MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

CADRUL NAȚIONAL AL CALIFICĂRILOR

COORDONAT
Ministerul Dezvoltării Economice și Digitalizării

Doina NISTOR, Ministră

„02" iunie 2025

APROBAT
Ministerul Educației și Cercetării

Dan PERCIUN, Ministru

„23" iulie 2025

DECIZIA
Consiliului Național pentru Calificări

nr. 33 din „12" iunie 2025

STANDARD DE CALIFICARE

DOMENIUL GENERAL DE STUDIU	**061 Tehnologii ale informației și comunicațiilor**
DOMENIUL DE FORMARE PROFESIONALĂ	**0613 Dezvoltarea produselor program și a aplicațiilor**
PROGRAMUL DE STUDII	**0613.2 Securitate informațională**
CALIFICAREA	**Inginer licențiat**
NIVELUL CALIFICĂRII	**6 CNC**

2025

FIȘA DE VALIDARE A CONFORMITĂȚII

Nr. crt.	Instituția/ organizația/ structura	Numele, prenumele	Funcția, titlul științific/ gradul didactic	Semnătura	Data
MEMBRII GRUPULUI DE LUCRU CARE AU ELABORAT STANDARDUL DE CALIFICARE					
1.	Universitatea Tehnică a Moldovei, Facultatea Calculatoare, Informatică și Microelectronică, Departamentul Ingineria Software și Automatică	FIODOROV Ion	Șef Departament, dr. în informatică, conf. univ.		30.05.25
2.		BOLUN Ion	dr. hab., prof. univ.		30.05.25
3.		ALEXEI Arina	dr., lectoră univ.		30.05.25
4.	Academia de Studii Economice din Moldova, Departamentul Tehnologia Informației și Management Informațional, Facultatea Tehnologii Informaționale și Statistică Economică	ZGUREANU Aureliu	dr., conf. univ.		30.05.25
5.	Universitatea de Stat din Moldova, Departamentul Fizică Aplicată și Informatică, Facultatea Fizică și Inginerie	BELDIGA Maria	Prodecan, dr. în informatică, conf. univ.		30.05.25
6.	BC "MAIB" S.A., Direcția Dezvoltare Servicii .net, Departament Dezvoltare tehnologii informaționale, Divizia Tehnologii informaționale	COJOCARU Sergiu	Senior software engineer		30.05.25
7.	Asociația Companiilor IT (ATIC)	CUNEV Veaceslav	Președinte al Asociației, dr. în informatică		30.05.25
8.	BC "MAIB" S.A. Direcția Platforme analitice, Departamentul Platforme principale, Divizia Tehnologii informaționale	BULAI Rodica	Data analist		30.05.25
9.	Î.C.S. „Allied Testing-M" S.R.L.	NASTASENCO Veaceslav	Director		30.05.25

COMISIA DE VALIDARE A STANDARDULUI DE CALIFICARE					
Nr. crt.	**Instituția/ organizația/ structura**	**Numele, prenumele**	**Funcția, titlul științific/ gradul didactic**	**Semnătura**	**Data**
1.	Ministerul Dezvoltării Economice şi Digitalizării, Direcţia politici în domeniul tehnologiei informaţiei şi digitaizării	Andrei CUŞCĂ	Şef direcţie		23.05.25
2.	Agenţia de Guvernare Electronică, Serviciu tehnologia informaţiei	Igor ARAMĂ	Şef serviciu		23.05.25
3.	Academia de Studii Economice din Moldova, Facultatea Relaţii Economice Internaţionale	Larisa DODU-GUGEA	Doctor, conferenţiar universitar, decan		23.05.25
4.	Ministerul Dezvoltării Economice şi Digitalizării, Direcţia politici în domeniul tehnologiei informaţiei şi digitalizării	Viorica STROICI	Consultant principal		23.05.25

FIȘA DE CONSULTARE

Nr. crt.	Instituția/ organizația/ structura	Numele, prenumele	Funcția, titlul științific/ gradul didactic	Semnătura	Data
PARTENERI SOCIALI					
1.	Moldova IT Park	Bzovîi Marina	Director		07/04/2025
2.	S.R.L. ENDAVA	Panfil Veaceslav	Manager		10.04.25
3.	S.R.L. AMDARIS	Haheu Petru	Director		18/04/25
4.	S.R.L. M-TESTING	Crotov Serghei	Director		07/04/2025
5.	S.R.L. PENTALOG CHI	Burlac Mihail	Director tehnic		10/04/2025
6.	Asociația Națională a Companiilor din Domeniul TIC	Chirița Ana	Director proiecte strategice		10.04.2025
7.	S.A. ORANGE SYSTEMS	Plăcintă Sergiu	Director of International Operations		30.05.2025
8.	AddCode & Comitetul HR & Educație ATIC	Malbaș-Rotaru Alina	Co-președinte		10/04/25
9.	S.R.L. CRUNCHYROLL	Ivanova Elena	Director		10/04/25
10.	Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică	Coreţchi Alexandru	Director		02/04/2025

11.	S.R.L. CODWER	Dumitrașcu Marius	Director		10.04.2025
12.	S.R.L. IT-LAB GRUP	Cioban Alexei	Director		
13.	ÎCS GILAT SATELLITE NETWORKS MDC SRL	Andronic Alexandru	Manager		01.04.25
14.	S.R.L EBS Integrator	Barbaroș Vasile	Inginer de sistem software		04.04.25
15.	S.R.L. WINIFY	Poștaru Andrei	Director		03.04.25
16.	Facultatea Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei	Ciorbă Dumitru	Decan, dr., conf. univ.		02.04.2025
17.	Facultatea Tehnologii Informaționale și Statistică Economică, Academia de Studii Economice din Moldova	Toacă Zinovia	Decană, dr., conf. univ.		01.04.2025
18.	Facultatea de Matematică și Informatică, Universitatea de Stat din Moldova	Niculiță Angela	Decană, dr., conf. univ.		04.2025
19.	Facultatea Informatică, Inginerie, Design, Universitatea Liberă Internațională din Moldova	Mitev Lilia	Decană, dr., conf. univ.		08.04.2025

FORMULARUL CALIFICĂRII

Descrierea calificării	Inginerul licențiat în *Securitate informațională*, nivel 6 CNC, domeniul de formare profesională *0613 Dezvoltarea produselor program și a aplicațiilor,* domeniul general de studiu *061 Tehnologii ale informației și comunicațiilor,* un domeniu interdisciplinar al științei și tehnologiei, este specialistul cu studii superioare de licență care își desfășoară activitatea de muncă în companii și întreprinderi din sectorul secundar (producție și industrie), sectorul terțiar (servicii), sectorul cuaternar (cunoaștere, tehnologie) și este capabil să soluționeze probleme profesionale atribuite diverselor domenii de activitate: securitate operațională și managementul riscurilor, securitate aplicată și protecția infrastructurilor, testare de penetrare și evaluarea vulnerabilităților, criptografie și protecția datelor, cercetare și educație. *Componenta de securitate operațională* se orientează pe monitorizarea, detectarea și răspunsul la incidente de securitate pentru a proteja infrastructurile TI ale organizației. *Componenta de securitate aplicată* presupune implementarea și menținerea controalelor de securitate în rețele, cloud și infrastructuri critice. În cadrul *activităților de penentrare și evaluare a vulnerabilităților* are loc identificarea și exploatarea vulnerabilităților prin simularea atacurilor cibernetice. *Componenta de criptografie și protecția datelor* îi atribuie inginerului licențiat în securitate informațională rolul de dezvoltare și implementare a algoritmilor de criptare pentru protecția datelor organizației. În cadrul *activităților de cercetare profesională*, inginerul licențiat în securitate informațională analizează vulnerabilitățile sistemelor informatice, dezvoltă și implementează soluții avansate de protecție a datelor, elaborează modele de securitate cibernetică și algoritmi criptografici, evaluează riscurile asociate amenințărilor cibernetice și contribuie la inovarea și optimizarea strategiilor de apărare digitală. *Activitatea managerială* constă în coordonarea echipelor de lucru, elaborarea și monitorizarea planurilor de activitate a subdiviziunilor primare, elaborarea documentației tehnice conform formularelor aprobate, selectarea și argumentarea soluțiilor tehnice și manageriale în baza datelor inițiale inclusiv cu caracter economic.
Nivelul de calificare	6 CNC
Grup/grupuri-țintă	- Absolvenți de liceu, colegiu, centru de excelență; - prestatori de programe de educație și formare profesională; - angajatori; - alte părți interesate.
Tipul programului de studii	Program de studii superioare de licență, ciclul I.
Forma de organizare a studiilor	- cu frecvență; - cu frecvență redusă; - la distanță.
Durata și volumul studiilor	– 4 ani – 240 de credite de studii - în cazul învățământului cu frecvență redusă și la distanţă durata programului de studii este mai mare cu un an
Condiții de acces	- *Nivelul minim necesar de studii*: studii liceale. - *Acte de studii pentru acces*: - diplomă de bacalaureat;

	- diplomă de studii profesionale; - alt act de studii echivalent, recunoscut de autoritatea competentă.
Stagii de practică	Tipurile stagiilor de practică: - de specialitate (de inițiere, constructiv-tehnologică, în producție); - practica de documentare pentru proiectul de licență. Numărul de credite de studii alocate stagiilor de practică se încadrează în limita 15-20% din numărul de credite per program.
Actul de studii, titlul/calificarea atribuită	- Diplomă de studii superioare de licență și Supliment descriptiv conform Europass Titlul: *Inginer licențiat* (conform Anexei nr. 2 la ordinul MEC nr. 1223/2024, cu privire la punerea în aplicare a HG nr 412/2024)
Dezvoltare profesională/ proiectarea carierei	- Continuarea studiilor la ciclul II, studii superioare de master (nivel 7 CNC). - Formarea profesională continuă: a) programe de perfecționare/specializare, cu durata 150-900 ore/5-30 credite de studii; b) programe de recalificare profesională conexe specialității, formării profesionale inițiale absolvite, cu durata de 1800-3600 ore/60-120 credite de studii; c) programe de calificare parțială (microcalificare) în baza diplomei de studii superioare de licență/actului de studii echivalent, cu durata de 150-1800 de ore/5-60 de credite de studii.
Oportunități de angajare în câmpul muncii	Inginerul licențiat în Securitate Informațională în cadrul întreprinderilor/companiilor poate fi angajat în calitate de: 241242 Specialist/specialistă în securitatea informației 252905 Specialist/specialistă în securitatea sistemelor informatice 215319 Inginer/ingineră manager securitate informationala 215323 Inginer/ingineră politici de securitate informațională
Cerințe legale speciale	Apt de muncă din punct de vedere fizic și psihic. Nu sunt alte cerințe legale speciale care limitează obținerea calificării de către persoanele care îndeplinesc condițiile de acces stipulate mai sus.

LISTA OCUPAȚIILOR TIPICE

Programul de studii	Ocupații tipice conform CORM (006-2021)	Ocupații tipice conform ESCO 08	Ocupații tipice conform ISCO-08	Alte clasificări relevante (CAEM/ISIC/OMC după caz)
0613.2 Securitate informațională	121906 Manager (Șef/Șefa) securitatea informației din cadrul organizației 251910 Specialist/specialistă în proceduri și instrumente de securitate a sistemelor informaționale 241242 Specialist/specialistă în securitatea informației 252905 Specialist/specialistă în securitatea sistemelor informatice 252902 Administrator/ administratoare securitatea sistemelor informatice 251106 Analist/analistă securitatea sistemelor informaționale 215319 Inginer/ingineră manager securitate informaționala 215323 Inginer/ingineră politici de securitate informațională 215247 Inginer/ingineră securitatea sistemelor electronice și de telecomunicații	1219.1.2 Manager securitate 2529.6 Administrator securitate TIC 3512.3 Tehnician securitate TIC 2529.1 Ofițer șef securitate TIC 2529.3 Inginer de securitate a sistemelor încorporate 2529.7 Respondent la incidente cibernetice 2529.8 Manager risc cibernetic 1213.9 Director pentru conformitate și securitatea informațiilor 2413.1.4 Analist securitate	2511 Analiști de sisteme 2512 Dezvoltatori de software 2513 Dezvoltatori web și multimedia 2514 Programatori de aplicații 2521 Designeri și administratori de baze de date 2522 Administratori de sisteme 2523 Profesioniști în rețele de calculatoare	J. INFORMAȚII ȘI COMUNICAȚII 6201 Activități de programare pe calculator 6202 Activități de consultanță informatică și management al instalațiilor informatice 6209 Alte activități în domeniul tehnologiei informației și serviciilor informatice 6311 Prelucrarea datelor, găzduirea și activități conexe 6312 Portaluri web M. ACTIVITATE PROFESIONALĂ, ȘTIINȚIFICĂ ȘI TEHNICĂ 7490 Alte activități profesionale, științifice și tehnice (Consultant în securitate)

COMPETENŢE RELEVANTE CALIFICĂRII

COMPETENȚE TRANSVERSALE (CT)	**CT 1.** Gestionarea timpului și autodisciplină **CT 2.** Luarea deciziilor și leadership **CT 3.** Demonstrarea integrității, eticii și transparenței **CT 4.** Manifestarea flexibilității, adaptabilității și rezilienței	**CT 5.** Empatizarea și inteligența emoțională **CT 6.** Comunicarea eficientă, lucru în echipă și colaborarea **CT 7.** Orientarea spre învățare **CT 8.** Gestionarea informației
COMPETENȚE GENERALE (CG)	**CG 1.** Utilizarea în activitatea profesională a conceptelor, teoriilor şi metodelor ştiinţelor fundamentale **CG 2.** Operarea cu concepte de bază din ştiinţa calculatoarelor, tehnologia informaţiei şi comunicaţiilor **CG 3.** Aplicarea aspectelor de legislație, economie, marketing, afaceri și asigurare a calității în context managerial **CG 4.** Asigurarea respectării cadrului normativ în domeniul securității și sănătății în muncă și protecției mediului	
COMPETENȚE PROFESIONALE (CP)	**CP 1.** Utilizarea principiilor fundamentale ale securității informației pentru managementul strategiilor și sistemelor de securitate **CP 2.** Dezvoltarea soluțiilor de securitate pentru protecția infrastructurilor TI, aplicațiilor și datelor **CP 3.** Administrarea securității sistemelor TIC prin configurare, monitorizare și evaluare **CP 4.** Gestionarea riscurilor de securitate informațională conform standardelor și reglementărilor în vigoare	

TRANSPUNEREA COMPETENȚELOR
DIN STANDARDUL DE COMPETENȚĂ ÎN REZULTATE ALE ÎNVĂȚĂRII

Aria de competență	**Competențe generale/profesionale conform standardului de competență**	**Rezultate ale învățării conform nivelului CNC** *Absolventul/candidatul la atribuirea calificării poate:*	**Module/discipline ce conduc la formarea de competențe profesionale**
1. Elaborarea soluțiilor de securitate pentru infrastructuri TI 3. Aplicarea metodelor de protecție a datelor 5. Evaluarea vulnerabilităților și testarea securității	**CG 1.** Utilizarea în activitatea profesională a conceptelor, teoriilor şi metodelor ştiinţelor fundamentale	**1.** aplica conceptele și metodele științelor fundamentale pentru identificarea, formularea și argumentarea soluțiilor în domeniul ingineriei **2.** interpreta date colectate în proiecte de dezvoltare a produselor program și a aplicațiilor, utilizând concepte matematice, statistice și logice pentru analiza acestora	Module/discipline de matematică; fizică; metode numerice; probabilitate și statistică.
1. Elaborarea soluțiilor de securitate pentru infrastructuri TI 3. Aplicarea metodelor de protecție a datelor 4. Detectarea și gestionarea incidentelor de securitate 6. Asigurarea securității aplicațiilor și dezvoltarea sigură	**CG 2.** Operarea cu concepte de bază din ştiinţa calculatoarelor, tehnologia informaţiei şi comunicaţiilor	**3.** dezvolta produse program şi aplicaţii, utilizând conceptele de bază din știința calculatoarelor, tehnologia informației și comunicațiilor **4.** implementa proiectarea hardware-software integrată pentru a soluționa probleme tehnice și a optimiza procesele informatice	Module/discipline de limbaje și medii de programare; structuri de date și algoritmi; dispozitive electronice și numerice; arhitecturi de calculatoare; sisteme incorporate; rețele de calculatoare; securitate informațională.
2. Gestionarea riscurilor și asigurarea conformității cu standardele de securitate 7. Elaborarea politicilor și formarea în domeniul securității cibernetice 8. Managementul activităților și resurselor de securitate	**CG 3.** Aplicarea aspectelor de legislație, economie, marketing, afaceri și asigurare a calității în context managerial	**5.** elabora documentația tehnică în proiectele de dezvoltare a produselor program și a aplicațiilor, respectând reglementările și standardele specifice domeniului de activitate **6.** planifica activitățile de dezvoltare a produselor program și a aplicațiilor, asigurând conformitatea cu principiile de management, reglementările legale și cerințele de calitate	Module/discipline de legislație; economie; gestiune a proiectelor; filosofie; comunicare și comportament organizațional.

