Aprobat
Ședința Senatului
din data 04.06.2026

UNIVERSITATEA „ȘTEFAN CEL MARE" DIN SUCEAVA
Facultatea de Inginerie Electrică și Știința Calculatoarelor
Domeniul: Inginerie Electronică, Telecomunicaţii și Tehnologii Informaționale
Program de studiu: Securitate Cibernetică (SC)
Ciclul de studii: masterat profesional
Forma de învăţământ: ÎF
Durata studiilor: 2 ani
Valabil începând cu anul I, anul universitar: **2026- 2027**

AVIZAT
Ședința Consiliului de administrație
din data 28.05.2026

PLAN DE ÎNVAŢAMÂNT

Cerinţe pentru obţinerea diplomei de masterat

120 credite acordate pentru promovarea examenului de finalizare a studiilor
10 credite acordate pentru promovarea examenului de disertație

UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA
Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor

Aprobat
Şedinţa Senatului
din data 04.06.2026

PLAN DE ÎNVĂŢĂMÂNT

Domeniul: Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
Program de studiu: Securitate Cibernetică (SC)
Ciclul de studii: masterat profesional
Forma de învăţământ: ÎF
Durata studiilor: 2 ani
Valabil începând cu anul I, anul universitar: 2026- 2027

ANUL I

Nr. crt.	Discipline obligatorii	Cod disciplina USV.FIESC.SC	Sem. 1 C	S	L	P	I*	Forma verificare	Nr. credite**	Sem. 2 C	S	L	P	I*	Forma verificare	Nr. credite**
1	NOŢIUNI AVANSATE DE COMUNICAŢII ŞI REŢELE DE CALCULATOARE	DF.01.01	2		1		83	E	5							
2	MODELAREA ŞI FUNCŢIONAREA SISTEMELOR WIRELESS	DF.01.02	2		1		83	E	5							
3	CRIPTOGRAFIA	DF.01.03	1		1	1	83	E	5							
4	MANAGEMENTUL PROIECTELOR ŞI PROBLEMELOR COMPLEXE	DF.01.04	2	1			83	V	5							
5	PRACTICĂ PROFESIONALĂ I **	DS.01.05				3	108	C	6							
6	SECURITATEA CRIPTOGRAFICĂ A SISTEMELOR ŞI A REŢELELOR DE COMUNICAŢII	DS.02.06								1		1	1	83	E	5
7	COMUNICAŢII MOBILE ŞI PRIN SATELIT ŞI SECURITATEA LOR	DS.02.07								2		1		83	E	5
8	ATACURI CIBERNETICE ŞI PROTECŢIE CIBERNETICĂ	DS.02.08								2		2		69	E	5
9	CREATIVITATE ŞTIINŢIFICĂ, COMUNICARE TEHNICĂ ŞI INOVARE	DF.02.09								1	1			72	V	4
10	PRACTICĂ PROFESIONALĂ II **	DS.02.10											3	108	C	6
	Total ore obligatorii pe săptămână		7	1	3	4	440	3E 1C 1V	26	6	1	4	4	415	3E 1C 1V	25
			15							15						

Nr. crt.	Discipline opţionale	Cod disciplina USV.FIESC.SC	Sem. 1 C	S	L	P	I*	Forma verificare	Nr. credite**	Sem. 2 C	S	L	P	I*	Forma verificare	Nr. credite**
11	REŢELE DE SENZORI ŞI AD-HOC	DF.01.11	1		1		72	E	4							
12	NANOTEHNOLOGII ÎN INGINERIA COMUNICAŢIILOR	DF.01.12														
13	TEHNOLOGII WEB AVANSATE ŞI ARHITECTURI ORIENTATE PE SERVICII	DS.02.13								1		1		97	E	5
14	INGINERIE SOFTWARE AVANSATĂ	DS.02.14														
	Total ore opţionale pe săptămână		1		1		72	1E	4	1		1		97	1E	5
			2							2						

	RECAPITULAŢIE		8	1	4	4	512	4E 1C 1V	30	7	1	5	4	512	4E 1C 1V	30
			17							17						

Nr. crt.	Discipline facultative	Cod disciplina	Sem. 1 C	S	L	P	I*	Forma verificare	Nr. credite**	Sem. 2 C	S	L	P	I*	Forma verificare	Nr. credite**
15	Psihopedagogia adolescenţilor, tinerilor şi adulţilor	USV.DSPP.NIV2. DF.0101	2	1			83	E	5							
16	Comunicare educaţională Metodologia cercetării educaţionale Educaţie interculturală Consiliere şi orientare	USV.DSPP.NIV2. DC.0102	1	2			83	E	5							
17	Proiectarea şi managementul programelor educaţionale	USV.DSPP.NIV2. DF.0203								2	1			83	E	5
18	Didactica domeniului şi dezvoltări în didactica specialităţii (învăţământ liceal, postliceal, universitar)	USV.DSPP.NIV2. DS.0204								2	1			83	E	5
	Total ore facultative pe săptămână		3	3			166	2E	10	4	2			166	2E	10
			6							6						

NOTĂ: C/S/L/P - Numărul de ore de curs/seminar/laborator/proiect/ săptămânal pe parcursul semestrului
I* - ore de studiu individual pe semestru
** Practica se poate realiza cumulat la sfârşitul semestrelor, sau distribuită pe parcursul acestora.

