PLAN DE ÎNVĂȚĂMÂNT
al promoției 2025 - 2027

Universitatea Transilvania din Braşov

Programul de studii universitare de masterat	**Securitate Cibernetică (în limba engleză)**
Domeniul fundamental	**Ştiințe inginereşti**
Domeniul de masterat	**Inginerie electronică, telecomunicații și tehnologii informaționale**
Facultatea	**Facultatea de Inginerie electrică și știința calculatoarelor**
Durata studiilor:	**2 ANI**
Forma de învățământ:	**cu frecvență**

1. OBIECTIVE DE FORMARE ŞI COMPETENȚE

Obiectivul general al programului de masterat este de a dezvolta deprinderi şi competențe pentru o carieră profesională /de cercetare în interacțiunea ramurilor de știință și tehnologie de electronică, comunicații digitale, ingineria calculatoarelor și tehnologia informației. Totodată, se urmărește formarea de capabilități de a administra și a transforma contextul de studiu sau de lucru la cerințe noi, neprevizibile, care solicită abordări strategice noi în situația dinamică a tehnologiei în electronica programată, cu extensii și către comunicațiile digitale, urmărind să se respecte și cerințele EQF-Level 7 – Master.

Scopul masteratului este de a asigura deprinderi și competențe pentru o carieră profesională/de cercetare pentru proiectarea și implementarea securității cibernetice la nivel de organizație, local, național și regional. Pregătirea specialiștilor în securitate cibernetică va fi bazată pe prezentarea conceptelor de securitate cibernetică, infrastructuri critice, securitate informațională și pe dobândurea de abilități practice în ce privește determinarea amenințărilor, riscurilor și vulnerabilitățilr de securitate cibernetică și de gestionare rapidă și eficientă a sistemelor în cazul unor incidente de securitate.

Grupa de bază din COR/ISCO-08/ESCO reprezentativă a programului de studii Securitate Cibernetică este Cod ESCO 2529 - Specialisti în baze de date si retele neclasificati în grupele de bază anterioare. Ocupațiile cu care programul este înscris la RNCIS sunt: Cod COR: 252911/ Denumire cor: inginer în domeniul securitățtii TIC și Cod COR: 252904/ Denumire cor: expert în securitate cibernetică.

Evoluția societății umane către o societate informațională în care internetul și tehnologiile aferente, conectivitatea și impunerea Industry 4.0, atrage după sine nevoia de specialiști în acest domeniu.

Obiectivul general al programului de studii este pregătirea de cadre tehnice cu pregătire superioară în domeniul electronicii astfel încât să se asigure o formare complexă ce vizează competențe asociate cu rezultate ale învățării structurate pe trei dimensiuni: Cunoaștere, Aptitudini şi Responsabilitate și autonomie.

Activitățile/Sarcinile aferente profesiei de Inginer Electronist sunt următoarele:

(a) elaborarea de planuri pentru a proteja fișierele computerizate împotriva modificărilor, distrugerii sau dezvăluirii accidentale sau neautorizate și pentru a satisface nevoile de prelucrare a datelor de urgență;

(b) formarea utilizatorilor și promovarea conștientizării securității pentru a asigura securitatea sistemului și pentru a îmbunătăți eficiența serverului și a rețelei;

(c) discutarea cu utilizatorii pentru a discuta probleme precum nevoile de acces la date computerizate, încălcările securității și modificările de programare;

(d) monitorizarea rapoartelor curente privind virușii informatici pentru a determina când să actualizeze sistemele de protecție împotriva virușilor;

(e) modificarea fișierelor de securitate a computerului pentru a încorpora software-ul nou, corectarea erorilor sau modificarea statutului de acces individual;

(f) monitorizarea utilizării fișierelor de date și reglementarea accesului la informațiile de salvgardare din fișierele computerizate;

(g) efectuarea de evaluări de risc și efectuarea de teste ale sistemului de prelucrare a datelor pentru a asigura funcționarea activităților de prelucrare a datelor și a măsurilor de securitate;

(h) criptarea transmisiilor de date și construirea de firewall-uri pentru a ascunde informațiile confidențiale pe măsură ce acestea sunt transmise și pentru a evita transferurile digitale afectate.

