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

"Aprob"
Directorul Centrului de Excelenţă în Informatică şi Tehnologii Informaţionale

_____ Andrei Ciobanu

"___"_____2025

Curriculumul modular
S.07.O.022 Asistenţă în securitatea rețelelor de calculatoare
S.03.O.022 Asistenţă în securitatea rețelelor de calculatoare
P.04.O.024 Asistenţă în securitatea rețelelor de calculatoare

Specialitatea**: 0611.2 Rețele de calculatoare**

2025

Aprobat:

La ședința Consiliului metodico-ştiinţific din 20.06.2025 al Centrului de Excelenţă în Informatică şi Tehnologii Informaţionale, proces verbal Nr. 7

Director adjunct _____ Obadă Liuba

La ședința Catedrei de Informatică I din 20.05.2025 al Centrului de Excelenţă în Informatică şi Tehnologii Informaţionale, proces verbal Nr. 10

Șef catedra _____ Golub Andrian

Coordonat cu:

Centrul de Excelenţă în Informatică şi Tehnologii Informaţionale
Centrul de Excelență în Energetică și Electronică
Colegiul Politehnic din Bălți
Colegiul Universității Tehnice a Moldovei

Autori:

Nicșan Adrian, grad didactic întâi*,* Centrul de Excelență în Informatică și Tehnologii Informaționale
Siminițchi Gheorghe, grad didactic doi, Colegiul Politehnic din Bălți

Recenzenţi:

Sudacevschi Viorica, șefa departamentului Informatică și Ingineria Sistemelor, UTM
Rogojinaru Tatiana, manager serviciul customer, StarLab SRL

Cuprins

I. Preliminarii

Asistența în securitatea rețelelor de calculatoare constă în securizarea, supravegherea, monitorizarea rețelelor de calculatoare. În ansamblu, asistenţa 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 reţea şi asigură utilizarea resurselor companiei conform standardelor stabilite pentru utilizatorii de reţele. Totodată, asistentul rulează teste în scopul depistării eventualelor atacuri de rețea.
Ca parte a securizării reţelelor, 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 reţea, modifică, dacă este cazul, configuraţia reţelei.

II. Motivaţia, utilitatea unității de curs pentru dezvoltarea profesională

Motivația pentru studierea unității de curs „Asistență în securitatea rețelelor de calculatoare" fundamentează pe necesitatea tot mai mare a protecției datelor și a infrastructurilor digitale în contextul actual, marcat de creșterea amenințărilor cibernetice. Elevii sunt motivați de oportunitatea de a dobândi competențe esențiale care le permit să înțeleagă, să prevină și să combată riscurile de securitate, devenind astfel profesioniști capabili să asigure integritatea și confidențialitatea informațiilor într-un mediu tehnologic în continuă evoluție. Acest curs le oferă șansa de a contribui activ la siguranța rețelelor, un domeniu vital pentru orice organizație, ceea ce le sporește încrederea și relevanța pe piața muncii.

Utilitatea unității de curs este reflectată în aplicabilitatea directă a cunoștințelor și abilităților dobândite în dezvoltarea profesională a viitorilor specialiști în rețele de calculatoare. Prin studierea acestui curs, elevii învață să identifice vulnerabilitățile rețelelor, să implementeze soluții de securitate (cum ar fi firewall-uri, sisteme de detectare a intruziunilor, politici de securitate) și să răspundă eficient la incidente de securitate. Aceste competențe sunt indispensabile în contextul cererii în creștere de experți în securitate cibernetică, oferindu-le absolvenților avantajul de a se integra rapid în echipe IT din diverse sectoare. De asemenea, cursul dezvoltă gândirea critică și abilitățile de rezolvare a problemelor, pregătind elevii să facă față provocărilor complexe ale domeniului și să evolueze profesional într-o industrie dinamică și competitivă.

