr.ing. Marius-George MARCU



Misiunea programului de studii:

Pregătirea superioară a masteranzilor, prin aprofundarea cadrului teoretic și a aplicațiilor din domeniul securității informațiilor și a sistemelor cibernetice.

Obiectivele programului de studii:

Formarea de specialiști care să dețină cunoștințele necesare pentru identificarea/evaluarea vulnerabilităților și a metodelor de atac în sisteme informatice și cibernetice precum și proiectarea și implementarea de măsuri de securitate pentru prevenirea și contracararea acestor atacuri. Programul acoperă, prin materiile propuse, elemente specifice pentru securitatea sistemelor mobile, industriale, bancare, cloud, web și a rețelelor de calculatoare. Aplicațiile practice contribuie la cunoașterea uneltelor și metodologiilor specifice, utilizate pentru analiza securității sistemelor informatice și cibernetice. O componentă importantă a programului constă în activități de cercetare științifică în domeniul securității informației și a sistemelor cibernetice.

Competențele programului de studii:

Competențe profesionale:

- a. Identificarea și evaluarea vulnerabilităților și a metodelor de atac în sisteme informatice și cibernetice precum și proiectarea și implementarea de măsuri de securitate pentru prevenirea și contracararea acestor atacuri (C1).
- b. Proiectarea, implementarea și evaluarea de soluții de securitate specifice sistemelor mobile, industriale, cloud și web (C2).
- c. Utilizarea de unelte și metodologii specifice securității sistemelor informatice și cibernetice (C3).
- d. Cercetare științifică în domeniul securității informației și a sistemelor cibernetice (C4).

Competențe transversale:

- CT1. Aplicarea valorilor și eticii profesiei de cercetător și executarea responsabilă a sarcinilor profesionale în condiții de autonomie și luare de decizii bazate pe evaluare și autoevaluare.
- CT2. Realizarea activităților și exercitarea rolurilor specifice muncii în echipă, pe diferite paliere ierarhice, manifestând spirit de inițiativă și antreprenorial și rol de lider bazat pe promovarea dialogului, cooperării, atitudinii pozitive, respectului reciproc, diversității și multiculturalității și îmbunătățire continuă a propriei activități.
- CT3. Autoevaluarea obiectivă a nevoii de formare profesională, continuă, în scopul inserției pe piața muncii și al adaptării la dinamica cerințelor acesteia și pentru dezvoltarea personală și profesională și utilizarea eficientă a abilităților multilingvistice și a cunoștințelor de tehnologia informației și a comunicării.