Competențe profesionale

Absolventul

Nr. Comp.	Denumire competență	Tip RI	Rezultatele învățării (ce trebuie să știe sau să știe să facă)
1	Gestioneaza securitatea sistemului	Cunoștințe	R.Î.1.2. Enumeră tehnicile de atac cibernetic si pune în aplicare contramasuri eficiente
		Aptitudini	R.Î.1.3.Aplica tehnici de detectare pentru securitate
			R.Î.1.4. Analizeaza activele critice ale unei întreprinderi si identifica punctele slabe si vulnerabilitatile care au condus la intruziune sau atac
		Responsabilitate și autonomie	R.Î.1.5. Derulează procese din managementul proiectelor de securitate cibernetică, cu preluarea diferitelor roluri în echipă și descrierea clară și concisă, verbal și în scris, a rezultatelor.
2	Defineste politici de securitate	Cunoștințe	R.Î.2.1. Definește normele și politicile de acces la date
		Aptitudini	R.Î.2.2. Concepe si executa un set de norme si 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
		Responsabilitate și autonomie	R.Î.2.3. Derulează procese din managementul proiectelor de securitate cibernetică, cu preluarea diferitelor roluri în echipă și descrierea clară și concisă, verbal și în scris, a rezultatelor.
3	Implementeaza gestionarea riscurilor în TIC	Cunoștințe	R.Î.3.1. Identifică posibilitățile de micșorare a riscurilor de securitate cibernetică
		Aptitudini	R.Î.3.2. 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
			R.Î.3.3. Analizeaza si gestioneaza riscurile si incidentele de securitate
			R.Î.3.4. Recomanda masuri de îmbunatatire a strategiei de securitate digitala
		Responsabilitate și autonomie	R.Î.3.5. Are o comportare responsabilă, etică, în spiritul legii pentru a realiza proceduri pentru identificarea amenințărilor cibernetice
4	Efectueaza audituri în TIC	Cunoștințe	R.Î.4.1. Identifica si colecteaza eventualele probleme critice si recomanda solutii bazate pe standardele si solutiile necesare
		Aptitudini	R.Î.4.2. Organizeaza si efectueaza audituri în vederea evaluarii sistemelor TIC, a conformitatii componentelor sistemelor, a sistemelor informatice de prelucrare a informatiilor si a securitatii informatiilor
		Responsabilitate și autonomie	R.Î.4.3.Derulează procese din managementul proiectelor de securitate cibernetică, cu preluarea diferitelor roluri în echipă și descrierea clară și concisă, verbal și în scris, a rezultatelor
5	Gestioneaza conformitatea cu standardele de securitate în TI	Cunoștințe	R.Î. 5.1 Enumeră practicile, standardele și cerințele de securitate a informațiilor
		Aptitudini	R.Î. 5.2 Asigură punerea în aplicare a practicilor relevante, a standardelor și a cerințelor de securitate a informațiilor la nivelul industriei.
		Responsabilitate și autonomie	R.Î. 5.3 Arată spirit de inițiativă și acțiune pentru îndrumarea punerii în aplicare a măsurilor și cerințelor din domeniul securitățiiinformațiilor.
6	Protejeaza dispozitive TIC	Cunoștințe	R.Î.6.1. Identifică masurile de siguranta si securitate si tine seama în mod corespunzator de încredere si de viata privata
		Aptitudini	R.Î.6.2. Protejeaza dispozitive TIC si continutul digital si întelege riscurile si amenintarile din mediile digitale
			R.Î.6.3. Utilizeaza instrumente si metode care sa maximizeze securitatea dispozitivelor si informatiilor TIC prin controlul accesului, cum ar fi parolele, semnaturile digitale, biometria si sistemele de protectie precum firewall, antivirus, filtre spam