Aria de competență	Competențe generale/profesionale conform standardului de competență	Rezultate ale învățării conform nivelului CNC *Absolventul/candidatul la atribuirea calificării poate:*	Module/discipline ce conduc la formarea de competențe profesionale
2.Gestionarea riscurilor și asigurarea conformității cu standardele de securitate 7. Elaborarea politicilor și formarea în domeniul securității cibernetice 8. Managementul activităților și resurselor de securitate	**CG 4.** Asigurarea respectării cadrului normativ în domeniul securității și sănătății în muncă și protecției mediului	**7.** aplica prevederile legale privind securitatea și sănătatea în muncă (SSM) și protecția mediului în procesele de dezvoltare a produselor program și a aplicațiilor; **8.** evalua riscurile, propunând măsuri preventive pentru protecția mediului și siguranța în muncă în cadrul activităților specifice domeniului	Module/discipline de asigurare a securității și sănătății în muncă; protecția mediului.
1. Elaborarea soluțiilor de securitate pentru infrastructuri TI 2. Gestionarea riscurilor și asigurarea conformității cu standardele de securitate 7. Elaborarea politicilor și formarea în domeniul securității cibernetice 8. Managementul activităților și resurselor de securitate	**CP 1.** Utilizarea principiilor fundamentale ale securității informației pentru managementul strategiilor și sistemelor de securitate	**9.** aplica principiile fundamentale ale securității informației în dezvoltarea și implementarea strategiilor de securitate pentru protecția sistemelor informatice **10.** implementa sisteme de securitate bazate pe principiile fundamentale ale securității informației pentru protecția infrastructurilor IT și a datelor organizaționale	Module/discipline de management al securității informaționale, cadrul legal al securității informaționale; tehnologii ale securității informaționale.
1. Elaborarea soluțiilor de securitate pentru infrastructuri TI 3. Aplicarea metodelor de protecție a datelor 6. Asigurarea securității aplicațiilor și dezvoltarea sigură	**CP 2.** Dezvoltarea soluțiilor de securitate pentru protecția infrastructurilor TI, aplicațiilor și datelor.	**11.** proiecta soluții de securitate pentru protecția infrastructurilor TI, aplicațiilor și datelor împotriva amenințărilor cibernetice **12.** utiliza tehnologii și instrumente specifice pentru detectarea, prevenirea și răspunsul la incidente de securitate în cadrul infrastructurilor TI	Module/discipline de tehnologii ale securității informaționale; criptografie; ingineria inversă; sisteme de operare; rețele de calculatoare; programe malițioase; testarea produselor program.

Aria de competență	Competențe generale/profesionale conform standardului de competență	Rezultate ale învățării conform nivelului CNC *Absolventul/candidatul la atribuirea calificării poate:*	Module/discipline ce conduc la formarea de competențe profesionale
1. Elaborarea soluțiilor de securitate pentru infrastructuri TI 3. Aplicarea metodelor de protecție a datelor 4. Detectarea și gestionarea incidentelor de securitate 5. Evaluarea vulnerabilităților și testarea securității	**CP 3.** Administrarea securității sistemelor TIC prin configurare, monitorizare și evaluare.	**13.** implementa controale de securitate pentru sistemele TIC, asigurând detectarea, monitorizarea și remedierea vulnerabilităților **14.** proiecta mecanisme de audit și control al securității TIC, evaluând impactul riscurilor și implementând măsuri proactive de protecție	Module/discipline de arhitecturi de calculatoare; rețele de calculatoare; sisteme de operare; metode și mijloace tehnice de protecție a informației, arhitectura și operațiunile SOC.
2. Gestionarea riscurilor și asigurarea conformității cu standardele de securitate 4. Detectarea și gestionarea incidentelor de securitate 5. Evaluarea vulnerabilităților și testarea securității 7. Elaborarea politicilor și formarea în domeniul securității cibernetice	**CP 4.** Gestionarea riscurilor de securitate informațională conform standardelor și reglementărilor în vigoare.	**15.** analiza riscurile de securitate informațională cu evaluarea impactului acestora asupra infrastructurilor TIC, propunând măsuri de reducere a vulnerabilităților **16.** implementa strategii de gestionare a riscurilor de securitate informațională, în conformitate cu standardele și reglementările în vigoare	Module/discipline de inginerie inversă; managementul și auditul securității informaționale, baze de date; programe malițioase, răspuns la incidente.

DETALIEREA REZULTATELOR ÎNVĂȚĂRII, CORESPUNZĂTOR COMPETENȚELOR GENERALE ȘI PROFESIONALE, ÎN TERMENI DE CUNOȘTINȚE, APTITUDINI, RESPONSABILITATE ȘI AUTONOMIE ȘI STABILIREA NIVELULUI MINIM DE COMPETENȚĂ NECESAR DE ATINS/DEMONSTRAT

COMPETENȚA GENERALĂ/PROFESIONALĂ (CG/CP$_{1-N}$)			**NIVELUL MINIM DE COMPETENȚĂ NECESAR DE ATINS/DEMONSTRAT**
REZULTATE ALE ÎNVĂȚĂRII ($_{1-N}$)			
CUNOȘTINȚE (K)	**APTITUDINI (S)**	**RESPONSABILITATE ȘI AUTONOMIE (RA)**	
Rezultatele învățării, nivel 6 CNC, conform descriptorilor de definire a nivelurilor *https://europa.eu/europass/system/files/2020-05/Legal%20text-RO.pdf (Anexa II)*			
Cunoștințe avansate într-un domeniu de muncă sau de studiu, care implică **înțelegerea critică** a teoriilor și principiilor**.**	**Aptitudini avansate,** care denotă **control și inovare,** necesare pentru **a rezolva probleme complexe și imprevizibile** într-un domeniu de muncă sau de studiu specializat.	**Gestionarea de activități sau proiecte** tehnice sau profesionale **complexe,** prin **asumarea responsabilității pentru luarea deciziilor** în situații de muncă sau de studiu imprevizibile. **Asumarea responsabilității** pentru gestionarea dezvoltării profesionale a indivizilor și a grupurilor.	
CG 1. Utilizarea în activitatea profesională a conceptelor, teoriilor şi metodelor ştiinţelor fundamentale.			
Rezultatul învățării 1. *Absolventul/candidatul la atribuirea calificării poate* aplica conceptele și metodele științelor fundamentale pentru identificarea, formularea și argumentarea soluțiilor în domeniul ingineriei.			
K$_1$. Legități fizice și mecanice. **K$_2$.** Metode de analiză și modelare matematică. **K$_3$.** Modele matematice ale proceselor. **K$_4$.** Metode de simulare și optimizare a proceselor. **K$_5$.** Principii, legi fundamentale și	**S$_1$.** Explică problemele inginerești prin noțiunile, legile și teoriile fundamentale din fizica clasică și modernă. **S$_2$.** Descrie metodele de analiză și modelare matematică pentru soluționarea problemelor inginerești. **S$_3$.** Descrie principalele modele matematice ale comportamentului proceselor fizice și a mecanismelor. **S$_4$.** Aplică metode de simulare și optimizare a proceselor.	Absolventul identifică autonom soluțiile în domeniul ingineriei, fiind responsabil de argumentele aduse în baza conceptelor și	Absolventul: - descrie metodele de analiză și modelare matematică; - stabilește legitățile fizice și mecanice;

fenomene specifice circuitelor electrice.	**S5.** Interpretează principalele noțiuni și legi specifice ale circuitelor electrice.	metodelor științelor fundamentale.	- interpretează principalele noțiuni și legi specifice ale circuitelor electrice.
Rezultatul învățării 2. *Absolventul/candidatul la atribuirea calificării poate* interpreta date colectate în proiecte de dezvoltare a produselor program și a aplicațiilor, utilizând concepte matematice, statistice și logice pentru analiza acestora.			
K1. Tehnici de analiză statistică. **K2.** Metode de modelare probabilistică și inferență statistică. **K3.** Relații și operații ale algebrei relaționale. **K4.** Noțiuni specifice din teoria grafurilor. **K5.** Principii de vizualizare a datelor și interpretare grafică a rezultatelor.	**S1.** Utlizează tehnici de analiză statistică aplicate în analiza și prelucrarea datelor experimentale și teoretice. **S2.** Aplică metode de modelare probabilistică și inferență statistică în luarea deciziilor. **S3.** Utilizează relații și operații ale algebrei relaționale în gestionarea bazelor de date. **S4.** Analizează structuri de date complexe utilizând teoria grafurilor. **S5.** Utilizează principii de vizualizare a datelor și interpretare grafică a rezultatelor.	Absolventul interpretează autonom datele experimentale și teoretice, fiind responsabil de utilizarea conceptelor matematice, statistice și logice în analiza acestora.	Absolventul: - explică tehnicile de analiză statistică aplicate în analiza și prelucrarea datelor; - identifică tipurile de grafuri; - utilizează principii de vizualizare și interpretare a datelor.
CG 2. Operarea cu concepte de bază din ştiinţa calculatoarelor, tehnologia informaţiei şi comunicaţiilor.			
Rezultatul învățării 3. *Absolventul/candidatul la atribuirea calificării poate* dezvolta produse program şi aplicaţii, utilizând conceptele de bază din știința calculatoarelor, tehnologia informației și comunicațiilor.			
K1. Legi și axiome ale algebrei booleene. **K2.** Metode de sinteză a circuitelor logice. **K3.** Fundamentele arhitecturii calculatoarelor și organizarea sistemelor de calcul. **K4.** Principii și structuri ale sistemelor de operare. **K5.** Topologii și echipamente ale reţelelor de calculatoare. **K6.** Modele și protocoale de comunicații în rețelele informatice. **K7.** Limbaje, medii şi tehnologii de programare. **K8.** Structuri de date și algoritmi.	**S1.** Clasifică circuitele logice. **S2.** Identifică metodele de sinteză a circuitelor logice, aplicând legile și axiomele algebrei booleene. **S3.** Selectează arhitecturile sistemelor de calcul în funcție de structura și caracteristicile acestora. **S4.** Analizează componentele sistemelor de operare pentru gestionarea eficientă a resurselor software și hardware. **S5.** Definește topologia și echipamentele rețelelor de calculatoare potrivite pentru comunicații optimale de date. **S6.** Aplică protocoale de comunicație pentru optimizarea transferului de date în rețelele informatice. **S7.** Utilizează limbajele, mediile și tehnologiile de programare pentru dezvoltarea aplicațiilor software.	Absolventul dezvoltă autonom produse program şi aplicaţii, fiind responsabil de aplicarea corectă a conceptelor de bază din știința calculatoarelor, tehnologia informației și comunicațiilor.	Absolventul: - identifică metodele de sinteză a circuitelor logice; - clasifică arhitecturile sistemelor de calcul; - definește topologia și echipamentele rețelelor de calculatoare; - identifică limbajele, mediile și tehnologiile de programare.

K9. Concepte de securitate cibernetică și protecție a datelor în sistemele informatice. **K10.** Sisteme de gestiune a bazelor de date.	**S8**. Implementează structuri de date și algoritmi pentru optimizarea performanței aplicațiilor. **S9**. Aplică tehnici de securitate cibernetică pentru protejarea datelor și a sistemelor informatice. **S10**. Elaborează baze de date, utilizând sisteme de gestiune a acestora, pentru stocarea și gestionarea eficientă a informației.		
Rezultatul învățării 4. *Absolventul/candidatul la atribuirea calificării poate* implementa proiectarea hardware-software integrată pentru a soluționa probleme tehnice și a optimiza procesele informatice.			
K1. Principii de sinteză și analiză a circuitelor și schemelor logice. **K2**. Metode de implementare a structurilor sistemelor de calcul. **K3**. Principii de gestionare a memoriei, magistralelor și interfețelor calculatorului. **K4.** Criterii de elaborare a arhitecturilor rețelelor de calculatoare. **K5**. Principii de funcționare a componentelor arhitecturale și de infrastructură a rețelelor de calculatoare. **K6.** Principii de proiectare și integrare hardware-software. **K7.** Arhitecturi de microcontrolere și sisteme embedded. **K8.** Interfațarea hardware și comunicarea dintre componentele electronice și software. **K9.** Tehnologii IoT. **K10.** Modelarea și simularea proceselor hardware-software.	**S1**. Proiectează circuite logice utilizând metode de sinteză și analiză a schemelor digitale. **S2**. Implementează structuri ale sistemelor de calcul, optimizând performanța resurselor hardware și software. **S3**. Configurează arhitecturi ale rețelelor de calculatoare. **S4**. Selectează componentele arhitecturale hardware, software și de comunicații ale rețelelor de calculatoare. **S5.** Proiectează și integrează componente hardware și software pentru sisteme informatice performante. **S6.** Configurează arhitecturi de microcontrolere și sisteme embedded pentru aplicații specifice. **S7.** Dezvoltă și implementează soluții de interfațare între componente hardware și software. **S8.** Utilizează tehnologii IoT pentru integrarea sistemelor informatice distribuite. **S9.** Simulează și validează modele hardware-software pentru optimizarea funcționalității sistemelor informatice.	Absolventul autonom propune soluții pentru problemele tehnice prin proiectarea hardware-software integrată, fiind responsabil de nivelul atins în optimizarea proceselor informatice.	Absolventul: - proiectează circuite logice; - implementează structuri ale sistemelor de calcul; - configurează arhitecturi ale rețelelor de calculatoare; - selectează componentele de bază ale rețelelor de calculatoare; - integrează componente hardware și software pentru sisteme informatice.
CG 3. Aplicarea aspectelor de legislație, economie, marketing, afaceri și asigurare a calității în context managerial.			
Rezultatul învățării 5. *Absolventul/candidatul la atribuirea calificării poate* elabora documentația tehnică în proiectele de dezvoltare a produselor program și a aplicațiilor, respectând reglementările și standardele specifice domeniului de activitate.			