Rezultatele învățării specifice programului de studii:		
Cunoștințe	Aptitudini	Responsabilitate și autonomie
C1. Studentul/absolventul are cunoștințe fundamentale în domeniul securității informației, cunoaște fundamentele teoretice ale criptografiei și fundamentele teoretice care stau la baza mecanismelor de securitate la nivelul sistemelor de operare și comunicațiilor de date în rețele de calculatoare. C2. Studentul/absolventul are cunoștințe asupra soluțiilor de securitate într-un context practic specific, în domeniul sistemelor automotiv, dispozitivelor mobile, sistemelor industriale, sistemelor informatice financiar bancare, precum și alte domenii conexe. C3. Studentul/absolventul are cunoștințe cu privire la soluții defensive, înțelege și explică metode, concepte și biblioteci software, pentru arhitecturi de securitate, detecție și prevenție a intruziunilor, managementul și acoperirea vulnerabilităților. C4. Studentul/absolventul are cunoștințe cu privire la soluții ofensive, testare asupra penetrării sistemelor, inginerie inversă, dezvoltare de exploatare asupra sistemelor. C5. Studentul/absolventul are cunoștințe cu privire la standardele în domeniu, politici de securitate comun adoptate și managementul riscului.	A1.1 Studentul/absolventul explică soluția și argumentează soluția propusă pe baza principiilor fundamentale din securitatea informației. A1.2 Studentul/absolventul interpretează și explică la nivel fundamental probleme specifice securității informației folosind noțiuni din criptografie, sisteme de operare, rețele de calculatoare. A1.3 Studentul/absolventul determină și aplică concepte specifice ale criptografiei pentru designul unor soluții de securitate în sisteme de operare și rețele de calculatoare. A2.1 Studentul/absolventul este capabil să analizeze și să evalueze riscurile de securitate specifice diverselor domenii aplicative, precum sistemele automotiv, dispozitivele mobile, infrastructurile industriale și cele financiar-bancare. A2.2 Studentul/absolventul poate proiecta și implementa soluții de securitate adaptate contextului practic particular al fiecărui tip de sistem, integrând tehnologii și metodologii corespunzătoare. A2.3 Studentul/absolventul demonstrează aptitudinea de a adapta și corela concepte teoretice de securitate cu cerințele operaționale și constrângerile specifice mediilor aplicative distincte. A3.1 Studentul/absolventul este capabil să proiecteze și să implementeze soluții defensive adaptate diverselor arhitecturi de securitate, utilizând metodologii și instrumente software specializate, inclusiv tehnologii emergente în domeniul inteligenței artificiale. A3.2 Studentul/absolventul poate identifica, evalua și gestiona vulnerabilități în infrastructuri informatice complexe, aplicând proceduri de detecție, prevenție și remediere conform celor mai bune practici. A3.3 Studentul/absolventul demonstrează aptitudinea de a integra și corela diverse tehnologii și biblioteci software pentru securitatea informației, dar și din domenii emergente precum inteligența artificială în vederea dezvoltării unor mecanisme eficiente de monitorizare și răspuns la incidente de securitate cibernetică. A4.1 Studentul/absolventul este capabil să planifice și să execute teste de penetrare asupra unor infrastructuri informatice, aplicând metodologii standardizate. A4.2 Studentul/absolventul poate utiliza tehnici de inginerie inversă pentru a analiza funcționalitatea, vulnerabilitățile și comportamentul aplicațiilor sau componentelor software. A4.3 Studentul/absolventul demonstrează aptitudinea de a dezvolta și adapta exploit-uri în scop didactic sau de cercetare, evidențiind înțelegerea mecanismelor de compromitere și a contramăsurilor corespunzătoare. A5.1 Studentul/absolventul este capabil să interpreteze și să aplice standarde și bune practici din domeniul securității informației eliberate de organisme recunoscute în domeniu (ISO, IEC, NIST, SAE, etc.), traducându-le în soluții operaționale adaptate problemei abordate. A5.2 Studentul/absolventul poate elabora, implementa și evalua politici de securitate și proceduri operaționale, asigurând alinierea lor cu cerințele organizaționale și de reglementare. A5.3 Studentul/absolventul demonstrează aptitudinea de a conduce evaluări ale riscului și de a propune măsuri de management și atenuare a riscurilor, incluzând monitorizare, audit și raportare către factorii de decizie.	RA1.1 Studentul/absolventul are responsabilitatea de a utiliza cunoștințele teoretice în mod critic și riguros, evitând interpretările superficiale sau aplicările eronate care ar putea compromite securitatea sistemelor. RA1.2 Studentul/absolventul este responsabil de actualizarea și aprofundarea continuă a cunoștințelor teoretice, pentru a ține pasul cu dinamica rapidă a domeniului securității cibernetice. RA1.3 Studentul/absolventul lucrează autonom, dar se asigură și de colaborarea eficientă cu alte echipe de specialitate. RA2.1 Studentul/absolventul își asumă responsabilitatea de a aplica soluții de securitate adaptate specificului fiecărui domeniu, prevenind afectarea funcționalității critice a sistemelor și siguranței utilizatorilor. RA2.2 Studentul/absolventul acționează cu responsabilitate în identificarea, evaluarea și comunicarea vulnerabilităților, evitând expunerea inutilă a datelor cu caracter personal sau periclitatea proceselor industriale ori financiare. RA2.3 Studentul/absolventul lucrează autonom, dar se asigură și de colaborarea eficientă cu alte echipe de specialitate. RA3.1 Studentul/absolventul își asumă responsabilitatea de a proiecta și implementa soluții defensive care protejează confidențialitatea, integritatea și disponibilitatea informațiilor. RA3.2 Studentul/absolventul acționează cu responsabilitate în monitorizarea și gestionarea incidentelor de securitate, limitând impactul acestora asupra utilizatorilor și organizațiilor. RA3.3 Studentul/absolventul respectă principiile de confidențialitate și protecția datelor cu caracter personal atunci când configurează, testează sau administrează soluții defensive. RA4.1 Studentul/absolventul își asumă responsabilitatea de a aplica cunoștințele și aptitudinile dobândite exclusiv în scopuri etice, respectând legislația în vigoare și normele de conduită profesională. RA4.2 Studentul/absolventul acționează cu diligență și integritate în procesul de testare și evaluare a securității, evitând generarea de riscuri suplimentare sau afectarea funcționalității sistemelor evaluate și a datelor. RA4.3 Studentul/absolventul demonstrează responsabilitate socială și profesională prin raportarea corectă și transparentă a vulnerabilităților identificate, în vederea remedierii acestora și protejării intereselor organizaționale și publice. RA5.1 Studentul/absolventul își asumă responsabilitatea de a respecta și integra în activitatea sa standardele internaționale și politicile organizaționale de securitate, contribuind la crearea unui mediu conform și sigur. RA5.2 Studentul/absolventul are responsabilitatea de a asigura alinierea soluțiilor de securitate cu cerințele legale și de reglementare, evitând practicile care ar putea genera neconformități sau sancțiuni. RA5.3 Studentul/absolventul demonstrează responsabilitate prin documentarea și raportarea transparentă a proceselor de management al riscului, astfel încât factorii de decizie să beneficieze de informații clare și relevante.

