

Ministerul Educației și Cercetării al Republicii Moldova  
Academia de Studii Economice din Moldova

**COORDONAT**

Ministerul Educației și Cercetării

nr. \_\_\_\_\_  
din \_\_\_\_\_

Ministru \_\_\_\_\_ Dan PERCIUN

**APROBAT**

La ședința Senatului ASEEM

Proces verbal nr. 6  
din 25 februarie 2026

Rector  Alexandru STRATAN



**PLAN DE ÎNVĂȚĂMÂNT**  
pentru ciclul II, studii superioare de master

Nivelul calificării conform ISCED și CNC:

Domeniul general de studii:

Domeniul de formare profesională:

Programul de master:

Tipul programului de master

Numărul total de credite de studiu ECTS:

Titlul obținut la finele studiilor:

Baza admiterii:

Limba de instruire:

Forma de organizare a învățământului:

7 ISCED și 7 CNC

061 Tehnologii ale Informației și Comunicațiilor

0613 Dezvoltarea produselor program și aplicațiilor

Securitatea sistemelor informatice

Master profesional - MP

90 ECTS

Master în *Inginerie*

Diplomă de licență în domeniul general de studii

Tehnologii ale Informației și Comunicațiilor

Română

Învățământ cu frecvență

Înregistrat

Agencia Națională de Asigurare a Calității în Educație și Cercetare

Nr. \_\_\_\_\_ din \_\_\_\_\_

**RESPONSABIL DE PROGRAM**

Șef departament „Tehnologia Informației și Management Informațional”

Y. Gujuman GUJUMAN Lucia, dr., conf. univ.

Aprobat

**Proces verbal nr. 5** din 17 februarie 2026

**APROBAT**

**Președintele Consiliului Calității ASEM**

[Signature] CASIAN Angela, dr., conf. univ.

**Proces verbal nr. 3**

din 24 februarie 2026

**APROBAT**

**Președintele Consiliului Școlii Masterale de Excelență în Economie și Business**

[Signature] BULGAC Corina, dr., conf. univ.

**Proces verbal nr. 4**

din 23 februarie 2026

<b>Calendarul universitar</b>						
<b>Termene (date calendaristice exprimate în luni) și durată</b>						
<b>Anul de studii</b>	<b>Activități didactice și de examinare*</b>		<b>Stagii de practică</b>	<b>Vacanțe</b>		
	<b>Sem. I</b>	<b>Sem. II</b>		<b>Iarnă</b>	<b>Primăvară</b>	<b>Vară</b>
<b>Anul I</b>	octombrie-ianuarie 17 săpt.	martie –iunie 12 săpt.	Sem. II februarie - martie 5 săpt.	decembrie-ianuarie 2 săpt.	Paști 1 săpt.	iunie – august 10 săpt.
<b>Anul II</b>	septembrie-decembrie 14 săpt.	-	Sem. III octombrie 3 săpt.	ianuarie 1 săpt.	-	-
<b>Total nr. săpt.</b>	<b>29 săpt.</b>	<b>12 săpt.</b>	<b>8 săpt.</b>	<b>3 săpt.</b>	<b>1 săpt.</b>	<b>10 săpt.</b>

\* Activitățile didactice se desfășoară sub formă de module. Fiecare modul este succedat de examen