K1. Principii de redactare a documentației tehnice pentru produsele software. **K2.** Prevederile actelor normative, standardelor și reglementărilor specifice domeniului dezvoltării produselor program. **K3.** Aspectele legale privind protecția intelectuală și drepturile de autor. **K4.** Metode și instrumente de gestionare a versiunilor documentației tehnice. **K5.** Principii de management al proiectelor. **K6.** Concepte economice și indicatori ai eficienței economice. **K7.** Principiile, funcțiile și standardele de management a calității. **K8.** Metodologii Total Quality Management (TQM) în documentarea și optimizarea proceselor software.	**S1.** Elaborează documentația tehnică conform metodologiilor, cerințelor funcționale și tehnice ale proiectelor software. **S2.** Aplică standardele internaționale, reglementările specifice și prevederile actelor normative în procesul de realizare și implementare a proiectelor software. **S3.** Utilizează metode și instrumente de gestionare a versiunilor pentru actualizarea, organizarea și trasabilitatea documentației tehnice. **S4.** Planifică și documentează etapele de proiectare și implementare a produselor software, optimizând utilizarea resurselor tehnologice și umane. **S5.** Estimează costurile de realizare și implementare a proiectelor software, luând în considerare indicatorii eficienței economice și principiile managementului resurselor. **S6.** Verifică și validează conformitatea documentației tehnice cu cerințele proiectului, normele de asigurare a calității și sistemele de management al calității (ISO, TQM). **S7.** Aplică aspecte legale privind protecția drepturilor de autor, proprietatea intelectuală și respectarea reglementărilor în dezvoltarea software. **S8.** Documentează fazele tehnologice critice, defectele potențiale și cauzele acestora, stabilind măsuri de prevenire pentru asigurarea calității produselor software.	Absolventul elaborează autonom documentația tehnică în proiectele de dezvoltare a produselor program și a aplicațiilor, asumându-şi responsabilitatea pentru respectarea reglementărilor și standardelor în vigoare.	Absolventul: - elaborează documentația tehnică pentru proiectele specifice domeniului; - aplică prevederile actelor normative și a standardelor specifice domeniului; - estimează costurile de realizare și implementare a proiectelor; - interpretează corect procedurile operaționale specifice sistemului de management al calității.
Rezultatul învățării 6. *Absolventul/candidatul la atribuirea calificării poate* coordona activitățile de dezvoltare a produselor program și a aplicațiilor, asigurând conformitatea cu principiile de management, reglementările legale și cerințele de calitate.			
K1. Principii de management al proiectelor software. **K2.** Norme și reglementări legale aplicabile în dezvoltarea, comercializarea și protecția juridică a produselor software.	**S1.** Aplică documentația specifică organizării procesului de execuție și implementare a proiectelor software. **S2.** Analizează conformitatea activităților și documentațiilor cu normele legislative, economice, manageriale și de asigurare a calității în domeniul dezvoltării software.	Absolventul planifică autonom activitățile de dezvoltare a produselor program și a aplicațiilor, fiind responsabil de asigurarea conformității	Absolventul: - interpretează documentația specifică organizării procesului de execuţie şi

K3. Metode și tehnici de planificare, alocare a resurselor și monitorizare a activităților în proiectele software. **K4.** Principii de management financiar aplicate în evaluarea costurilor proiectelor software. **K5.** Strategii de leadership, formare și motivare a personalului. **K6.** Metode, tehnici și instrumente de management al calității. **K7.** Strategii de îmbunătățire continuă a calității produsului final. **K8.** Acte normative și standarde aplicabile în domeniul dezvoltării produselor program. **K9.** Principii de etică profesională. **K10.** Tehnici de comunicare și negociere.	**S3.** Realizează etapele de proiectare, execuție și implementare a produselor software, asigurând optimizarea proceselor. **S4.** Asigură utilizarea eficientă a tehnologiilor, instrumentelor software, echipamentelor, resurselor financiare și resurselor umane în cadrul proiectelor. **S5.** Implementează tehnici, metode și instrumente specifice managementului calității pentru dezvoltarea produselor software. **S6.** Aplică procedurile sistemului de management al calității pentru asigurarea conformității produselor software cu standardele în vigoare. **S7.** Aplică principii de leadership, etică profesională și tehnici de comunicare eficientă pentru gestionarea echipelor și a relațiilor cu colegii sau echipa de proiect.	cu principiile de management, reglementările legale și cerințele de calitate.	implementare a proiectelor software; - planifică activitățile specifice proceselor de proiectare și implementare a sistemelor informatice; - utilizează eficient tehnologiile, instrumentele software; - aplică procedurile sistemului de management al calității.
CG 4. Asigurarea respectării cadrului normativ în domeniul SSM și protecției mediului.			
Rezultatul învățării 7. *Absolventul/candidatul la atribuirea calificării poate* aplica prevederile legale privind securitatea și sănătatea în muncă (SSM) și protecția mediului în procesele de dezvoltare a produselor program și a aplicațiilor.			
K1. Legislația și actele normative în domeniul SSM și protecției mediului. **K2.** Principii de organizare a activității în domeniul SSM pentru asigurarea unui mediu de lucru sigur. **K3.** Cerințe normative privind ergonomia și siguranța echipamentelor. **K4.** Reglementări privind gestionarea sustenabilă a resurselor și reducerea impactului ecologic în activitățile din domeniul.	**S1.** Identifică prevederile legislației și actelor normative privind SSM și protecția mediului în domeniul dezvoltării software. **S2.** Aplică normele specifice SSM și protecției mediului în cadrul activităţilor de laborator. **S3.** Respectă cerințele normative privind ergonomia și siguranța echipamentelor utilizate. **S4.** Implementează măsuri pentru gestionarea sustenabilă a resurselor și reducerea impactului ecologic în activitățile de dezvoltare, implementare și utilizare a produselor program.	Absolventul aplică autonom prevederile legale privind securitatea și sănătatea în muncă (SSM) și protecția mediului în procesele de dezvoltare a produselor program și a aplicațiilor, fiind responsabil de identificarea măsurilor optime pentru gestionarea sustenabilă a resurselor și reducerea impactului ecologic.	Absolventul: - identifică actele normative de bază în domeniul SSM și protecției mediului ambiant; - aplică normele specifice SSM și protecției mediului în cadrul activităţilor de laborator.

Rezultatul învățării 8. *Absolventul/candidatul la atribuirea calificării poate* evalua riscurile, propunând măsuri preventive pentru protecția mediului și siguranța în muncă în cadrul activităților specifice domeniului.			
K1. Factori nocivi și periculoși în mediul de activitate și măsuri de prevenire a acestora. **K2.** Metode și tehnici de analiză a riscurilor profesionale și de mediu. **K3.** Cerințe normative pentru protecția mediului și gestionarea responsabilă a echipamentelor. **K4.** Tehnici de monitorizare și control a calității mediului de muncă.	**S1.** Analizează factorii nocivi și periculoși din mediul de activitate pentru prevenirea accidentelor de muncă și a riscurilor profesionale. **S2.** Aplică metode și tehnici de analiză a riscurilor pentru siguranța persoanelor și protecția mediului. **S3.** Determină condițiile optime de microclimat, nivelul de zgomot, intensitatea vibrațiilor și iluminarea la locurile de muncă. **S4.** Respectă cerințele normative privind protecția mediului și gestionarea responsabilă a echipamentelor tehnologice. **S5.** Propune măsuri de optimizare a siguranței la locul de muncă și reducerea impactului ecologic al activităților.	Absolventul autonom evaluează riscurile, fiind responsabil de eficienţa măsurilor preventive propuse pentru protecția mediului și siguranța în muncă în cadrul activităților specifice domeniului.	Absolventul: - identifică factorii nocivi și periculoși din mediul de activitate; - aplică metode și tehnici de analiză a riscurilor pentru siguranța persoanelor și protecția mediului; - determină condițiile optime de microclimat, nivelul de zgomot, intensitatea vibrațiilor și iluminarea la locurile de muncă.
CP 1. Utilizarea principiilor fundamentale ale securității informației pentru managementul strategiilor și sistemelor de securitate.			
Rezultatul învățării 9. *Absolventul/candidatul la atribuirea calificării poate* aplica principiile fundamentale ale securității informației în dezvoltarea și implementarea strategiilor de securitate pentru protecția sistemelor informatice.			
K1. Principii fundamentale ale securității informației – confidențialitate, integritate, disponibilitate. **K2.** Standarde internaționale în securitatea informației – ISO/IEC 27001, NIST, ETSI, GDPR. **K3.** Modele de învățare automată (Machine Learning - ML) aplicate securității. **K4.** Arhitecturi, politici și modele de securitate. **K5.** Proceduri de securitate. **K6**. Cadrul legal național și european al securității informaționale. **K7.** Managementul resurselor.	**S1.** Analizează politici, standarde, metodologii și cadre de securitate. **S2.** Elaborează propuneri pentru implementarea strategiei de securitate pentru protecția sistemelor informatice. **S3.** Inițiază și implementează proceduri de securitate potrivite pentru protecția sistemelor informatice. **S4.** Asigură confomitatea cu legislația în vigoare. **S5.** Aplică modele de maturitate pentru managementul securității informațiilor. **S6.** Identifică și rezolvă probleme aferente securității informațiilor. **S7.** Selectează resursele necesare implementării strategiei de securitate.	Absolventul aplica autonom principiile fundamentale ale securității informației în dezvoltarea și implementarea strategiilor de securitate pentru protecția sistemelor informatice, fiind responsabil pde aplicarea bazei normative aferente procesului.	Absolventul: - aplică principiile de securitate; - determină strategia de securitate; - implementează modele, cadre, standarde și proceduri; - identifică indicatori de evaluare a nivelului de implementare a strategiei de securitate.

K8. Standarde de management al riscului, metodologii și cadre.			
Rezultatul învățării 10. *Absolventul/candidatul la atribuirea calificării poate* implementa sisteme de securitate, bazate pe principiile fundamentale ale securității informației, pentru protecția infrastructurilor TI și a datelor organizaționale.			
K1. Modele de referință ale arhitecturilor de securitate. **K2.** Standarde, metodologii, cadre și recomandări de securitate. **K3.** Controale de securitate. **K4.** Metodologii de evaluare și management al riscurilor și amenințărilor de securitate. **K5.** Tehnologii și soluții de securitate. **K6.** Standarde, metodologii și cadre pentru confidențialitate prin concepție. **K7.** Inteligența artificială pentru detecția intruziunilor.	**S1.** Analizează funcționalitatea sistemului de management al securității informației (SMSI) al organizației. **S2.** Elaborează specificații arhitecturale și funcționale pentru asigurarea securității informației. **S3.** Proiectează sisteme și arhitecturi bazate pe principiile de securitate prin design și implicit. **S4.** Analizează sistemele de securitate pentru a dezvolta cerințe de securitate și a identifica soluții eficiente. **S5.** Selectează specificații și controale de securitate adecvate. **S6.** Planifică integrarea soluțiilor de securitate. **S7.** Implementează și îmbunătățește algoritmii de detecție a intruziunilor folosind AI.	Absolventul implementează autonom sisteme de securitate, fiind responsabil de nivelul de protecție a infrastructurilor TI și a datelor organizaționale asigurat de acestea.	Absolventul: - aplică modele, arhitecturi și cadre de securitate; - dezvoltă și implementează sisteme de management al securității informației; - analizează performanțele sistemului proiectat.
CP 2. Dezvoltarea soluțiilor de securitate pentru protecția infrastructurilor TI, aplicațiilor și datelor.			
Rezultatul învățării 11. *Absolventul/candidatul la atribuirea calificării poate* proiecta soluții de securitate pentru protecția infrastructurilor TI, aplicațiilor și datelor împotriva amenințărilor cibernetice.			
K1. Principii de funcționare și caracteristici tehnice ale tehnologiilor de securitate. **K2.** Securitatea rețelelor de calculatoare. **K3.** Modelarea sistemelor și programare. **K4.** Ciclul de viață al dezvoltării securizate. **K5.** Principii de securitate a sistemelor de operare. **K6.** Soluții și controale de securitate. **K7.** Practici de securitate ofensivă și defensivă. **K8.** Standarde, metodologii, cadre și proceduri de testare.	**S1.** Integrează soluțiile de securitate informațională în infrastructura TI. **S2.** Configurează soluțiile de securitate conform cerințelor stabilite. **S3.** Evaluează securitatea și performanța soluțiilor. **S4.** Identifică și rezolvă probleme specifice de securitate. **S5.** Colaborează cu ceilalți membri ai echipei în cadrul proiectelor comune. **S6.** Elaborează și implementează teste de penetrare pentru evaluarea sistemului de securitate. **S7.** Implementează tehnologii AI pentru protecția aplicațiilor, infrastructurilor TI, datelor.	Absolventul proiectează autonom soluții de securitate pentru protecția infrastructurilor TI, aplicațiilor și datelor împotriva amenințărilor cibernetice, fiind responsabil de performanța acestora.	Absolventul: - determină tehnologiile și soluțiile de securitate potrivite; - configurează sistemele TIC pentru a asigura securitatea conform cerințelor de performanță impuse; - asigură mentenanța și actualizarea securității sistemelor, serviciilor și produselor;

K9. Tehnici și metode de protecție a datelor. **K10.** Modele de inteligență artificială utilizate pentru protecția datelor și infrastructurilor TIC.	**S8.** Utilizează modele și tehnologii AI pentru testele de penetrare.		- implementează și monitorizează controale și proceduri de securitate; - implementează, aplică și gestionează corecțiile de securitate
Rezultatul învățării 12. *Absolventul/candidatul la atribuirea calificării poate* utiliza tehnologii și instrumente specifice pentru detectarea, prevenirea și răspunsul la incidente de securitate în cadrul infrastructurilor TI.			
K1. Tehnici de inginerie inversă. **K2.** Tipuri de atacuri cibernetice și programe malițioase, actorii amenințărilor de securitate. **K3.** Standarde, metodologii și cadre pentru gestionarea incidentelor de securitate. **K4.** Tehnologii de securitate pentru răspunsul la incidentele cibernetice. **K5.** Principii de securitate pentru sistemele de operare și rețelele de calculatoare. **K6.** Vulnerabilități ale sistemelor, serviciilor și produselor. **K7.** Principii de învestigare a incidentelor de securitate. **K8.** Proceduri automatizate de gestionare a amenințărilor de securitate și răspunsul la incidente.	**S1.** Definește principiile de funcţionare, caracteristicile tehnice necesare și cerinţele standardelor aplicabile pentru tehnologiile de securitate. **S2.** Dezvoltă și evaluează proceduri pentru managementul incidentelor de securitate. **S3.** Evaluează și gestionează vulnerabilitățile tehnice ale sistemului informatic. **S4.** Evaluează reziliența sistemelor TIC, a controalelor de securitate, precum și acțiuni de atenuare a impactului post-incident. **S5.** Dezvoltă și implementează tehnici de testare pentru gestionarea incidentelor. **S6.** Stabilește proceduri pentru analiza rezultatelor incidentelor. **S7.** Automatizează procedurile de gestionare a informațiilor despre amenințările de securitate. **S8.** Implementează și îmbunătățește algoritmii de detecție a intruziunilor folosind AI.	Absolventul utilizează autonom tehnologii și instrumente specifice pentru detectarea, prevenirea și răspunsul la incidente de securitate în cadrul infrastructurilor TI, fiind responsabil de modul de gestionare a informațiilor despre amenințările de securitate.	Absolventul: - definește principiile de funcţionare, caracteristicile tehnice necesare și cerinţele standardelor aplicabile pentru tehnologiile de securitate; - integrează tehnologii de securitate specifice pentru răspunsul la incidentele de securitate; - automatizează procesul de răspuns la incidente și evaluează performanța controalelor și procedurilor implementate.

