



Ministerul Educației și Cercetării al Republicii Moldova

I.P. Centrul de Excelență în Energetică și Electronică

„Aprob”

Mariana BARLADEAN

Directoare I.P. Centrul de Excelență în
Energetică și Electronică

15 septembrie 2025



Curriculum la modulul

S.08.O.023 Securitatea informațională

Specialitatea: **0611.1 Calculatoare**

Calificarea: **0611.1.1 Tehnician/tehniciană suport tehnic al
calculatoarelor**

Chișinău 2025 Curriculumul a fost elaborat în baza ordinului Ministerului Educației și Cercetării al Republicii Moldova, numărul 1229/2024, cu privire la aprobarea listei instituțiilor de învățământ desemnate responsabile pentru elaborarea planurilor de învățământ la programele de formare profesională postsecundară și postsecundar nonterțială.



Aprobat la:

Consiliul metodic-științific al I.P. Centrul de Excelență în Energetică și Electronică din
15 septembrie 2025, directoare Mariana BARLADEAN



Autor:

1) Ana IAȚCO, profesor discipline de specialitate, grad didactic II, I.P. CEEE

Recenzenți:

1. GAMA COMPUTER SRL, adresa: str. Meșterul Manole 12/2, mun. Chișinău, Director: Mincheivici Sergiu;

2. S.R.L. RC-ELECTRON, str. Calea Ieșilor, 16/1, mun. Chișinău, Director: Cebanu Radu.

Adresa Curriculumului în Internet:

Portalul național al învățământului profesional tehnic:

<http://www.ipt.md/ro/produse-educationale>

Cuprins

<i>I. Preliminarii</i>	<i>4</i>
<i>II. Motivația, utilitatea modulului pentru dezvoltarea profesională</i>	<i>4</i>
<i>III. Competențele profesionale specifice modulului</i>	<i>5</i>
<i>IV. Administrarea modulului</i>	<i>5</i>
<i>V. Unitățile de învățare</i>	<i>6</i>
<i>VI. Repartizarea orientativă a orelor pe unități de învățare</i>	<i>9</i>
<i>VII. Studiu individual ghidat de profesor</i>	<i>9</i>
<i>VIII. Lucrările practice recomandate</i>	<i>10</i>
<i>IX. Sugestii metodologice</i>	<i>11</i>
<i>X. Sugestii de evaluare a competențelor profesionale.....</i>	<i>12</i>
<i>XI. Resursele necesare pentru desfășurarea procesului de studii</i>	<i>13</i>
<i>XII. Resursele didactice recomandate elevilor.....</i>	<i>13</i>

I. Preliminarii

Curriculumul pentru modulul *Securitatea informațională* este elaborat în baza ordinului MEC 768/2024 *Cu privire la aprobarea Referențialului de corelare a programelor de studii (specialităților) și calificărilor pentru învățământul profesional tehnic postsecundar și postsecundar nonterțiar și a planului de învățământ ediția 2024*, aprobat prin Ordinul MEC nr. 1229/2024. Modulul *Securitatea informațională* este un element formativ al pachetului curricular pentru calificările din domeniul de formare profesională *Utilizarea calculatorului* și face parte din componenta de specialitate a planului de învățământ la programul de studii 0611.1 Calculatoare.

Scopul acestui curs este de a preda elevilor fundamentele metodologice, procedurale și organizaționale privind protecția informațiilor, precum și utilizarea specializată a software-lor și hardware-lor pentru securitatea informației la utilizarea rețelelor de calculatoare.

La predarea acestei discipline se stabilesc următoarele sarcini:

- ✓ formularea principalelor sarcini și metode de protecție a informațiilor;
- ✓ familiarizarea elevilor cu principiile elaborării politicilor de securitate a informațiilor;
- ✓ studierea mecanismelor de securitate a informațiilor;
- ✓ analiza algoritmilor criptografici;
- ✓ studierea principiilor verificării integrității informației;
- ✓ identificarea programelor distructive;
- ✓ găsirea soluțiilor teoretice și practice de reducere/eliminare a pericolelor;
- ✓ implementarea suitelor de protocoale de securitate în rețelele de comunicații.

Scopul studierii acestui modul constă în formarea competenței profesionale specifice privind aplicarea mecanismelor pentru securitatea informațională.

Modulul în cauză poate fi studiat după însușirea în mod obligatoriu a următoarelor unități de curs:

- Informatica;
- G.01.O.001 Tehnologia informației.