Planul de învățământ pe anii de studii									
Cod	Denumire a unității de curs	Total ore			Număr de ore pe tipuri de activități			Forma de evaluare	Nr. credite
		Total	Contact Direct	Studiu Individual	Curs	Seminar	Laborator / Practice		
<b>ANUL I de STUDII</b>									
<b>SEMESTRUL I</b>									
F.01.O.01.61	Reglementări juridice în TI și proprietatea intelectuală	150	36	114	24	12	0	E	5
F.01.O.02.21	Gestiunea riscurilor de securitate a informațiilor.	150	36	114	20	16	0	E	5
F.01.O.03.61	Gestiunea proiectelor informatice	150	36	114	20	16	0	E	5
F.01.O.04.61	Protocoale criptografice	150	36	114	20	0	16	E	5
F.01.O.05.61	Metodologia și etica cercetării în domeniul de formare profesională	150	36	114	24	12	0	E	5
S.01.O.06.21	Internet of things	150	48	102	24	0	24	E	5
<b>Total discipline semestrul I</b>		<b>900</b>	<b>228</b>	<b>672</b>	<b>132</b>	<b>56</b>	<b>40</b>	<b>6E</b>	<b>30</b>
<b>SEMESTRUL II</b>									
S.02.O.07.61	Gestiunea securității informatice	150	48	102	22	0	26	E	5
S.02.O.08.61	Auditul securității informatice	150	48	102	22	0	26	E	5
S.02.O.09.21	<b>MODUL:</b> 1. Guvernanța sistemelor informaționale 2. Business Process Management	180 (90/90)	60 (30/30)	120 (60/60)	40 (20/20)	20 (10/10)	0	E	6 (3/3)
S.02.A.10.61	Securitatea e-guvernării Securitatea tranzacțiilor electronice	150	48	102	22	0	26	E	5
S.02.O.11.61	Practica de master I (de profesionalizare)	270	220	50	0	0	0	E	9
<b>Total discipline semestrul II</b>		<b>900</b>	<b>424</b>	<b>476</b>	<b>106</b>	<b>20</b>	<b>78</b>	<b>5E</b>	<b>30</b>
<b>Total pe anul I de studii</b>		<b>1800</b>	<b>652</b>	<b>1148</b>	<b>238</b>	<b>76</b>	<b>118</b>	<b>11E</b>	<b>60</b>
<b>ANUL II de STUDII</b>									
<b>SEMESTRUL III</b>									
S.03.A.12.61	MODUL 1: Instrumente de analiză a datelor Inteligența artificială aplicată MODUL 2: Programarea ERP Cloud Computing	240 (120/120)	80 (40/40)	160 (80/80)	32 (16/16)	0	48 (24/24)	E	8 (4/4)
S.03.O.13.61	Practica de master II (de cercetare)	120	100	20	0	0	0	E	4
	Teza de master	540	0	540	0	0	0	E	18
<b>Total discipline semestrul III</b>		<b>900</b>	<b>180</b>	<b>720</b>	<b>32</b>	<b>0</b>	<b>48</b>	<b>3E</b>	<b>30</b>
<b>TOTAL GENERAL pe anii de studii</b>		<b>2700</b>	<b>832</b>	<b>1868</b>	<b>270</b>	<b>76</b>	<b>166</b>	<b>14E</b>	<b>90</b>

Unități de curs	Nr. total de ECTS	Ponderea, %
Fundamentale (F)	25	27,8
Specialitate (S)	34	37,8
Stagii de practică (SP)	13	14,4
Teza de master	18	20
<b>TOTAL</b>	<b>90</b>	<b>100</b>

Stagiile de practică						
Tipul stagiului de practică		Semestrul	Durata		Perioada desfășurării	Număr ECTS
			Nr. săpt.	Nr. ore		
1.	Practica de master I (de profesionalizare)	II	5	270	februarie-martie	9
2.	Practica de master II (de cercetare)	III	3	120	octombrie	4

Forma de evaluare finală a studiilor			
Nr. crt.	Forma de evaluare finală a studiilor	Termene de organizare	Nr. crt.
1.	TEZA DE MASTER	Ianuarie	18

Unități de curs la libera alegere									
Cod	Denumire a unității de curs	Total ore			Număr de ore pe tipuri de activități			Forma de evaluare	Nr. credite
		Total	Contact direct	Studiu individual	Curs	Seminar	Laboratoare/Practice		
<b>Anul I</b>									
<b>Semestrul I</b>									
G.01.L.32	Limbă străină aplicată în domeniul profesional	150	36	114	0	36	0	E	5
<b>Semestrul II</b>									
G.02.L.11	<b>MODUL</b> 1. Managementul public și conducerea organizațională bazate pe fundamente socio-etice 2. Managementul strategic al economiei circulare/	180	44 (22/22)	136 (68/68)	32 (16/16)	12 (6/6)	0	E	6 (3/3)

