



Ministerul Educației și Cercetării al Republicii Moldova
Centrul de Excelență în Informatică și Tehnologii Informaționale

"Aprob"

Directorul Centrului de Excelență în
Informatică și Tehnologii Informaționale



Vitalie Zavadschi

Curriculumul modular

S.07.O.023 Asistență în securitatea rețelelor de calculatoare

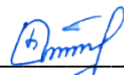
Specialitatea: **61230 Rețele de calculatoare**

Calificarea: **Tehnician pentru rețele de calculatoare**

Aprobat de:

Consiliul metodico-științific al Centrului de Excelență în Informatică și Tehnologii Informaționale, proces verbal
Nr. 3 din 31.10.2022

Director adjunct



Obadă Liuba

Autori:

Zavadschi Vitalie, grad didactic superior, Centrul de Excelență în Informatică și Tehnologii Informaționale.

Nicșan Adrian, grad didactic doi, Centrul de Excelență în Informatică și Tehnologii Informaționale.

Actualizat în baza Planului de învățământ, aprobat prin OMEC Nr.1310, din 23.11.2020.

Recenzenți:

1. *Bejenari Constanța*, manager direcția administrare și dezvoltare personal, SA "Moldtelecom"
2. *Guțu Cătălin*, manager proiecte, "VICTIANA" SRL.

Adresa Curriculumului în Internet:

<https://mecc.gov.md/ro/content/curriculum-invatamintul-profesional-tehnic-postsecundar>

Cuprins

I. Preliminarii	4
II. Motivația, utilitatea modulului pentru dezvoltarea profesională	4
III. Competențele profesionale specifice modulului	4
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 practice recomandate	8
IX. Sugestii metodologice	9
X. Sugestii de evaluare a competențelor profesionale	10
XI. Resursele necesare pentru desfășurarea procesului de studii	12
XII. Resursele didactice recomandate elevilor	12

I. Preliminarii

Asistența în securitatea rețelelor de calculatoare constă în securizarea, supravegherea, monitorizarea rețelelor de calculatoare. În ansamblu, asistența în securitatea rețelelor de calculatoare presupune:

- securizarea echipamentelor de rețea;
- monitorizarea echipamentelor;
- filtrarea pachetelor;
- securizarea stațiilor de lucru;
- construirea politicilor de securitate.

Efectuând lucrările de securizare, tehnicianul monitorizează activitatea cotidiană din rețea și asigură utilizarea resurselor companiei conform standardelor stabilite pentru utilizatorii de rețea. Totodată, asistentul rulează teste în scopul depistării eventualelor atacuri de rețea.

Ca parte a securizării rețelelor, tehnicianul monitorizează traficul, efectuând, după caz, filtrarea acestuia. De asemenea, asistentul în securitatea rețelelor de calculatoare setează servicii de filtrare a traficului, configurează i-Bariere, efectuează configurările echipamentelor de rețea, modifică, dacă este cazul, configurația rețelei.

Unitățile de curs ce trebuie studiate până la demararea procesului de instruire la modulul în cauză sunt:

- F.02.O.011 Structura și funcționarea calculatoarelor
- F.03.O.013 Programarea calculatorului;
- S.05.O.018 Arhitectura rețelelor de calculatoare;
- S.06.O.020 Mentenanța rețelelor de calculatoare;

II. Motivația, utilitatea modulului pentru dezvoltarea profesională

În fiecare zi rețelele de calculatoare și Internetul sunt folosite de milioane de persoane pentru a comunica. Rareori ne gândim la serverele și echipamentele de rețea folosite pentru a oferi clienților posibilitatea de a citi mesajele email, de a scrie pe un blog sau de a achiziționa produse online. Multe dintre cele mai utilizate aplicații de Internet se bazează pe un sistem complex de componente de rețea, servere și clienți. Securitatea rețelelor de calculatoare are o importanță deosebită, pentru a oferi clienților utilizarea în siguranță a tuturor serviciilor de rețea.

Beneficiile unei asistențe bune în securitatea rețelelor de calculatoare sunt:

- reducerea probabilităților de atacuri în rețea;
- securizarea rețelelor de calculatoare;
- securizarea stațiilor de lucru;
- funcționarea stabilă și fiabilă a rețelelor.

După studierea acestui modul elevul va fi capabil să:

- monitorizeze echipamentele;
- securizeze accesul la echipamente;
- filtreze pachete;
- monitorizeze conexiunile;
- construiască rețele private virtuale;
- administreze o rețea securizată;
- construiască politici de securitate.