II. Motivația, utilitatea modulului pentru dezvoltarea profesională

Studierea modulului *Securitatea informațională* va contribui la formarea și dezvoltarea de competențe profesionale ce corespund nivelului patru de calificare:

- cunoștințe factice, principii, procese și concepte generale în domeniul securității informaționale;
- abilități practice necesare pentru instalarea, configurarea și întreținerea softwar-ului și hardwar-ului pentru asigurarea securității informaționale;
- asumarea responsabilității pentru crearea unui mediu adecvat de muncă și remediarea situațiilor de risc.

Competențele formate și dezvoltate în cadrul acestui modul vor fi necesare pentru comunicarea și respectarea eticii profesionale în relațiile cu utilizatorii calculatoarelor personale.

III. Competențele profesionale specifice modului

Modulul *Securitatea Informațională* va contribui la formarea rezultatelor învățării descrise în *Standardul de calificare Tehnician/tehniciană suport tehnic al calculatoarelor*, care, la rândul lor, vor asigura formarea competențelor profesionale specificate în standardul ocupațional:

Rezultate ale învățării (RÎ) din standardul de calificare	Competențe profesionale (CP) din standardul ocupațional
RÎ10. Absolventul poate identifica și configura sisteme și aplicații pentru asigurarea integrității, confidențialității și disponibilității informațiilor.	CP10. Elaborează și implementează politici, proceduri și standarde privind securitatea informației în organizații.

Pentru a atinge rezultatul învățării din *Standardul de calificare Tehnician/tehniciană pentru suportul tehnic al calculatoarelor*, după studierea modului *Securitatea Informațională*, elevii vor fi capabili:

- să evalueze securitatea sistemului informatic;
- să laboreze politici de securitate;
- să aplice sistemele criptografice în practică;
- să utilizeze software specializate;
- să aplice metode de protecție a informațiilor în sfera profesională și să utilizeze un model de comportament sigur pe Internet.

IV. Administrarea modului

Semestrul	Numărul de ore			Modalitatea de evaluare	Numărul de credite	
	Total	Contact direct				Lucrul individual
		Prelegeri	Practică/ laborator			
VIII	90	40	20	30	Examen	3

V. Unitățile de învățare

Rezultatele învățării	Unități de conținut	Abilități
RÎ1. Identificarea problemelor de securitate informațională. Aplicarea mecanismelor securității informaționale	1. Asigurarea metodologică a securității informaționale 1.1. Introducere în securitatea informațională. Confidențialitate, Integritate, Disponibilitate (CIA) 1.2. Problemele securității informaționale. <i>Starea actuală, perspectivă și retrospectivă. Sisteme informaționale, mijloace, canale, rețele și medii. Concepte și definiții de bază a securității informaționale.</i> 1.3. Amenințări cibernetice moderne și tipologii de atacuri (ransomware, phishing, APT, botnet). 1.4. Politica securității informaționale. <i>Nivelul administrativ al securității informațiilor. Politică de securitate. Programe de securitate. Nivelul procedural al securității informaționale.</i> 1.5. Mecanismele securității informaționale. <i>Identificare, autentificare. Autentificarea biometrică. Controlul accesului. Înregistrarea și auditul.</i>	1. Identificarea problemelor de securitate informațională. 2. Clasificarea atacurilor informaționale. 3. Tablirea principalelor sarcini de protecție a informației. 4. Utilizarea mecanismelor securității informaționale. 5. Explicarea principiilor confidențialității, integrității și disponibilității informației. 6. Identificarea tipurilor de amenințări și scenariilor de atac în mediul digital. 7. Crearea de parole sigure și aplicarea metodelor moderne de autentificare. 8. Deosebirea metodelor de criptare și rolul lor în securizarea datelor.
	2. Criptografia 2.1. Definiții și noțiuni de bază. <i>Tehnici utilizate în criptografie. Substituția. Permutarea sau transpoziția. Cifrul lui Vernam. Ascunderea informațiilor. Steganografia. Filigranarea.</i> 2.2. Criptografie modernă: criptare simetrică, asimetrică, hashing. Algoritmi actuali (AES, RSA, SHA). ** 2.3. Sisteme de criptare prin chei simetrice (private). 2.4. Sisteme de criptare prin chei asimetrice (publice).	1. Definirea conceptelor fundamentale de criptosecuritate. 2. Aplicarea algoritmilor de criptare în rezolvarea problemelor date. 3. Distingerea tipurilor de criptosisteme. 4. Aplicarea metodei steganografice la protecția datelor. 5. Aplicarea principiilor semnăturii digitale
RÎ2. Aplicarea algoritmilor de criptare. Utilizarea metodei steganografice de protecție a datelor cu caracter confidențial		