**Lista competențelor și a rezultatelor învățării aferente programului de studii**

Competențe generale/profesionale	Rezultate ale învățării conform nivelului CNC
	<i>Absolventul/candidatul la atribuirea calificării poate:</i>
<b>CG 1.</b> Lansarea afacerilor bazate pe dezvoltarea produselor program și a aplicațiilor	1. identifica oportunități pentru lansarea și dezvoltarea afacerilor în domeniul dezvoltării produselor program și a aplicațiilor, analizând resursele disponibile și tendințele tehnologice; 2. elaborează un plan de afaceri în domeniul sistemelor informaționale în baza analizei surselor de finanțare și a riscurilor potențiale;
<b>CG 2.</b> Managementul proceselor și resurselor în sistemele informaționale	3. gestionează procesele de proiectare, dezvoltare și administrare a sistemelor informaționale, asigurând calitatea și securitatea acestora; 4. dezvoltă relații constructive și strategii de colaborare cu beneficiarii implicați în gestionarea și administrarea sistemelor informatice;
<b>CG 3.</b> Utilizarea tehnologiilor emergente în dezvoltarea și administrarea sistemelor informaționale	5. identifica soluții software potrivite pentru dezvoltarea și optimizarea sistemelor informaționale, analizând tendințele de dezvoltare a tehnologiilor emergente; 6. implementează soluții și strategii originale de integrare a tehnologiilor avansate pentru îmbunătățirea performanței sistemelor informaționale;
<b>CG 4.</b> Realizarea activității de cercetare în domeniul sistemelor informaționale	7. definește probleme de cercetare specifice proiectării și administrării sistemelor informaționale, având o abordare critică și creativă; 8. aplică metode și tehnici de cercetare pentru analiza, proiectarea și îmbunătățirea soluțiilor propuse;
<b>CP5.</b> Aplicarea metodelor de cercetare în securitatea cibernetică și protecția informației	17. aplică metode de identificare a vulnerabilităților, optimizând soluțiile de securitate cibernetică în baza analizei riscurilor; 18. realizează studii comparative a tehnologiilor și strategiilor de protecție a datelor pentru a dezvolta soluții de securitate;
<b>CP6.</b> Analiza incidentelor de securitate cibernetică	19. monitorizează incidentele de securitate cibernetică, utilizând metode criminalistice digitale și tehnici de detectare a atacurilor; 20. aplică soluții de răspuns prompt la incidente de securitate, minimizând impactul acestora asupra infrastructurilor informatice;
<b>CP7.</b> Implementarea măsurilor de securitate cibernetică	21. proiectează mecanisme de protecție a datelor și infrastructurilor informatice conform normelor legislației și a standardelor internaționale de securitate 22. integrează soluții de criptografie, autentificare și gestiune al accesului la protejarea sistemelor informatice contra amenințărilor cibernetică
<b>CP8.</b> Auditul securității în sisteme informatice	23. efectuează audit de securitate pentru a evalua conformitatea sistemelor informatice cu cerințele legislative și standardele de securitate; 24. analizează riscurile și vulnerabilitățile sistemelor informatice, propunând măsuri de remediere pentru a îmbunătăți nivelul lor de securitate.

### Matricea de corelare a competențelor și a rezultatelor învățării din standardul de calificare cu disciplinele/modulele din planul de învățământ

Denumirea unității de curs/moduleului	Codul unității de curs/moduleului	Nr. ECTS.	Competențe															
			Generale								Profesionale							
			CG 1		CG2		CG3		CG4		CP5		CP6		CP7		CP8	
			Rezultatele învățării conform CNC															
			1	2	3	4	5	6	7	8	17	18	19	20	21	22	23	24
Reglementări juridice în TI și proprietatea intelectuală	F.01.O.01.61	5	0,5	0,5	0,5	0,5	0	0	0	0,5	0,5	0,5	0	0	0,5	0,5	0,5	0
Gestiunea riscurilor de Securitate a informațiilor	F.01.O.02.61	5	0	0	0,5	0,5	0,5	0	0	0,5	1	1	0,5	0	0	0	0,5	0
Gestiunea proiectelor informatice	F.01.O.03.61	5	0	0	1,5	0,5	0	0	0,5	0,5	0	0,5	0,5	0	0	0	0,5	0,5
Protocoale criptografice	F.01.O.04.61	5	0	0	0	0	0,5	0,5	0	0	0,5	0,5	0,5	0,5	1	1	0	0
Metodologia și etica cercetării în domeniul de formare profesională	F.01.O.05.61	5	0	0	0	0	0	0	2	2	0,5	0,5	0	0	0	0	0	0
Internet of things	S.01.O.06.21	5	0	0	0	0	0,5	1	0	0	0	0	0,5	0,5	1	1	0,5	0
Gestiunea securității informatice	S.02.O.07.61	5	0	0	0,5	0,5	0,5	0,5	0	0	1	1	0,5	0,5	0	0	0	0
Auditul securității informatice	S.02.O.08.61	5	0	0	0,5	0	0,5	0,5	0	0	0,5	0,5	0,5	0,5	1	1	0	0
<b>MODUL</b>																		
1. Guvernanța sistemelor informaționale	S.02.O.09.21	6 (3/3)	0	0	0,5	0,5	0	0	0	0	0,5	0,5	0,5	0,5	0	0	0	0
2. Business Process Management			0	0	0,5	0,5	0	0	0	0	0	0	0	0,5	0	0,5	0,5	0,5
Securitatea e-guvernării	S.02.A.10.61	5	0	0	0,5	0	0,5	0,5	0	0	0,5	0,5	0,5	0,5	1	0,5	0	0
Securitatea tranzacțiilor electronice			0	0	0	0	0,5	0,5	0	0	0,5	0,5	0,5	0,5	1	1	0	0
Practica de master I (de profesionalizare)	S.02.O.11.61	9	0,5	0,5	1	1	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
<b>MODUL 1:</b>																		
1. Instrumente de analiză datelor	S.03.A.12.61	8 (4/4)	0	0	0	0	0,5	0,5	0	0	0,5	0,5	0	0	1	1	0	0
2. Inteligența artificială aplicată			0	0	0	0	0,5	0,5	0,5	0	0,5	0,5	0	0	0,5	1	0	0