Ordonator de credite,
Prof.univ.dr. ec. Gabriela PRELIPCEAN

Decan,
Prof.univ.dr.ing. L. Dan MILICI

Director departament,
Conf.univ.dr.ing. Eugen COCA

Responsabil program de studii,
Conf.univ.dr.ing. Alexandra Ligia BALAN

MINISTERUL EDUCAŢIEI ŞI CERCETĂRII
UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA

UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA
Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor

Aprobat
Şedinţa Senatului
din data 04.06.2026

PLAN DE ÎNVĂŢĂMÂNT

Domeniul: Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
Program de studiu: Securitate Cibernetică (SC)
Ciclul de studii: masterat profesional
Forma de învăţământ: ÎF
Durata studiilor: 2 ani
Valabil începând cu anul I, anul universitar: 2026- 2027

ANUL II

Nr. crt.	Discipline obligatorii	Cod disciplina USV.FIESC.SC	Sem. 3 C	S	L	P	I*	Forma verificare	Nr. credite**	Sem. 4 C	S	L	P	I*	Forma verificare	Nr. credite**
1	SECURITATEA SISTEMELOR CLOUD ŞI GRID	DS.03.01	1		2		83	E	5							
2	MANAGEMENTUL ŞI AUDITAREA SECURITĂŢII SISTEMELOR INFORMATICE ŞI DE COMUNICAŢII	DS.03.02	1		2	1	69	E	5							
3	COMUNICAŢII OPTICE ŞI SECURITATEA LOR	DF.03.03	2		1		83	E	5							
4	ETICĂ ŞI INTEGRITATE ACADEMICĂ	DC.03.04	0.5	0.5			36	V	2							
5	PRACTICĂ ÎN POLIGON DE SECURITATE CIBERNETICĂ	DS.03.05				1	186	V	8							
6	SISTEME IoT SECURIZATE PRIN TEHNICI DE INTELIGENŢĂ ARTIFICIALĂ ŞI ÎNVĂŢARE AUTOMATĂ	DF.04.06								1		1		97	E	5
7	PROTECŢIA DATELOR PERSONALE ŞI LEGISLAŢIE ÎN DOMENIUL SECURITĂŢII CIBERNETICE	DC.04.07									1			61	E	3
8	CERCETARE PENTRU ELABORAREA DISERTAŢIEI	DS.04.08											3	108	V	6
9	ELABORARE DISERTAŢIE	DS.04.09											8	288	V	16
	Total ore obligatorii pe săptămână		4.5	0.5	5	2	457	3E2V	25	1	1	1	11	554	2E 2V	30
			12							14						

Nr. crt.	Discipline opţionale	Cod disciplina USV.FIESC.SC	Sem. 3 C	S	L	P	I*	Forma verificare	Nr. credite**	Sem. 4 C	S	L	P	I*	Forma verificare	Nr. credite**
10	SECURITATEA APLICAŢIILOR WEB	DS.03.10	1		2		83	E	5							
11	SECURITATEA SISTEMELOR CLIENT SERVER ŞI A BAZELOR DE DATE	DS.03.11														
	Total ore opţionale pe săptămână		1		2		83	1E	5							
			3													

	RECAPITULAŢIE		5.5	0.5	7	2	540	4E 2V	30	1	1	1	11	554	2E 2V	30
			15							14						

Nr. crt.	Discipline facultative	Cod disciplina	Sem. 3 C	S	L	P	I*	Forma verificare	Nr. credite**	Sem. 4 C	S	L	P	I*	Forma verificare	Nr. credite**
12	ANTREPRENORIAT	USV.FIESC.SC. DC.03.12	2	1			8	V	2							
13	Practică pedagogică (în învăţământul liceal, postliceal şi universitar)	USV.DSPP.NIV2. DS. 0301				3	83	C	5							
14	Sociologia educaţiei Managementul organizaţiei şcolare Politici educaţionale E-educaţie Educaţie interculturală	USV.DSPP.NIV 2. DC.0302	1	2			83	E	5							
	Total ore facultative pe săptămână		3	3		3	174	1E,1V, 1C	12							
			9													

NOTĂ: C/S/L/P - Numărul de ore de curs/seminar/laborator/proiect/ săptămânal pe parcursul semestrului
I* - ore de studiu individual pe semestru
** Practica se poate realiza cumulat la sfârşitul semestrelor, sau distribuită pe parcursul acestora.

Ordonator de credite,
Prof.univ.dr. ec. Gabriela PREDUT

Decan,
Prof.univ.dr.ing. L. Dan MILICI

Director departament,
Conf.univ.dr.ing. Eugen COCA

Responsabil program de studii,
Conf.univ.dr.ing. Alexandra Ligia BALAN

MINISTERUL EDUCAŢIEI ŞI CERCETĂRII
UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA

UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA
Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor

Aprobat
Şedinţa Senatului
din data 04.06.2026

PLAN DE ÎNVĂŢĂMÂNT

Domeniul: Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
Program de studiu: Securitate Cibernetică (SC)
Ciclul de studii: masterat profesional
Forma de învăţământ: ÎF
Durata studiilor: 2 ani
Valabil începând cu anul I, anul universitar: 2026- 2027

Structura anului universitar	Nr. săptămâni		Nr.ore practică		Nr.ore fizice	
Anul de studii	Sem. I	Sem. II	Sem. I	Sem. II	Sem. I	Sem. II
I	14	14	56	56	14	14
II	14	14	14		14	14

*Discipline obligatorii + opţionale 784

BILANŢ

Nr. crt.	CATEGORIA DISCIPLINEI	Total nr. ore	% realizat	% recom.
1	DISCIPLINE OBLIGATORII	686	89.23	
	Practică	126		
2	DISCIPLINE OPŢIONALE	98	10.77	
	TOTAL Obligatorii şi opţionale	**910**		
3	DISCIPLINE FACULTATIVE	294	24.42	
	TOTAL ore program de studiu	**1204**	**100.00**	

Nr. crt.	CATEGORIA DISCIPLINEI	Total nr. ore	Nr. de ore		
			Curs	Aplicaţii	
1	DISCIPLINE FUNDAMENTALE	294	168	126	
2	DISCIPLINE DE SPECIALIZARE	462	126	336	
3	DISCIPLINE COMPLEMENTARE	28	7	21	
	TOTAL	784	301	483	329

Număr ore aplicaţii/Număr ore curs	1.60
Număr ore studiu individual/Număr ore pregătire universitară	2.33

Nr. crt.	Forma de verificare	Nr. forme de verificare		Total	
		An I	An II	Nr.	%
1	Examen	8	6	14	63.64
2	Verificări	2	4	6	27.27
3	Colocviu	2		2	9.09
	TOTAL	12	10	22	100.00