III. Competenţele profesionale și rezultatele învățării

În cadrul modulului vor fi formate şi dezvoltate următoarele competențe profesionale specifice:

CP5. Respectarea normelor, cerințelor și standardelor la executarea lucrărilor.
CP10. Aplicarea metodelor de testare a funcționalității rețelei.
CP11. Aplicarea metodelor de securizare a rețelei.

Absolventul programului la atribuirea calificării poate:

RÎ5. Aplica standardele tehnice și normele de securitate în toate etapele procesului de instalare și configurare a rețelei, prevenind riscurile tehnice și profesionale pe toată perioada executării lucrărilor.
RÎ10. Aplica metode de testare pentru a evalua funcționalitatea rețelei, identificând și diagnosticând problemele posibile, oferind soluții de remediere în cel mai scurt timp.
RÎ11. Aplica metode de securizare a rețelei conform politicilor de securitate, asigurând protecția datelor, prin monitorizarea constantă a stării de securitate și intervenind în caz de incidente cibernetice.

După finalizarea acestui modul, elevul va fi capabil să:

RÎ1. Identifice și clasifice corect tipurile de atacuri cibernetice prin analiza unor scenarii practice, demonstrând capacitatea de a recunoaște caracteristicile specifice ale fiecărui atac.

RÎ2. Implementeze măsuri de securitate pentru a proteja o rețea locală simulată împotriva mai multor vulnerabilități comune, reducând riscul de penetrare.

RÎ3. Configureze un firewall pentru filtrarea traficului conform regulilor stabilite pentru funcționarea securizată a rețelei.

RÎ4. Aplice măsuri de securitate pe o stație de lucru, asigurând conformitatea cu standardele de securitate de bază și elimină vulnerabilitățile identificate inițial printr-un audit.

RÎ5. Construiască o rețea privată virtuală (VPN) funcțională, utilizând protocoalele și metodele de securitate.

RÎ6. Analizeze traficul de rețea, identificând și raportând anomalii cu precizie într-un raport structurat.

RÎ7. Implementeze reguli de control al traficului într-o rețea, utilizând liste de acces pentru a restricționa sau permite comunicarea între dispozitive, protocoale și porturi, asigurând astfel securitatea și performanța rețelei.

IV. Administrarea unității de curs

Învățământ clasic (4 ani)

Semestrul	Numărul de ore				Forma de evaluare	Numărul de credite
	Total ore	Contact direct		Studiu individual		
		Teorie	Laborator			
VII	150	30	60	60	Examen	5

Învățământ clasic (2 ani)

Semestrul	Numărul de ore				Forma de evaluare	Numărul de credite
	Total ore	Contact direct		Studiu individual		
		Teorie	Laborator			
III	150	30	60	60	Examen	5

Învățământ dual (2 ani)

Semestrul	Numărul de ore					Forma de evaluare	Numărul de credite
	Total ore	Contact direct			Studiu individual		
		T	IT	IP			
IV	120	100	40	60	20	Examen	4

V. Repartizarea orientativă a orelor pe unități de învățare

Învățământ clasic (4 ani)

Nr. crt.	Unităţi de învăţare	Numărul de ore			
		Total ore	Contact direct		Studiu individual
			Teorie	Laborator	
1.	Amenințările de securitate într-o rețea	18	4	6	8
2.	Securizarea echipamentelor de rețea	24	4	10	10
3.	Implementarea firewall-urilor	22	6	10	6
4.	Securizarea dispozitivelor finale	22	2	10	10
5.	Implementarea Criptografiei	22	6	8	8
6.	Implementarea rețelelor private virtuale	22	4	8	10
7.	Administrarea și testarea rețelei de calculatoare securizată	20	4	8	8
	Total	**150**	**30**	**60**	**60**

Învățământ clasic (2 ani)