--	--	--

Rezultatele complementare ale învățării:

Cunoștințe	Aptitudini	Responsabilitate și autonomie
CC1 Studentul/absolventul cunoaște, înțelege și explică regulile de bază, conceptele și principiile cercetării academice în contextul proiectelor și lucrărilor dezvoltate. CC2. Studentul/absolventul cunoaște, înțelege și explică principiile eticii și integrității științifice în activitățile de cercetare.	AC1. Studentul/absolventul efectuează cercetare științifică, concepe, creează și validează noi cunoștințe prin formularea de întrebări în legătură cu cercetarea, prin îmbunătățirea sau dezvoltarea de teorii, modele, instrumente, software sau metodologii operaționale, utilizând metode și tehnici științifice consacrate. AC2.1 Studentul/absolventul aplică principiile fundamentale de etică și legislația în domeniul cercetării științifice, inclusiv în ceea ce privește aspectele legate de integritatea cercetării. AC2.2 Studentul/absolventul dezvoltă și revizuieste lucrări de cercetare, evitând abordări și comportamente greșite, cum ar fi falsificarea rezultatelor și plagiatul.	RA1. Studentul/absolventul manifestă inițiativă și responsabilitate privind cercetările efectuate, precum și capacitate de colaborare cu alte colective de cercetare. RA2. Studentul/absolventul manifestă un comportament onorabil și, responsabil, în spiritul eticii, legii și integrității academice, în vederea susținerii reputației profesiei.

Finalități:

Absolvenții programului de studii universitare de master vor accesa următoarele ocupații posibile conform Clasificării Ocupațiilor din România ISCO-08:

- Specialist în proceduri și instrumente de securitate a sistemelor informatice - 251402

Domeniul de licență:
Programul de studii univ. de master profesional:

INGINERIA SISTEMELOR
SECURITATEA INFORMAȚIILOR ȘI A SISTEMELOR CIBERNETICE

Forma de învățământ:
Durata studiilor:

IF - Învățământ cu frecvență
2 ani

Domeniul fundamental (DFI):
Ramura de știință (RSI):
Domeniul de studii universitare de master (DSU_M):

ȘTIINȚE INGINEREȘTI
INGINERIA SISTEMELOR, CALCULATOARE ȘI TEHNOLOGIA INFORMAȚIEI
INGINERIA SISTEMELOR

Cod DFI	Cod RSI	Cod DSU_M
20	60	20

ciclul	c1c2c3	a1a2
M	025	25

PLAN DE ÎNVĂȚĂMÂNT
Pentru seria de studenți 2025-2027
ANUL I (2025-2026)