CP 3. Administrarea securității sistemelor TIC prin configurare, monitorizare și evaluare.			
Rezultatul învățării 13. *Absolventul/candidatul la atribuirea calificării poate* implementa controale de securitate pentru sistemele TIC, asigurând detectarea, monitorizarea și remedierea vulnerabilităților.			
K1. Principii fundamentale ale securității informaționale și arhitecturilor de protecție TIC. **K2.** Metode și tehnologii de monitorizare a securității sistemelor TIC. **K3.** Protocoale și mecanisme de detecție a intruziunilor și atacurilor cibernetice (IDS/IPS). **K4.** Proceduri de evaluare a vulnerabilităților și implementarea măsurilor de mitigare. **K5.** Modele de inteligență artificială pentru managementul vulnerabilităților. **K6.** Politici și proceduri de securitate a informației, conform standardelor și reglementărilor în vigoare. **K7.** Tehnici de configurare și securizare a sistemelor de operare și a infrastructurii TIC.	**S1.** Clasifică tipurile de amenințări cibernetice și măsurile de protecție aplicabile sistemelor TIC. **S2.** Determină nivelul de securitate al unui sistem TIC prin analiza configurărilor și a politicilor de acces. **S3.** Elaborează strategii de detecție și răspuns la incidente de securitate utilizând sisteme de monitorizare și analiză. **S4.** Reprezintă arhitectura tehnologiilor de securitate implementate într-un sistem TIC, incluzând firewall-uri, IDS/IPS și VPN-uri. **S5.** Analizează jurnalele de evenimente și traficul de rețea pentru identificarea anomaliilor și potențialelor atacuri cibernetice. **S6.** Selectează soluțiile optime pentru remedierea vulnerabilităților identificate în sistemele TIC. **S7.** Validează conformitatea măsurilor de securitate cu standardele și reglementările în vigoare. **S8.** Optimizează mecanismele de protecție a infrastructurilor TIC prin configurarea și actualizarea politicilor de securitate. **S9.** Testează eficacitatea măsurilor de protecție implementate, utilizând instrumente specifice de audit și scanare a vulnerabilităților. **S10.** Implementează controale de securitate pentru protejarea infrastructurilor TIC și a datelor confidențiale. **S11.** Implementează algoritmi de AI pentru identificarea și gestionarea vulnerabilităților în sisteme informatice.	Absolventul configurează și monitorizează autonom controale de securitate pentru sistemele TIC, evaluând și remediind vulnerabilitățile pentru asigurarea protecției infrastructurii informatice, fiind responsabil de nivelul de securitate al sistemului şi eficacitatea măsurilor de protecție implementate.	Absolventul: - implementează controale de securitate a sistemelor TIC și le monitorizează; - aplică tehnici de detecție, prevenire și remediere a vulnerabilităților în infrastructurile TIC; - implementează protocoale și mecanisme de securitate pentru protecția rețelelor și sistemelor informatice; - elaborează strategii de monitorizare și răspuns la incidente de securitate cibernetică.

Rezultatul învățării 14. *Absolventul/candidatul la atribuirea calificării* poate proiecta mecanisme de audit și control al securității TIC, evaluând impactul riscurilor și implementând măsuri proactive de protecție.			
K1. Principii și metodologii de audit al securității informaționale. **K2.** Indicatori și metrici pentru evaluarea eficienței măsurilor de securitate TIC. **K3.** Procese și tehnici de gestionare a jurnalelor de evenimente și analizei log-urilor. **K4.** Metode de identificare și analiză a riscurilor de securitate informațională. **K5.** Tehnici și instrumente de detecție și analiză a comportamentului anormal în rețele și sisteme. **K6.** Proceduri de audit și conformitate cu standardele de securitate cibernetică (ISO 27001, NIST, CIS Controls). **K7.** Strategii de prevenire a incidentelor și planificare a măsurilor proactive de protecție. **K8.** Principii de investigare și răspuns la incidente de securitate cibernetică. **K9.** Metode de testare a securității sistemelor TIC și analiza post-incident. **K10.** Aspecte legislative și etice privind monitorizarea și auditul securității informaționale.	**S1.** Clasifică tipurile de audit și metodele de control utilizate în securitatea TIC. **S2.** Determină indicatorii și metricile relevante pentru evaluarea eficienței măsurilor de securitate. **S3.** Elaborează strategii de colectare, analiză și interpretare a jurnalelor de securitate și a log-urilor de evenimente. **S4.** Reprezintă diagrame și structuri de audit al securității sistemelor TIC. **S5.** Analizează riscurile de securitate și impactul acestora asupra infrastructurilor TIC. **S6.** Selectează metode și instrumente pentru monitorizarea și auditul sistemelor informatice. **S7.** Validează conformitatea sistemelor TIC cu standardele de securitate și reglementările în vigoare. **S8.** Optimizează procesele de detectare a amenințărilor și planifică măsuri de protecție proactivă. **S9.** Testează măsurile de securitate și identifică posibile vulnerabilități prin audituri interne. **S10.** Implementează proceduri de răspuns la incidente și măsuri corective pentru prevenirea atacurilor cibernetice.	Absolventul proiectează autonom mecanisme de audit și control al securității TIC, evaluând riscurile și implementând măsuri proactive pentru prevenirea incidentelor de securitate, fiind responsabil de conformitatea sistemelor TIC cu standardele de securitate și reglementările în vigoare.	Absolventul: - clasifică tipurile de audit și metodele de control utilizate în securitatea TIC. - aplică tehnici și proceduri pentru colectarea și analiza jurnalelor de evenimente; - implementează mecanisme de detecție și răspuns la incidente de securitate; - elaborează planuri de audit și strategii de monitorizare a securității sistemelor TIC.

CP 4. Gestionarea riscurilor de securitate informațională conform standardelor și reglementărilor în vigoare.			
Rezultatul învățării 15. *Absolventul/candidatul la atribuirea calificării* poate analiza riscurile de securitate informațională cu evaluarea impactului acestora asupra infrastructurilor TIC, propunând măsuri de reducere a vulnerabilităților.			
K1. Principii fundamentale ale managementului riscurilor de securitate informațională. **K2.** Tipuri de amenințări și atacuri cibernetice asupra infrastructurilor TIC. **K3.** Metode și modele de analiză a riscurilor de securitate informațională. **K4.** Indicatori și metrici pentru evaluarea riscurilor cibernetice. **K5.** Standarde și cadre de referință utilizate în gestionarea riscurilor (ISO 27005, NIST RMF, OCTAVE, FAIR). **K6.** Procese de identificare, clasificare și prioritizare a riscurilor de securitate. **K7.** Corelări ale riscurilor de securitate cu cerințele de conformitate și reglementările aplicabile. **K8.** Măsuri tehnice și administrative pentru reducerea vulnerabilităților și atenuarea riscurilor. **K9.** Tehnici de automatizare a procesului de gestionare a riscurilor de securitate. **K10.** Modele și metode de raportare a riscurilor și incidentelor de securitate în cadrul organizațiilor.	**S1.** Clasifică riscurile de securitate informațională în funcție de impact și probabilitate. **S2.** Determină amenințările cibernetice și punctele vulnerabile ale infrastructurilor TIC. **S3.** Elaborează analize de risc utilizând metode și cadre de referință standardizate. **S4.** Reprezintă diagrame de evaluare a riscurilor și corelarea acestora cu măsurile de securitate. **S5.** Analizează impactul potențial al riscurilor asupra infrastructurii TIC și proceselor organizaționale. **S6.** Selectează metode adecvate pentru identificarea și evaluarea riscurilor de securitate informațională. **S7.** Validează scenariile de risc prin simulări și teste de penetrare. **S8.** Optimizează strategiile de gestionare a riscurilor în funcție de tendințele actuale de securitate. **S9.** Testează eficiența măsurilor de reducere a vulnerabilităților prin evaluări periodice. **S10.** Implementează proceduri de management al riscurilor în conformitate cu reglementările în vigoare. **S11.** Utilizează algoritmi de detecție a anomaliilor pentru a analiza comportamentele neobișnuite în rețelele informatice și pentru a semnala riscuri emergente.	Absolventul analizează autonom riscurile de securitate informațională, fiind responsabil de evaluarea impactului acestora asupra infrastructurilor TIC și de măsurile propuse pentru reducerea vulnerabilităților.	Absolventul: - clasifică riscurile de securitate informațională în funcție de severitate și probabilitate; - aplică metode de identificare și analiză a vulnerabilităților în infrastructurile TIC; - descrie și utilizează modele de evaluare a riscurilor conform standardelor internaționale; - elaborează rapoarte de analiză a riscurilor și propune măsuri de reducere a acestora; - analizează impactul amenințărilor cibernetice asupra infrastructurii TIC și recomandă soluții.

Rezultatul învățării 16. *Absolventul/candidatul la atribuirea calificării poate* implementa strategii de gestionare a riscurilor de securitate informațională, în conformitate cu standardele și reglementările în vigoare.			
K1. Strategii și metodologii de gestionare a riscurilor cibernetice. **K2.** Procese și etape ale ciclului de gestionare a riscurilor. **K3.** Tehnici și metode de optimizare a măsurilor de securitate și reducere a riscurilor. **K4.** Indicatori și metrici pentru măsurarea eficienței strategiilor de gestionare a riscurilor. **K5.** Politici de securitate și strategii de management al riscurilor. **K6.** Modele de inteligență artificială pentru analiza și implementarea conformității. **K7.** Tehnici de luare a deciziilor privind prioritizarea riscurilor și măsurilor de protecție. **K8.** Reglementări și cerințe de conformitate în domeniul gestionării riscurilor de securitate informațională. **K9.** Metode de audit și evaluare a eficienței strategiilor de gestionare a riscurilor.	**S1.** Determină strategiile adecvate de gestionare a riscurilor pentru diverse infrastructuri TIC. **S2.** Elaborează planuri de management al riscurilor conform standardelor și reglementărilor aplicabile. **S3.** Reprezintă diagrame și structuri de gestionare a riscurilor pentru implementarea strategiilor de securitate. **S4.** Analizează eficiența măsurilor de securitate implementate și propune îmbunătățiri. **S5.** Selectează metode și instrumente de analiză și reducere a riscurilor cibernetice. **S6.** Validează conformitatea strategiilor de gestionare a riscurilor cu cerințele legale și operaționale. **S7.** Optimizează politicile și procedurile de securitate pentru reducerea riscurilor. **S8.** Testează strategiile implementate prin simulări și audituri de securitate. **S9.** Implementează măsuri de securitate pentru prevenirea amenințărilor cibernetice și reducerea expunerii la riscuri. **S10.** Utilizează AI pentru procesarea limbajului natural (NLP) pentru a analiza documentele de politici și reglementări și pentru a evalua conformitatea cu standardele de securitate.	Absolventul implementează și optimizează autonom strategii de gestionare a riscurilor de securitate informațională, asigurând conformitatea cu standardele și reglementările în vigoare și adoptând măsuri proactive pentru protecția infrastructurilor TIC. eficiența măsurilor de securitate implementate și propune îmbunătățiri	Absolventul: - clasifică și evaluează riscurile de securitate informațională; - aplică metode și tehnici de gestionare a riscurilor pentru protecția infrastructurilor TIC; - descrie și implementează strategii de reducere a riscurilor cibernetice; - elaborează politici și proceduri de securitate în conformitate cu standardele și reglementările actuale.

CERINȚE ȘI CRITERII DE EVALUARE
A REZULTATELOR ÎNVĂȚĂRII ÎN VEDEREA ATRIBUIRII CALIFICĂRII

1. CERINȚE GENERALE

Nr. crt.	Cerințe	Descriptori
1.	**Condiții de admitere pentru evaluarea finală**	Realizarea integrală a Planului de învățământ cu acumularea creditelor aferente disciplinelor/modulelor obligatorii și opționale urmate.
2.	**Forma de evaluare finală a rezultatelor învățării**	Susținerea examenului și/sau tezei/proiectului de licență (art. 89 (6), Codul Educației al RM).
3.	**Condiții organizatorice de realizare a evaluării finale și certificării calificării**	Organizarea și desfășurarea examenului de finalizare a studiilor superioare de licență trebuie să fie conforme prevederilor cadrului normativ. Pentru desfășurarea examenului de licență se constituie Comisii pentru de licență pe domenii de formare profesională/specialități. Subiectele pentru probele examenului de licenţă sunt elaborate de departamentele/catedrele de specialitate, în baza programelor în vigoare. Tematica proiectelor de licenţă este elaborată la departamentele/catedrele de specialitate şi aprobată de către Consiliul facultăţii. Coordonarea activităților de elaborare a proiectului de licență se realizează de un conducător/îndrumător de proiect. Probele examenului de licență pot fi susținute în scris, oral, combinat, asistate de calculator. Susținerea proiectelor de licență este publică. Susținerea probelor examenului de licență are loc în cadrul instituției organizatoare desemnate. În cazul susţinerii probelor în scris codificarea lucrărilor/testelor este obligatorie. Lucrările/testele se decodifică numai după finalizarea acţiunii de verificare a tuturor lucrărilor şi după înscrierea rezultatelor pe lista de examinare, în dreptul codului respectiv, în prezenţa membrilor Comisiei. La susținerea publică, în comisie sunt admise proiectele de licență care au îndeplinit criteriile verificării la plagiat.
4.	**Cerințe generale față de modalitatea de evaluare și instrumentele utilizate în procesul de evaluare**	Proba teoretică a examenului de licență permite evaluarea nivelului de atingere a rezultatelor învățării stabilite prin prezentul standard de calificare. În calitate de instrument de evaluare se utilizează bilete de examinare/teste de evaluare, elaborate în baza subiectelor teoretice, incluzând cel puțin o sarcină practică. Proiectul de licență permite evaluarea competențelor absolvenților de a efectua studii în vederea conceptualizării, proiectării și/sau realizării și implementării sistemelor de securitate, destinate protecției infrastructurii TIC a organizațiilor. În procesul evaluării, proiectul de licență va fi apreciat conform următoarelor criterii: realizarea studiului/cercetării propriu-zise, conținutul și forma prezentării lucrării, susținerea proiectului de licență (prezentarea cercetării, utilizarea mijloacelor tehnice, discuțiile la subiect).

Nr. crt.	Cerințe	Descriptori
5.	**Cerințe generale față de evaluatori**	Comisia de licență se constituie din președinte, vicepreședinte, 3 membri ai comisiei (examinatori) și secretar. În componența Comisiei de licență pot fi incluse persoane cu titlu științific și titlu ştiinţifico-didactic de la departamentele/catedrele de specialitate din cadrul instituției organizatoare/din alte instituții de învățământ superior sau cercetători științifici din instituții de cercetare-dezvoltare. Se permite includerea în componența Comisiei de licență a unui specialist practician de înaltă calificare, cu experiență bogată și autoritate profesională. În calitate de președinte al comisiei de licență pot fi desemnați specialiști în domeniul respectiv (profesori universitari, conferențiari universitari, cercetători științifici, deținători ai titlurilor onorifice, specialiști practicieni de înaltă calificare), care nu activează în cadrul instituției vizate. Aceeași persoană poate fi numită președinte al unei Comisii de licență nu mai mult de doi ani consecutiv.
6.	**Cerințe normative privind certificarea calificării**	În baza promovării examenului de licență se acordă titlul și calificarea de Inginer licențiat cu eliberarea Diplomei de studii superioare de licență. Diploma de studii superioare de licență atestă că titularul acesteia a atins rezultatele învățării conform prezentului standard și poate continua studiile la ciclul II sau se poate angaja în câmpul muncii conform calificării atribuite. Diploma de studii superioare de licență este însoțită de suplimentul la diplomă, redactat în limbile română și engleză.