III. Competențele profesionale specifice modulului

Competențele profesionale specifice modulului sunt:

- CS1. Operarea cu tipuri de atacuri.
- CS2. Securizarea unei rețele locale de calculatoare.
- CS3. Configurarea serviciului FIREWALL.

- CS4. Securizarea stațiilor de lucru.
- CS5. Construirea rețelelor virtuale private.
- CS6. Monitorizarea traficului din rețea.

IV. Administrarea modulului

Semestrul	Numărul de ore				Modalitatea de evaluare	Numărul de credite
	Total	Contact direct		Lucrul individual		
		Prelegeri	Practică/ Seminar			
VII	150	30	60	60	Examen	5

V. Unitățile de învățare

Unități de competență	Unități de conținut	Abilități
1. Amenințările de securitate într-o rețea		
UC1. Tipuri de atacuri	1. Principiile fundamentale ale unei rețele de calculatoare securizată 2. Viermi, viruși și intruși 3. Metodologia atacurilor	A1. Detectarea atacurilor de rețea. A2. Distingerea tipului atacului de rețea. A3. Folosirea de aplicații pentru detectarea malware. A4. Utilizarea sistemelor de detectare a intruziunilor. A5. Utilizarea programelor de tip antivirus.
2. Securizarea echipamentelor de rețea		
UC2. Securizarea echipamentelor	4. Securizarea accesului la echipamente și fișiere 5. Serverul RADIUS. 6. Autentificarea în rețea 7. Monitorizarea echipamentelor 8. Utilizarea funcțiilor automate	A6. Setarea accesului la echipamente. A7. Monitorizarea echipamentelor. A8. Activarea serviciilor la echipamente. A9. Configurarea clientului și serverului RADIUS A10. Dezactivarea serviciilor la echipamente . A11. Utilizarea funcțiilor automate la echipamente. A12. Monitorizarea traficului. A13. Scanarea porturilor.
3. Implementarea i-Barierilor (FIREWALLS)		
UC3. Setarea i-Barierilor	9. Liste de control al accesului 10. Filtrarea pachetelor 11. Monitorizarea conexiunilor 12. Sistemul de translatare a adreselor	A14. Setarea serviciului Firewall pe echipamente. A15. Setarea regulilor pentru filtrarea traficului. A16. Inspectarea fluxului de date. A17. Configurarea server proxy. A18. Setarea serviciului NAT. A19. Utilizarea instrumentelor de verificare a serviciului Firewall.

4. Securizarea rețelelor locale de calculatoare		
UC4. Securizarea LAN	13. Securizarea stațiilor de lucru 14. Securizarea echipamentelor Wireless și VoIP 15. Configurarea opțiunilor de securitate a comutatoarelor	A20. Instalarea programelor de tip antivirus. A21. Setarea serviciului Firewall pe stațiile de lucru. A22. Setarea protocoalelor de acces protejat la echipamente wireless. A23. Limitarea conexiunilor la echipamente wireless. A24. Utilizarea cheilor de criptare. A25. Setarea filtrului după MAC adrese.
5. Implementarea Criptografiei		
UC5. Criptarea datelor	16. Serviciul criptografic 17. Semnăturile digitale 18. Criptarea simetrică și asimetrică	A26. Folosirea protocoalelor de criptare. A27. Utilizarea semnăturilor digitale. A28. Criptarea și decriptarea informației. A29. Utilizarea cheilor de criptare. A30. Semnarea documentelor electronice. A31. Gestionarea cheilor publice.
6. Implementarea rețelelor private virtuale		
UC6. Configurarea VPN-urilor	19. VPN-urile 20. Componentele și operațiile IPSec 21. Implementarea accesului la distanță prin VPN 22. Implementarea VPN-urilor SSL	A32. Construirea rețelelor private virtuale. A33. Setarea protocoalelor de tunelare. A34. Crearea tunelurilor. A35. Configurarea serviciului IPSec. A36. Configurarea accesului la distanță. A37. Configurarea mecanismului de autentificare.
7. Administrarea rețelei de calculatoare securizată		
UC7. Utilizarea politicilor de securitate	23. Ciclu de viață a unei rețele de calculatoare securizată 24. Construirea politicilor de securitate	A38. Utilizarea listelor de acces la echipamente active deja existente în rețea. A39. Analiza istoricului a fișierilor cu log-uri. A40. Folosirea sistemelor de alertă în caz de atacuri.