		Responsabilitate și autonomie	R.Î.6.4. Arată spirit de inițiativă și acțiune pentru actualizarea cunoștințelor profesionale din domeniul securității software și hardware, maximizând siguranța dispozitivelor informatice
7	**Raspunde la incidentele din cloud**	Cunoștințe	R.Î.8.1. Definește modul de funcționare a cloud-ului
		Aptitudini	R.Î.8.2. Remediaza problemele legate de cloud si stabileste modalitatile de restabilire a operatiunilor
			R.Î.8.3. Concepe si automatizeaza strategii de recuperare în caz de dezastru si evalueaza implementarea pentru punctele critice
		Responsabilitate și autonomie	R.Î.8.4. Arată spirit de inițiativă și acțiune pentru actualizarea cunoștințelor profesionale din domeniul securității software prin salvarea datelor în cloud, cu aspecte economice și de cultură organizațională.
8	**Gestioneaza conformitatea cu standardele de securitate în TI**	Cunoștințe	R.Î. 9.1 Enumeră practicile, standardele și cerințele de securitate a informațiilor
		Aptitudini	R.Î. 9.2 Asigură punerea în aplicare a practicilor relevante, a standardelor și a cerințelor de securitate a informațiilor la nivelul industriei.
		Responsabilitate și autonomie	R.Î. 9.3 Arată spirit de inițiativă și acțiune pentru îndrumarea punerii în aplicare a măsurilor și cerințelor din domeniul securitățiiinformațiilor.
9	**Realizeaza conservarea dispozitivelor digitale în scopuri criminalistice**	Cunoștințe	R.Î.10.1. Identifică moduri în care se conservă integritatea dispozitivelor și informației stocate pe acestea în vederea regăsirii lor și utilizarea în scop legal, ca probe
		Aptitudini	R.Î. 10.2. Concepe metode de conservare fizică a dispozitivelor informatice și de salvare a datelor, astfel ca acestea să poată fi păstrate și utilizate în scopuri criminalistice
		Responsabilitate și autonomie	R.Î. 10.3 Are o comportare responsabilă, etică, în spiritul legii pentru a realiza proceduri pentru conservarea informațiilor și dispozitivelor în scopul păstrării acestora în scopuri criminalistice
10	**Mentine planul pentru continuitatea operatiunilor**	Cunoștințe	R.Î. 11.1 Actualizează și aplică metodologia necesară unui sistem informatic să funcționeze în cazul unor evenimente neprevăzute.
		Aptitudini	R.Î.11.2. Actualizeaza metodologia care contine masuri de asigurare a faptului ca unitatile unei organizatii pot functiona în continuare în cazul unei game largi de evenimente neprevazute
		Responsabilitate și autonomie	R.Î.11.3. Derulează procese din managementul proiectelor de securitate cibernetică, cu preluarea diferitelor roluri în echipă și descrierea clară și concisă, verbal și în scris, a rezultatelor.

Competențe transversale

Absolventul

Nr. Comp.	Denumire competență	Rezultatele învățării (ce trebuie să știe sau să știe să facă)
11	**Soluționează probleme**	**R.Î.12.1.** Dezvoltă strategii pentru rezolvarea problemelor
		R.Î.12.2. Găsește soluții la probleme
		R.Î.12.3. Aplică diverse strategii pentru rezolvarea problemelor
12	**Demonstrează spirit antreprenorial**	**R.Î.13.1.** Analizează procese de afaceri pornind de la raportul cost/beneficiu al unui proiect pornind de la bugetul unei societăți de profil sau al unei întreprinderi proprii
		R.Î.13.2. Stabilește contribuția proceselor de lucru la obiectivele comerciale și planifică alocarea de resurse și măsuri investiționale și operaționale de mare productivitate

2. STRUCTURA PE SĂPTĂMÂNI A ANULUI UNIVERSITAR

Număr de semestre: 4 semestre.

Număr de credite pe semestru: 30 de credite

Număr de ore de activități didactice /săptămână: 26

Numărul de săptămâni:

	Activități didactice		Sesiuni de examene			Vacanțe		
	Sem. I	Sem. II	Iarnă	Vară	Restanțe	Iarnă	Primăvară	Vară
Anul I	14	14	3	4	2	3	1	10
Anul II	14	14	3	4	2	3	1	-

3. ASIGURAREA FLEXIBILIZĂRII INSTRUIRII. CONDIȚIONĂRI

Flexibilizarea programului de studii este asigurată prin discipline opționale şi discipline facultative.

Disciplinele opționale sunt propuse pentru semestrele 2-4, prin pachete de discipline de specialitate.

Prezentul Plan de învățământ cuprinde, pe lângă disciplinele obligatorii şi la alegere (opționale) şi discipline facultative.