Denumirea unității de curs/modulului	Codul unității de curs/modulului	Nr. ECTS.	Competențe															
			Generale								Profesionale							
			CG 1		CG2		CG3		CG4		CP5		CP6		CP7		CP8	
			Rezultatele învățării conform CNC															
			1	2	3	4	5	6	7	8	17	18	19	20	21	22	23	24
<b>MODUL 2:</b> 1. Programare ERP 2. Cloud Computing			0	0	0,5	0,5	0	0	0	0	0	0	0,5	0,5	1	1	0	0
			0	0	0	0	0,5	0,5	0	0	0,5	0,5	0,5	0,5	1	0	0	0
Practica de master II (de cercetare)	S.03.O.13.61	4	0	0	0	0	0	0	1	1	0,5	0,5	0,5	0,5	0	0	0	0
<b>Teza de master</b>		18	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1
<b>Total</b>		<b>90</b>																

## NOTA EXPLICATIVĂ

### 1. Descrierea programului de studii

Programul de studii universitare de master *Securitatea Sistemelor Informatice* se înscrie în domeniul fundamental al științei, culturii și tehnicii *Tehnologii ale informației și comunicațiilor*, domeniului general de studiu 061. *Tehnologii ale informației și comunicațiilor*, domeniului de formare profesională 0613. *Dezvoltarea produselor program și a aplicațiilor*.

Programul de studii universitare de master *Securitatea Sistemelor Informatice* a fost elaborat în corespundere cu [Codul Educației al Republicii Moldova, Legea nr. 152 / 2014](#), cu modificările ulterioare; [Nomenclatorul domeniilor de studii și al specialităților în învățământul superior, aprobat prin Hotărârea Guvernului nr. 412/2024](#); [Cadrul Național al Calificărilor din Republica Moldova, aprobat prin Hotărârea Guvernului nr. 330/2023](#); [Planul-cadru pentru studii superioare de licență, master și integrate, aprobat prin Ordinul MEC nr. 510/2025](#); [Regulamentul cu privire la organizarea și desfășurarea studiilor superioare de master – ciclul II, aprobat prin Hotărârea Guvernului nr. 80/2022](#); [Standardul de calificare pentru titlul de Master în inginerie, nivelul 7 CNC, domeniul de formare profesională 0613 – Dezvoltarea produselor program și a aplicațiilor](#), aprobat prin Ordinul Ministerului Educației și Cercetării din 6 decembrie 2018.

**Caracteristicile-cheie** ale programului de master *Securitatea Sistemelor Informatice* sunt:

**Forma de organizare** – învățământ cu frecvență.

**Durata studiilor** – 1,5 ani.

**Credite de studii** – 90 credite ECTS, 1 credit ECTS = 30 ore.

**Limba de studiu** – română.

**La studiile de master la programul *Securitatea Sistemelor Informatice*** se pot înscrie – deținătorii diplomelor de studii superioare de licență în domeniul general de studiu *Tehnologii ale Informației și Telecomunicațiilor*.