Ordonator de credite,
Prof.univ.dr. ec. Gabriela PRELIPCEAN

Decan,
Prof.univ.dr.ing. L. Dan MILICI

Director departament,
Conf.univ.dr.ing. Eugen COCA

Responsabil program de studii,
Conf.univ.dr.ing. Alexandra Ligia BALAN

MINISTERUL EDUCAŢIEI ŞI CERCETĂRII
UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA

Aprobat
Ședința Senatului
din data 04.06.2026

UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA
Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor

PLAN DE ÎNVĂŢĂMÂNT

Domeniul: Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
Program de studiu: Securitate Cibernetică (SC)
Ciclul de studii: masterat profesional
Forma de învăţământ: ÎF
Durata studiilor: 2 ani
Valabil începând cu anul I, anul universitar: 2026- 2027

COMPETENŢE

Competenţe profesionale	
CP 1	Implementeaza gestionarea riscurilor în TIC
CP 2	Dezvolta strategia de securitate a informatiilor
CP 3	Efectueaza teste de securitate TIC
CP 4	Efectueaza audituri în TIC
CP 5	Gestionează securitatea sistemului
CP 6	Gestionează conformitatea cu standardele de securitate în TI
CP 7	Identifica riscurile la adresa securitatii TIC
CP 8	Defineşte politici de securitate
CP 9	Identifică punctele slabe ale sistemelor TIC
CP 10	Asigură securitatea informatiilor
CP 11	Efectuează analiza riscurilor
CP 12	Stabileşte un plan de securitate a TIC

Competenţe transversale	
CT 1	Lucrează în echipe
CT 2	Îşi asumă responsabilitatea
CT 3	Solutionează probleme

Ocupaţii conform COR ISCO 08:
252904 expert în securitate cibernetică
252905 expert în investigaţii digitale
252906 auditor de securitate cibernetică
252907 consultant de securitate cibernetică
252908 administrator de securitate în domeniul TIC

Ordonator de credite,	Decan,	Director departament,	Responsabil program de studii,
Prof.univ.dr. ec. Gabriela PRELIPCEAN	Prof.univ.dr.ing. L. Dan MILICI	Conf.univ.dr.ing. Eugen COCA	Conf.univ.dr. Alexandra Ligia BALAN

MINISTERUL EDUCAŢIEI ŞI CERCETĂRII
UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA

UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA
Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor
Domeniul: Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
Program de studiu: Securitate Cibernetică (SC)
Ciclul de studii: masterat profesional
Forma de învăţământ: ÎF
Durata studiilor: 2 ani
Valabil începând cu anul I, anul universitar: 2026- 2027

Aprobat
Şedinţa Senatului
din data 04.06.2026

Grila competenţelor

Repartizarea pe discipline a creditelor acumulate în funcţie de creditele alocate pentru fiecare dintre competenţele atribuite

Nr. Crt.	Denumire disciplină	Denumire competenţe															
		CP 1	CP 2	CP 3	CP 4	CP 5	CP 6	CP 7	CP 8	CP 9	CP 10	CP 11	CP 12	CT 1	CT 2	CT 3	Total credite
		Implementeaza gestionarea riscurilor în TIC	Dezvolta strategia de securitate a informatiilor	Efectueaza teste de securitate TIC	Efectueaza audituri în TIC	Gestionează securitatea sistemului	Gestionează conformitatea cu standardele de securitate în TI	Identifica riscurile la adresa securitatii TIC	Defineşte politici de securitate	Identifică punctele slabe ale sistemelor TIC	Asigură securitatea informatiilor	Efectuează analiza riscurilor	Stabileşte un plan de securitate a TIC	Lucrează în echipe	Îşi asumă responsabilitatea	Soluţionează probleme	
	AN I																
1	NOŢIUNI AVANSATE DE COMUNICAŢII SI REŢELE DE CALCULATOARE	2	1			1		1									5
2	MODELAREA ŞI FUNCŢIONAREA SISTEMELOR WIRELESS	1	1					1		1						1	5
3	CRIPTOGRAFIA		1	1		1					1	1					5
4	MANAGEMENTUL PROIECTELOR ŞI PROBLEMELOR COMPLEXE		1										1	1	1	1	5
5	PRACTICĂ PROFESIONALĂ I			1		0.5	1						1	1	0.5	1	6
6	SECURITATEA CRIPTOGRAFICA A SISTEMELOR ŞI A REŢELELOR DE COMUNICAŢII	1					1	1	1			1					5
7	COMUNICAŢII MOBILE ŞI PRIN SATELIT ŞI SECURITATEA LOR			1		1				1	1	1					5
8	ATACURI CIBERNETICE ŞI PROTECŢIE CIBERNETICĂ			1	1			1			1		1				5
9	CREATIVITATE ŞTIINŢIFICĂ, COMUNICARE TEHNICĂ ŞI INOVARE		1										1	0.5	1	0.5	4
10	PRACTICĂ PROFESIONALĂ II			1					1			0.5	1	1	0.5	1	6
11	REŢELE DE SENZORI ŞI AD-HOC	1	1			1		1									4
12	NANOTEHNOLOGII ÎN ELECTRONICĂ ŞI COMUNICAŢII																
13	TEHNOLOGII WEB AVANSATE ŞI ARHITECTURI ORIENTATE PE SERVICII	1	1			1		1		1							5
14	INGINERIE SOFTWARE AVANSATĂ																
	AN II																
1	SECURITATEA SISTEMELOR CLOUD ŞI GRID	1				1	1		1		1						5
2	MANAGEMENTUL ŞI AUDITAREA SECURITĂŢII SISTEMELOR INFORMATICE ŞI DE COMUNICAŢII				2				2			1					5
3	COMUNICAŢII OPTICE ŞI SECURITATEA LOR			1		1	1			1	1						5
4	ETICĂ ŞI INTEGRITATE ACADEMICĂ														2		2
5	PRACTICĂ ÎN POLIGON DE SECURITATE CIBERNETICĂ			2				2		1		1		1	0.5	0.5	8
6	SISTEME IoT SECURIZATE PRIN TEHNICI DE INTELIGENŢĂ ARTIFICIALĂ ŞI ÎNVĂŢARE AUTOMATĂ						1	1		1	1	1					5
7	PROTECŢIA DATELOR PERSONALE ŞI LEGISLAŢIE ÎN DOMENIUL SECURITĂŢII CIBERNETICE				2				1								3
8	CERCETARE PENTRU ELABORAREA DISERTAŢIEI		1			1	2			1	1	1	2	1	1	1	12
9	ELABORARE DISERTAŢIE				1				1	1	1	1	2	1	1	1	10
10	SECURITATEA APLICAŢIILOR WEB	1								1	1	1	1				5
11	SECURITATEA SISTEMELOR CLIENT SERVER ŞI A BAZELOR DE DATE																
	TOTAL CREDITE	8	8	8	6	8.5	7	9	7	9	9	9.5	10	6.5	7.5	7	120

