



Ministerul Educației și Cercetării al Republicii Moldova

Centrul de Excelență în Energetică și Electronică

Aprob
Directorul Centrului de Excelență
în Energetică și Electronică

Mariana BARLADEAN

18 septembrie 2023

Curriculum modular

S.08.O.024 Securitatea sistemelor de calcul și a rețelelor de calculatoare

Specialitatea: 61110 – Calculatoare

Calificarea: Tehnician pentru suportul tehnic al calculatoarelor

Chișinău 2023

Curriculumul a fost elaborat în baza ordinului Ministerului Educației și Cercetării al Republicii Moldova, numărul 83, din data de 14.02.2022, cu privire la aprobarea listei instituțiilor de învățământ desemnate responsabile pentru elaborarea planurilor de învățământ la programele de formare profesională postsecundară și postsecundar nonterțială



Autori:

Lucia SINEAVSCHI, grad didactic superior, Centrul de Excelență în Energetică și Electronică.

Victoria CATANĂ, grad didactic unu, Colegiul Politehnic din Bălți.

Aprobat de:

Consiliul metodic științific al Centrului de Excelență în Energetică și Electronică.

Director adjunct pentru instruire

Gheorghe ZVEZDENCO

18 septembrie 2023

Recenzenți:

1. GAMA COMPUTER SRL adresa: str. Meșterul Manole, 12/2, Chișinău, Director: Minchevici Sergiu.
2. VIC-COM INFO SRL, adresa: str. Albișoara 68/3 of. 72, MD, mun. Chișinău, Director: Tabuci Victor.

Adresa Curriculumului în Internet:

<https://ceee.md/programe-de-formare-profesionala/>

Cuprins

I. Preliminarii.....	4
II. Motivația, utilitatea modulului pentru dezvoltarea profesională.....	4
III. Competențele profesionale specifice modulului.....	5
IV. Administrarea modulului.....	5
V. Unitățile de învățare.....	6
VI. Repartizarea orientativă a orelor pe unități de învățare	8
VII. Studiu individual ghidat de profesor	8
VIII. Lucrările de laborator/practice recomandate.....	9
IX. Sugestii metodologice	10
X. Sugestii de evaluare a rezultatelor învățării	11
XI. Resursele necesare pentru desfășurarea procesului de studiu	12
XII. Resursele didactice recomandate elevilor	13

I. Preliminarii

Disciplina Securitatea sistemelor de calcul și a rețelelor de calculatoare are orientare profesională și științifică generală. 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 principiile 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:

- G.01.O.001 Tehnologia informației
- S.06.O.017 Sisteme de operare
- S.07.O.019 Arhitectura și asamblarea sistemelor de calcul
- S.07.O.020 Rețele de calculatoare

II. Motivația, utilitatea modulului pentru dezvoltarea profesională

Studierea modulului *Securitatea sistemelor de calcul și a rețelelor de calculatoare* 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 software-ului și hardware-ului pentru asigurarea securității informaționale;
- asumarea responsabilității pentru crearea unui mediu adecvat de muncă și remedierea 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

Elementul de bază al Curriculumului sunt competențele ce trebuie formate și dezvoltate în procesul de instruire profesională. Competențele profesionale specifice modului *Securitatea sistemelor de calcul și a rețelelor de calculatoare* includ:

- CS1. Identificarea tipurilor de atacuri informatice și a mecanismelor de protecție pentru prevenirea acestora;
- CS2. Aplicarea unor concepte și metode noi pentru asigurarea securității, siguranței și ușurinței în exploatare sistemelor de calcul;
- CS3. Utilizarea aplicațiilor și tehnologiilor pentru securitatea sistemelor de calcul și a rețelelor de calculatoare;
- CS4. Configurarea sistemelor de operare și a mecanismelor de asigurare a securității;
- CS5. Aplicarea metodelor de protecție a informațiilor în sfera profesională și utilizarea unui 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	120	30	30	60	Examen	4