2. FORMELE DE EVALUARE A REZULTATELOR ÎNVĂȚĂRII ÎN VEDEREA ATRIBUIRII CALIFICĂRII

Studiile superioare de licență, ciclul I, se finalizează cu susținerea examenului și/sau proiectului de licență.

Rezultatele învățării evaluate prin probele Examenului de licență

Prin proba teoretică a Examenului de licență, se vor evalua următoarele rezultate ale învățării:

Nr. crt.	Rezultate ale învățării ***Absolventul poate:***
1.	aplica conceptele și metodele științelor fundamentale pentru identificarea, formularea și argumentarea soluțiilor în domeniul ingineriei
2.	interpreta date colectate în proiecte de dezvoltare a produselor program și a aplicațiilor, utilizând concepte matematice, statistice și logice pentru analiza acestora
3.	dezvolta produse program şi aplicaţii, utilizând conceptele de bază din știința calculatoarelor, tehnologia informației și comunicațiilor
4.	implementa proiectarea hardware-software integrată pentru a soluționa probleme tehnice și a optimiza procesele informatice
5.	aplica principiile fundamentale ale securității informației în dezvoltarea și implementarea strategiilor de securitate pentru protecția sistemelor informatice

Proba teoretică a Examenului de licență poate fi organizată în scris, oral, combinat, inclusiv asistată de calculator.

În contextul autonomiei universitare, responsabilitatea pentru elaborarea itemilor/subiectelor pentru teste/bilete revine departamentului/catedrei care gestionează programul de studii superioare de licență. Conținutul biletelor/testelor se elaborează în baza subiectelor pentru probele Examenului de licență făcute publice în modul stabilit de legislația în vigoare.

Rezultatele învățării evaluate prin Proiectul de licență

Prin proiectul de licență, vor fi evaluate următoarele rezultate ale învățării:

Nr. crt.	Rezultate ale învățării ***Absolventul poate:***
1.	elabora documentația tehnică în proiectele de dezvoltare a produselor program și a aplicațiilor, respectând reglementările și standardele în vigoare
2.	aplica principiile fundamentale ale securității informației în dezvoltarea și implementarea strategiilor de securitate pentru protecția sistemelor informatice
3.	implementa sisteme de securitate bazate pe principiile fundamentale ale securității informației pentru protecția infrastructurilor TI și a datelor organizaționale.
4.	proiecta soluții de securitate pentru protecția infrastructurilor TI, aplicațiilor și datelor împotriva amenințărilor cibernetice
5.	utiliza tehnologii și instrumente specifice pentru detectarea, prevenirea și răspunsul la incidente de securitate în cadrul infrastructurilor TI
6.	Implementa controale de securitate pentru sistemele TIC, asigurând detectarea, monitorizarea și remedierea vulnerabilităților
7.	proiecta mecanisme de audit și control al securității TIC cu evaluarea impactului acestora asupra infrastructurilor TIC, propunând măsuri de reducere a vulnerabilităților

8.	analiza riscurile de securitate informațională, evaluând impactul acestora asupra infrastructurilor TIC și propune măsuri de reducere a vulnerabilităților
9.	implementa strategii de gestionare a riscurilor de securitate informațională, în conformitate cu standardele și reglementările în vigoare

Tematica proiectelor de licență este elaborată la departamentul/catedra de specialitate, aprobată de Consiliul facultății și făcută publică în termenele stabilite de regulamentele instituționale.

Tema proiectului de licență se definitivează la finalizarea etapei de documentare, dar nu mai târziu de 3 luni până la susținerea publică a lucrării de finalizare a studiilor. Etapa de documentare se realizează printr-un stagiu de practică realizat, de regulă, în cadrul întreprinderilor și companiilor din domeniile electronică, automatizări, tehnologiilor informaționale și comunicațiilor cu durata 4-5 săptămâni.

Instituțiile de învățământ superior vor detalia etapele și conținutul procesului de elaborare a proiectului de licență în regulamente/ghiduri/proceduri instituționale.

3. CRITERIILE DE EVALUARE A REZULTATELOR ÎNVĂȚĂRII ȘI DESCRIPTORII DE NOTE PENTRU PROIECTUL DE LICENȚĂ

Descriptorii de note sunt aplicați pentru stabilirea nivelului rezultatelor învățării demonstrate de către candidat prin Proiectul de licență. Descriptorii explică semnificația notei acordate candidatului pentru prezentarea produselor specificate în conținutul lucrării. Descriptorii de nivel se utilizează de către Comisia pentru Examenul de licență în procesul de stabilire a notei alocate corespunzător nivelului de realizare a sarcinii.

Nota finală la Proiectul de licență se va calcula ținând cont de ponderea fiecărui criteriu de evaluare, specificat în tabelul de mai jos.

Criterii de evaluare	**Descriptori**				**Ponderea criteriului de evaluare în nota finală**
	Nivel maxim (nota 10-9,00)	**Nivel mediu (nota 8,99-7,00)**	**Nivel minim (nota 6,99-5,00)**	**Nivel insuficient (nota <5,00)**	
PREZENTAREA PROIECTULUI					
Conținutul prezentării PowerPoint	– Prezentarea este foarte bine structurată și conține toate componentele necesare; – Elementele grafice și textuale sunt redate clar, succint și original.	– Prezentarea, în general, este structurată bine și conține toate componentele necesare; – Elementele grafice și textuale sunt redate suficient de clar și original.	– Prezentarea este parțial structurată; – Elementele grafice sunt parțial clare și conțin unele erori de interpretare; – Volumul textului este prea mare și puțin informativ.	– Prezentarea nu este structurată conform conținutului PL; – Elementele grafice lipsesc sau nu se referă la subiectul prezentării; – Conținutul textului nu redă clar sarcina abordată în proiect.	**0.05**
Prestația de prezentare	– Subiectul este expus într-un limbaj de specialitate exact și vast, corespunzător conținutului.	– Subiectul este expus cu utilizarea termenilor de specialitate, dar limitat.	– Informația este expusă într-un limbaj de specialitate acceptabil.	– Prezentarea nu corespunde subiectului.	**0.1**
Răspunsul la întrebări	– Răspunde prompt și corect la toate întrebările formulate de membrii CEL.	– Răspunde corect la majoritatea întrebărilor formulate de membrii CEL.	– Răspunde neîncrezut la întrebările formulate de membrii CEL, are puține răspunsuri corecte.	– Nu poate răspunde la întrebările formulate de membrii CEL.	**0.1**
PRODUSUL (Produs program sau aplicație)					
Corespunderea cu scopul și obiectivele PL	– Produsul program sau aplicația dezvoltate corespund totalmente	– Produsul program sau aplicația dezvoltate corespund în mare măsură	– Produsul program sau aplicația sunt dezvoltate parțial și nu soluționează	– Produsul program sau aplicația nu sunt dezvoltate.	**0.1**

	scopului și obectivelor proiectului de licență.	scopului și obectivelor proiectului de licență.	toate problemele propuse în proiectul de licență.		
Calitatea implementării produsului program sau a aplicației	– Toate componentele produsului program sunt elaborate utilizând instrumente și tehnologii care corespund în totalitate specificațiilor tehnice și cerințelor funcționale; – Produsul conține toate componentele necesare; – Componentele produsului sunt funcționale și compatibile între ele; – Performanța, fiabilitatea și securitatea produsului corespund totalmente cerințelor.	– Toate componentele produsului program sunt elaborate utilizând instrumente și tehnologii care corespund în general specificațiilor tehnice și cerințelor funcționale; – Produsul conține majoritatea componentelor necesare; – Componentele produsului sunt funcționale și compatibile între ele; – Performanța, fiabilitatea și securitatea produsului corespund în mare parte cerințelor.	– Componentele produsului program sunt elaborate utilizând instrumente și tehnologii care corespund parțial specificațiilor tehnice și cerințelor funcționale; – Produsul nu conține toate componentele necesare; – Componentele produsului sunt parțial funcționale și compatibile între ele; – Performanța, fiabilitatea și securitatea produsului nu corespund cerințelor. –	– Componentele produsului nu corespund specificațiilor tehnice și cerințelor funcționale sau produsul nu este elaborat.	**0.1**
Originalitatea produsului program sau a aplicației	– Produsul elaborat este original, inovativ și aduce ceva nou și diferit față de soluțiile existente în domeniu.	– Produsul elaborat este, în general, original și inovativ.	– Produsul elaborat abordează o problemă tipică și nu aduce ceva nou față de soluțiile existente în domeniu.	– Produsul nu este elaborat și originalitatea nu poate fi apreciată.	**0.05**
MEMORIUL EXPLICATIV					
Actualitatea temei PL	– Tema proiectului de licență corelează totalmente cu tendințele actuale de dezvoltare a produselor program și a aplicațiilor.	– Tema proiectului de licență corelează în temei cu tendințele actuale de dezvoltare a produselor program și a aplicațiilor.	– Tema proiectului de licență corelează parțial cu tendințele actuale de dezvoltare a produselor program și a aplicațiilor.	– Tema proiectului de licență nu corelează cu tendințele actuale de dezvoltare a produselor program și a aplicațiilor.	**0.05**
Structurarea memoriului explicativ pe	– Memoriul explicativ conține toate componentele de bază, capitolele fiind aranjate într-o succesiune	– Memoriul explicativ conține toate componentele de bază, capitolele fiind aranjate într-o succesiune	– Memoriul explicativ conține toate componentele de bază, capitolele fiind aranjate într-o succesiune	– Memoriul explicativ nu conține toate componentele de bază, iar numărul și volumul capitolelor este	**0.05**

componente de bază	logică, iar numărul și volumul acestora corespunde totalmente cerințelor de elaborare.	logică, iar numărul și volumul acestora este suficient de echilibrat.	logică, iar numărul și volumul acestora este parțial dezechilibrat.	dezechilibrat.	
Argumentarea teoretică	– Calitatea argumentării teoretice este efectuată la un nivel înalt și acoperă totalmente aspectele proiectului elaborat.	– Calitatea argumentării teoretice este efectuată la un nivel bun și acoperă parțial aspectele proiectului elaborat.	– Calitatea argumentării teoretice este efectuată la un nivel satisfăcător și acoperă în mică măsură aspectele proiectului elaborat.	– Argumentarea teoretică nu corespunde tematicii proiectului elaborat.	**0.05**
Realizarea obiectivelor proiectului	– Obiectivele proiectului sunt realizate totalmente.	– Obiectivele proiectului sunt în general realizate.	– Obiectivele proiectului sunt realizate parțial.	– Obiectivele proiectului nu sunt realizate.	**0.1**
Argumentarea tehnologiilor selectate	– Tehnologiile selectate sunt optimale și alegerea lor este argumentată pe deplin.	– Tehnologiile selectate sunt adecvate și alegerea lor este parțial argumentată.	– Tehnologiile selectate sunt parțial potrivite și alegerea lor nu este suficient argumentată.	– Tehnologiile selectate nu corespund cerințelor.	**0.05**
Relevanţa practică a proiectului	– Produsul elaborat este aplicabil și necesar în domeniul de referință, corespunde totalmente specificațiilor și cerințelor tehnice.	– Produsul elaborat corespunde în mare parte specificațiilor și cerințelor tehnice.	– Produsul este elaborat cu erori remediabile de la specificațiile și cerințele tehnice.	– Produsul este elaborat cu abateri de la specificațiile și cerințele tehnice.	**0.1**
Expunerea și argumentarea concluziilor	– Concluziile sunt concludente și conțin prezentarea succintă și clară a rezultatelor, dificultăților și perspectivelor.	– Concluziile sunt expuse bine și conțin prezentarea succintă a rezultatelor și perspectivelor.	– Concluziile sunt expuse generalizat, fără referință la rezultatele obținute.	– Concluziile lipsesc sau sunt expuse fără referință la rezultatele obținute.	**0.05**
Calitatea referințelor bibliografice	– Referințele bibliografice sunt actuale și acoperă totalmente aspectele studiate.	– Referințele bibliografice sunt actuale și acoperă parțial aspectele studiate.	– Referințele bibliografice sunt actuale, dar nu acoperă toate aspectele studiate.	– Referințele bibliografice nu sunt actuale și nu acoperă aspectele studiate.	**0.05**

4. STABILIREA NIVELULUI MINIM DE COMPETENȚĂ

Proba teoretică a Examenului de licență

Testul de evaluare finală/biletele de examinare vor fi elaborate în baza rezultatelor învățării stipulate în prezentul standard, precum și în baza Curriculum-ului universitar, prezentând în mod obligatoriu baremul de notare. Candidații trebuie să acumuleze minim 40% din punctajul prevăzut de barem.

Proiectul de licență

La susținerea publică a proiectelor de licență membrii Comisiei pentru Examenul de licență vor stabili nivelul minim de competență (notat cu 6,99 – 5,00) a candidaților în baza criteriilor de evaluare a rezultatelor învățării și descriptorii de nivel stabiliți în prezentul standard.

5. STABILIREA NECESARULUI MINIM DE RESURSE PENTRU EVALUAREA REZULTATELOR ÎNVĂȚĂRII ȘI ATRIBUIREA CALIFICĂRII

Instrumente de evaluare

Pentru realizarea probei teoretice (scrise) a Examenului de licență, grupul de lucru responsabil de elaborarea instrumentelor de evaluare de la departamentul/catedra de specialitate responsabilă de programul de studii, va elabora bilete/teste și sarcini practice pentru evaluarea finală a rezultatelor învățării obținute.

Pentru proba scrisă a Examenului de licență va fi elaborat un set de bilete (în conformitate cu numărul studenților evaluați plus 5 pentru a asigura posibilitatea extragerii de către fiecare student) sau teste (în număr de 3 - 5 variante), care vor avea același grad de complexitate, aceeași structură și același număr și tipuri de itemi de evaluare. Testul scris va fi însoțit de baremul de verificare și modalitatea de convertire a punctelor în note.

Pentru proba practică a Examenului de licență vor fi elaborate:

1. Formularul evaluatorului, care include criteriile de evaluare a Proiectului de licență, care include dovezi de realizare a proiectului și produsului.
2. Baremul de apreciere a probei practice.

Pentru desfășurarea probei teoretice și probei practice a Examenului de licență, sunt necesare:

2. resurse umane:
   a) elaboratori de bilete/teste;
   b) observatori;
   c) evaluatori ai probei scrise realizate prin bilete/teste;
   d) evaluatori ai proiectelor de licență;
   e) verificatori ai evaluării;
3. resurse materiale:
   a) hârtie pentru tipărirea biletelor/testelor;
   b) imprimante pentru multiplicarea biletelor/testelor;
   c) auditorii/aule pentru administrarea biletelor/testelor;
   d) spații/încăperi pentru verificarea lucrărilor scrise/testelor;
   e) spații/încăperi pentru prezentarea proiectelor de licență.