Ordonator de credite,
Prof.univ.dr. ec. Gabriela PRELIPCEAN

Decan,
Prof.univ.dr.ing. L. Dan MILICI

Director departament,
Conf.univ.dr.ing. Eugen COCA

Responsabil program de studii,
Conf.univ.dr.ing. Alexandra Ligia BALAN

UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA
Facultatea de Inginerie Electrică şi Ştiinţa Calculatoarelor
Domeniul: Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
Program de studiu: Securitate Cibernetică (SC)
Ciclul de studii: masterat profesional
Forma de învăţământ: IF
Durata studiilor: 2 ani
Valabil începând cu anul I, anul universitar: 2026- 2027

Aprobat
Şedinţa Senatului
din data 04.06.2026

Grila rezultatelor învăţării

Nr. crt.	REZULTATELE ÎNVĂŢĂRII			Discipline care contribuie la obţinerea rezultatelor învăţării
	Cunoştinţe	Aptitudini	Responsabilitate şi autonomie	
CP1	**Implementeaza gestionarea riscurilor în TIC**			
	Descriere competenţă: Dezvolta si implementeaza proceduri pentru identificarea, evaluarea, tratarea si atenuarea riscurilor TIC, cum ar fi accesul neautorizat sau scurgerile de date, în conformitate cu strategia, procedurile si politicile de risc ale societatii. Analizeaza si gestioneaza riscurile si incidentele de securitate. Recomanda masuri de îmbunatatire a strategiei de securitate digitala.			
	Studentul/absolventul: a) **identifică** ameninţările şi vulnerabilităţile din infrastructura TIC, pe baza analizelor de securitate. b) **evaluează** riscurile cibernetice, utilizând metode calitative şi cantitative de analiză. c) **cunoaşte** instrumente software pentru managementul riscurilor.	Studentul/absolventul: a) **stabileşte** măsuri de control al riscurilor, în funcţie de nivelul de ameninţare şi impact. b) **elaborează** planuri de tratare şi atenuare a riscurilor, conform standardelor ISO/IEC relevante. c) **implementează** măsuri de securitate pentru reducerea riscurilor, atât la nivel tehnic cât şi organizaţional. d) **propune** măsuri eficiente de control şi tratament al riscurilor.	Studentul/absolventul: a) **monitorizează şi actualizează** periodic riscurile şi măsurile aplicate, în funcţie de evoluţia ameninţărilor. b) **documentează şi comunică** riscurile şi soluţiile adoptate, în cadrul unei organizaţii.	NOŢIUNI AVANSATE DE COMUNICAŢII SI REŢELE DE CALCULATOARE, MODELAREA ŞI FUNCŢIONAREA SISTEMELOR WIRELESS, SECURITATEA CRIPTOGRAFICA A SISTEMELOR ŞI A REŢELELOR DE COMUNICAŢII, REŢELE DE SENZORI ŞI AD-HOC/NANOTEHNOLOGII ÎN ELECTRONICĂ ŞI COMUNICAŢII, TEHNOLOGII WEB AVANSATE ŞI ARHITECTURI ORIENTATE PE SERVICII/INGINERIE SOFTWARE AVANSATĂ, SECURITATEA SISTEMELOR CLOUD ŞI GRID, SECURITATEA APLICAŢIILOR WEB/SECURITATEA SISTEMELOR CLIENT SERVER ŞI A BAZELOR DE DATE
CP2	**Dezvolta strategia de securitate a informatiilor**			
	Descriere competenţă: Creeaza strategia întreprinderii legata de siguranta si securitatea informatiilor, pentru a maximiza integritatea informatiilor, disponibilitatea si confidentialitatea datelor.			
	Studentul/absolventul: a) **analizează** cerinţele de securitate ale organizaţiei, în funcţie de natura activităţii şi infrastructura TIC. b) **evaluează** nivelul actual de protecţie a informaţiilor, pe baza auditului de securitate.	Studentul/absolventul: a) **stabileşte** obiectivele strategice de securitate a informaţiilor, aliniate la viziunea şi politicile organizaţiei. b) **analizează şi corelează** date privind nivelul de securitate. c) **elaborează** planul strategic de securitate a informaţiilor, conform standardelor internaţionale d) **integrează** politicile de protecţie a datelor şi gestionarea riscurilor în strategia generală, respectând reglementările în vigoare.	Studentul/absolventul: a) **propune** resursele necesare (tehnice, umane, financiare) pentru implementarea strategiei. b) **monitorizează şi evaluează** implementarea strategiei, ajustând obiectivele în funcţie de evoluţia riscurilor şi ameninţărilor.	NOŢIUNI AVANSATE DE COMUNICAŢII SI REŢELE DE CALCULATOARE, MODELAREA ŞI FUNCŢIONAREA SISTEMELOR WIRELESS, CRIPTOGRAFIA, MANAGEMENTUL PROIECTELOR ŞI PROBLEMELOR COMPLEXE, CREATIVITATE ŞTIINŢIFICĂ, COMUNICARE TEHNICĂ ŞI INOVARE, REŢELE DE SENZORI ŞI AD-HOC/NANOTEHNOLOGII ÎN ELECTRONICĂ ŞI COMUNICAŢII, TEHNOLOGII WEB AVANSATE ŞI ARHITECTURI ORIENTATE PE SERVICII/INGINERIE SOFTWARE AVANSATĂ, CERCETARE PENTRU ELABORAREA DISERTAŢIEI,
CP3	**Efectueaza teste de securitate TIC**			
	Descriere competenţă: Executa anumite tipuri de teste de securitate, cum ar fi testele de penetrare a retelei, testarea fara fir, evaluarile codurilor, evaluarile de tip wireless si/sau firewall, în conformitate cu metodele si protocoalele acceptate la nivel de industrie pentru a identifica si a analiza eventuale vulnerabilitati.			
	Studentul/absolventul: a) **stabileşte** obiectivele testelor de securitate, în funcţie de infrastructura şi nevoile organizaţiei. b) **selectează** tipul de test adecvat (vulnerabilitate, penetrare, audit) pentru fiecare componentă TIC.	Studentul/absolventul: a) **configurează** mediul de testare şi defineşte parametrii tehnici de execuţie. b) **utilizează** instrumente specializate de testare. c) **efectuează** teste de securitate asupra sistemelor, reţelelor şi aplicaţiilor, documentând fiecare pas.	Studentul/absolventul: a) **evaluează** rezultatele testelor, identificând vulnerabilităţile şi nivelul de risc asociat. b) **propune** măsuri de remediere, respectând bunele practici de securitate TIC. c) **respectă** cadrul legal şi etic al testării, asigurând confidenţialitatea şi integritatea datelor.	CRIPTOGRAFIA, PRACTICĂ PROFESIONALĂ I, COMUNICAŢII MOBILE ŞI PRIN SATELIT ŞI SECURITATEA LOR, ATACURI CIBERNETICE ŞI PROTECŢIE CIBERNETICĂ, PRACTICĂ PROFESIONALĂ II, COMUNICAŢII OPTICE ŞI SECURITATEA LOR, PRACTICĂ ÎN POLIGON DE SECURITATE CIBERNETICĂ
CP4	**Efectueaza audituri în TIC**			