Nr. crt.	Unităţi de învăţare	Numărul de ore			
		Total ore	Contact direct		Studiu individual
			Teorie	Laborator	
1.	Amenințările de securitate într-o rețea	18	4	6	8
2.	Securizarea echipamentelor de rețea	24	4	10	10
3.	Implementarea firewall-urilor	22	6	10	6
4.	Securizarea dispozitivelor finale	22	2	10	10
5.	Implementarea Criptografiei	22	6	8	8
6.	Implementarea rețelelor private virtuale	22	4	8	10
7.	Administrarea și testarea rețelei de calculatoare securizată	20	4	8	8
	Total	**150**	**30**	**60**	**60**

Învățământ dual (2 ani)

Nr. crt.	Unităţi de învăţare	Numărul de ore			
		Total ore	Contact direct		Studiu individual
			IT	IP	
1.	Amenințările de securitate într-o rețea	12	4	6	2
2.	Securizarea echipamentelor de rețea	18	4	10	4
3.	Implementarea firewall-urilor	20	8	10	2
4.	Securizarea dispozitivelor finale	18	4	10	4
5.	Implementarea Criptografiei	18	8	8	2
6.	Implementarea rețelelor private virtuale	20	8	8	4
7.	Administrarea și testarea rețelei de calculatoare securizată	14	4	8	2
	Total	**120**	**40**	**60**	**20**

VI. Unităţile de învăţare

Unităţi de competenţă	Unităţi de conţinut	Abilităţi
1. Ameninţările de securitate într-o rețea		
UC1. Identificarea și clasificarea corectă a tipurile de atacuri cibernetice prin analiza unor scenarii practice, demonstrând capacitatea de a recunoaște caracteristicile specifice ale fiecărui atac.	1. Principiile fundamentale ale unei rețele de calculatoare securizată. 2. Viermi, viruși și intruși. 3. Tipuri de unelte de atac. 4. Metodologia atacurilor. 5. Atenuarea amenințărilor.	A1. Detectarea atacurilor de rețea. A2. Distingerea tipului atacului de rețea. A3. Folosirea de aplicații pentru detectarea malware. A4. Distingerea metodelor și uneltelor de atac. A5. Utilizarea metodelor de atenuarea amenințărilor.
2. Securizarea echipamentelor de rețea		
UC2. Implementarea măsurilor de securitate pentru a proteja o rețea locală simulată împotriva mai multor vulnerabilități comune, reducând riscul de penetrare.	6. Securizarea accesului la echipamente și fișiere. 7. Autentificarea și autorizarea în reţea. 8. Monitorizarea și administrarea echipamentelor. 9. Configurarea accesului administrativ securizat. 10. Liste de control al accesului.	A6. Setarea accesului la echipamente. A7. Configurarea parolelor la echipamente. A8. Monitorizarea echipamentelor. A9. Activarea/Dezactivarea serviciilor la echipamente. A10. Configurarea clientului şi serverului RADIUS. A11. Configurarea metodelor de acces securizat la echipamente. A12. Monitorizarea traficului. A13. Scanarea porturilor. A14. Configurarea listelor de acces.
3. Implementarea firewall-urilor		
UC3. Configurarea unui firewall pentru filtrarea traficului conform regulilor stabilite pentru funcționarea securizată a rețelei.	11. Securizarea rețelelor cu firewall-uri. 12. Filtrarea pachetelor. 13. Monitorizarea conexiunilor. 14. Sistemul de translatare a adreselor. 15. Firewall-uri bazate pe zone.	A15. Configurarea serviciului Firewall pe echipamente. A16. Setarea regulilor pentru filtrarea traficului. A17. Inspectarea fluxului de date. A18. Configurarea server proxy. A19. Setarea serviciului NAT.