ASIGURAREA CALITĂȚII STANDARDULUI DE CALIFICARE

Etape	Descriptori/Dovezi
Inițierea procesului de elaborare a standardului de calificare	- *Ministerul Educației și Cercetării,* în cadrul Proiectului „Învățământul superior din Moldova" (Moldovan Hight Education), finanțat de Banca Mondială, au inițiat procesul de elaborare a standardului de calificare. - MEC, prin ordinul nr. 1310/2024 *Cu privire la constituirea Grupurilor de lucru pentru elaborarea standardelor de calificare,* a dispus elaborarea standardelor de calificare pentru domeniul general de studiu *061 Tehnologii ale informației și comunicațiilor*. - Standardul de calificare a fost avizat de 14 angajatori, Asociaţia Naţională a Companiilor din Domeniul TIC din Moldova și 4 facultăți ale universităților din RM care gestionează programe de studii din domeniul general de studiu *061 Tehnologii ale informației și comunicațiilor*. Reprezentanții acestora au fost implicați în procesul de elaborare în calitate de membri ai Grupului de lucru pentru elaborarea standardului de calificare *Inginer licențiat* în *Securitate informațională.*
Elaborarea standardului de calificare	La baza elaborării standardului de calificare este standardul de competență pentru calificarea *Inginer licențiat în Securitate informațională*. Standardul de competență este parte integrantă a Standardului de calificare și este prezentat în Anexă la acesta. Membrii grupului de lucru: - au participat la trainingul de instruire a grupurilor de lucru în vederea formării competențelor de elaborare a standardelor de calificare pentru învățământul superior, nivel 6, 7 și 8 CNC; - au participat la elaborarea standardelor de competență din domeniul *Tehnologii ale informației și comunicațiilor*; - au participat la elaborarea standardelor de calificare din domeniul *Tehnologii ale informației și comunicațiilor*; - sunt desemnați în calitate de experți în dezvoltarea standardelor de calificare profesională prin ordinul Ministerului Educației și Cercetării; - au participat la elaborarea documentelor de politici educaționale privind elaborarea, revizuirea și validarea standardelor de calificare profesională; - au elaborat și recenzat Curriculum-uri la programul de studii Securitate informațională. La elaborarea Standardului de calificare au participat cadre științifico-didactice de la *Facultatea Calculatoare, Informatică și Microelectronică,* UTM; *Facultatea Tehnologii Informaționale și Statistică Economică,* ASEM; *Facultatea Fizică și Inginerie,* USM, precum și specialiști de la întreprinderile din domeniul TIC: Asociația Companiilor IT (ATIC), BC "MAIB" S.A. și Î.C.S. ,,Allied Testing-M" S.R.L. Standardul de calificare a fost coordonat cu Asociaţia Naţională a Companiilor din Domeniul TIC din Moldova; Moldova IT Park; S.R.L. ENDAVA; S.R.L. AMDARIS; S.R.L. M-TESTING; S.R.L. PENTALOG CHI; S.A. ORANGE SYSTEMS; AddCode & Comitetul HR & Educație ATIC; S.R.L. CRUNCHYROLL; Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică; S.R.L. CODWER; S.R.L. IT-LAB GRUP; ÎCS GILAT SATELLITE NETWORKS MDC SRL; S.R.L. EBS Integrator; S.R.L. WINIFY;

	Facultatea Calculatoare, Informatică și Microelectronică, UTM; Facultatea Tehnologii Informaționale și Statistică Economică, ASEM; Facultatea de Matematică şi Informatică, USM; Facultatea Informatică, Inginerie, Design, ULIM.
Validarea	- Standardul de calificare a fost validat de către Comisia de validare aprobată prin Ordinul Ministrului Dezvoltării Economice și Digitalizării nr. 45 din 15.04.2025 din care fac parte reprezentanții Ministerului Dezvoltării Economice și Digitalizării; Agenţiei de Guvernare Electornică, Academiei de Studii Economice din Moldova. - Standardul de competență a fost validat prin procesul-verbal nr. 6 din 15.09.2023. - Standardul de calificare a fost avizat de Comisia de validare la 15.09.2023.
Implementarea	Prestatorul programului de studii superioare de licență *Securitate informațională* va*:* - revizui și adapta Planul de învățământ și Curricula disciplinelor pentru programul de studii superioare de licență *Securitate informațională* conform cerințelor standardului de calificare; - organiza și desfășura evaluarea rezultatelor învățării absolvenților programului de studii superioare de licență în scopul acordării calificării *Inginer licențiat*, în temeiul rezultatelor învățării din prezentul standard de calificare.
Mecanisme de feedback și de îmbunătățire continuă a calității	- *Facultatea Calculatoare, Informatică și Microelectronică a UTM* este responsabilă pentru colectarea feedback-ului de la părțile interesate în această calificare. - Drept temei pentru revizuirea standardului de calificare va servi actualizarea standardului de competență, implementarea pe piața muncii a tehnologiilor avansate și armonizarea politicilor naționale cu cele europene în scopul îmbunătățirii flexibilității forței de muncă. - Standardul de calificare va fi revizuit în termen de șase luni de la actualizarea standardului de competență, luând în considerare schimbarea continuă a contextului socioeconomic, în general, precum și tendințele de dezvoltare din domeniul *Tehnologii ale informației și comunicațiilor*, în special.
Asigurarea transparenței	Standardul de calificare va fi publicat pe pagina web oficială a *Ministerului Educației și Cercetării* și înscris în Registrul național al calificărilor.

Anexă
la Standardul de calificare
SECURITATE INFORMAȚIONALĂ

STANDARD DE COMPETENȚĂ

INGINER LICENȚIAT,
SECURITATE INFORMAȚIONALĂ

(titlul și denumirea programului de studii)

NIVEL 6 CNC

Domeniul de formare profesională:
DEZVOLTAREA PRODUSELOR PROGRAM ȘI A APLICAȚIILOR

Membrii
Comisiei de validare

Andrei CUȘCĂ, şef direcţie politici în domeniul tehnologiei informaţiei şi digitaizării, Ministerul Dezvoltării Economice şi Digitalizării

Igor ARAMĂ, şef serviciu tehnologia informaţiei, Agenţia de Guvernare Electronică

Larisa DODU-GUGEA, doctor, conferenţiar universitar, decan Facultatea Relaţii Economice Internaţionale, Academia de Studii Economice din Moldova

Viorica STROICI, consultant principal Direcţia politici în domeniul tehnologiei informaţiei şi digitalizării, Ministerul Dezvoltării Economice şi Digitalizării

„ 23 ” 05 2025

Standardul de competență pentru calificarea *Inginer licențiat* în **SECURITATE INFORMAȚIONALĂ** constituie un cadru de referință privind competențele profesionale, tendințele existente și de perspectivă ale pieței muncii în raport cu necesitățile domeniului de formare profesională **DEZVOLTAREA PRODUSELOR PROGRAM ȘI A APLICAȚIILOR.**

Standardul reflectă competențele profesionale prin corelarea cu clasificatoarele naționale și internaționale ale pieței muncii: Clasificatorul ocupațiilor din Republica Moldova CORM (006-2021); Clasificarea internațională Standard al Ocupațiilor (ISCO 08); Clasificarea europeană a aptitudinilor /competențelor, calificărilor și ocupațiilor (ESCO 08), clasificatoarele naționale și internaționale ale activităților economice: Clasificatorul activităților economice din Republica Moldova *CAEM (Rev. 2),* Clasificarea Statistică a Activităților Economice din Comunitatea Europeană (Statistical Classification of Economic Activities in the European Community) *NACE Rev. 2,* Clasificarea Internațională Industrială Standard a tuturor Activităților Economice (International Standard Industrial Classification of All Economic Activities, ISIC Rev. 4) și corelarea calificării conform Clasificatoarelor educaționale: Nomenclatorul domeniilor de formare profesională și al specialităților în învățământul superior (HG nr. 412/2024); Clasificarea Internațională Standard a Educației (ISCED-2011) și Clasificarea domeniilor educației și formării profesionale (ISCED-F 2013).

Standardul de competență se aplică la elaborarea fișelor de post, evaluarea competențelor și performanțelor angajaților, dezvoltarea standardelor de calificare și la proiectarea programelor de studii pentru domeniul de formare profesională *Dezvoltarea produselor program şi a aplicaţiilor*.

1. INFORMAȚII GENERALE

1.1. Informații privind elaborarea și aprobarea standardului de competență	
Standardul de competență elaborat de Grupul de lucru, aprobat prin ordinul Ministerului Educației și Cercetării nr. 1310 din 24.09.2024	FIODOROV Ion, doctor în Informatică, conferențiar universitar, șeful Departamentului Ingineria Software și Automatică, Facultatea Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei; BOLUN Ion, doctor habilitat, profesor universitar, Departamentul Ingineria Software și Automatică, Facultatea Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei; ALEXEI Arina, doctor, lectoră universitară, Departamentul Ingineria Software și Automatică, Facultatea Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei; ZGUREANU Aureliu, doctor, conferențiar universitar, Departamentul Tehnologia Informației și Management Informațional, Facultatea Tehnologii Informaționale și Statistică Economică, Academia de Studii Economice din Moldova; BELDIGA Maria, doctor, conferențiar universitar, prodecan, Departamentul Fizică Aplicată și Informatică, Facultatea Fizică și Inginerie, Universitatea de Stat din Moldova; COJOCARU Sergiu, senior software engineer Direcția Dezvoltare Servicii .net, Departament Dezvoltare tehnologii informaționale, Divizia Tehnologii informaționale, , BC "MAIB" S.A.; CUNEV Veaceslav, doctor în Informatică, președinte al Asociației Companiilor IT (ATIC); BULAI Rodica, data analist, Direcția Platforme analitice, Departamentul Platforme principale, Divizia Tehnologii informaționale, BC "MAIB" S.A.; NASTASENCO Veaceslav, director Î.C.S. ,,Allied Testing-M” S.R.L.
Perioada elaborării	**01.11.2024 – 27.04.2025**

Standardul de competență a fost consultat cu:	BZOVÎI Marina, Director Moldova IT Park PANFIL Veaceslav, Manager SRL ENDAVA HAHEU Petru, Director SRL AMDARIS CROTOV Serghei, Director SRL M-TESTING BURLAC Mihail, Director tehnic SRL PENTALOG CHI CHIRIȚA Ana, Director proiecte strategice, Asociaţia Naţională a Companiilor din Domeniul TIC PLĂCINTĂ Sergiu, Director of International Operations, SA ORANGE SYSTEMS MALBAȘ-ROTARU Alina, Coprşedinte AddCode&Comitetul HR&Educație ATIC IVANOVA Elena, Director, SRL CRUNCHYROLL COREȚCHI Alexandru, Director Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică DUMITRAȘCU Marius, Director SRL CODWER CIOBAN Alexei, Director SRL IT-LAB GRUP ANDRONIC Alexandru, Manager ÎCS GILAT SATELLITE NETWORKS MDC SRL BARBAROȘ Vasile, Inginer de sistem software, SRL EBS Integrator POȘTARU Andrei, Director SRL WINIFY CIORBĂ Dumitru, Decan, dr., conf. univ., Facultatea Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei TOACĂ Zinovia, Decană, dr., conf. univ., Facultatea Tehnologii Informaționale și Statistică Economică, Academia de Studii Economice din Moldova NICULIŢĂ Angela, Decană, dr., conf. univ., Facultatea de Matematică şi Informatică, Universitatea de Stat din Moldova MITEV Lilia, Decană, dr., conf. univ., Facultatea Informatică, Inginerie, Design, Universitatea Liberă Internațională din Moldova
Standardul de competență validat și aprobat de Comisia de validare, aprobată prin ordinul Ministerului Dezvoltării Economice și Digitalizării nr. 45 din 15.04.2025	Proces-verbal nr. 6 din 15.09.2023 de validare a Standardului de competență pentru *Inginerul licențiat* în *Securitate informațională*, nivel 6 CNC.

1.2. INFORMAȚII PRIVIND CORELAREA CU CLASIFICATOARELE NAȚIONALE ȘI INTERNAȚIONALE		
1.2.1 CARACTERISTICILE OCUPAȚIONALE CONFORM CLASIFICATOARELOR PIEȚEI MUNCII		
Clasificatorul ocupațiilor din Republica Moldova CORM (006-2021)	**Clasificarea europeană a aptitudinilor/ competențelor, calificărilor și ocupațiilor (ESCO 08)**	**Clasificarea internațională Standard al Ocupațiilor (ISCO 08)**
2 SPECIALIȘTI/SPECIALISTE ÎN DIVERSE DOMENII DE ACTIVITATE 25 Specialiști/specialiste în tehnologia informației și comunicațiilor	**2 SPECIALIȘTI ÎN DIVERSE DOMENII DE ACTIVITATE** 25 Specialiști în tehnologia informației și comunicațiilor	**2 PROFESIONIȘTI** 25 Profesioniști în tehnologia informației și comunicațiilor
1.2.2. CARACTERISTICILE OCUPAȚIONALE CONFORM CLASIFICATOARELOR ACTIVITĂȚILOR ECONOMICE		
Clasificatorul activităților economice din Republica Moldova CAEM Rev. 2	**Clasificarea Statistică a Activităților Economice din Comunitatea Europeană (Statistical Classification of Economic Activities in the European Community) NACE Rev. 2**	**Clasificarea Internațională Industrială Standard a tuturor Activităților Economice (International Standard Industrial Classification of All Economic Activities, ISIC Rev. 4)**
J. INFORMAȚII ȘI COMUNICAȚII 62 Activități de servicii în tehnologia informației 63 Activități de servicii informatice	**J. INFORMAȚII ȘI COMUNICAȚII** J.62 Programarea calculatoarelor, consultanță și activități conexe J.63 Activități de servicii informatice	**J. INFORMAȚII ȘI COMUNICAȚII** J.62 Programarea calculatoarelor, consultanță și activități conexe J.63 Activități de servicii informatice
1.1.3. CORELAREA CALIFICĂRII CONFORM CLASIFICATOARELOR EDUCAȚIONALE		
Nomenclatorul domeniilor de formare profesionalăprofesională și al specialităților în învățământul superior	**Clasificarea Internațională Standard a Educației (ISCED-2011)**	**Clasificarea domeniilor educației și formării profesionale (ISCED-F-2013)**
06 TEHNOLOGII ALE INFORMAȚIEI ȘI COMUNICAȚIILOR ***061 Tehnologii ale informației și comunicațiilor*** **0613 Dezvoltarea produselor program și a aplicațiilor** 0613.2 Securitate informațională	**Învățământ superior de licență, ciclul I, nivelul 6 ISCED** **4 Știință** ***48 Calculatoare***	**06 TEHNOLOGII ALE INFORMAȚIEI ȘI COMUNICAȚIILOR** ***061 Tehnologii ale informaţiei şi comunicaţiilor***

Nivel de competență/abilitate, conform ISCO-08	**4**
Cadrul național al calificărilor	Nivel 6 CNC
Referire la Cadrul European al Calificărilor (EQF)	Echivalent nivel 6 EQF
Identificarea ocupațiilor tipice	
Ocupații tipice (CORM)	**Ocupații tipice (ESCO)**
121906 Manager (Șef/Șefa) securitatea informației din cadrul organizației 251910 Specialist/specialistă în proceduri și instrumente de securitate a sistemelor informaționale 241242 Specialist/specialistă în securitatea informației 252905 Specialist/specialistă în securitatea sistemelor informatice 252902 Administrator/administratoare securitatea sistemelor informatice 251106 Analist/analistă securitatea sistemelor informaționale 215319 Inginer/ingineră manager securitate informationala 215323 Inginer/ingineră politici de securitate informațională 215247 Inginer/ingineră securitatea sistemelor electronice și de telecomunicații	1219.1.2 Manager securitate 2529.6 Administrator securitate TIC 2529.1 Ofițer șef securitate TIC 2529.3 Inginer de securitate a sistemelor încorporate 2529.7 Respondent la incidente cibernetice 2529.8 Manager risc cibernetic 1213.9 Director pentru conformitate și securitatea informațiilor 2413.1.4 Analist securitate
Specializări/opțiuni (arii ocupaţionale)	
Tendințe și preocupări de viitor în domeniul de formare profesională	- Utilizarea tehnologiilor emergente, precum inteligența artificială și învățarea automată, pentru a detecta și preveni atacurile cibernetice. - Aplicarea tehnologiilor “blockchain” pentru a spori securitatea și integritatea datelor. - Creșterea utilizării soluțiilor de automatizare privind gestionarea incidentelor de securitate. - Îmbunătățirea autentificării multifactoriale (MFA) pentru a fortifica securitatea sistemelor și datelor prin: autentificare biometrică sporită, autentificare bazată pe comportamentul utilizatorului, tehnici de autentificare fără parole. - Creșterea securității și a opțiunilor de control în serviciile cloud. Dezvoltarea soluțiilor de securitate adaptate pentru mediul cloud. - Adoptarea și implementarea modelelor de securitate bazate pe ”zero trust”, care presupun verificarea continuă a autenticității și a autorizării oricărui dispozitiv sau utilizator. - Integrarea soluțiilor de securizare a dispozitivelor IoT (Internet of Things), care devin tot mai omniprezente în mediul de afaceri, stabilirea și implementarea standardelor de securitate pentru dispozitivele IoT.