	Descriere competenţă: Organizeaza si efectueaza audituri în vederea evaluarii sistemelor TIC, a conformitatii componentelor sistemelor, a sistemelor informatice de prelucrare a informatiilor si a securitatii informatiilor. Identifica si colecteaza eventualele probleme critice si recomanda solutii bazate pe standardele si solutiile necesare.			
	Studentul/absolventul: a) **identifică** obiectivele auditului TIC, în funcţie de contextul organizaţional şi cerinţele de conformitate.	Studentul/absolventul: a) **planifică** activităţile de audit, stabilind domeniul, criteriile şi metodologia utilizată. b) **colectează şi analizează** informaţii relevante, prin interviuri, observaţii, examinarea documentelor şi testarea controalelor. c) **evaluează** conformitatea sistemelor TIC cu politicile interne, standardele şi reglementările legale. d) **identifică** abaterile, neconformităţile şi riscurile asociate, în urma auditului efectuat.	Studentul/absolventul: a) **formulează** recomandări pentru îmbunătăţirea securităţii şi eficienţei sistemelor TIC. b) **întocmeşte şi prezintă** raportul de audit, într-un format clar şi profesionist, destinat factorilor de decizie.	ATACURI CIBERNETICE ŞI PROTECŢIE CIBERNETICĂ, MANAGEMENTUL ŞI AUDITAREA SECURITĂŢII SISTEMELOR INFORMATICE ŞI DE COMUNICAŢII, PROTECŢIA DATELOR PERSONALE ŞI LEGISLAŢIE ÎN DOMENIUL SECURITĂŢII CIBERNETICE, ELABORARE DISERTAŢIE
CP5	**Gestionează securitatea sistemului**			
	Descriere competenţă: Analizeaza activele critice ale unei întreprinderi si identifica punctele slabe si vulnerabilitatile care au condus la intruziune sau atac. Aplică tehnici de detectare pentru securitate. Înţelege tehnicile de atac cibernetic si pune în aplicare contramasuri eficiente.			
	Studentul/absolventul: a) **evaluează** nivelul de securitate al sistemelor informatice, prin monitorizarea continuă a evenimentelor şi jurnalelor de sistem.	Studentul/absolventul: a) **implementează** politici şi proceduri de securitate, în conformitate cu standardele şi reglementările în vigoare. b) **configurează şi administrează** mecanisme de control al accesului, autentificare, autorizare şi criptare. c) **aplică** măsuri proactive de prevenire a incidentelor de securitate, inclusiv actualizări, patch-uri şi reguli firewall. d) **monitorizează** performanţa şi integritatea sistemelor, utilizând instrumente specializate. e) **gestionează** incidentele de securitate, prin detectare, izolare, analiză şi remediere.	Studentul/absolventul: a) **asigură** continuitatea activităţii şi recuperarea în caz de dezastru, prin implementarea de soluţii de backup şi redundanţă. b) **comunică** eficient riscurile şi măsurile de securitate, către utilizatori şi echipa IT.	NOŢIUNI AVANSATE DE COMUNICAŢII SI REŢELE DE CALCULATOARE, CRIPTOGRAFIA, PRACTICĂ PROFESIONALĂ I, COMUNICAŢII MOBILE ŞI PRIN SATELIT ŞI SECURITATEA LOR, REŢELE DE SENZORI ŞI AD-HOC/NANOTEHNOLOGII ÎN ELECTRONICĂ ŞI COMUNICAŢII, TEHNOLOGII WEB AVANSATE ŞI ARHITECTURI ORIENTATE PE SERVICII/INGINERIE SOFTWARE AVANSATĂ, SECURITATEA SISTEMELOR CLOUD ŞI GRID, COMUNICAŢII OPTICE ŞI SECURITATEA LOR, CERCETARE PENTRU ELABORAREA DISERTAŢIEI
CP6	**Gestionează conformitatea cu standardele de securitate în TI**			
	Descriere competenţă: Îndrumă punerea în aplicare şi îndeplinirea standardelor, a celor mai bune practici şi a cerinţelor legale în materie de securitate a informatiilor relevante la nivelul industriei.			
	Studentul/absolventul: a) **identifică** cerinţele de conformitate specifice domeniului TI, în baza legislaţiei şi reglementărilor aplicabile. b) **analizează** standardele relevante de securitate a informaţiilor	Studentul/absolventul: a) **evaluează** nivelul de conformitate al sistemelor şi proceselor TI faţă de standardele şi politicile interne. b) **elaborează** planuri de acţiune pentru corectarea neconformităţilor identificate.	Studentul/absolventul: a) **colaborează** cu echipele tehnice şi juridice pentru asigurarea respectării normelor în vigoare. b) **monitorizează** periodic respectarea cerinţelor de conformitate şi actualizează documentaţia corespunzătoare. c) **informează** factorii de decizie şi personalul privind responsabilităţile de conformitate şi riscurile asociate nerespectării.	PRACTICĂ PROFESIONALĂ I, SECURITATEA CRIPTOGRAFICA A SISTEMELOR ŞI A REŢELELOR DE COMUNICAŢII, SECURITATEA SISTEMELOR CLOUD ŞI GRID, COMUNICAŢII OPTICE ŞI SECURITATEA LOR, SISTEME IoT SECURIZATE PRIN TEHNICI DE INTELIGENŢĂ ARTIFICIALĂ ŞI ÎNVĂŢARE AUTOMATĂ, CERCETARE PENTRU ELABORAREA DISERTAŢIEI
CP7	**Identifica riscurile la adresa securitatii TIC**			
	Descriere competenţă: Aplica metode si tehnici de identificare a eventualelor amenintari la adresa securitatii, a breselor de securitate si a factorilor de risc prin utilizarea de instrumentele TIC pentru supravegherea sistemelor TIC, analizarea riscurilor, a vulnerabilitatilor si a amenintarilor si evaluarea planurilor de urgenta.			
	Studentul/absolventul: a) **recunoaşte** ameninţările şi vulnerabilităţile în infrastructura TIC. b) **clasifică** tipurile de riscuri (tehnice, organizaţionale, umane, externe). c) **analizează** impactul potenţial al riscurilor asupra confidenţialităţii, integrităţii şi disponibilităţii datelor	Studentul/absolventul: a) **evaluează** probabilitatea şi severitatea riscurilor. b) **elaborează** rapoarte de analiză a riscurilor. c) **utilizează** metode şi instrumente de identificare a riscurilor	Studentul/absolventul: a) **recomandă** măsuri preliminare de prevenire şi reducere a riscurilor.	NOŢIUNI AVANSATE DE COMUNICAŢII SI REŢELE DE CALCULATOARE, MODELAREA ŞI FUNCŢIONAREA SISTEMELOR WIRELESS, SECURITATEA CRIPTOGRAFICA A SISTEMELOR ŞI A REŢELELOR DE COMUNICAŢII, ATACURI CIBERNETICE ŞI PROTECŢIE CIBERNETICĂ,REŢELE DE SENZORI ŞI AD-HOC/NANOTEHNOLOGII ÎN ELECTRONICĂ ŞI COMUNICAŢII, TEHNOLOGII WEB AVANSATE ŞI ARHITECTURI ORIENTATE PE SERVICII/INGINERIE SOFTWARE AVANSATĂ, PRACTICĂ ÎN POLIGON DE SECURITATE CIBERNETICĂ, SISTEME IoT SECURIZATE PRIN TEHNICI DE INTELIGENŢĂ ARTIFICIALĂ ŞI ÎNVĂŢARE AUTOMATĂ,

