

PLAN DE ÎNVĂȚĂMÂNT

începând cu anul universitar 2024-2025

Facultate:	Matematică și Informatică
Ciclul de studii universitare:	Masterat
Denumirea programului de studii universitare de masterat:	Cybersecurity
Denumirea calificării¹ dobândită în urma absolvirii programului de studii:	Specialist în Cybersecurity
Titlul acordat	Master în Informatică
Durata studiilor (în ani):	2 ani
Numărul de credite (ECTS):	120
Forma de învățământ²:	cu frecvență (IF)
Limba de predare:	engleză
Locația geografică de desfășurare a studiilor:	Timișoara
Încadrarea programului de studii în domenii de știință	
Domeniul fundamental:	Matematică și științe ale naturii
Ramura de știință:	Informatică
Domeniul de studii universitare de licență:	Informatică
Denumirea domeniului <u>larg</u> de studii (conform DL-ISCED F-2013):	Tehnologia informației și comunicațiilor (TIC)
Denumirea domeniului <u>restrâns</u> de studii (conform DR-ISCED F-2013):	Tehnologia informației și comunicațiilor (TIC)
Denumirea domeniului <u>detaaliat</u> de studii (conform DDS-ISCED F-2013):	Dezvoltare și analiză soft și aplicații

¹ *Calificarea (qualification)* este rezultatul formal al unui proces de evaluare și validare, care este obținut atunci când un organism/o autoritate competent/ă stabilește că o persoană a dobândit rezultate ale învățării corespunzătoare unor standarde prestabilite. Calificările dobândite de absolvenții programelor de studii din învățământul superior Învățământ cu frecvență (IF), învățământ cu frecvență redusă (IFR) sau învățământ la distanță (ID) sunt atestate prin diplome, prin certificate și prin alte acte de studii eliberate numai de către instituțiile de învățământ superior acreditate.

² Învățământ cu frecvență (IF), învățământ cu frecvență redusă (IFR) sau învățământ la distanță (ID)