4.CONDIȚII DE ÎNSCRIERE ÎN ANUL DE STUDII URMĂTOR. CONDIȚII DE PROMOVARE A UNUI AN DE STUDII

Înscrierea în anul următor este condiționată de întrunirea condițiilor de promovare cuprinse în Regulamentul privind activitatea profesională a studenților.

5. EXAMENUL DE DISERTAȚIE

Condițiile de susținere a examenului de disertație sunt prezentate în Metodologia de finalizare a studiilor, aprobată de Senatul Universității. Conform acestei metodologii, prezentarea la examenul de disertație este condiționată de promovarea tuturor disciplinelor prevăzute în planul de învățământ.

1 Perioada de întocmire a disertației: semestrele 3 – 4;
2 Perioada de finalizare a disertației: ultimele 3 săptămâni din anul terminal;
3. Perioada de susținere a examenului de disertație:
4. Numărul de credite pentru susținerea disertației: 10 credite.

6. DISCIPLINELE DE STUDII PE ANI

Ministerul Educației și Cercetării

Universitatea Transilvania din Brașov — Plan de învățământ valabil în an universitar 2025-2026

Facultatea de Inginerie electrică și știința calculatoarelor

Programul de studii universitare de masterat: **Securitate Cibernetică (în limba engleză)**

Domeniul fundamental: **Ştiinţe inginereşti**

Domeniul de masterat: **Inginerie electronică şi telecomunicaţii**

Durata studiilor: **2** ani

Forma de învățământ: **Cu frecvență**

ANUL I

Nr. crt.	Discipline cu criteriul: Obligatoriu	C_1**	C_2**	Semestrul I								Semestrul II							
				C	S	L	P	Pr	SI	V	Cr	C	S	L	P	Pr	SI	V	Cr
1	Fundamente de criptografie scenarii de aplicare	DS	DOB	2	0	2	0	0	94	E	5								
2	Securitatea cibernetică a sistemelor și serviciilor informatice	DS	DOB	2	0	2	1	0	80	E	5								
3	Gestionarea identității și accesului în spațiul virtual	DS	DOB	2	0	2	0	0	94	E	5								
4	Tipuri de atacuri și amenințări cibernetice	DS	DOB	1	0	1	0	0	92	E	4								
5	Etică și integritate academică	DC	DOB	1	0	0	0	0	106	C	4								
6	Practică I	DS	DOB	0	0	0	10	0	70	C	7								
7	Gestionarea incidentelor de securitate cibernetică	DS	DOB									1	0	1	1	0	78	E	4
8	Securitatea rețelelor și izolarea perimetrală	DS	DOB									2	0	2	0	0	94	E	5
9	Securitatea infrastructurilor critice	DS	DOB									1	0	1	0	0	92	E	4
10	Securitatea sistemelor de control industrial	DS	DOB									1	0	2	0	0	78	E	4
11	Gestionarea proceselor de afaceri	DS	DOB									1	0	0	0	0	76	C	3
12	Practică II	DS	DOB									0	0	0	10	0	40	C	6
Total				8	0	7	11	0	536	E: 4, C: 2, V: 0	30	6	0	6	11	0	458	E: 4, C: 2, V: 0	26
Total ore didactice pe săptămână				26								23							

Nr. crt.	Discipline cu criteriul: Optional	C_1**	C_2**	Semestrul I								Semestrul II							
				C	S	L	P	Pr	SI	V	Cr	C	S	L	P	Pr	SI	V	Cr
1	Tehnologii securizate de web și internet	DS	DOP									2	0	1	0	0	78	C	4
1	Securitate în programare și securitatea aplicațiilor	DS	DOP									2	0	1	0	0	78	C	4
Total				0	0	0	0	0	0	E: 0, C: 0, V: 0	0	2	0	1	0	0	78	E: 0, C: 1, V: 0	4

Total ore didactice pe săptămână	**0**	**3**

Legendă:

C_1^* = *criteriul conținutului*: **DF – Discipline fundamentale** **DS – discipline de specializare** **DC – discipline complementare**

C_2^{**} = *criteriul obligativității*: **DOB – discipline obligatorii (impuse)** **DOP–discipline opționale** **DFA–discipline facultative**