CP8	**Defineşte politici de securitate**			
	Descriere competenţă: Concepe şi executa un set de norme şi politici scrise care au scopul de a asigura o organizare în ceea ce priveste constrângerile legate de comportamentul partilor interesate, constrângerile mecanice de protectie si constrângerile legate de accesul la date.			
	Studentul/absolventul: a) **Identifică** cerinţele părţilor interesate privind securitatea informaţiilor.	Studentul/absolventul: a) **elaborează** politici de securitate care reglementează protecţia resurselor TIC. b) **integrează** standarde şi bune practici în conţinutul politicilor de securitate c) **monitorizează** respectarea politicilor şi propune îmbunătăţiri	Studentul/absolventul: a) **colaborează** cu părţile interesate pentru validarea politicilor. b) **documentează** şi comunică politicile în mod clar şi accesibil. c) **evaluează** eficienţa politicilor şi le actualizează periodic.	SECURITATEA CRIPTOGRAFICA A SISTEMELOR ŞI A REŢELELOR DE COMUNICAŢII, PRACTICĂ PROFESIONALĂ II, SECURITATEA SISTEMELOR CLOUD ŞI GRID, MANAGEMENTUL ŞI AUDITAREA SECURITĂŢII SISTEMELOR INFORMATICE ŞI DE COMUNICAŢII, PROTECŢIA DATELOR PERSONALE ŞI LEGISLAŢIE ÎN DOMENIUL SECURITĂŢII CIBERNETICE, ELABORARE DISERTAŢIE
CP9	**Identifică punctele slabe ale sistemelor TIC**			
	Descriere competenţă: Analizeaza sistemul si arhitectura retelei, componentele hardware si software, precum si datele pentru a identifica punctele slabe si vulnerabilitatile la intruziuni sau atacuri. Efectueaza operatiuni de diagnosticare privind infrastructura cibernetica, inclusiv cercetarea, identificarea, interpretarea si clasificarea vulnerabilitatilor, a atacurilor asociate si a codului daunator (de exemplu, pentru activitati specifice analizei criminalistice malware si activitati rau-intentionate în retea). Compara indicatorii sau elementele observabile cu cerintele si revizuieste jurnalele pentru a identifica dovezi ale unor intruziuni din trecut.			
	Studentul/absolventul: a) **recunoaşte** componentele şi arhitectura sistemelor TIC pentru a înţelege posibilele surse de vulnerabilităţi. b) **analizează** configurările reţelelor şi sistemelor pentru a identifica deficienţele de securitate.	Studentul/absolventul: a) **utilizează** instrumente specifice (scanere de vulnerabilităţi, analizatoare de trafic etc.) pentru a detecta punctele slabe. b) **evaluează** impactul potenţial al vulnerabilităţilor identificate asupra confidenţialităţii, integrităţii şi disponibilităţii datelor. c) **evaluează** severitatea unei vulnerabilităţi şi recomandă măsuri corective	Studentul/absolventul: a) **redactează** rapoarte tehnice privind vulnerabilităţile identificate şi recomandările aferente b) **comunică** eficient rezultatele analizei echipelor tehnice sau factorilor decidenţi	MODELAREA ŞI FUNCŢIONAREA SISTEMELOR WIRELESS, COMUNICAŢII MOBILE ŞI PRIN SATELIT ŞI SECURITATEA LOR, TEHNOLOGII WEB AVANSATE ŞI ARHITECTURI ORIENTATE PE SERVICII/INGINERIE SOFTWARE AVANSATĂ, COMUNICAŢII OPTICE ŞI SECURITATEA LOR, PRACTICĂ ÎN POLIGON DE SECURITATE CIBERNETICĂ,SISTEME IoT SECURIZATE PRIN TEHNICI DE INTELIGENŢĂ ARTIFICIALĂ ŞI ÎNVĂŢARE AUTOMATĂ, CERCETARE PENTRU ELABORAREA DISERTAŢIEI, ELABORARE DISERTAŢIE, SECURITATEA APLICAŢIILOR WEB/SECURITATEA SISTEMELOR CLIENT SERVER ŞI A BAZELOR DE DATE
CP10	**Asigură securitatea informatiilor**			
	Descriere competenţă: Se asigura ca informatiile colectate în timpul supravegherii sau al investigatiilor ramân în mâinile persoanelor autorizate sa le primeasca si sa le utilizeze si ca acestea nu ajung la inamici sau în posesia persoanelor neautorizate.			