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.	Amenințările de securitate într-o rețea	18	4	6	8
2.	Securizarea echipamentelor de rețea	22	4	8	10
3.	Implementarea i-Barierilor (FIREWALLS)	22	6	10	6
4.	Securizarea rețelelor de calculatoare locale	22	2	10	10
5.	Implementarea Criptografiei	22	6	8	8
6.	Implementarea rețelelor private virtuale	22	4	8	10
7.	Administrarea rețelei de calculatoare securizată	22	4	10	8
	Total	150	30	60	60

VII. Studiu individual ghidat de profesor

Materii pentru studiul individual	Produse de elaborat	Modalități de evaluare	Termeni de realizare
1. Securizarea echipamentelor de rețea			
Securizarea accesului la echipamente și fișiere	Proiect individual	Susținerea proiectului	Săptămâna 7
2. Implementarea Criptografiei			
Criptarea simetrică și asimetrică	Prezentare	Comunicare	Săptămâna 10
3. Implementarea rețelelor private virtuale			
Implementarea accesului la distanță prin VPN	Proiect individual	Susținerea proiectului	Săptămâna 13

VIII. Lucrările practice recomandate

1. Principiile fundamentale ale unei rețele de calculatoare securizată.
2. Viermi, viruși și intruși într-o rețea de calculatoare.
3. Securizarea accesului la echipamente și fișiere.
4. Utilizarea i-Barierilor (FIREWALLS).
5. Securizarea rețelelor de calculatoare locale.
6. Securizarea echipamentelor Wireless și VoIP.
7. Configurarea opțiunilor de securitate a comutatoarelor.
8. Implementarea rețelelor private virtuale.

9. Administrarea unei rețele de calculatoare securizată.
10. Ciclul de viață a unei rețele de calculatoare securizată.
11. Construirea politicilor de securitate.

IX. Sugestii metodologice

Elementul de bază al Curriculumului sunt competențele ce trebuie formate și dezvoltate în procesul de formare profesională. Acestea vor fi formate prin organizarea eficientă a procesului de instruire. Pentru aceasta sunt necesare două condiții:

1. Organizarea activităților. Pentru buna organizare a procesului didactic ambii participanți necesită de a-și organiza activitățile. De modul cum sunt organizate acestea depinde în mare măsură nivelul de formare a competențelor. În această ordine de idei, în procesul de organizare a activităților se vor asigura:

- condiții optime pentru buna colaborare dintre elev și profesor;
- un set de procese care duc la îmbunătățirea relațiilor dintre părți;
- un nivel de implicare a părților acționând în baza unor reguli și acțiuni prestabilite.

2. Selectarea adecvată a metodelor de instruire. Se recomandă utilizarea metodelor de instruire precum:

Simularea și modelarea. Simularea este utilizată pentru prezentarea la faza inițială a unor concepte, oferind posibilitatea de ghidare a activității studentului în bază de situații practice. Prin intermediul acestei metode se pot reda, prin analogie, diverse situații, raționamente, care pot să reprezinte relații dintre obiecte, fenomene, procese etc. Această metodă se recomandă pentru predarea-învățarea-evaluarea următoarelor unități de conținut:

- Amenințările de securitate într-o rețea.
- Implementarea i-Barierilor (FIREWALS)
- Implementarea rețelelor virtuale private

Problematizarea mai poate fi denumită și predare prin rezolvare de probleme sau predare productivă de probleme. Conform acestei metode instruitul 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. La crearea situației de tip problemă se va ține cont de următoarele caracteristici:

- Situația trebuie să prezinte o dificultate pentru instruit, iar pentru a găsi soluția, acesta se va confrunta cu efort de gândire;
- Situația trebuie să prezinte interes, astfel încât acesta să acționeze spre a rezolva problema;
- Situația trebuie să orienteze activitatea instruitului spre a rezolva problema și de al cointeresa pe acesta de a dobândi noi cunoștințe;
- Rezolvarea situației nu va fi posibilă fără a apela la resursele recent dobândite.

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:

1. Formularea problemei – este descrisă situația problemă, explicarea, după necesitate a diferitor puncte cheie, care ar permite instruitului să perceapă problema;
2. Studiarea problemei – se lucrează în mod independent, sunt reactualizate anumite resurse;
3. 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;

4. Obținerea rezultatului final – se analizează rezultatul obținut și formate anumite concluzii.

Această metodă se recomandă pentru predarea-învățarea-evaluarea următoarelor unități de conținut:

- Administrarea unei rețele de calculatoare securizată.
- Securizarea rețelelor de calculatoare locale.