	- Utilizarea de soluții de criptare avansate privind protecția datelor sensibile și tehnologii de prevenire a pierderii de date, în special în contextul reglementărilor în vigoare. - Creșterea nivelului de securitate în lanțul de aprovizionare (Supply Chain), o zonă care devine din ce în ce mai expusă la atacuri cibernetice. Implementarea unor practici de securitate robuste în parteneriatele și relațiile de afaceri. - Eficientizarea măsurilor de securitate a aplicațiilor cu un focus pe testarea securității în ciclul de viață al dezvoltării software (DevSecOps). - Implementarea de soluții dedicate de protecție a aplicațiilor, cum ar fi firewalls pentru aplicații web (WAF).
Ocupații de viitor	- Proiectant sisteme de securitate cibernetică. - Inginer automatizare sisteme de gestionare a incidentelor de securitate. - Specialist securitate IoT. - Inginer securitate Cloud. - Specialist în dezvoltarea instrumentelor de instruire în securitate. - Expert în politici, modele și standarde de securitate. - Inginer în sisteme inteligente de securitate. - Inginer în securitatea sistemelor ciber-fizice. - Specialist în securitate cibernetică industrială. - Specialist în blockchain.

1.3. ALTE INFORMAȚII RELEVANTE

Titlul calificării profesionale în limba străină:

Română	Engleză	Rusă
Inginer, inginer licențiat, nivel 6 CNC	Engineer, Bachelor of engineering, level 6 NQF	Инженер, лиценциат в инженерии, 6 уровень НРК
Franceză	Germană	Italiană
Ingénieur, Baccalaureat en genie, niveau 6 CNQ	Ingenieur, Bachelor of Engineering, Stufe 6 des NQS	Ingegnere, Laurea in ingegneria, first-cicle degrees, livello 6 QNQ

Anexe la standardul de competență:

Anexa 1	Codul de conduită al inginerului/Code of Ethics for Engineers Code of Quality for European Chartered Engineers NSPE Code of Ethics for Engineers
Anexa 2	Cadru de e-Competențe 2024 Grilă de auto-evaluare a competențelor digitale Europass, 2021
Anexa 3	Competențe lingvistice. Cadrul European Comun de Referință pentru Limbi: Învățare, Predare, Evaluare (rom.) Descrieri ale nivelurilor de competență lingvistică (l. engleza)
Anexa 4	Cadrul de competențe antreprenoriale EntreComp Despre EntreComp: Cadrul de competențe antreprenoriale
Anexa 5	Cadrul de competențe în economia verde/economia circulară Programul de promovare a economiei verzi și circulare în Republica Moldova pentru perioada 2024 – 2028

2. DESCRIEREA OCUPAȚIONALĂ A CALIFICĂRII

2.1 Descrierea activității de muncă /

Scopul activităților *Inginerului licențiat* în *Securitate informațională* este de a proteja și asigura confidențialitatea, integritatea și disponibilitatea datelor și a infrastructurilor TI ale organizațiilor. Un asemenea specialist se concentrează pe identificarea, evaluarea și gestionarea riscurilor legate de securitatea informațiilor, contribuind la prevenirea incidentelor cibernetice și la reducerea vulnerabilităților în diferite sectoare de activitate.

Activitatea acestora se axează pe realizarea la un nivel calitativ a următoarelor atribuţii:

a) Implementarea și/sau gestionarea strategiilor de securitate informațională a organizațiilor în vederea asigurării securizării și protejării în mod corespunzător a sistemelor, serviciilor și activelor digitale;
b) Monitorizarea și gestionarea securității informaționale, incluzând identificarea, evaluarea și tratarea riscurilor, pentru a asigura continuitatea operațională și protecția organizației;
c) Analiza datelor și generarea de rapoarte acționabile, cu diseminarea către părțile interesate relevante;
d) Proiectarea și implementarea soluțiilor de securitate (security by design) pentru infrastructuri, sisteme software și hardware, asigurând operarea acestora în mod eficient;
e) Efectuarea auditurilor de securitate informațională, incluzând evaluarea eficacității controalelor de securitate, analiza vulnerabilităților și conformitatea cu cerințele legale, de reglementare și standardele din industrie.

2.2 Arii de competențe și descriptori

Aria de competență	Descriptori
1. Elaborarea soluțiilor de securitate pentru infrastructuri TI	1.1. Studiază arhitecturile de rețea pentru a identifica vulnerabilitățile și nevoile de securitate. 1.2. Stabilește configurările necesare pentru tehnologiile de securitate. 1.3. Identifică activitățile neobișnuite prin monitorizarea continuă a traficului din rețelele de comunicații. 1.4. Determină politicile de segmentare ale rețelelor pentru a limita accesul neautorizat în rețea.
2. Gestionarea riscurilor și asigurarea conformității cu standardele de securitate	2.1. Evaluează riscurile asociate de amenințările cibernetice și vulnerabilitățile infrastructurii TI. 2.2. Stabilește măsuri pentru a asigura conformitatea cu reglementările în vigoare (ex. GDPR, ISO/IEC 27001). 2.3. Determină strategiile de reducere a riscurilor pentru a minimiza impactul potențial. 2.4. Monitorizează procesele și politicile pentru a menține alinierea la standardele de securitate.
3. Aplicarea metodelor de protecție a datelor	3.1. Utilizează tehnici criptografice pentru a proteja datele în tranzit și cele stocate. 3.2. Stabilește proceduri de gestionare a cheilor criptografice pentru a asigura securitatea datelor. 3.3. Asigură integritatea datelor prin utilizarea semnăturii digitale și a algoritmilor criptografici. 3.4. Evaluează metodele de criptare pentru a alege soluțiile potrivite în funcție de nivelul de protecție necesar.
4. Detectarea și gestionarea incidentelor de securitate	4.1. Monitorizează sistemele și activitățile de rețea pentru a identifica incidentele de securitate. 4.2. Identifică natura și impactul incidentelor analizând log-urile și alertele. 4.3. Stabilește pașii de răspuns și comunicare necesari în cazul unui incident de securitate. 4.4. Îmbunătățește planurile de răspuns la incidente pe baza analizelor post-incident.
5. Evaluarea vulnerabilităților și testarea securității	5.1. Realizează teste de penetrare pentru a identifica și evalua vulnerabilitățile sistemelor. 5.2. Detectează punctele slabe prin scanări de vulnerabilitate și evaluări periodice.

	5.3. Documentează constatările din testele de securitate și propune soluții de remediere. 5.4. Monitorizează îmbunătățirile aduse pentru a menține un nivel înalt de securitate.
6. Asigurarea securității aplicațiilor și dezvoltarea sigură	6.1. Revizuiește codul și arhitectura aplicațiilor pentru a identifica vulnerabilități. 6.2. Stabilește măsuri de securitate în cadrul procesului de dezvoltare software. 6.3. Instruiește echipele de dezvoltare în practici de programare sigură. 6.4. Testează aplicațiile pentru a identifica și remedia potențiale breșe de securitate.
7. Elaborarea politicilor și formarea în domeniul securității cibernetice	7.1. Dezvoltă politici și proceduri de securitate cibernetică adaptate organizației. 7.2. Instruiește personalul privind riscurile și bunele practici de securitate. 7.3. Stabilește programe de conștientizare a securității pentru a preveni riscurile interne. 7.4. Monitorizează implementarea politicilor și evaluează eficiența acestora.
8. Managementul activităților și resurselor de securitate	8.1. Planifică activitățile de securitate și alocă resursele necesare pentru desfășurarea acestora. 8.2. Coordonează echipele implicate în proiecte de securitate cibernetică pentru a asigura coerența și eficiența operațiunilor. 8.3. Monitorizează progresul activităților de securitate pentru a identifica și remedia eventualele întârzieri sau deficiențe. 8.4. Optimizează utilizarea resurselor pentru a maximiza eficiența și a reduce costurile proiectelor de securitate.

2.3 Sectoare de activitate

J. INFORMAȚII ȘI COMUNICAȚII
6201 Activități de programare pe calculator
6202 Activități de consultanță informatică și management al instalațiilor informatice
6209 Alte activități în domeniul tehnologiei informației și serviciilor informatice
6311 Prelucrarea datelor, găzduirea și activități conexe
6312 Portaluri web
M. ACTIVITATE PROFESIONALĂ, ȘTIINȚIFICĂ ȘI TEHNICĂ
7490 Alte activități profesionale, științifice și tehnice (Consultant în securitate)

2.4 Mediul de lucru, specificul activității și riscurile profesionale / Rodica BULAI

Munca inginerului în *Securitate informațională* se desfășoară în laboratoare, oficii sau centre de operațiuni de securitate. Principalii factori de risc pentru sănătatea unui angajat sunt munca într-o poziție forțată (muncă pe șezute sau în picioare), muncă obositoare și intensă la calculator (solicitare a ochilor) și munca stresantă din punct de vedere emoțional în situațiile de risc și al responsabilității ridicate.

2.5 Instrumente de lucru, echipamente, utilaje și materiale, soft-uri (Microsoft Office și soft-uri specifice)

Calculatoare, stații de lucru, server-e, medii cloud, medii de programare pentru dezvoltarea software-ului și instrumente de securitate, care pot fi organizate în câteva categorii: monitorizarea securității rețelei, criptare, scanarea vulnerabilităților web, teste de penetrare, software antivirus, detectarea intruziunilor din rețea și interceptor de pachete, firewall etc.

2.6 Calități personale necesare pentru muncă: abilități, caracteristici și cerințe specifice

Munca inginerului în *Securitate informațională* necesită creativitate și ingeniozitate, capacități de concentrare, de investigare, evaluare și gestionare sistematică a situațiilor de risc, gândire analitică, matematică și strategică, abilități antreprenoriale, de comunicare, colaborare și lucru în echipă, de înțelegere cuprinzătoare a riscului entității și de rezolvare rapidă a problemelor survenite. Totodată, inginerul în securitate informațională necesită de a poseda astfel de calități ca integritate, flexibilitate, adaptabilitate și reziliență, inteligență emoțională, perseverență și orientare spre învățare continuă.

2.7 Formare profesională inițială și continuă

Un inginer în *Securitate informațională* de nivel 6 CNC a dobândit cel puțin studii superioare de licență (ciclul I), urmează cursuri de formare profesională continuă conform reglementărilor legislației în vigoare și certificărilor de securitate cibernetică.

2.8 Cele mai răspândite denumiri ale ocupației profesionale (rom/eng/ru)

RO: Specialist/specialistă în securitatea informației, Specialist/specialistă în securitatea sistemelor informatice, Inginer/ingineră politici de securitate informațională, Inginer/ingineră securitatea sistemelor electronice și de telecomunicații.

EN: Information security specialist, Specialist in IT systems security, Information security policy engineer, Electronic and telecommunications systems security engineer.

RU: Специалист по информационной безопасности, Специалист по безопасности информационных систем, Инженер по политике информационной безопасности, Инженер по безопасности электронных и телекоммуникационных систем.

2.9 Reglementări de exercitare a profesiei (naționale/internaționale)

Legislația națională comunitară/internațională sectorială:

1. Hotărârea Guvernului RM nr. 495/2024 cu privire la aprobarea Programului de promovare a economiei verzi și circulare în Republica Moldova pentru perioada 2024-2028
2. Directiva europeană 2005/36/CE privind profesiile reglementate
3. Directiva 2013/35/UE a Parlamentului European și a Consiliului din 26 iunie 2013 privind cerințele minime de sănătate și securitate referitoare la expunerea lucrătorilor la riscuri generate de agenții fizici (câmpuri electromagnetice)
4. Sectoral Qualifications Framework – European Experiences
5. Pactul ecologic european. Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul economic și social european și Comitetul regiunilor, Bruxelles, 11.12.2019
6. Un nou Plan de acțiune privind economia circulară Pentru o Europă mai curată și mai competitivă, Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul economic și social european și Comitetul regiunilor, Bruxelles
7. Comunicarea privind munca decentă la nivel mondial pentru o tranziție globală justă și o redresare durabilă. Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul economic și social european și Comitetul regiunilor, Bruxelles, 23.02.2022
8. Directiva (UE) 2024/1760 a Parlamentului European și a Consiliului din 13 iunie 2024 privind diligența necesară în materie de durabilitate a întreprinderilor și de modificare a Directivei (UE) 2019/1937 și a Regulamentului (UE) 2023/2859Text cu relevanță pentru SEE.
9. Asigurarea faptului că produsele sustenabile devin normă. Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul economic și social european și Comitetul regiunilor, Bruxelles, 30.03.2022
10. Strategia de dezvoltare digitală 2023-2030.