	16. Tehnologii de prevenire a intruziunilor.	A20. Configurarea NAT pentru redirecționarea porturilor. A21. Utilizarea instrumentelor de verificare a serviciului Firewall. A22. Configurarea sistemelor IPS și IDS.
4. Securizarea dispozitivelor finale		
UC4. Aplicarea măsurilor de securitate pe o stație de lucru, asigurând conformitatea cu standardele de securitate de bază și elimină vulnerabilitățile identificate inițial printr-un audit.	17. Securizarea stațiilor de lucru. 18. Securizarea echipamentelor Wireless și VoIP. 19. Configurarea opțiunilor de securitate a comutatoarelor.	A23. Instalarea programelor de tip antivirus. A24. Setarea serviciului Firewall pe stațiile de lucru. A25. Setarea protocoalelor de acces protejat la echipamente wireless. A26. Limitarea conexiunilor la echipamente wireless. A27. Configurarea VLAN-urilor. A28. Setarea filtrului dupa MAC adrese. A29. Securizarea comutatoarelor
5. Implementarea Criptografiei		
UC5. Aplicarea tipurilor de criptare, hash-urile și semnăturile digitale pentru a oferi confidențialitate, integritate și autentificare a datelor într-o rețea de calculatoare.	20. Criptarea simetrică și asimetrică. 21. Serviciul criptografic. 22. Semnăturile digitale. 23. Integritatea și autentificarea datelor.	A30. Folosirea protocoalelor de criptare. A31. Utilizarea semnăturilor digitale. A32. Criptarea și decriptarea informației. A33. Distingerea tipurilor de chei de criptare. A34. Utilizarea cheilor de criptare. A35. Semnarea documentelor electronice. A36. Gestionarea cheilor publice.
6. Implementarea rețelelor private virtuale		
UC6. Construirea rețelei privată virtuală (VPN) funcțională, utilizând protocoalele și metodele de securitate.	24. Tipuri de VPN-uri. 25. Protocoale specifice VPN-urilor. 26. Componentele și operațiile IPSec. 27. Implementarea accesului la distanță prin VPN.	A37. Construirea rețelelor private virtuale. A38. Setarea protocoalelor de tunelare. A39. Crearea tunelurilor. A40. Configurarea serviciului IPSec. A41. Configurarea accesului la distanță. A42. Configurarea mecanismului de autentificare.

7. Administrarea și testarea rețelei de calculatoare securizată		
UC7. Analizarea traficul de rețea, identificând și raportând anomalii cu precizie într-un raport structurat.	28. Testarea securității rețelelor. 29. Unelte specializate pentru testarea rețelelor securizate. 30. Ciclu de viață a unei rețele de calculatoare securizată. 31. Construirea politicilor de securitate.	A43. Utilizarea tehnicilor de testare a securizării rețelelor. A44. Utilizarea uneltelor pentru testarea rețelelor securizate. A45. Analiza istoricului a fișierilor cu log-uri. A46. Folosirea sistemelor de alertă în caz de atacuri. A47. Implementarea politicilor de securitate.

VII. Studiu individual ghidat de profesor

Învățământ clasic (4 ani)

Materii pentru studiul individual	Produse de elaborat	Modalităţi de evaluare	Număr de ore
RÎ2. Implementează măsuri de securitate pentru a proteja o rețea locală simulată împotriva mai multor vulnerabilități comune, reducând riscul de penetrare.			
Securizarea accesului la echipamente și fișiere	Schemă pe calculator	Prezentarea schemei Demonstrarea la calculator	25
RÎ4. Aplică măsuri de securitate pe o stație de lucru, asigurând conformitatea cu standardele de securitate de bază și elimină vulnerabilitățile identificate inițial printr-un audit.			
Criptarea simetrică și asimetrică	Proiect elaborat	Prezentarea proiectului	10
RÎ5. Construiește o rețea privată virtuală (VPN) funcțională, utilizând protocoalele și metodele de securitate.			
Implementarea accesului la distanță prin VPN	Schemă pe calculator	Prezentarea schemei Demonstrarea la calculator	25

Învățământ clasic (2 ani)