PREZENTAREA GENERALĂ A PROGRAMULUI DE STUDII UNIVERSITARE

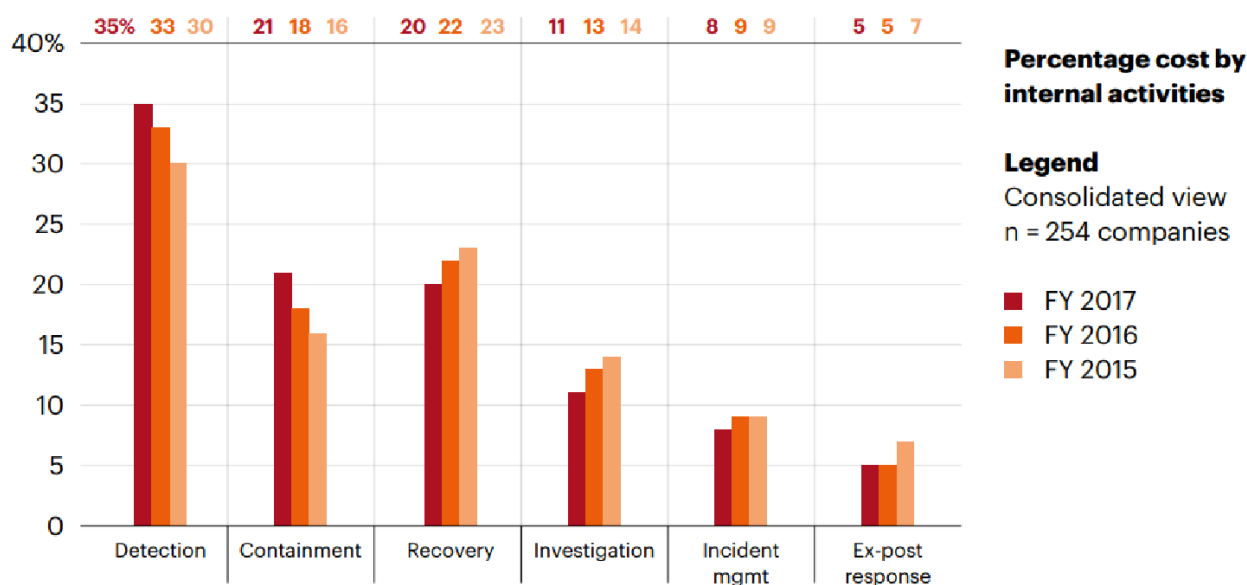
1. Misiunea programului de studii

Contextul mondial actual, alături de tendințele pieței IT și cererea pe această piață, impun coroborativ pregătirea accentuată a experților în Securitatea cibernetică. Situația la nivel global, crimele cibernetice în continuă creștere, nevoia de a pregăti și instrui personalul din mediul informațional în legătură cu modurile de a contracara amenințările de natură cibernetică, respectiv expunerea clară și concisă a metodelor de mitigare a atacurilor cibernetice, determină ca programul de studii de masterat *Cybersecurity* să își găsească locul într-un context bine definit și concis, cu o cotă și cerere de piață din ce în ce mai mari.

Programul de studii universitare de masterat *Cybersecurity* își propune să inoculeze noțiuni generice de securitate cibernetică, care să ajute familiarizarea studenților din cadrul ciclului de studii universitare de masterat cu conceptele fundamentale care definesc securitatea în mediul informațional, precum malware, atacuri cibernetice, exploatare „zero-day”, etc. Ulterior, setul de cunoștințe continuă cu expunerea gestiunii amenințărilor cibernetice asociate celor mai comune zone ale pieței IT unde securitatea cibernetică are un impact major, nu doar din punct de vedere financiar, dar și din punctul de vedere al infrastructurii asociate: în mediul privat, în medii virtualizate/cloud, respectiv în mediul academic.

Consecințele unui astfel de impact sunt imediat vizibile și în mediul de afaceri. Anul 2017 a adus un impact economic al securității cibernetice semnificativ mai mare, cu 23%, din punct de vedere financiar față de 2016³. Aspectele esențiale de securitate din acest context, cum ar fi detecția, izolarea, recuperarea și investigarea au avut toate de suferit, însă tendințele variază și devin îngrijorătoare: aplicațiile de tip malware încă domină tipul atacurilor cibernetice de astăzi, iar aplicațiile de tip ransomware s-au dublat ca și număr pe parcursul a doar un an de zile, ceea ce demonstrează că securitatea devine nu doar importantă, ci și imperativ necesară pentru protecția datelor cu caracter personal și pentru evitarea costurilor semnificative ca rezultat al breșelor de securitate.

³ https://www.accenture.com/t20170926T072837Z_w_us-en/acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf (retrieved 16th of November, 2017)



Consecințele unui astfel de impact sunt imediat vizibile și în mediul de afaceri. Într-un studiu realizat de Accenture, în noiembrie 2021, spre exemplu, comparativ cu ianuarie 2020, numărul mediu de atacuri asupra companiilor a crescut⁴ cu 31%, ceea ce a dus la o creștere a bugetelor alocate securității cibernetice în cazul a 82% dintre companiile afectate. Același studiu evidențiază costul mediu per incident de securitate cibernetică al unei firme ca fiind \$611,000 USD. În 2021, crimele cibernetice au crescut⁵ cu peste 600% comparativ cu 2020, o statistică alimentată și de pandemie, rezultând un cost mediu per breșă de date de \$4.24 milioane USD (față de \$2.5 milioane USD în anul precedent). Până în 2025, se estimează că, la nivel mondial, costul asociat crimelor cibernetice se va ridica la peste 10.5 mii de miliarde USD.

Numeroși factori afectează în 2023, la nivel global securitatea sistemelor de calcul, în special aceia susținuți de elementul geopolitic (e.g. conflictul dintre Rusia și Ucraina). Într-un raport publicat în noiembrie 2022 de către ENISA⁶, ținta predominantă a atacurilor cibernetice în perioada iunie-iulie 2022 au fost administrațiile publice și guvernele, cu o pondere dominantă de 24.21%, urmate de furnizorii de servicii digitale cu puțin peste 13%, adică aproape de două ori mai puține incidente. Același raport arată și că impactul economic asupra aceluiași administrații publice și guverne este de peste două ori mai puternic decât sectorul serviciilor.