Absolvenții programului de studii universitare de master *Securitatea Sistemelor Informatice* se certifică prin Diplomă de master în Inginerie, titlul obținut fiind Master în Inginerie.

### 2. Obiectivele programului de studii, inclusiv corespunderea acestora misiunii universității

Programul de studii universitare de master *Securitatea Sistemelor Informatice* este aliniat la [Misiunea ASEM](#) de a forma specialiști de înaltă calificare, adaptabili cerințelor pieței muncii și capabili de dezvoltare profesională continuă. Curriculumul este corelat cu tendințele internaționale în domeniul securității cibernetice, punând accent pe protecția infrastructurilor critice, analiza riscurilor, criptografie aplicată și managementul incidentelor de securitate. Programul este construit în conformitate cu cerințele [Clasificării Internaționale Standard a Educației \(ISCED-F 2013\)](#) și ale [Cadrului Național al Calificărilor din Republica Moldova \(nivel 7\)](#), precum și cu bunele practici promovate în Spațiul European al Învățământului Superior (ESG).

În ASEM este creat un mediu educațional centrat pe student, calitativ și favorabil performanței, organizat în baza următoarelor principii:

- asigurarea unui mediu de învățare autentic, orientat spre practică, conectat la nevoile sectorului IT și de securitate informatică;
- îmbinarea cunoștințelor teoretice cu dezvoltarea de competențe tehnice avansate, relevante pentru activitatea în domeniul securității cibernetice;
- promovarea metodelor de învățare activă și dezvoltarea competențelor de analiză, proiectare și implementare a soluțiilor de securitate;
- utilizarea tehnologiilor moderne și a resurselor digitale de învățare, pentru a încuraja inovația și creativitatea.

Misiunea programului derivă din misiunea ASEM, stipulată în [Carta ASEM](#), Statutul ASEM, [Planul strategic de dezvoltare](#), [Strategia de cercetare](#) și [Strategia de internaționalizare](#). Programul urmărește formarea unor specialiști capabili să protejeze infrastructurile informatice, să asigure integritatea, confidențialitatea și disponibilitatea datelor și să contribuie activ la reziliența cibernetică a organizațiilor.

Obiectivul general al programului constă în pregătirea de specialiști în domeniul securității sistemelor informatice, capabili să proiecteze, implementeze și gestioneze politici și soluții de securitate IT, în contexte organizaționale complexe, marcate de digitalizare accelerată și provocări cibernetice majore.

Obiectivele specifice ale programului includ:

- dezvoltarea de cunoștințe avansate privind arhitecturile de securitate, metodele criptografice și protecția datelor;
- formarea competențelor de analiză a vulnerabilităților, evaluare a riscurilor informatice și reacție la incidente cibernetice;
- familiarizarea cu standardele internaționale și cadrul legal privind securitatea informației;
- promovarea unei culturi a securității, integrității și eticii profesionale în mediile digitale;
- stimularea abilităților de cercetare aplicată în securitatea cibernetică și implicarea în proiecte multidisciplinare.

Planul de învățământ este elaborat în conformitate cu [Standardul de calificare Master în inginerie, nivelul 7 CNC, domeniul de formare profesională 0613 – Dezvoltarea produselor program și a aplicațiilor](#), aprobat prin Ordinul MEC nr. 148/2023. Structura curriculară este compatibilă cu cerințele [Clasificării Internaționale Standard a Educației \(ISCED-F 2013\)](#) și asigură implementarea componentelor formative, de acumulare și evaluare prevăzute în [Planul-cadru pentru studii superioare de master, aprobat prin Ordinul MEC nr. 510/2025](#).

La elaborarea și actualizarea conținuturilor disciplinelor s-au valorificat bunele practici internaționale și expertiza acumulată în cadrul proiectelor de cooperare europeană ([Erasmus+](#), [Horizon Europe](#)), precum și din rețele profesionale din domeniul securității cibernetice, ingineriei software și guvernății digitale. Se acordă prioritate tematicilor actuale precum securitatea infrastructurilor critice, analiza malware, răspunsul la incidente, protecția datelor personale și securitatea aplicațiilor web.

Programul a fost structurat în urma consultării programelor similare oferite de universități europene de prestigiu, asigurând compatibilitatea internațională, mobilitatea academică și recunoașterea diplomelor. Accentul este pus pe dezvoltarea competențelor transversale și profesionale necesare inserției pe piața muncii și adaptării continue la noile provocări din domeniul securității informatice.