Materii pentru studiul individual	Produse de elaborat	Modalităţi de evaluare	Număr de ore
RÎ2. Implementează măsuri de securitate pentru a proteja o rețea locală simulată împotriva mai multor vulnerabilități comune, reducând riscul de penetrare.			
Securizarea accesului la echipamente și fișiere	Schemă pe calculator	Prezentarea schemei Demonstrarea la calculator	25
RÎ4. Aplică măsuri de securitate pe o stație de lucru, asigurând conformitatea cu standardele de securitate de bază și elimină vulnerabilitățile identificate inițial printr-un audit.			
Criptarea simetrică și asimetrică	Proiect elaborat	Prezentarea proiectului	10
RÎ5. Construiește o rețea privată virtuală (VPN) funcțională, utilizând protocoalele și metodele de securitate.			
Implementarea accesului la distanță prin VPN	Schemă pe calculator	Prezentarea schemei Demonstrarea la calculator	25

Învățământ dual (2 ani)

Materii pentru studiul individual	Produse de elaborat	Modalităţi de evaluare	Număr de ore
RÎ2. Implementează măsuri de securitate pentru a proteja o rețea locală simulată împotriva mai multor vulnerabilități comune, reducând riscul de penetrare.			
Securizarea accesului la echipamente și fișiere	Schemă pe calculator	Prezentarea schemei Demonstrarea la calculator	6
RÎ4. Aplică măsuri de securitate pe o stație de lucru, asigurând conformitatea cu standardele de securitate de bază și elimină vulnerabilitățile identificate inițial printr-un audit.			
Criptarea simetrică și asimetrică	Proiect elaborat	Prezentarea proiectului	6
RÎ5. Construiește o rețea privată virtuală (VPN) funcțională, utilizând protocoalele și metodele de securitate.			
Implementarea accesului la distanță prin VPN	Schemă pe calculator	Prezentarea schemei Demonstrarea la calculator	8

VIII. Lucrările de laborator recomandate

1. Identificarea și analizarea amenințărilor cibernetice în infrastructuri de rețea.
2. Clasificarea și investigarea tipurilor de malware utilizând unelte de analiză.
3. Simularea unui atac DoS și evaluarea vulnerabilităților asociate.
4. Capturarea și interpretarea traficului malițios folosind analizatoare de pachete.
5. Aplicarea metodelor de prevenire și atenuare a atacurilor în rețele locale.
6. Configurarea accesului administrativ securizat și a parolelor pe echipamente.
7. Implementarea autentificării locale pentru controlul accesului la resurse.
8. Activarea și testarea autentificării centralizate cu server RADIUS.
9. Monitorizarea și administrarea fiabilă a echipamentelor de rețea.
10. Configurarea listelor de control al accesului (ACL) pentru filtrarea traficului.
11. Aplicarea regulilor de firewall pentru segmentarea traficului între zone.
12. Configurarea și verificarea translării adreselor (NAT) și a redirecționării porturilor.
13. Monitorizarea conexiunilor active și logarea activităților în firewall.
14. Implementarea politicilor bazate pe zone pentru protecția traficului critic.
15. Utilizarea uneltelor de verificare pentru testarea funcționării firewall-ului.
16. Instalarea și configurarea soluțiilor antivirus pe stații de lucru.
17. Activarea firewall-ului local și configurarea regulilor de securitate.
18. Aplicarea filtrelor MAC și criptării WPA2 pentru rețele wireless.
19. Crearea și gestionarea VLAN-urilor pentru segmentarea logică a rețelei.
20. Activarea funcțiilor de protecție Layer 2: DHCP Snooping și Port Security.
21. Criptarea și decriptarea datelor utilizând unelte CLI și grafice.
22. Generarea și verificarea semnăturilor digitale pentru protecția documentelor.
23. Aplicarea funcțiilor hash pentru validarea integrității fișierelor.
24. Crearea și administrarea unei infrastructuri PKI în scop educațional.
25. Semnarea și criptarea comunicațiilor în rețelele interne și externe.
26. Configurarea unei rețele VPN site-to-site utilizând protocoale Ipsec.