În acest context, devine critică importanța conștientizării la nivel mondial a rolului vital pe care securitatea cibernetică, alături de toate ramurile sale, le are în ecosistemul global, puternic zguduit permanent de evenimente geopolitice și de atacuri cibernetice devastatoare, cu un recul puternic în industriile critice, precum sănătatea și finanțele.

⁴ https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

⁵ <https://purplesec.us/resources/cyber-security-statistics/>

⁶ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

2. Competențe și rezultate așteptate ale învățării formate în cadrul programului de studii

A. COMPETENȚE

Competențe-cheie:

- Competențe în domeniul științei, tehnologiei, ingineriei și matematicii;
- Competențe multilingvistice;
- Competențe de conștientizare și exprimare culturală;
- Competențe digitale;
- Competențe antreprenoriale.

Competențe profesionale:

- Capacitatea de a utiliza tehnologii recente din domeniul securității cibernetice;
- Capacitatea de a modela/proiecta/implementa politici și metode de securitate cibernetică în diverse domenii științifice și tehnice;
- Capacitatea de a propune, analiza, demonstra și dezvolta concepte și teorii inovatoare din sfera științifică și tehnică a securității cibernetice;
- Capacitatea de a configura, administra, întreține și monitoriza un sistem, o infrastructură sau un mediu virtual, din perspectiva securității cibernetice;
- Capacitatea de a identifica, optimiza și implementa metode specifice conceptelor și abordărilor curente din domeniul securității cibernetice.

Competențe transversale:

a) Competențe personale:

- Angajarea în sarcină;
- Asumarea responsabilităților;
- Capacitatea de identificare a tehnicilor de securitate noi;
- Capacitate de analiză și sinteză;
- Gândire critică și inovativă

b) Competențe interpersonale:

- Capacitatea de interacțiune și colaborare în echipă;
- Managementul echipelor și al conflictelor;
- Capacitatea de a vorbi în public.

c) Competențe de cetățenie globală:

- Solidaritate;
- Capacitate de înțelegere etnică și interculturală;
- Toleranță și respect pentru diversitate;
- Respect pentru valorile și legile naționale, dar și pentru cele europene/internaționale.

B. REZULTATE AȘTEPTATE ALE ÎNVĂȚĂRII

a) Cunoștințe:

- Metode de identificare și reprezentare a aspectelor de securitate cibernetică, de identificare a algoritmilor relevanți în securitatea cibernetică;
- Principii și metode de identificare, aplicare și mitigare a atacurilor cibernetice;
- Identificarea standardelor relevante în contextul securității cibernetice, aplicabile în mediul privat și/sau public;
- Principii de bază ale analizei, implementării și întreținerii de tehnici și metode software și hardware relevante în securitatea cibernetică;
- Identificarea, înțelegerea și utilizarea limbajelor esențiale în domeniul securității cibernetice;
- Standarde, metode și practici de asigurare a calității în contextul securității cibernetice (verificare și validare);
- Principiile proiectării și implementării de soluții relevante și eficiente de securitate cibernetică;
- Cunoștințe avansate de analiză statică, dinamică în contextul securității cibernetice;
- Cunoștințe avansate de tehnici de analiză și investigație în contextul securității cibernetice.

b) Abilități:

- Analiza, identificarea și utilizarea unor instrumente pentru asigurarea securității cibernetice;
- Implementarea de standarde și politici de securitate în contextul securității cibernetice, în mediile private și publice;
- Identificarea soluțiilor relevante din perspectiva securității cibernetice, în contextul tehnologiilor orientate spre servicii (cloud/edge/fog computing);
- Utilizarea unor instrumente de modelare și simulare, relevante pentru analiza, înțelegerea și inocularea conceptelor de securitate cibernetică;
- Analiza, proiectarea și documentarea soluțiilor de securitate cibernetică, în contextul aplicabil acestora, public sau privat;
- Identificarea, îmbunătățirea și documentarea tehnicilor de mitigare a atacurilor cibernetice.