Rezultatele învățării	Unități de conținut	Abilități
	2.5. Semnătura digitală. Sisteme de certificare a cheilor publice. Infrastructura cheilor publice (PKI).	pentru verificarea autenticității unui document. 6. Identificarea măsurilor de protecție de bază pentru rețele locale.
3. Protecția programelor și a datelor		
R13. Implementarea software-lor și hardware-lor specializate pentru securitatea datelor.	3.1. Software pentru securitatea datelor. <i>Organizarea protecției prin parolă. Software și hardware pentru asigurarea securității informațiilor în rețele de calculatoare. Protecția documentelor.</i> 3.2. Malware actual: viruși, troieni, ransomware, spyware, rootkit-uri și metode de răspândire 3.2. Viruși și antiviruși. <i>Protejarea software-ului de viruși ce distrug acțiunile și modifică programul. Virușii computerizați, clasificarea, tipuri de acțiuni distructive. Software antivirus. Principii de lucru, exemple.</i> 3.3. Ingineria socială și manipularea utilizatorilor. Atacuri psihologice în mediul online. 3.4. Securitatea parolelor. Autentificare cu doi factori (2FA/MFA) și politici moderne de parole. 3.5. Securitatea rețelor de calculatoare: firewall, IDS/IPS, segmentare, VLAN și protecția traficului. 3.6. Protocoale securizate: HTTPS, TLS, SSH, IPsec și securizarea comunicațiilor. 3.7. VPN — tehnologii și utilizarea lor în protecția datelor. 3.8. Securitatea sistemelor de operare. Actualizări, patching,	1. Identificarea software-lor specializate. 2. Aplicarea politicilor de securitate. 3. Instalarea software-lui antivirus. 4. Aplicarea mecanismelor în securizarea rețelor de calculatoare. 5. Asigurarea securității în sistemele de operare moderne. 6. Alegerea și utilizarea protocoale sigure pentru transmiterea datelor. 7. Configurarea / utilizarea un VPN pentru protejarea traficului. 8. Aplicarea politicilor de actualizare, patching și configurare sigură a sistemelor. 9. Evaluarea riscurilor din cloud și setarea corectă a opțiunii de securitate. 10. Protejarea dispozitivelor mobile și IoT împotriva atacurilor specifice. 11. Monitorizarea evenimentelor de securitate și raportarea incidentelor informatice. 12. Analizează tendințe lor și anticiparea

Rezultatele învățării	Unități de conținut	Abilități
	configurări sigure. 3.9. Backup, recuperarea datelor și strategii anti-ransomware. 3.10. Protecția datelor cu caracter personal. Legislație și GDPR.	riscurile viitoare în securitate.

VI. Repartizarea orientativă a orelor pe unități de învățare

Nr. crt.	Unități de învățare	Numărul de ore			
		Total	Contact direct		Lucrul individual
			Prelegeri	Practică/ Seminar	
1.	Asigurarea metodologică a securității informaționale.	24	10	4	10
2.	Metode criptografice pentru protecția informației.	26	10	6	10
3.	Protecția programelor și a datelor	40	20	10	10
	Total	90	40	20	30

VII. Studiu individual ghidat de profesor

Materii pentru studiul individual	Produse de elaborat	Modalități de evaluare
1. Asigurarea metodologică a securității informaționale.		
1.1. Problemele securității informaționale. 1.2. Politica securității informaționale. Mecanismele securității informaționale.	Studiu de caz	Raport Prezentare PPT
2. Metode criptografice pentru protecția informației.		
2.1. Concepte fundamentale de criptosecuritate. Modele de criptosisteme. 2.2. <i>Sisteme criptografice cu cheie secretă. Sisteme criptografice cu cheie public. Exemple de algoritmi.</i> 2.3. Controlul integrității datelor. 2.4. Metoda steganografică de protecție a datelor.	Algoritmi simple de criptare Cod program Studiu de caz Metoda steganografică de protecție a datelor.	Prezentarea programului. Interpretarea și prezentarea rezultatelor Demonstrarea aplicațiilor

Materii pentru studiul individual	Produse de elaborat	Modalități de evaluare
3. Protecția programelor și a datelor		
3.1. Software pentru securitatea datelor. 3.2. Vruși și antivirusi. 3.3. Securitatea rețelelor de calculatoare	Analiza gamei software-lor specializate. Studiu de caz	Prezentarea studiului

Notă: Termenele de executare a studiului individual ghidat de profesor vor fi specificate în Planul de lungă durată.