27. Implementarea unui VPN remote-access cu autentificare locală
28. Capturarea și analizarea traficului criptat într-un tunel VPN activ
29. Compararea protocoalelor de tunelare și validarea autentificării
30. Testarea și auditarea unei politici de securitate într-un laborator complet integrat

IX. Sugestii metodologice

Elementele de bază ale Curriculumului sunt competențele ce trebuie formate şi dezvoltate în procesul de instruire profesională. Aceste scop va fi atins 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-şi 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 părţi;
- un nivel de implicare a părților acționând în baza unor reguli şi acțiuni prestabilite.

Activitățile pot fi organizate cât cu prezența fizică, atât și online. Pentru a crea un mediu de învățare cât mai aproape de o clasă reală, este suficient de utilizat trei tipuri de resurse:

O platformă de interacțiune în timp real, cu video și text, cu elevii printre care sunt: Google Meet, Jitsi Meet, Zoom, Discord, Cisco Webex, Microsoft Teams etc.

Aplicații sau platforme de colaborare online, care facilitează schimbul de documente, teste sau teme pentru acasă, între profesori și elevi și înregistrează o evidență a acestora, care permite și feedback din partea profesorului. Aici recomandăm Moodle, Google Classroom și alternative folosite de profesori, precum Edmodo, EasyClass și ClassDojo.

Resurse și aplicații de învățare pe care le poate crea profesorul sau resurse deja existente sub formă de prezentări, lecții, fișe, imagini și clipuri care pot fi folosite atât în timpul lecțiilor live, cât și ca teme de lucru pentru acasă. Aici lista e mai lungă și include aplicații precum TestMoz, LearningApps, Mentimetr, LinoIt, ASQ, Kahoot, Quizziz, Wordwall, Padlet, Twinkl sau Digitaliada, precum și surse de inspirație pentru filme, teme și studiu individual.

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

Simularea şi modelarea. Simularea este utilizată pentru prezentarea la faza inițială a unor concepte, oferind posibilitatea de ghidare a activității elevului 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 unităţi de conținut:

- Securizarea rețelelor cu firewall-uri;
- Monitorizarea conexiunilor;
- Tipuri de VPN-uri;
- Implementarea accesului la distanță prin VPN;
- Unelte specializate pentru testarea rețelelor securizate.

Problematizarea mai poate fi denumită şi predare prin rezolvare de probleme sau predare productivă de probleme. Conform acestei metode instruitului este pus în fața unor dificultăți create în mod deliberat, şi 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 situație de tip problemă se va ține cont de următoarele caracteristici:

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

Prin intermediul situației create, instruitul este cointeresat de a studia, analiza şi 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) Studierea 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 şi este analizat modul de aplicare a acestora în determinarea soluției;
4) Obținerea rezultatului final – se analizează rezultatul obținut şi formate anumite concluzii.

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

- Metodologia atacurilor;
- Atenuarea amenințărilor;
- Implementarea accesului la distanță prin VPN;
- Testarea securității rețelelor.

Instruirea asistată de calculator este o metodă didactică care valorifică principiile de modelare şi 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 organizarea informației conform cerințelor programei adaptabile la capacitățile fiecărui elev; stimularea cognitivă a elevului prin secvențe didactice şi 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. Această metodă se recomandă pentru predarea-învățarea-evaluarea următoarelor unităţi de conținut:

- Monitorizarea și administrarea echipamentelor;
- Securizarea stațiilor de lucru;
- Semnăturile digitale;
- Componentele și operațiile IPSec;
- Testarea securității rețelelor.

Metoda studiul de caz valorifică o situație reală care se analizează şi se rezolvă. Așa cum problemele rezolvate în stilul orientat pe obiecte au un grad sporit de dificultate, sunt cazuri când este necesar de a prezenta elevului probleme deja rezolvate. Avantajul metodei, constă în faptul că fiecare dintre elev îşi va aduce aportul la analiza şi rezolvarea problemei. În utilizarea acestei metode se conturează câteva etape:

1) Selectarea şi prezentarea cazului;

2) Organizarea echipelor de lucru;
3) Prelucrarea şi conceptualizarea;
4) Structurarea finală a studiului.