c) Responsabilitate și autonomie:

- Respectarea confidențialității și protejarea proprietății intelectuale în relațiile cu colaboratorii;
- Respectarea confidențialității angajatorului și a clienților. Protejarea proprietății intelectuale a acestora;
- Păstrarea autonomiei, integrității și independenței în opiniile profesionale;
- Comportament etic, cinstit și colegial în practicarea profesiei;
- Perfecționarea continuă în domeniul de activitate;

- Reprezentarea corectă a nivelului de competență și acceptarea de sarcini în limitele acestuia;
- Responsabilitatea de a respecta cele mai înalte standarde profesionale în implementarea conceptelor studiate.

3. Ocupații care pot fi practicate pe piața muncii

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

4. Asigurarea traseelor flexibile de învățare în cadrul programului de studii

Flexibilizarea programului de studii este asigurată prin discipline opționale, discipline facultative și discipline complementare.

Disciplinele la alegere (opționale) sunt propuse pentru semestrele 1-3 și sunt grupate în **pachete opționale**, care completează traseul de specializare a studentului. Alegerea traseului se face de către student, înainte de începerea fiecărui an universitar.

Disciplinele facultative sunt propuse pentru semestrele 1-4 de către Facultatea de Matematică și Informatică (care gestionează programul de studii), dar pot fi alese și din pachetele oferite de alte facultăți ale UVT.

În conformitate cu prevederile *Regulamentului privind elaborarea planurilor de învățământ pentru programele de studii de la Universitatea de Vest din Timișoara*, pentru ca studenții să poată beneficia de **credite pentru activități de voluntariat** în baza prevederilor Legii învățământului superior nr. 199/2023, cu modificările și completările ulterioare (articolul 127, alineatul (9), disciplina Voluntariat este disponibilă în fiecare semestru în planurile de învățământ ale tuturor programelor de studii universitare de licență și de masterat, cu statut de disciplină facultativă, cu un număr de 2 credite ECTS.

5. Activitatea profesională și evaluarea studenților

Drepturile, obligațiile și condițiile desfășurării activității profesionale a studenților la Universitatea de Vest din Timișoara sunt reglementate prin *Codul drepturilor și obligațiilor studentului și Regulamentul privind activitatea profesională a studenților de la ciclurile de studii universitare de licență și de masterat din UVT*, aprobat de Senatul UVT.

Forma și metodele de evaluare/examinare pentru fiecare disciplină din planul de învățământ se stabilesc prin fișele disciplinelor.

6. Examenul de finalizare a studiilor

În conformitate cu *Regulamentul privind organizarea și desfășurarea examenelor de finalizare a studiilor universitare de licență și de masterat la Universitatea de Vest din Timișoara*, aprobat de Senatul UVT, examenul de finalizare a studiilor universitare de masterat la orice

program de studii universitare de masterat organizat la UVT constă într-o probă de elaborare și susținere a lucrării de disertație, pentru care se acordă **10 credite**.

Tematica și bibliografia corespunzătoare probelor examenului de finalizare a studiilor se publică pe site-ul propriu al fiecărei facultăți și/sau pe site-ul UVT înainte de începutul fiecărui an universitar.

Înscrierea la examenul de finalizare a studiilor este condiționată de alegerea de către student a temei lucrării de finalizare a studiilor în cel mult 60 de zile de la începutul anului universitar al anului de studii terminal.

Depunerea variantei finale a lucrării de finalizare a studiilor pe platforma de e-learning se face cu cel puțin 5 zile lucrătoare înainte de data programată pentru începerea examenului.

Fiecare lucrare de finalizare a studiilor va fi însoțită, în momentul depunerii, de *Raportul de similaritate* rezultat ca urmare a verificării originalității lucrării de finalizare a studiilor universitare printr-un soft specializat, pe platforma de e-learning a UVT.