	SEMESTRUL 1										SEMESTRUL 2									
1	Tehnici criptografice moderne										Virusologie și vulnerabilități ale sistemelor informatice									
	M025.25.01.S1	6	E	28	0	14	14		DS	94	M025.25.02.S1	5	E	21	0	14	14		DS	76
2	Securitatea rețelelor de calculatoare										Securitatea aplicațiilor cloud									
	M025.25.01.F2	6	E	28	0	14	14		DF	94	M025.25.02.F2	5	E	28	0	14	14		DF	69
3	Securitatea aplicațiilor mobile										Disciplină opțională independentă 1 Standarde și metodologii pentru evaluarea securității // Baze de date avansate // Sisteme bazate pe cunoștințe									
	M025.25.01.S3	5	E	28	0	14	14		DS	69	M025.25.02.F3-ij	5	E	21	0	7	14		DF	83
4	Securitatea aplicațiilor web										Disciplină opțională independentă 2 Securitatea informației în sisteme financiar-bancare // Rețele neuronale, sisteme fuzzy și algoritmi genetici									
	M025.25.01.S4	6	E	28	0	14	14		DS	94	M025.25.02.F4-ij	5	E	21	0	0	21		DF	83
5	Practică profesională 1										Etică și integritate academică									
	M025.25.01.S5	7	V	0	0	0	0	147	DS	28	M025.25.02.C5	2	V	14	7	0	0		DC	29
6											Practică profesională 2									
											M025.25.02.S6	8	V	0	0	0	0	147	DS	53
7																				
8																				
9																				
10											Disciplină facultativă									
											M025.25.02.f10-ij								f	
total / sem.	VAi:	224	VPI:	379	VAi:	210	VPI:	393			VAi:	210	VPI:	393						
	VA (VAi+VAp):	371	VCA (VA+VPI):	750	VA (VAi+VAp):	357	VCA (VA+VPI):	750			VA (VAi+VAp):	357	VCA (VA+VPI):	750						
	credite:	30	evaluări:	4E,1V,0C	credite:	30	evaluări:	4E,2V,0C			credite:	30	evaluări:	4E,2V,0C						
total / săptăm.	VAi:	16.0	VPI:	27.1	VAi:	15.0	VPI:	28.1			VAi:	15.0	VPI:	28.1						
	VA (VAi+VAp):	26.5	VCA (VA+VPI):	53.6	VA (VAi+VAp):	25.5	VCA (VA+VPI):	53.6			VA (VAi+VAp):	25.5	VCA (VA+VPI):	53.6						
	din care:		8.0	0.0	4.0	4.0	10.5	(c, s, l, p, VAp)			din care:		7.5	0.5	2.5	4.5	10.5	(c, s, l, p, VAp)		

Observatii:

Pentru seria de studenti 2025-2027

ANUL II (2026-2027)

	SEMESTRUL 3										SEMESTRUL 4									
1	Securitate în sisteme embedded și automotive										Practică profesională 4									
	M025.25.03.S1	6	E	28	0	14	14		DS	94	M025.25.04.S1	15	V	0	0	0	0	196	DS	179
2	Securitatea sistemelor industriale										Elaborarea lucrării de disertație									
	M025.25.03.F2	6	E	28	0	14	14		DF	94	M025.25.04.S2	15	V	0	0	0	196	0	DS	179
3	Disciplină opțională independentă 3 Tratarea incidentelor de securitate și măsuri de prevenție // Sisteme haotice // Managementul proiectelor // Tehnologii Java										Examen de disertație									
	M025.25.03.F3-ij	5	E	21	0	7	14		DF	83	M025.25.04.F3	10	E						DF	
4	Disciplină opțională independentă 4 Comunicații de date intervehiculare // Modele bioinformatic																			
	M025.25.03.F4-ij	5	E	21	0	0	21		DF	83										
5	Practică profesională 3																			
	M025.25.03.S5	8	V	0	0	0	0	154	DS	46										
6																				
7																				
8																				
9																				
10											Disciplină facultativă									
											M025.25.04.f10-ij								f	
total / sem.	VAi:	196	VPI:	400	VAi:	196	VPI:	358												
	VA (VAi+VAp):	350	VCA (VA+VPI):	750	VA (VAi+VAp):	392	VCA (VA+VPI):	750												
	credite:	30	evaluări:	4E,1V,0C	credite:	30+10*	evaluări:	1E,2V,0C												
total / săptăm.	VAi:	14.0	VPI:	28.6	VAi:	14.0	VPI:	25.6												
	VA (VAi+VAp):	25.0	VCA (VA+VPI):	53.6	VA (VAi+VAp):	28.0	VCA (VA+VPI):	53.6												
	din care:		7.0	0.0	2.5	4.5	11.0	(c, s, l, p, VAp)	din care:		0.0	0.0	0.0	14.0	14.0	(c, s, l, p, VAp)				

* Credite suplimentare alocate Examenului de disertație

Observatii:

RECTOR,
Conf.univ.dr.ing. Florin DRĂGAN

DECAN,
Prof.univ.dr.ing. Marius-George MARCU

DISCIPLINE OPTIONALE
Pentru seria de studenti 2025-2027

ANUL I (2025-2026)