V. Unități de învățare

Unități de competență	Unități de conținut	Abilități
1. Asigurarea metodologică a securității informaționale		
UC1. Identificarea problemelor de securitate informațională UC2. Aplicarea mecanismelor securității informaționale	Problemele securității informaționale. Starea actuală, perspectivă și retrospectivă. Sisteme informaționale, mijloace, canale, rețele și medii. Concepte și definiții de bază a securității informaționale. Amenințări informaționale. Atac informațional. Canale tehnice de scurgere a informației. Principalele sarcini de protecție a informației. Politica securității informaționale. Nivelul administrativ al securității informațiilor. Politică de securitate. Programe de securitate. Nivelul procedural al securității informaționale. Mecanisme securității informaționale. Identificare, autentificare. Autentificarea biometrică. Controlul accesului. Înregistrarea și auditul.	A1. Identificarea problemelor de securitate informațională. A2. Clasificarea atacurilor informaționale. A3. Stabilirea principalelor sarcini de protecție a informației. A4. Utilizarea mecanismelor securității informaționale.
2. Amenințările de securitate a sistemelor de calcul și a rețelelor de calculatoare		
UC3. Implementarea software-lor și hardware-lor specializate pentru securitatea datelor.	Software pentru securitatea sistemele de calcul Organizarea protecției prin parolă. Software și hardware pentru asigurarea securității informațiilor în rețelele de calculatoare. Protecția documentelor. Control integrității. Protecția copiilor. Viermi, viruși și intruși. Protejarea software-ului de viruși ce distrug acțiunile și modifică programul. Virușii computerizați, clasificarea, tipuri de acțiuni distructive. Software antivirus. Principii de lucru, exemple. Metodele de securitate Modele de securitate multinivel. Modele de securitate multilaterale. Configurarea serviciilor de jurnalizare și audit la sistemele de operare. Utilizarea softurilor specializate.	A5. Detectarea atacurilor. A6. Aplicarea instrumentelor de eliminare a software-ului rău intenționat. A7. Aplicarea softurilor pentru restabilirea informațiilor. A8. Aplicarea programelor de tip antivirus. A9. Asigurarea securității în sistemele de operare moderne.

Unități de competență	Unități de conținut	Abilități
3. Criptografia		
UC4. Aplicarea algoritmilor de criptare UC5. Implementarea software-lor și hardware-lor specializate pentru securitatea datelor. UC6. Utilizarea metodei steganografice de protecție a datelor cu caracter confidențial	Definiții și noțiuni de bază. Tehnici utilizate în criptografie. Substituția. Permutarea sau transpoziția. Cifrul lui Cezar. Cifrul lui Vernam. Ascunderea informațiilor. Steganografia. Filigranarea. Sisteme de criptare prin chei simetrice (private). Sisteme de criptare prin chei asimetrice (publice). Semnătura digital. Sisteme de certificare a cheilor publice. Infrastructura cheilor publice (PKI).	A10. Definirea conceptelor fundamentale de criptosecuritate. A11. Aplicarea algoritmilor de criptare în rezolvarea problemelor date. A12. Distingerea tipurilor de criptosisteme. A.13. Aplicarea metodei steganografice la protecția datelor.
4. Securizarea rețelelor de calculatoare		
UC7. Utilizarea barierelor pentru securizarea rețelelor UC8. Configurarea VPN-urilor pentru a securiza rețelelor și a sistemelor de calcul UC9. Asigurarea securității în rețelele wired și wireless	Implementarea barierelor - firewall Mecanisme utilizate în securizarea rețelelor. Noțiuni privind securizarea rețelei. Filtrarea pachetelor. Monitorizarea conexiunilor. Rolul și menirea unui firewall. Actualizarea unui firewall. Configurarea unui firewall. Sistemul de traducere a adreselor. Securizarea echipamentelor de rețea (wired și wireless). Tipuri de atacuri. Criptarea în rețelele WLAN. Tehnici de securitate wireless. WI-FI Protected Access (WPA). Securitatea în rețelele WiFi. Securitatea în rețelele WiMax. Limitarea accesului la rețelele WLAN. Procesul de autentificare în cadrul rețelelor WLAN. Filtrarea traficului în rețelele WLAN.	A14. Setarea regulilor pentru filtrarea traficului. A15. Distingerea tipurilor de atac în rețea. A16. Utilizarea instrumentelor de verificare a serviciului Firewall. A17. Utilizarea aplicațiilor pentru detectarea atacurilor de tip malware. A18. Configurarea accesului la distanță. A19. Configurarea mecanismului de autentificare. A20. Limitarea accesului la rețelele WLAN. A21. Criptarea datelor în rețelele Wireless. A22. Filtrarea traficului în rețelele Wireless. A23. Planificarea operațiilor de întreținere a rețelelor fără fir.