Conform structurii anului universitar, la UVT examenele de finalizare a studiilor universitare se pot organiza în 3 sesiuni, de regulă în lunile iulie, septembrie și februarie.

În anul 2 de studii, semestrul 2 este dedicat în principal întocmirii lucrării de disertație. Alegerea tematică a disertației se va face înainte de acest moment, iar studenții pot solicita discuții și își pot alege sau propune temele pentru elaborarea lucrării de disertație, cu și de la cadrele didactice asociate. Tipul probelor de examen pentru finalizarea programului de studii va fi anunțat în prealabil de către Facultatea de Matematică și Informatică.

7. Pregătirea pentru profesia didactică (*dacă este cazul*)

Studenții care doresc să opteze și pentru o carieră didactică în învățământul preuniversitar trebuie să parcurgă (complementar prezentului program de studii) și să finalizeze *Programul de formare psihopedagogică în vederea certificării competențelor pentru profesia didactică* și să obțină Certificatul de absolvire a acestui program. În Universitatea de Vest din Timișoara acest program este organizat prin intermediul Departamentului pentru Pregătirea Personalului Didactic (DPPD) și poate fi urmat în paralel cu studiile universitare sau în regim postuniversitar. Pentru mai multe informații, accesați linkul: <https://dppd.uvt.ro>.

LISTA DISCIPLINELOR STUDIATE, GRUPATE PE ANI ȘI SEMESTRE DE STUDII

Anul de studii I
An universitar 2024-2025

Nr. crt.	Disciplina	C1	C2	Cod disciplină	Semestrul I					Număr de credite	Semestrul II				Număr de credite
					Număr de ore/ săptămână				C		S	L	P		
					C	S	L	P							
1.	Cryptography and information security	DF	DO	FMIIM116	2		1		6						
2.	Law of communications and new technologies	DS	DO	FMIIM117	2	1			6						
3.	Research ethics	DC	DO	FMIIM103	1				2						
4.	Introduction to cybersecurity. Prevention, detection and mitigation techniques	DF	DO	FMIIM111	2		1		6						
5.	Financial-banking security	DS	DOP	FMIIM127	2		1		5						
	Introduction to Quantum Computing			FMIIM308											
6.	Security of distributed applications	DS	DOP	FMIIM119	2		1		5						
	Computer Vision			FMIIM303											
7.	Applications, approaches and challenges in cybersecurity in the modern digital era	DF	DO	FMIIM220						2		1		5	
8.	Big Data Technologies	DS	DO	FMIIM210						2		1		5	
9.	Cloud security	DS	DO	FMIIM218						2		1		5	
10.	Digital forensics and data analysis techniques in cybercrime	DF	DO	FMIIM219						2		1		5	

Nr. crt.	Disciplina	C1	C2	Cod disciplină	Semestrul I				Număr de credite	Semestrul II				
					Număr de ore/ săptămână					Număr de ore/ săptămână				Număr de credite
					C	S	L	P		C	S	L	P	
11.	Data mining	DS	DOP	FMIIM206						2		1		5
	DevSecOps			FMIIM221										
12.	Quality and reliability of software systems	DS	DOP	FMIIM212						2		1		5
	Multi-agent systems			FMIIM203										
Total					11	1	4		30	12		6		30
Total ore didactice pe săptămână					16					18				

Discipline facultative⁷

Discipline facultative ⁷														
Nr. crt.	Disciplina	C1	C2	Cod disciplină	Semestrul I					Semestrul II				
					Număr de ore/ săptămână				Număr de credite	Număr de ore/ săptămână				Număr de credite
					C	S	L	P		C	S	L	P	
1.	Database	DF	DFAC	FMIL303	2		2		2					
2.	Programming I	DF	DFAC	FMIL102	2		2		2					
3.	Programare III (Java)	DS	DFAC	FMIL304	2		2		2					
4.	Volunteering I (60h/semester)	DC	DFAC	FMIIM100				60						
5.	Programare II (C/C++)	DC	DFAC	FMIL204						2		3		6
6.	Algorithms and data structures II	DS	DFAC	FMIL201						2		2		5
7.	Volunteering II (60h/semester)	DC	DFAC	FMIIM200									60	2