VIII. Lucrările de laborator recomandate

Unități de învățare	Lista lucrărilor de laborator	Ore
1. Asigurarea metodologică a securității informaționale.	1. Probleme de securitate a informațiilor. Evaluarea amenințărilor. Mecanisme de securitate. 2. Gestionarea drepturilor de acces la fișiere și dosare (SO Windows, Linux.)	4
2. Metode criptografice pentru protecția informației.	1. Managementul parolelor. 2. Crearea unui token de securitate (Rohos Logon Key, Rohos face Logon). 3. Copiile de siguranță și restabilirea informațiilor (Backup&Restore). 4. Criptarea ca metodă de securitate a informațiilor. Tehnologii de criptare. 5. Criptosisteme cu cheie publică. Algoritmul DES. Criptosistem cu cheie privată. Algoritmul RSA. 6. Metode steganografice de protecție a informațiilor. 7. Steganografia. Filigranarea. 8. Studiarea funcționării și a rolului unui firewall în securitatea sistemelor informatice: pornirea și configurarea firewall-ului sistemului de operare.	16
Total		20

IX. Sugestii metodologice

Curriculumul la modulul *Securitatea informațională* are drept scop formarea și dezvoltarea competențelor profesionale ale elevilor din învățământul profesional tehnic postsecundar.

Strategiile, metodele și tehnicile utilizate în procesul de formare a competențelor se vor realiza în cadrul unor forme de organizare a acțiunii didactice. În procesul de instruire, componentele competenței se formează prin sarcini didactice cu caracter de problemă, prin adaptarea unei game de tehnici interactive care asigură o educație dinamică, formativă, motivațională, reflexivă și continuă.

Metodele recomandate pentru a fi utilizate în procesul de predare-învățare sunt:

Instruirea asistată de calculator este o metodă didactică care valorifică principiile de modelare și analiză cibernetică. Prin intermediul calculatorului se pune la dispoziția elevului un set de probleme, care necesită a fi analizate, completate sau elaborate. Utilizarea metodei va oferi posibilitatea de organizare a informației conform cerințelor programei adaptabile la capacitățile fiecărui elev; stimularea cognitivă a elevului prin secvențe didactice și întrebări ce vizează depistarea unor lacune, probleme, situații-problemă; rezolvarea sarcinilor didactice prezentate anterior prin reactivarea sau obținerea informațiilor necesare de la resursele informatice apelate prin intermediul calculatorului; realizarea unor sinteze recapitulative după parcurgerea unor teme, module de studiu, lecții; asigurarea unor exerciții suplimentare de stimulare a creativității elevului.

Problematizarea mai poate fi denumită și predare prin rezolvare de probleme sau predare productivă de probleme. Conform acestei metode instruitului este pus în fața unor dificultăți create în mod deliberat, și prin depășirea lor învață ceva nou. „Punctul forte” al metodei îl constituie situația-problemă. Din această cauză este necesar de a formula corect situația. Prin intermediul situației create, instruitul este cointerestat de a studia, analiza și a participa la rezolvarea problemei. Aplicarea acestei metode presupune parcurgerea a patru etape:

- *Formularea problemei* – este descrisă situația problemă, explicarea, după necesitate a diferitor puncte cheie, care ar permite instruitului să perceapă problema;
- *Studierea problemei* – se lucrează în mod independent, sunt reactualizate anumite resurse;
- *Determinarea soluției* – în cadrul acestei etape sunt pregătite resursele necesare, se descoperă mijloacele care duc la rezolvarea problemei și este analizat modul de aplicare a acestora în determinarea soluției;
- *Obținerea rezultatului final* – se analizează rezultatul obținut și formate anumite concluzii.

Algoritmizarea reprezintă o metodă de predare-învățare bazată pe utilizarea și valorificarea algoritmilor în procesul de instruire. Algoritmul de instruire se reprezintă sub forma unui grup de scheme, unui set de operații, iar prin parcurgerea lor într-o ordine bine stabilită duce la rezolvarea unui set de probleme caracteristice unei familii de situații. În rezultatul aplicării acestei metode se va oferi posibilitatea studentului de a elabora treptat propriile scheme, aplicabile în diferite circumstanțe didactice.

Metoda studiul de caz valorifică o situație reală care se analizează și se rezolvă. Avantajul metodei, constă în faptul că fiecare dintre elevi își va aduce aportul la analiza și rezolvarea problemei. În utilizarea acestei metode se conturează câteva etape:

- Selectarea și prezentarea cazului;
- Organizarea echipelor de lucru;
- Prelucrarea și conceptualizarea;
- Structurarea finală a studiului.