### **3. Evaluarea așteptărilor sectorului economic și social**

Programul de master *Securitatea Sistemelor Informatice* a fost elaborat în cadrul proiectului ERASMUS+ LMPI - N°573901-EPP-1-2016-1-IT-PKA2-CBHE-JP „Licență, masterat profesional în administrarea, gestiunea, protecția sistemelor și rețelelor informatice în întreprinderi din Moldova, Kazahstan și Vietnam.

Pentru evaluarea așteptărilor sectorului economic în cadrul acestui proiect, în anul 2017 a fost realizat un „Sondaj de identificare a profesiilor țintă și a nevoilor de instruire în domeniul securității informatice în Moldova”. Conform raportului acestui sondaj, aproape 69% din profesioniștii în domeniu (specialiști cu studii superioare), care au participat în sondaj, au specificat că au nevoie de instruire în securitatea informatică. Eșantionul de participanți la sondaj este reprezentativ. Chestionarul a fost completat de 199 respondenți, reprezentând și așa companii bine cunoscute din domeniu ca: Endava, Moldtelecom, Centrul de Telecomunicații Speciale, Centrul de Guvernare Electronică, Fiscservinform ș.a. Aproape 23% din respondenți reprezintă companii cu peste 500 angajați. Peste 58% din respondenți au experiență profesională în domeniul securității informatice.

De asemenea acest raport a stat la baza conceptului general al programului de master *Securitatea Sistemelor Informatice*.

### **4. Consultarea partenerilor în procesul de elaborare a programului de studii**

La elaborarea programului de studii universitare de master *Securitatea Sistemelor Informatice*, procesul de consultare s-a realizat atât în format letric (scris pe hârtie) în cadrul practicii de master, prin completarea chestionarelor de evaluare a competențelor practice ale studenților, cât și în formă participativă, în timpul susținerii proiectului examenului de master. De asemenea, s-a efectuat: analiza documentelor normative și reglatoare cu referire la procesele educaționale în învățământul superior; analiza prealabilă referitoare la nevoile

specifice exprimate de clienți, beneficiari și parteneri (cadre științifico-didactice, absolvenți, studenți și firme sau organizații interesate); analiza celor mai noi direcții de dezvoltare în domeniul de formare; analiza comparativă a planurilor de studii pe baza unor modele de la universități de prestigiu din țară și străinătate; analiza metodologiilor specifice actuale de predare în domeniu; analiza și evaluarea prealabilă a propunerilor venite din partea unor specialiști externi/studenți; analiza neconformităților constatate pe parcursul anilor universitari precedenți.

Din considerentele de mai sus, formarea de specialiști conform Programului de master Securitatea sistemelor informatice pentru piața muncii din Republica Moldova este actuală.

### **5. Relevanța programului de master pentru piața forței de muncă**

Pentru prevenirea și combaterea fraudelor informatice, la nivel internațional și național sunt elaborate acte legislative și normative care reglementează protecția informației, securitatea sistemelor informatice și protecția datelor cu caracter personal. În Republica Moldova, cadrul juridic relevant include o serie de acte normative care stabilesc cerințe privind securitatea informațională și utilizarea tehnologiilor informaționale, printre care: [Legea privind accesul la informație nr. 982/2000](#), [Legea privind comerțul electronic nr. 284/2004](#), [Legea privind prevenirea și combaterea criminalității informatice nr. 20/2009](#), [Legea privind protecția datelor cu caracter personal nr. 133/2011](#), [Legea privind semnătura electronică și documentul electronic nr. 91/2014](#), precum și [Legea nr. 48/2023 privind securitatea cibernetică](#).

Totodată, respectarea stipulărilor legislației și a altor documente normative în domeniu, protejarea suportului informatic al activităților persoanelor fizice, al mediului de afaceri, al administrației publice și al altor organizații și instituții, inclusiv a resurselor informaționale și informațiilor cu care aceste entități operează, necesită cunoștințe speciale; condițiile majore în domeniu pot fi asigurate doar de către specialiști de înaltă calificare în domeniul Securității sistemelor informatice. Aceștia trebuie să formuleze cerințele, să implementeze și dezvolte mijloacele și să asigure mentenanța, monitorizarea și actualizarea produselor informatice speciale respective.