SI = ore de studiu individual

RECTOR,
PROF. DR. IOAN VASILE ABRUDAN

DECAN,
PROF. DR. TITUS CONSTANTIN BALAN

DIRECTOR DEPARTAMENT,
LECT. DR. AUREL CORNEL STANCA

COORDONATOR PROGRAM STUDII,
PROF. DR. TITUS CONSTANTIN BALAN

Ministerul Educației și Cercetării

Universitatea Transilvania din Brașov — Plan de învățământ valabil în an universitar 2026-2027

Facultatea de Inginerie electrică și știința calculatoarelor

Programul de studii universitare de masterat: **Securitate Cibernetică (în limba engleză)**

Domeniul fundamental: **Ştiinţe inginereşti**

Domeniul de masterat: **Inginerie electronică şi telecomunicaţii**

Durata studiilor: **2** ani

Forma de învățământ: **Cu frecvență**

ANUL II

Nr. crt.	Discipline cu criteriul: Obligatoriu	C_1**	C_2**	Semestrul I									Semestrul II								
				C	S	L	P	Pr	SI	V			Cr	C	S	L	P	Pr	SI	V			Cr
1	IT forensics	DS	DOB	1	0	1	0	0	92	E			4										
2	Tehnici de prelucrare a datelor și învățare automată aplicate în securitate cibernetică	DS	DOB	2	0	2	0	0	94	E			5										
3	Hacking etic si audit de securitate	DS	DOB	1	0	1	2	0	64	E			4										
4	Asigurarea informațională și managementul riscului	DS	DOB	1	0	0	1	0	92	C			4										
5	Practica 1 - Proiect imersiv de securitate ciberentica	DS	DOB	0	0	0	10	0	40	C			6										
6	Practică II	DS	DOB											0	0	0	10	0	160	C			10
7	Practica pentru elaborarea lucrarii de disertatie	DS	DOB											0	0	0	8	0	188	C			10
8	Elaborarea lucrarii de disertatie	DS	DOB											0	0	0	8	0	188	C			10
Total				5	0	4	13	0	382	E	C	V	23	0	0	0	26	0	536	E	C	V	30
										3	2	0								0	3	0	
Total ore didactice pe săptămână				22										26									

Nr. crt.	Discipline cu criteriul: Optional	C_1**	C_2**	Semestrul I									Semestrul II								
				C	S	L	P	Pr	SI	V			Cr	C	S	L	P	Pr	SI	V			Cr
1	Analiză malware	DS	DOP	1	0	1	0	0	92	E			4										
1	Securitatea cibernetică a dispozitivelor mobile	DS	DOP	1	0	1	0	0	92	E			4										
2	Protecția datelor și legislația privind securitatea	DS	DOP	1	1	0	0	0	62	C			3										
2	Arhitectura organizației și performanța afacerii	DS	DOP	1	1	0	0	0	62	C			3										
Total				2	1	1	0	0	154	E	C	V	7	0	0	0	0	0	0	E	C	V	0
										1	1	0								0	0	0	
Total ore didactice pe săptămână				4										0									

Nr.	Discipline cu criteriul:	C_1**	C_2**	Semestrul I	Semestrul II

crt.	Facultativ			C	S	L	P	Pr	SI	V			Cr	C	S	L	P	Pr	SI	V			Cr
1	Atacuri cibernetice si aparare cibernetica	DS	DFA	2	0	1	0	0	138	E			6										
2	Atacuri cibernetice si aparare cibernetica (în limba engleză)	DS	DFA	2	0	1	0	0	138	E			6										
Total				4	0	2	0	0	276	E	C	V	12	0	0	0	0	0	0	E	C	V	0
										2	0	0								0	0	0	
Total ore didactice pe săptămână				6										0									

Legendă:

C_1^* = *criteriul conținutului*: **DF** – Discipline fundamentale **DS** – discipline de specializare **DC** – discipline complementare

C_2^{**} = *criteriul obligativității*: **DOB** – discipline obligatorii (impuse) **DOP**–discipline opționale **DFA**–discipline facultative

SI = ore de studiu individual

RECTOR,
PROF. DR. IOAN VASILE ABRUDAN

DECAN,
PROF. DR. TITUS CONSTANTIN BALAN

DIRECTOR DEPARTAMENT,
LECT. DR. AUREL CORNEL STANCA

COORDONATOR PROGRAM STUDII,
PROF. DR. TITUS CONSTANTIN BALAN