Instruirea prin proiecte reprezintă o modalitate de instruire/autoinstruire grație căreia elevii, dar mai ales elevii efectuează o cercetare orientată spre obiective practice și finalizată într-un produs ce poate fi un obiect, un aparat, o instalație, o culegere tematică, un album, o lucrare științifică etc.

X. Sugestii de evaluare a competențelor profesionale

Axarea procesului de învățare–predare–evaluare pe competențe presupune efectuarea evaluării pe parcursul întregului proces de instruire. Evaluarea continuă va fi structurată în evaluări formative și evaluări sumative (finale). Pornind de la caracterul aplicativ al disciplinei „*Securitate informațională*”, evaluarea va viza mai mult aspectele ce țin de interpretarea creativă a informațiilor și capacitatea de a rezolva situațiile de problemă.

Activitățile de evaluare vor fi orientate spre motivarea elevilor și obținerea unui feedback continuu, fapt ce va permite corectarea operativă a procesului de învățare, stimularea autoevaluării și a evaluării reciproce, evidențierea succeselor, implementarea evaluării selective sau individuale. Pentru a eficientiza procesele de evaluare, înainte de a demara evaluările propriu-zise, cadrul didactic va aduce la cunoștința elevilor tematica lucrărilor, modul de evaluare (bareme/grile/criterii de notare) și condițiile de realizare a fiecărei evaluări.

În cazul modulului „*Sisteme de operare*”, un element inovator al evaluării este posibilitatea de utilizare a resurselor educaționale digitale, care includ teste ce pot fi administrate atât pe calculatoarele locale, cât și on-line.

Pentru a permite o individualizare a evaluării și o motivare suplimentară a elevilor, sarcinile de evaluare formativă vor fi ierarhizate pe grade de dificultate.

Metodele folosite pentru evaluarea continuă presupun chestionarea orală sau scrisă, studiile de caz, lucrările practice, proiectele, testările interactive asistate de calculator. În procesul evaluărilor continue se va da atât o apreciere obiectivă a cunoștințelor și competențelor elevilor, cât și a progreselor înregistrate de aceștia.

Evaluarea sumativă se va efectua la sfârșitul fiecărui semestru și an școlar. Instrumentele de evaluare sumativă vor include itemi de tip problemă pentru rezolvarea la calculator, testelor asistate de calculator, lucrării scrise, probe și lucrări practice.

Pentru desfășurarea evaluărilor asistate de calculator, se recomandă utilizarea instrumentarului de testare, elaborat de către marii producători de calculatoare, de echipamente de rețea și produse-program.

XI. Resursele necesare pentru desfășurarea procesului de studii

Instruirea teoretică – se va desfășura în săli de clasă, amenajate și echipate cu tablă interactivă și echipamente multimedia, seturi de planșe, proiector digital, laptop. Capacitatea sălii – 30 de locuri.

Instruirea practică – se va desfășura în laboratoare specializate, echipate cu tablă și calculatoare. Capacitatea sălii de laborator – 15 locuri de lucru (vezi tabelul de mai jos).

Cerințe față de sălile de curs	
Pentru orele de laborator	- Laborator de informatică care asigură fiecărui elev un calculator; - Tablă interactivă.
Cerințe tehnice	
Parametri tehnici minimi ale calculatorului	Procesor: 2 GHz Memorie operativă: 4 GB Unitate de stocare: 320 GB Afișaj și grafică: size: 22", resolution: 1366x768 Network: Ethernet, 100 Mb
Software	- Sisteme de operare; - Imagini de disc cu sisteme de operare ISO, MDF/MDS, DMG etc.
Consumabile:	- Discuri optice CD, DVD; - Stick-uri USB.

XII. Resursele didactice recomandate elevilor

Nr. crt.	Denumirea resursei	Locul în care poate fi consultată/ accesată/ procurată resursa
1.	Dumitru Oprea, Protecția și securitatea informațiilor, Polirom, 2007	Librăria „Mihai Eminescu”
2.	С. П. Расторгуев, Основы информационной безопасности, Академия, 2009.	Biblioteca digitală
3.	Bogdan Groza, Introducere în Criptografie, Editura Politehnica, 2007.	Biblioteca digitală
4.	Ioan-Cosmin MIHAI, Securitatea informațiilor, Editura Sitech, 2012.	Librăria „Mihai Eminescu”
5.	Popa Sorin Eugen, Securitatea sistemelor informatice, note de curs și aplicații, Universitatea din Bacău.	http://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf
6.	Lect. Dr. M. Apetrii, Introducere în securitatea rețelelor.	http://www.math.uaic.ro/~cefair/files/intr_in_securitatea_retelelor.pdf