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 student; stimularea cognitivă a studentului 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 studentului.

Această metodă se recomandă pentru predarea-învățarea-evaluarea următoarelor unități de conținut:

- Securizarea echipamentelor de rețea.
- Securizarea rețelelor de calculatoare locale.
- Implementarea rețelelor private virtuale.

Metoda studiul de caz valorifică o situație reală care se analizează și se rezolvă. Sunt cazuri când este necesar de a prezenta studentului probleme deja rezolvate. Avantajul metodei, constă în faptul că fiecare student își va aduce aportul la analiza și rezolvarea problemei. În utilizarea acestei metode se conturează câteva etape: 1) Selectarea și prezentarea cazului; 2) Organizarea echipelor de lucru; 3) Prelucrarea și conceptualizarea; 4) Structurarea finală a studiului.

Această metodă se recomandă pentru predarea-învățarea-evaluarea următoarelor unități de conținut:

- Securizarea rețelelor de calculatoare locale.
- Securizarea echipamentelor de rețea.
- Implementarea rețelelor private virtuale.

Instruirea prin proiecte reprezintă o modalitate de instruire/autoinstruire grație căreia 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.

Această metodă se recomandă pentru predarea-învățarea-evaluarea următoarelor unități de conținut:

- Implementarea Criptografiei.
- Amenințările de securitate într-o rețea modernă.

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) ce țin de interpretarea creativă a informațiilor și de 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, cadrul didactic va aduce la cunoștință elevilor tematica lucrărilor, modul de evaluare (bareme/grile/criterii de notare) și condițiile de realizare a fiecărei evaluări.

Lista orientativă a categoriilor de produse și procese, recomandate pentru evaluarea competențelor funcțional-acționare este prezentată în tabelul de mai jos:

Nr. crt.	Produse pentru măsurarea competenței	Criterii de evaluare a produselor
1.	Rețea de calculatoare securizată	• Corespunderea termenilor de referință • Corespunderea sarcinilor tehnice • Corespunderea standardelor și normativelor în vigoare • Corectitudinea calculelor • Fundamentarea deciziilor • Completitudinea setului de documente • Ținuta lingvistică • Respectarea termenilor de elaborare • Productivitatea

Pe parcursul modului se realizează evaluare formativă prin aplicarea produselor pentru măsurarea competențelor cognitive și funcțional-acționare din tabelele de mai sus, iar la sfârșitul lui se realizează evaluarea sumativă pentru verificarea atingerii competențelor prin aplicarea unui test electronic și a unei rețele de calculatoare securizată.

XI. Resursele necesare pentru desfășurarea procesului de studii

Cerințe față de sălile de curs	
Pentru orele teoretice	Mostre ale consumabilelor Trusa pentru rețelistică Proiector multimedia
Pentru orele de laborator	Laborator de informatică care asigură fiecărui elev un calculator
Cerințe față de lecțiile on-line	
Instruirea la distanță	Instrumente de comunicare sincronă/asincronă Platforme educaționale Instrumente digitale de predare/evaluare
Cerințe tehnice	
Parametri tehnici minimi ale calculatorului	Procesor: 2 GHz Memorie operativă: 4 GB Unitate de stocare: 500 GB Afișaj și grafică: size: 22", resolution: 1366x768 Network: Ethernet, 100 Mb
Software	Sistem de Operare Microsoft Windows Packet Tracer 6.0

XII. Resursele didactice recomandate elevilor

Nr. crt.	Denumirea resursei	Locul în care poate fi consultată/ accesată/ procurată resursa
1.	Ghidul administratorului de calculatoare. Colegiul național de informatică, Piatra Neamț	http://cni.nt.edu.ro/new/index.php/filmul-proiectului-leonardo-da-vinci-dezvoltarea-competentelor-profesionale-in-domeniul-retelelor-de-calculatoare/
2.	Banica Ion , Note de Curs: Comunicații între Calculatoare. Editura: Teora, 2005	https://ru.scribd.com/doc/103543173/Administrator-Retele-de-Calculatoare-Didactica
3.	Răzvan Rughiniș. Rețele locale. Editura PRINTECH, 2012	https://kupdf.net/download/rele-locale-de-calculatoare_59cdf75f08bbc54662686f2f_pdf
4.	Răzvan Rughiniș. Proiectarea Rețelelor de Calculatoare. Editura:PRINTECH, 2014	https://andrei.clubcisco.ro/index.php/anul-4/anul4-sem1/54-proiectarea-retelelor-de-calculatoare