În contextul digitalizării economiei și administrației publice, se constată o cerere tot mai mare pentru specialiști în domeniul securității sistemelor informatice. În Republica Moldova, specialiștii în securitate informatică sunt solicitați atât de companiile din sectorul IT și organizațiile economice, cât și de instituțiile publice. Deficitul de experți în domeniul securității cibernetică se menține și la nivel internațional, inclusiv în statele cu un nivel avansat de dezvoltare a societății informaționale. În acest context, programul de master contribuie la formarea competențelor profesionale necesare pentru integrarea absolvenților pe piața muncii.

Acestea, dar și obiectivele stabilite în conceptul [Strategiei de dezvoltare a educației pentru anii 2021-2030 „Educația 2030”](#), care etalează imperativitatea forței de muncă calificată, subliniază relevanța programului de master Securitatea Sistemelor Informatice.

### **6. Posibilități de angajare ale absolvenților**

Absolvenții programului de studii universitare de master *Securitatea Sistemelor Informatice* își pot valorifica competențele profesionale în diverse sectoare ale economiei Republicii Moldova. Aceștia sunt pregătiți pentru activități profesionale în întreprinderi, organizații și instituții publice sau private care utilizează și administrează sisteme informatice. Programul oferă competențe avansate care permit ocuparea funcțiilor prevăzute în [Clasificatorul Ocupațiilor din Republica Moldova \(CORM 006-2021\)](#) și în [Clasificarea Europeană a Aptitudinilor, Competențelor, Calificărilor și Ocupațiilor \(ESCO\)](#).

Clasificatorul Ocupațiilor din Republica Moldova (CORM 006-2021)	ESCO 08
133016 Manager de proiect în tehnologia informației și comunicațiilor	1330.6 Manager de produs în domeniul TIC
231002 Cercetător științific stagiar/cercetătoare științifică stagiară	1330.7 Manager de proiect în domeniul TIC
251103 Analist/analistă de afaceri în domeniul tehnologiei informației și comunicațiilor	2511.3 Analist de informații / analistă de informații
251208 Programator analist / programatoare analistă	2511.4 Expert în analiza informațiilor
251403 Specialist / specialistă în configurarea aplicațiilor informaționale	2511.8 Manager analiza de business în domeniul TIC
251106 Analist / analistă securitatea sistemelor informaționale	2511.9 Analist de afaceri în domeniul TIC/ analistă de afaceri în domeniul TIC
251107 Analist/ analistă sisteme informaționale	2511.12 Consultant de cercetare în domeniul TIC/ consultantă de cercetare în domeniul TIC
251118 Inginer / ingineră integrare a sistemelor informaționale	2511.13 Analist de sistem în domeniul TIC / analistă de sistem în domeniul TIC
251120 Specialist / specialistă în arhitectura organizațională	2512.1 Inginer în domeniul tehnologiilor cloud /ingineră în domeniul tehnologiilor cloud
251201 Analist / analistă software	2512.2 Analist de software / analistă de software
251205 Inginer / ingineră de sistem software	

### 7. Accesul la studii a titularilor de diplome obținute după finalizarea respectivului program de studii

Competențele, deprinderile și cunoștințele dobândite pe parcursul studiilor de masterat (nivelul 7 ISCED) pot fi aprofundate prin continuarea studiilor la programele doctorat (nivelul 8 ISCED), asigurându-se educația și dezvoltarea profesională continuă a absolvenților, în concordanță cu nevoile societății manifestate pe piața forței de muncă.

De asemenea, titularii diplomelor de master în *Securitatea Sistemelor Informatice* pot accesa programe postuniversitare de formare continuă, cursuri de perfecționare și certificări profesionale în domenii precum: audit și conformitate în securitate cibernetică, managementul riscurilor informatice, guvernanta IT, securitate în cloud computing, testare de penetrare (penetration testing) sau protecția datelor cu caracter personal (GDPR). Aceste forme de formare complementară contribuie la dezvoltarea unei cariere sustenabile în domeniul securității informatice și permit adaptarea continuă a competențelor la cerințele unei societăți digitalizate și interconectate.

### 8. Lista competențelor și a rezultatelor învățării

Competențele și rezultatele învățării ale programului de studii universitare de master *Securitatea Sistemelor Informatice* sunt definite în conformitate cu [Standardul de calificare Master în Științe Ingineresti, nivelul calificării 7 CNC](#), domeniul de formare profesională: 0613 – Dezvoltarea produselor program și a aplicațiilor, aprobat prin Ordinul Ministerului Educației și Cercetării 6 decembrie 2018. Acestea reflectă cerințele actuale ale pieței muncii în domeniul securității informatice și asigură alinierea cu standardele internaționale privind formarea specialiștilor în IT și securitate cibernetică.