2.10 Norme și reglementări specifice (etice, profesionale, de sănătate, tehnice etc.)

1. Codul de conduită al inginerului/Code of Ethics for Engineers
1. NSPE Code of Ethics for Engineers
2. NSPE Etics Reference Guide
3. Hotărârea Guverului nr. 1609/2003 despre aprobarea Regulamentului privind obiectele de proprietate intelectuală create în cadrul exercitării atribuțiilor de serviciu
4. Legea nr. 230/2022 privind dreptul de autor și drepturile conexe
5. Legea securităţii şi sănătăţii în muncă nr. 186/2008
6. Hotărârea Guvernului nr. 95/2009 pentru aprobarea unor acte normative privind implementarea Legii securității și sănătății în muncă nr. 186-XVI din 10 iulie 2008
7. Hotărârea Guvernului nr. 353/2010 cu privire la aprobarea cerinţelor minime de securitate şi sănătate la locul de muncă
8. Hotărârea Guvernului nr. 603/2011 privind cerinţele minime de securitate şi sănătate pentru folosirea de către lucrători a echipamentului de muncă la locul de muncă

9. Hotărârea Guvernului nr. 906/2020 privind aprobarea Cerințelor minime de securitate și sănătate pentru utilizarea de către lucrători a echipamentelor individuale de protecție la locul de muncă
10. Lege nr. 38/2008 privind protecţia mărcilor
11. Lege nr. 50/2008 privind protecţia invenţiilor
12. Lege nr. 114/2014 cu privire la Agenția de Stat pentru Proprietatea Intelectuală
13. Hotărârea Guvernului nr. 379/2018 cu privire la controlul de stat asupra activității de întreprinzător în baza analizei riscurilor
14. Lege nr. 116/2012 cu privire la Securitatea industrială a obiectelor industriale periculoase
15. Lege nr. 235/2011 cu privire la activitățile de acreditare și de evaluare a conformității
16. Lege nr. 20/2016 cu privire la standardizarea națională
17. Lege nr. 420/2006 cu privire la activitatea de reglementare tehnică
18. Lege 1069/2000 cu privire la informatică
19. Lege 48/2023 privind securitatea cibernetică
20. Lege 467/2003 cu privire la nformatizare şi la resursele informaţionale de stat
21. Lege 71/2007 cu privire la registre

3. CERINȚE DE COMPETENȚE

3.1. COMPETENȚE TRANSVERSALE (CT)

Aria de competență	Competența	Descriptori
1. Elaborarea soluțiilor de securitate pentru infrastructuri TI 2. Gestionarea riscurilor și asigurarea conformității cu standardele de securitate 3. Aplicarea metodelor de protecție a datelor 4. Detectarea și gestionarea incidentelor de securitate 5. Evaluarea vulnerabilităților și testarea securității 6. Asigurarea securității aplicațiilor și dezvoltarea sigură 7. Elaborarea politicilor și formarea în domeniul securității cibernetice 8. Managementul activităților și resurselor de securitate	**CT 1.** Gestionarea timpului și autodisciplină	1.1. Utilizează eficient tehnicile de management al timpului pentru realizarea sarcinilor cu resurse disponibile în termene stabilite. 1.2. Stabilește prioritatea acțiunilor și activităților de muncă.
	CT 2. Luarea deciziilor și leadership	2.1. Comunică viziunea și ideile care inspiră alte persoane să se dedice muncii. 2.2. Transmite un sentiment de încredere altora, facilitându-le succesul. 2.3. Este proactiv prin participare la activități și oferă sprijin membrilor grupului pentru a obține rezultate specifice. 2.4. Gestionează prioritățile și schimbările, adaptând planurile, comportamentele, strategiile la schimbarea contextelor. 2.5. Înțelege și soluționează problemele/ formulează soluțiile alternative cu alegerea celei mai potrivite.
	CT 3. Demonstrarea integrității, eticii și transparenței	3.1.Respectă standardele/codurile, principiile morale, etice, profesionale naționale și internaționale în luarea deciziilor și interacțiunea cu diverse auditorii de contact (întreprindere, piață). 3.2.Respectă standardele de transparență, securitate și comportament non-tolerant corupției. 3.3.Evaluează consecințele și impactul ideilor, oportunităților, acțiunilor proprii. 3.4.Recunoaște comportamentele deviate de la normele morale, etice și legale.
	CT 4. Manifestarea flexibilității, adaptabilității și rezilienței	4.1. Se adaptează eficient la mediul profesional în schimbare și la stările emoționale generate de interacțiuni interpersonale și interprofesionale la diferite niveluri de autoritate. 4.2. Susține schimbările prin atitudine, inițiative, metode și tehnologii noi de activitate. 4.3. Manifestă rezistența la stres și adaptare în situații de schimbare și capacitate de restabilire.

Aria de competență	Competența	Descriptori
		4.4. Își schimbă propriile acțiuni care nu conduc la rezultatul dorit sau nu corespund situației reale. 4.5. Posedă tehnici de autocontrol și aplică analiza autocritică.
	CT 5. Empatizarea și inteligența emoțională	5.1 Aplică tehnici reflective pentru a înțelege și gestiona propriile emoții. 5.2. Poate asculta cu empatie 5.3. Înțelege procesele emoționale în diverse contexte și asigură echilibrul emoțional.
	CT 6. Comunicarea eficientă, lucru în echipă și colaborarea	6.1. Creează un mediu de comunicare adecvat. 6.2. Comunică efectiv și adecvat cu reprezentanții altor culturi și generații. 6.3. Prezinta informațiile într-o maniera clară, logică și inteligibilă grupului țintă. 6.4. Utilizează eficient tehnici, metode și tehnologii de comunicare specifice scopului, contextului și audienței/publicului. 6.5. Posedă competențe multilingvistice. 6.6. Organizează și alege metodele de lucru, gestiona echipe cu diverse motivații și stiluri de lucru în vederea asigurării rezultatelor scontate. 6.7. Participă eficient cu idei inovative, oferă și primește feedback în cadrul activității grupului. 6.8. Construiește relații interpersonale, bazate pe încredere. 6.9. Este capabil să se simtă parte a echipei, să lucreze și să comunice calm și eficient în cadrul unui grup.
	CT 7. Orientarea spre învățare	7.1.Îmbunătățește competențele profesionale prin accesarea, procesarea și asimilarea de noi cunoștințe, utilizând diverse surse și forme de învățare. 7.2.Stabilește obiective, identifică oportunități și planifică propriul progres în carieră.
	CT 8. Gestionarea informației	8.1. Determină nevoile de informații/utilitatea informației, utilizează instrumentele potrivite de accesare a informației. 8.2. Își asumă responsabilitatea de a colecta, selecta, evalua și valida critic informațiile din diverse surse. 8.3. Procesează informațiile folosind instrumentele adecvate și evaluează obiectiv rezultatele obținute. 8.4. Respectă normele etice de utilizare și de securizare a informației.

3.2. COMPETENȚE GENERALE (CG) (transsectoriale și sectoriale)

Aria de competență	Competența	Descriptori
1. Elaborarea soluțiilor de securitate pentru infrastructuri TI 3. Aplicarea metodelor de protecție a datelor	**CG 1.** Utilizarea în activitatea profesională a conceptelor, teoriilor și metodelor	1.1. Identifică şi argumentează soluţiile în dezvoltarea produselor program şi a aplicaţiilor. 1.2. Analizează și interpretează datele colectate în diverse proiecte de dezvoltare a produselor program şi a aplicaţiilor 1.3. Formulează concluzii relevante şi argumentate pentru luarea deciziilor.

5. Evaluarea vulnerabilităților și testarea securității	științelor fundamentale	1.4. Soluționează probleme uzuale de dezvoltare a produselor program şi a aplicaţiilor. 1.5. Aplică metode de analiză, modelare matematică și simulare în rezolvarea problemelor complexe pentru integrarea, optimizarea și evaluarea produselor program şi a aplicaţiilor dezvoltate. 1.6. Estimează potenţialul, avantajele şi dezavantajele proiectelor de dezvoltare a produselor program şi a aplicaţiilor.
1.Elaborarea soluțiilor de securitate pentru infrastructuri TI 3. Aplicarea metodelor de protecție a datelor 4. Detectarea și gestionarea incidentelor de securitate 6.Asigurarea securității aplicațiilor și dezvoltarea sigură	**CG 2.** Operarea cu concepte de bază din ştiinţa calculatoarelor, tehnologia informaţiei şi comunicaţiilor	2.1. Utilizează limbaje, medii şi tehnologii de programare, ingineria programării şi instrumente specifice (algoritmi, scheme, modele, protocoale etc.). 2.2. Dezvoltă produse program şi aplicaţii. 2.3. Soluționează probleme tehnice și optimizează procesele informatice în dezvoltarea produselor program şi a aplicaţiilor. 2.4. Selectează, în calitate de utilizator, software dedicat şi alte mijloace informatice pentru dezvoltarea produselor program şi a aplicaţiilor. 1.7. Folosește proiectarea hardware-software integrată şi a ingineriei programării ca metodologii de dezvoltare a produselor program şi a aplicaţiilor, inclusiv in vederea unei modelări la nivel de sistem.
1.Gestionarea riscurilor și asigurarea conformității cu standardele de securitate 7. Elaborarea politicilor și formarea în domeniul securității cibernetice 8. Managementul activităților și resurselor de securitate	**CG 3.** Aplicarea aspectelor de legislație, economie, marketing, afaceri și asigurare a calității în context managerial	3.1. Asigură conformitatea cu reglementările în vigoare în procesele și proiectele de dezvoltare a produselor program şi a aplicaţiilor. 3.2. Elaborează planuri de afaceri ce țin de dezvoltarea produselor program şi a aplicaţiilor, ținând cont de tendințele pieței și nevoile clienților. 3.3. Implementează sisteme de asigurare a calității. 3.4. Evaluează și optimizează costurile și beneficiile proiectelor tehnologice. 3.5. Elaborează strategii eficiente de promovare a produselor program şi a aplicaţiilor dezvoltate. 2.5. Coordonează echipe și proiecte de dezvoltare a produselor program şi a aplicaţiilor, maximizând eficiența și productivitatea.
2.Gestionarea riscurilor și asigurarea conformității cu standardele de securitate 7. Elaborarea politicilor și formarea în domeniul securității cibernetice 2.8. Managementul activităților și resurselor de securitate	**CG 4.** Asigurarea respectării cadrului normativ în domeniul SSM și protecției mediului	4.1. Aplică prevederile cadrului normativ în domeniul SSM (securității și sănătății în muncă) și protecției mediului. 4.2. Evaluează riscurile și implementează măsuri preventive pentru protecția mediului în activitățile tehnologice. 4.3. Dezvoltă proceduri pentru respectarea normelor legale în domeniul SSM și protecției mediului. 4.4. Asigură instruirea personalului în privința regulilor de protecție a mediului și a procedurilor de securitate și sănătate în muncă. 3.6. Monitorizează respectarea standardelor de SSM și de protecție a mediului pe arii de activitate în cadrul entității.

3.3. COMPETENȚE PROFESIONALE (CP)

Aria de competență	Competența	Descriptori
1. Elaborarea soluțiilor de securitate pentru infrastructuri TI 2. Gestionarea riscurilor și asigurarea conformității cu standardele de securitate 7. Elaborarea politicilor și formarea în domeniul securității cibernetice 8. Managementul activităților și resurselor de securitate	**CP 1.** Utilizarea principiilor fundamentale ale securității informației pentru managementul strategiilor și sistemelor de securitate.	1.1. Aplică principiile fundamentale ale securității informației: confidențialitatea, integritatea și disponibilitatea și identifică tipurile de vulnerabilități și amenințări comune domeniului. 1.2. Definește obiectivele și politicile de securitate aliniate strategiei de afaceri. 1.3. Determină tehnologiile de criptare ce vor fi utilizate pentru protecția datelor, precum și soluții de securitate necesare. 1.4. Stabilește tipul de control al accesului pentru diverse active informaționale, în baza nivelului de criticitate și sensibilitate al acestora. 1.5. Promovează cultura organizațională de securitate prin sesiuni de educare și campanii de conștientizare a riscurilor de securitate, amenințărilor și impactul pe care îl pot avea asupra afacerii. 1.6. Dezvoltă planuri de securitate informațională și monitorizează progresul implementării planurilor, sistemelor de management al securității. 1.7. Planifică resurse adecvate pentru implementarea strategiei de securitate informațională, a soluțiilor și instrumentelor potrivite.
1. Elaborarea soluțiilor de securitate pentru infrastructuri TI 3. Aplicarea metodelor de protecție a datelor 6. Asigurarea securității aplicațiilor și dezvoltarea sigură	**CP 2.** Dezvoltarea soluțiilor de securitate pentru protecția infrastructurilor TI, aplicațiilor și datelor.	2.1. Aplică cerințele de asigurare a confidențialității, integrității, disponibilității, principiile de funcționare, caracteristicile tehnice, metodele de implementare, configurare, testare, asigurare a mentenanței față de soluțiile de securitate. 2.2. Utilizează metode de proiectare și limbaje de modelare pentru elaborarea schemelor și diagramelor de structură, comportament, de componente, de activități și de stare a instrumentelor de soluționare a problemelor de securitate. 2.3. Aplică concepte, metode și limbaje specifice dezvoltării de aplicații securizate sau de soluții de prevenire, detectare sau de protecție împotrivă amenințărilor și atacurilor de securitate: concurente, timp real, non-timp real, locale, distribuite, încorporate, non-încorporate, mobile, on-line etc. 2.4. Elaborează algoritmi, modele și organigrame de implementare software a strategiilor de monitorizare, identificare, autentificare, auditare și control pentru soluționarea problemelor de securitate. 2.5. Rezolvă probleme practice de răspuns la incidente și asigurare a continuității activităților prin selectarea și adaptarea celor mai adecvate controale și tehnologii informatice de securitate. 2.6. Evaluează modul de implementare și utilizare a aplicațiilor de securitate utilizând algoritmi, medii de programare și metode de analiză, testare, investigare.

1. Elaborarea soluțiilor de securitate pentru infrastructuri TI 3. Aplicarea metodelor de protecție a datelor 4. Detectarea și gestionarea incidentelor de securitate 5. Evaluarea vulnerabilităților și testarea securității	**CP 3.** Administrarea securității sistemelor TIC prin configurare, monitorizare și evaluare.	3.1. Evaluează vulnerabilitățile în sistemele TIC, utilizând analiza riscului, pentru a determina măsurile de protecție necesare. 3.2. Configurează sistemele TIC conform standardelor și politicilor de securitate prin aplicarea regulilor de control al accesului pentru utilizatori și resurse. 3.3. Determină tipul de criptare utilizat pentru protecția datelor sensibile prin monitorizarea continuă a soluțiilor de securitate implementate. 3.4. Utilizează instrumente de monitorizare a rețelelor și sistemelor TI pentru detectarea incidentelor de securitate, interpretarea alertelor de securitate log-urilor de sistem și identificarea activităților suspecte. 3.5. Investighează evenimentele de securitate prin elaborarea și implementarea planurilor de răspuns la incidente. 3.6. Realizează audituri și controale periodice de securitate pentru a verifica și evalua conformitatea sistemelor TIC. 3.7. Evaluează amenințările din domeniu, tendințele și tehnologiile noi pentru îmbunătățirea securității sistemelor TIC.
2. Gestionarea riscurilor și asigurarea conformității cu standardele de securitate 4. Detectarea și gestionarea incidentelor de securitate 5. Evaluarea vulnerabilităților și testarea securității 7. Elaborarea politicilor și formarea în domeniul securității cibernetice	**CP 4.** Gestionarea riscurilor de securitate informațională conform standardelor și reglementărilor în vigoare.	4.1. Stabilește metodologia de analiză a riscurilor de securitate. 4.2. Identifică activele care necesită a fi protejate, nivelul de clasificare, proprietarul și costul de înlocuire a lor. 4.3. Determină vulnerabilitățile existente, consultând bazele deschise de vulnerabilități sau cu ajutorul instrumentelor specializate. 4.4. Depistează amenințările care pot fi realizate prin intermediul vulnerabilităților asociate activelor și impactul posibil. 4.5. Întocmește planuri de tratare a riscurilor prin evaluarea nivelul de risc în baza metodologiei stabilite și prioritizarea riscurilor. 4.6. Identifică cele mai adecvate controale de securitate pentru a minimiza nivelul de risc până la cel acceptat. 4.7. Testează nivelele de maturitate ale controalelor implementate prin evaluarea nivelului de conformitate cu cerințele standardelor și reglementărilor aplicabile. 4.8. Stabilește procedurile de revizuire și optimizare a ciclului de gestionare a riscurilor de securitate.