	Studentul/absolventul: a) **Identifică** tipurile de informaţii sensibile gestionate în cadrul organizaţiei pentru a stabili nivelurile de protecţie necesare. b) **evaluează** riscurile şi vulnerabilităţile asociate informaţiilor în scopul selectării măsurilor adecvate de securitate. c) **utilizează** instrumente software pentru protecţia datelor	Studentul/absolventul: a) **aplică** politici şi proceduri de securitate a informaţiilor pentru a preveni accesul neautorizat, modificarea sau pierderea datelor. b) **utilizează** metode de criptare, autentificare şi control al accesului pentru a proteja informaţiile în tranzit şi în repaus.	Studentul/absolventul: a) **monitorizează** incidentele de securitate şi comportamentele suspecte pentru a detecta şi limita rapid potenţialele breşe de securitate. b) **contribuie** la instruirea personalului privind securitatea informaţiilor pentru a reduce riscurile cauzate de erori umane.	CRIPTOGRAFIA, COMUNICAŢII MOBILE ŞI PRIN SATELIT ŞI SECURITATEA LOR, ATACURI CIBERNETICE ŞI PROTECŢIE CIBERNETICĂ, SECURITATEA SISTEMELOR CLOUD ŞI GRID, COMUNICAŢII OPTICE ŞI SECURITATEA LOR, SISTEME IoT SECURIZATE PRIN TEHNICI DE INTELIGENŢĂ ARTIFICIALĂ ŞI ÎNVĂŢARE AUTOMATĂ, CERCETARE PENTRU ELABORAREA DISERTAŢIEI, ELABORARE DISERTAŢIE, SECURITATEA APLICAŢIILOR WEB/SECURITATEA SISTEMELOR CLIENT SERVER ŞI A BAZELOR DE DATE
CP11	**Efectuează analiza riscurilor**			
	Descriere competenţă: Identifica si evalueaza factorii care pot pune în pericol succesul unui proiect sau ameninta functionarea organizatiei. Pune în aplicare proceduri prin care sa se evite sau sa se reduca la minimum impactul acestora.			
	Studentul/absolventul: a) **Identifică** activele informaţionale şi resursele TIC care necesită protecţie împotriva riscurilor. b) **recunoaşte** tipurile de ameninţări şi vulnerabilităţi asociate activelor analizate. c) **evaluează** probabilitatea şi impactul potenţial al riscurilor asupra organizaţiei.	Studentul/absolventul: a) **aplică** metode şi tehnici de analiză a riscurilor b) **prioritizează** riscurile în funcţie de gravitate şi propune măsuri de control. c) **utilizează** instrumente de analiză a riscurilor (softuri specializate, foi de calcul etc.) d) **construieşte** şi interpretează matrice de risc	Studentul/absolventul: a) **redactează** rapoarte de analiză a riscurilor, cu recomandări pentru managementul acestora.	CRIPTOGRAFIA, SECURITATEA CRIPTOGRAFICA A SISTEMELOR ŞI A REŢELELOR DE COMUNICAŢII, COMUNICAŢII MOBILE ŞI PRIN SATELIT ŞI SECURITATEA LOR, PRACTICĂ PROFESIONALĂ II, MANAGEMENTUL ŞI AUDITAREA SECURITĂŢII SISTEMELOR INFORMATICE ŞI DE COMUNICAŢII, PRACTICĂ ÎN POLIGON DE SECURITATE CIBERNETICĂ, SISTEME IoT SECURIZATE PRIN TEHNICI DE INTELIGENŢĂ ARTIFICIALĂ ŞI ÎNVĂŢARE AUTOMATĂ, CERCETARE PENTRU ELABORAREA DISERTAŢIEI, ELABORARE DISERTAŢIE, SECURITATEA APLICAŢIILOR WEB/SECURITATEA SISTEMELOR CLIENT SERVER ŞI A BAZELOR DE DATE
CP12	**Stabileşte un plan de securitate a TIC**			
	Descriere competenţă: Stabileste un set de masuri si responsabilitati pentru a asigura confidentialitatea, integritatea si disponibilitatea informatiilor. Pune în aplicare politici de prevenire a încalcarilor securitatii datelor, detecteaza si intervine în caz de acces neautorizat la sisteme si resurse, inclusiv actualizând aplicatii de securitate si contribuind la educatia angajatilor.			
	Studentul/absolventul: a) **Identifică** necesităţile de securitate ale organizaţiei. b) **evaluează** infrastructura TIC din punctul de vedere al riscurilor şi vulnerabilităţilor.	Studentul/absolventul: a) **stabileşte** obiective clare pentru protecţia informaţiilor şi sistemelor. b) **elaborează** politici şi proceduri de securitate adaptate contextului organizaţional. c) **corelează** măsurile de securitate cu riscurile identificate	Studentul/absolventul: a) **redactează** planul de securitate, incluzând măsuri tehnice, organizatorice şi responsabili. b) **planifică** implementarea şi monitorizarea măsurilor de securitate TIC. c) **revizuieşte** periodic planul pentru a-l adapta schimbărilor	MANAGEMENTUL PROIECTELOR ŞI PROBLEMELOR COMPLEXE, PRACTICĂ PROFESIONALĂ I, ATACURI CIBERNETICE ŞI PROTECŢIE CIBERNETICĂ, CREATIVITATE ŞTIINŢIFICĂ, COMUNICARE TEHNICĂ ŞI INOVARE, PRACTICĂ PROFESIONALĂ II, CERCETARE PENTRU ELABORAREA DISERTAŢIEI ELABORARE DISERTAŢIE, SECURITATEA APLICAŢIILOR WEB/SECURITATEA SISTEMELOR CLIENT SERVER ŞI A BAZELOR DE DATE