⁷ Disciplinele facultative (mai puțin Stagiul de practică) sunt incluse în planul de învățământ al programului de licență Informatică și se adresează masteranzilor care nu au formare inițială în domeniul Informaticii cu excepția disciplinei Voluntariat

Anul de studii II

An universitar 2025-2026

Nr. crt.	Disciplina	C1	C2	Cod disciplină	Semestrul I				Număr de credite	Semestrul II				Număr de credite
					Număr de ore/săptămână					Număr de ore/săptămână				
					C	S	L	P		C	S	L	P	
1.	Common attack vectors and exploits in cybersecurity	DS	DO	FMIIM112	2		1		6					
2.	Computer Virusology	DF	DO	FMIIM319	2		1		6					
3.	Standards and protocols in cybersecurity	DF	DO	FMIIM320	2		1		6					
4.	Professional practice	DS	DO	FMIIM311				2	2					
5.	Penetration testing	DS	DOP	FMIIM321	2		1		5					
	Security and sharing of public and private data			FMIIM322										
	Cybercrime			FMIIM323										
6.	Machine Learning	DS	DOP	FMIIM302	2		1		5					
	Distributed Methods and Technologies based on XML			FMIIM109										
7.	Research and professional practice	DS	DO	FMIIM404									3	8
8.	MSc Thesis Preparation	DS	DO	FMIIM402								8		15
9.	Scientific Seminar	DS	DO	FMIIM403								3		7
Total					10		5	2	30			11	3	30
Total ore didactice pe săptămână					17					14				

Discipline facultative														
Nr. crt.	Disciplina	C1	C2	Cod disciplină	Semestrul I					Semestrul II				
					Număr de ore/ săptămână				Număr de credite	Număr de ore/ săptămână				Număr de credite
					C	S	L	P		C	S	L	P	
1.	Volunteering III (60h/semester)	DS	DFAC	FMIIM300				60	2					
2.	Volunteering IV (60h/semester)	DS	DFAC	FMIIM400									60	2
3.	Internship	DS	DFAC	FMIL216				1	2					

BILANȚ GENERAL I (după criteriul conținutului)

Nr. crt.	Tip disciplină	Număr total de ore							
		Anul I		Anul II		Întreg programul de studii			% din total
		Curs	S/L/P	Curs	S/L/P	Curs	S/L/P	Total	
1.	Fundamentale	112	56	56	28	168	84	252	28,57%
2.	De specialitate	182	112	84	238	266	350	616	69,84%
3.	Complementare	14	-	-	-	14	-	14	1,59%
TOTAL		308	168	140	266	448	434	882	100%

BILANȚ GENERAL II

(după criteriul obligativității)

Nr. crt.	Tip disciplină	Număr total de ore							
		Anul I		Anul II		Întreg programul de studii			% din total
		Curs	S/L/P	Curs	S/L/P	Curs	S/L/P	Total	
1.	Obligatorie	196	112	84	238	280	350	630	71,43%
2.	Opțională	112	56	56	28	168	84	252	28,57%
TOTAL		308	168	140	266	448	434	882	100%
3.	Facultative	140	278	-	134	140	408	548	<i>Suplimentar acestei structuri</i>
Raport total ore de curs și cele aplicative (seminar/laborator/practică)						1,03			

Corelarea dintre competențe, rezultatele așteptate ale învățării (cunoștințe, abilități și responsabilitate și autonomie) și disciplinele studiate se află la următorul [LINK](#).



Responsabil program de studii, Conf. univ. dr. Ciprian Pungilă	Director de departament, Lect. univ. dr. Loredana Tănasie	Decan, Conf. univ. dr. Cosmin Bonchiș
---	--	--

Rector,
Prof. univ. dr. Marilen Gabriel PIRTEA