VI. Repartizarea orientativă a orelor pe unități de învățare

Nr. crt.	Unități de învățare	Numărul de ore			
		Total	Contact direct		Lucrul individual
			Prelegeri	Practică/ Laborator	
1.	Asigurarea metodologică a securității informaționale	20	6	4	10
2.	Amenințările de securitate a sistemelor de calcul și a rețelelor de calculatoare	24	8	6	10
3.	Criptografia	38	8	10	20
4.	Securizarea rețelelor de calculatoare	38	8	10	20
	Total	120	30	30	60

VII. Studiu individual ghidat de profesor

Materii pentru studiul individual	Produse de elaborat	Modalități de evaluare	Termeni de realizare
1. Asigurarea metodologică a securității informaționale			
Problemele securității informaționale. Politica securității informaționale. Mecanismele securității informaționale.	Proiect individual Analiza softurilor de securitate.	Prezentarea proiectelor	Săptămâna 3
2. Amenințările de securitate a sistemelor de calcul și a rețelelor de calculatoare			
Software pentru securitatea sistemele de calcul. Viermi, viruși și intruși. Metodele de securitate.	Studiu de caz.	Analiza studiilor de caz	Săptămâna 6
3. Criptografia			
Sisteme de criptare prin chei simetrice (private). Sisteme de criptare prin chei asimetrice (publice).	Proiect de grup	Prezentarea proiectelor	Săptămâna 8

Materii pentru studiul individual	Produse de elaborat	Modalități de evaluare	Termeni de realizare
4. Securizarea rețelelor de calculatoare			
Implementarea barierelor – firewall. Securizarea echipamentelor de rețea (wired și wireless).	Proiect în grup Aplicarea metodelor de securitate.	Prezentarea proiectelor	Săptămâna 10

VIII. Lucrările de laborator recomandate

Tematica lucrărilor de laborator va include:

1. Gestionarea drepturilor de acces la fișiere și dosare (SO Windows, Linux). Tipuri de conturi de utilizator. Drepturi de acces la fișiere și dosare. Politicile de securitate privind conturile utilizatorilor.
2. Managementul parolelor. Sisteme de management al parolelor (KeePass, eWallet, LastPass, 1Password, RoboForm etc.).
3. Viermi, viruși și intruși într-o rețea de calculatoare.
4. Utilizarea antivirusilor pentru securizarea datelor.
5. Copiile de siguranță și restabilirea informațiilor. Sisteme de Backup&Restore.
6. Criptarea ca metodă de securitate a informațiilor. Algoritmi elementari.
7. Criosisteme cu cheie publică. Algoritmul DES.
8. Criosistem cu cheie privată. Algoritmul RSA.
9. Vulnerabilitatea algoritmilor criptografici
10. Metode steganografice de protecție a informațiilor.
11. Principiile fundamentale ale unei rețele de calculatoare securizată.
12. Scanarea rețelei. Scanarea la nivel de dispozitiv.
13. Studiarea funcționării și a rolului unui firewall în securitatea sistemelor informatice: pornirea și configurarea firewall-ului sistemului de operare.
14. Instalarea și configurarea dispozitivelor Bluetooth securizat.
15. Securizarea datelor în rețelele Wireless.

În activitățile de laborator, accentul se va pune pe îndeplinirea cu exactitate și la timp a sarcinilor de lucru. Realizarea sarcinilor în cadrul activităților de laborator va urmări nu numai dezvoltarea abilităților individuale, dar și a celor de lucru în echipă.

IX. Sugestii metodologice

Curriculumul la modulul *Securitatea sistemelor de calcul și a rețelelor de calculatoare* 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 elevul 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 elevului 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 *Securitatea sistemelor de calcul și a rețelelor de calculatoare*, 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 *Securitatea sistemelor de calcul și a rețelelor de calculatoare*, 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, lucrări 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

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