#### Lista competențelor:

<b>COMPETENȚE TRANSVERSALE (CT)</b>	<b>CT 1.</b> Gestionarea timpului și autodisciplină <b>CT 2.</b> Luarea deciziilor, rezolvarea problemelor și leadership <b>CT 3.</b> Creativitatea și inovația <b>CT 4.</b> Demonstrarea integrității, eticii și transparenței <b>CT 5.</b> Manifestarea flexibilității, adaptabilității și rezilienței <b>CT 6.</b> Comunicarea eficientă, lucru în echipă și colaborarea <b>CT 7.</b> Negocierea și crearea de parteneriate <b>CT 8.</b> Empatia și inteligența emoțională <b>CT 9.</b> Orientarea spre învățare <b>CT 10.</b> Managementul informațiilor și TIC
<b>COMPETENȚE GENERALE (CG)</b>	<b>CG 1.</b> Lansarea afacerilor bazate pe dezvoltarea produselor program și a aplicațiilor <b>CG 2.</b> Managementul proceselor și resurselor în sistemele informaționale <b>CG 3.</b> Utilizarea tehnologiilor emergente în dezvoltarea și administrarea sistemelor informaționale <b>CG 4.</b> Realizarea activității de cercetare în domeniul sistemelor informaționale
<b>COMPETENȚE PROFESIONALE (CP)</b>	<b>Aria ocupațională 2. Securitatea cibernetică și protecția informației</b> <b>CP5.</b> Aplicarea metodelor de cercetare în securitatea cibernetică și protecția informației <b>CP6.</b> Analiza incidentelor de securitate cibernetică <b>CP7.</b> Implementarea măsurilor de securitate cibernetică <b>CP8.</b> Auditul securității în sisteme informatice

**Lista rezultatelor învățării:**

*Absolventul/candidatul la atribuirea calificării poate:*

1. identifica oportunități pentru lansarea și dezvoltarea afacerilor în domeniul dezvoltării produselor program și a aplicațiilor, analizând resursele disponibile și tendințele tehnologice;
2. elabora un plan de afaceri în domeniul sistemelor informaționale în baza analizei surselor de finanțare și a riscurilor potențiale;
3. gestiona procesele de proiectare, dezvoltare și administrare a sistemelor informaționale, asigurând calitatea și securitatea acestora;
4. dezvolta relații constructive și strategii de colaborare cu beneficiarii implicați în gestionarea și administrarea sistemelor informatice;
5. identifica soluții software potrivite pentru dezvoltarea și optimizarea sistemelor informaționale, analizând tendințele de dezvoltare a tehnologiilor emergente;
6. implementa soluții și strategii originale de integrare a tehnologiilor avansate pentru îmbunătățirea performanței sistemelor informaționale;
7. defini probleme de cercetare specifice proiectării și administrării sistemelor informaționale, având o abordare critică și creativă;
8. aplica metode și tehnici de cercetare pentru analiza, proiectarea și îmbunătățirea soluțiilor propuse;
17. aplica metode de identificare a vulnerabilităților, optimizând soluțiile de securitate cibernetică în baza analizei riscurilor;
18. realiza studii comparative a tehnologiilor și strategiilor de protecție a datelor pentru a dezvolta soluții de Securitate;
19. monitoriza incidentele de securitate cibernetică, utilizând metode criminalistice digitale și tehnici de detectare a atacurilor;
20. aplica soluții de răspuns prompt la incidente de securitate, minimizând impactul acestora asupra infrastructurilor informatice;
21. proiecta mecanisme de protecție a datelor și infrastructurilor informatice conform normelor legislației și a standardelor internaționale de securitate;

22. integra soluții de criptografie, autentificare și gestiune al accesului la protejarea sistemelor informatice contra amenințărilor cibernetice;
23. efectua audit de securitate pentru a evalua conformitatea sistemelor informatice cu cerințele legislative și standardele de securitate;
24. analiza riscurile și vulnerabilitățile sistemelor informatice, propunând măsuri de remediere pentru a îmbunătăți nivelul lor de securitate.