CT1	**Lucrează în echipe**			
	Descriere competenţă: Lucreaza cu încredere în cadrul unui grup, fiecare facându-si partea lui în serviciul întregului.			
	Studentul/absolventul: a) Participă activ la activităţile de echipă, contribuind cu idei şi soluţii pentru atingerea obiectivelor comune.	Studentul/absolventul: a) Colaborează şi împărtăşeşte responsabilităţile în mod echitabil, respectând rolurile stabilite în echipă.	Studentul/absolventul: a) Demonstrează flexibilitate şi adaptabilitate în relaţia cu ceilalţi membri ai echipei, acceptând schimbările şi ajustările necesare.	MANAGEMENTUL PROIECTELOR ŞI PROBLEMELOR COMPLEXE, PRACTICĂ PROFESIONALĂ I, CREATIVITATE ŞTIINŢIFICĂ, COMUNICARE TEHNICĂ ŞI INOVARE, PRACTICĂ PROFESIONALĂ II, PRACTICĂ ÎN POLIGON DE SECURITATE CIBERNETICĂ, CERCETARE PENTRU ELABORAREA DISERTAŢIEI, ELABORARE DISERTAŢIE
CT2	**Îşi asumă responsabilitatea**			
	Descriere competenţă: Identifica si detecteaza diverse probleme si aspecte si ia decizii cu privire la cea mai buna cale de urmat. Raporteaza problemele în consecinta atunci când este necesar.			
	Studentul/absolventul: a) recunoaşte şi acceptă responsabilităţile proprii în cadrul activităţilor şi sarcinilor atribuite. b) respectă termenele şi standardele de calitate în realizarea atribuţiilor.	Studentul/absolventul: a) manifestă iniţiativă şi autonomie în îndeplinirea sarcinilor, fără a aştepta permanent instrucţiuni. b) răspunde pentru propriile acţiuni şi decizii, inclusiv pentru eventualele greşeli, şi caută soluţii pentru corectarea lor.	Studentul/absolventul: a) solicită ajutor sau clarificări atunci când este necesar, pentru a-şi îndeplini responsabilităţile în mod corect. b) contribuie la crearea unui mediu de încredere şi responsabilitate în echipă, respectând angajamentele asumate.	MANAGEMENTUL PROIECTELOR ŞI PROBLEMELOR COMPLEXE , PRACTICĂ PROFESIONALĂ I, CREATIVITATE ŞTIINŢIFICĂ, COMUNICARE TEHNICĂ ŞI INOVARE, PRACTICĂ PROFESIONALĂ II, ETICĂ ŞI INTEGRITATE ACADEMICĂ, PRACTICĂ ÎN POLIGON DE SECURITATE CIBERNETICĂ, CERCETARE PENTRU ELABORAREA DISERTAŢIEI, ELABORARE DISERTAŢIE
CT3	**Solutionează probleme**			
	Descriere competenţă: Găseşte solutii la probleme practice, operationale sau conceptuale într-o gama larga de contexte.			
	Studentul/absolventul: a) analizează corect problema identificată, evaluând cauzele şi implicaţiile acesteia. b) alege soluţia optimă în funcţie de resursele disponibile, impactul şi fezabilitatea acesteia.	Studentul/absolventul: a) aplică soluţia aleasă în mod organizat şi responsabil. b) monitorizează şi evaluează rezultatele aplicării soluţiei, ajustând acţiunile dacă este necesar.	Studentul/absolventul: a) colaborează cu echipa în procesul de rezolvare a problemelor, comunicând clar şi eficient pe parcurs.	MODELAREA ŞI FUNCŢIONAREA SISTEMELOR WIRELESS, MANAGEMENTUL PROIECTELOR ŞI PROBLEMELOR COMPLEXE, PRACTICĂ PROFESIONALĂ I, CREATIVITATE ŞTIINŢIFICĂ, COMUNICARE TEHNICĂ ŞI INOVARE, PRACTICĂ PROFESIONALĂ II, PRACTICĂ ÎN POLIGON DE SECURITATE CIBERNETICĂ, CERCETARE PENTRU ELABORAREA DISERTAŢIEI, ELABORARE DISERTAŢIE

Ordonator de credite,
Prof.univ.dr. ec. Gabriela PRELIPCEAN

Decan,
Prof.univ.dr.ing. I. Dan MILICI

Director departament,
Conf.univ.dr.ing. Eugen COCA

Responsabil program de studii,
Conf.univ.dr.ing. Alexandra Ligia BALAN

MINISTERUL EDUCAŢIEI ŞI CERCETĂRII ŞTIINŢIFICE — UNIVERSITATEA „ŞTEFAN CEL MARE" DIN SUCEAVA

Aprobat
Şedinţa Senatului
din data de 04.06.2026