	SEMESTRUL 1										SEMESTRUL 2									
01											Disciplină opțională independentă 1 Standarde și metodologii pentru evaluarea securității									
											M025.25.02.F3-01	5	E	21	0	7	14		DF	83
02											Disciplină opțională independentă 1 Baze de date avansate									
											M025.25.02.F3-02	5	E	21	0	7	14		DF	83
03											Disciplină opțională independentă 1 Sisteme bazate pe cunoștințe									
											M025.25.02.F3-03	5	E	21	0	7	14		DF	83
04											Disciplină opțională independentă 2 Securitatea informației în sisteme financiar-bancare									
											M025.25.02.F3-04	5	E	21	0	0	21		DF	83
05											Disciplină opțională independentă 2 Rețele neuronale, sisteme fuzzy și algoritmi genetici									
											M025.25.02.F3-05	5	E	21	0	0	21		DF	83
06																				
07																				
08																				
09																				
10																				

Observatii: (*) - discipline opționale activate în anul univ. 20__-20__

DISCIPLINE OPTIONALE
Pentru seria de studenti 2025-2027

ANUL II (2026-2027)

	SEMESTRUL 3										SEMESTRUL 4									
01	Disciplină opțională independentă 3 Tratarea incidentelor de securitate și măsuri de prevenție																			
	M025.25.03.F3-01	5	E	21	0	7	14		DF	83										
02	Disciplină opțională independentă 3 Sisteme haotice																			
	M025.25.03.F3-02	5	E	21	0	7	14		DF	83										
03	Disciplină opțională independentă 3 Managementul proiectelor																			
	M025.25.03.F3-03	5	E	21	0	7	14		DF	83										
04	Disciplină opțională independentă 3 Tehnologii Java																			
	M025.25.03.F3-04	5	E	21	0	7	14		DF	83										
05	Disciplină opțională independentă 4 Comunicații de date intervehiculare																			
	M025.25.03.F3-05	5	E	21	0	0	21		DF	83										
06	Disciplină opțională independentă 4 Modele bioinformatic																			
	M025.25.03.F3-06	5	E	21	0	0	21		DF	83										
07																				
08																				
09																				
10																				

Observatii: (*) - discipline opționale activate în anul univ. 20__-20__

Legenda

Nume disciplina									
Cod	nc	FE	c	s	l	p	VAp	CF	VPI

Cod = cod disciplina
nc = nr.credite transferabile
FE = forma de evaluare
FE ∈ {E, V, C}
E=examen
V=verificare
C=colocviu
c=nr.ore curs/semestru
s=nr.ore seminar
l=nr.ore laborator
p=nr.ore proiect
VAp- volum de ore necesar activitatilor partial asistate

Exemplu									
Tehnologii avansate de măsurare									
M170.17.01.V1	8	E	28	0	28	0	49	DC	50

CF=categorie formativa careia ii apartine disciplina
CF={DF, DS, DC}
DF - disciplina fundamentala
DS - disciplina de specializare
DC - disciplina complementara
VPI = volum de ore necesar pregatirii individuale pentru un semestru de 14 sapt. plus 4 sapt. de sesiune
VAi- volum de ore necesar activitatilor integral asistate=c+s+l+p
VA - volum de ore necesar activitatilor integral asistate si al celor asistate partial
=VAi+Vap
VCA - volum de ore cumulat al tuturor activitatilor = VA+VPI

RECTOR,
Conf.univ.dr.ing. Florin DRĂGAN

DECAN,
Prof.univ.dr.ing. Marius-George MARCU

DISCIPLINE FACULTATIVE
Pentru seria de studenti 2025-2027
ANUL I (2025-2026)

	SEMESTRUL 1										SEMESTRUL 2									
01											Voluntariat									
											M025.25.02.f10-01	2	C	0	0	0	28		f	22
02																				
03																				
04																				

Observatii:

DISCIPLINE FACULTATIVE
Pentru seria de studenti 2025-2027
ANUL II (2026-2027)

	SEMESTRUL 3										SEMESTRUL 4									
01											Voluntariat									
											M025.25.04.f10-01	2	C	0	0	0	28		f	22
02																				
03																				
04																				

Observatii:

RECTOR,
 Conf.univ.dr.ing. Florin DRĂGAN

DECAN,
 Prof.univ.dr.ing. Marius-George MARCU