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

- Metodologia atacurilor;
- Securizarea accesului la echipamente și fișiere;
- Securizarea rețelelor cu firewall-uri;
- Securizarea stațiilor de lucru;
- Integritatea și autentificarea datelor.

Instruirea prin proiecte reprezintă o modalitate de instruire/autoinstruire graţie căreia elevii efectuează o cercetare orientată spre obiective practice şi finalizată într-un produs ce poate fi un obiect, un aparat, o instalaţie, o culegere tematică, un album, o lucrare ştiinţifică etc. Această metodă se recomandă pentru predarea-învăţarea-evaluarea următoarelor unităţi de conţinut:

- Integritatea și autentificarea datelor;
- Implementarea accesului la distanță prin VPN.

X. Sugestii de evaluare

Evaluarea competențelor profesionale este procesul prin care sunt colectate şi analizate dovezile necesare pentru judecarea competenţei în raport cu cerințele calificării profesionale. Calificarea profesională este documentul în care se descriu rezultatele învăţării în concordanță cu cerințele pieței muncii, specificate în standardul ocupațional/ profilul ocupațional. Evaluarea competențelor profesionale este un proces complet diferit de sistemul tradițional de evaluare a cunoștințelor. Evaluarea competențelor profesionale este un proces care presupune consultarea şi colaborarea dintre elev şi profesor. Evaluarea competențelor are loc prin furnizarea de către elev a dovezilor de competentă care sunt interpretate de către profesor. Dovezile de competență acumulate sunt rezultate considerate parțiale şi atât elevul cât și profesorul pot solicita clarificări suplimentare.

Procedura de evaluare a competențelor profesionale pentru modulul „Asistență în securitatea rețelelor de calculatoare”, va oferi elevilor posibilitatea de a-şi demonstra atât cunoștințele teoretice şi practice. Metodele folosite în procesul de evaluare vor evidenția cunoștințele şi deprinderile necesare pentru efectuarea activităților de muncă şi, mai ales, capacitatea elevului de a obține rezultatele practice așteptate.

Activitățile de evaluare vor fi orientate spre motivarea elevilor şi obținerea unui feedback continuu, fapt ce va permite corectarea operativă a procesului de învățare, stimularea autoevaluării şi 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) şi condițiile de realizare a fiecărei evaluări.

Evaluarea curentă/formativă se va realiza prin diverse modalități: observarea comportamentului elevului, analiza rezultatelor activității elevului, discuția/conversația, prezentarea proiectelor individuale de activitate. Prin evaluarea curentă/formativă, cadrele didactice informează elevul despre nivelul de performanță; îl motivează să se implice în dobândirea competențelor profesionale.

Evaluarea sumativă se realizează la finele modulului în baza simulării în atelier a unei situații de problemă din contexte profesionale variate, care solicită elevului demonstrarea competenţei profesionale. Cadrele

didactice vor elabora sarcini prin care vor orienta comportamentul profesional al elevului spre demonstrarea sistemului de cunoștințe şi abilități. În acest scop, vor fi clar stabiliți indicatorii şi descriptorii de performanță ai procesului şi produsului realizat de către elev.

Portofoliul reprezintă o metodă complexă de evaluare în care un rezultat al evaluării este elaborat pe baza aplicării unui ansamblu variat de probe și instrumente de evaluare. Portofoliul, de regulă este realizat pe o perioadă mai îndelungată (în decursul mai multor ore). Conținutul unui portofoliu este reprezentat de rezultatele la: lucrări practice, studiul individual, investigații, referate și proiecte, observarea sistematică la clasă, autoevaluarea elevului, chestionare de atitudini etc. Alegerea elementelor ce formează portofoliul este realizată de către profesor (astfel încât acestea să ofere informații concludente privind pregătirea, evoluția, atitudinea elevului) sau chiar de către elev (pe considerente de performanță, preferințe etc.). Structurarea evaluării sub forma de portofoliu se dovedește deosebit de utilă, atât pentru profesor, cât și pentru elev sau părinții acestuia. Pentru a realiza o evaluare pe bază de portofoliu, profesorul:

- va comunica elevilor intenția de a realiza un portofoliu, adaptând instrumentele de evaluare ce constituie "centrul de greutate" ale portofoliului la specificul unității de învățare;
- va alege componentele ce formează portofoliul, dând și elevului posibilitatea de a adăuga piese pe care le consideră relevante pentru activitatea sa;
- va evalua separat fiecare piesă a portofoliului în momentul realizării ei, dar va asigura și un sistem de criterii pe baza cărora să realizeze evaluarea globală și finală a portofoliului;
- va pune în evidență evoluția elevului, particularitățile de exprimare și de raportare a acestuia la aria vizată;
- va integra rezultatul evaluării portofoliului în sistemul general de notare.

Competențele elevului se manifestă prin produse concrete, care sunt analizate de către profesor în raport cu aspectele critice stabilite pentru unitate/unitățile de competență pentru care este evaluat. Dovezile de competență sunt informațiile produse de un elev din care rezultă că îndeplinește toate aspectele descrise de unitatea/unitățile de competență pentru care este evaluat, respectiv are cunoștințele şi deprinderile necesare.

Evaluarea nivelului de dezvoltare a competențelor în cadrul orelor:

- ***teoretice*** se va realiza prin teste, exemple de aplicare a cunoștințelor teoretice în practică, machete etc.;
- ***de laborator*** se va realiza prin elaborarea de către elev, în termeni concreți, a aplicațiilor web având la bază unitățile de conținut studiate în cadrul orelor teoretice precum și abilitățile anterior dezvoltate;
- ***de studiu individual*** se va realiza prin studierea de către elev a materialelor suplimentare decât cele oferite în cadrul orelor de tip contact direct și prezentarea de portofolii pentru anumite unități de conținut și aplicații web complexe prin care elevul își va demonstra abilitățile formate.

Probe de evaluare a competențelor, în baza situațiilor de problemă de la viitoarele locuri de muncă:

- elaborarea aplicațiilor de consolă conform specificațiilor propuse;
- evaluarea aplicațiilor de consolă elaborate;
- selectarea structurii dinamice de date conform specificațiilor tehnice;
- elaborarea algoritmilor conform metodei;
- modificarea aplicațiilor de consolă conform specificațiilor propuse;

- testarea aplicațiilor de consolă elaborate.

În calitate de **produse pentru măsurarea competențelor** se vor folosi:

- aplicații de consolă elaborate conform specificațiilor propuse;
- algoritmi elaborați conform specificațiilor propuse;
- structuri dinamice de date gestionate conform specificațiilor propuse.

Criteriile de evaluare a produselor pentru măsurarea competenţei vor include:

- Utilizarea corectă a instrucțiunilor limbajului de programare;
- Corectitudinea algoritmilor elaborați;
- Fundamentarea deciziilor;
- Ținuta lingvistică;
- Respectarea termenilor de elaborare.

Forma finală de evaluare a unității de curs este examenul. Pentru a fi admis la examen elevul trebuie să susțină evaluările curente, să însușească materialul teoretic și să îndeplinească sarcinile propuse pentru studiul individual. Nota finală va fi formată: 60% - media notelor curente și 40% - nota de la examen.

XI. Resursele necesare pentru atingerea rezultatului învățării

Laboratorul destinat cursului "Asistența în securitatea rețelelor de calculatoare" trebuie să fie echipat cu resurse care să permită elevilor să dobândească competențe practice în configurarea, administrarea și securizarea rețelelor de calculatoare. Aceste resurse includ computere performante cu software specializat, dispozitive de rețea (routere, switch-uri, firewall-uri), mobilier ergonomic și instrumente pentru testarea și diagnosticarea rețelelor. Utilizarea echipamentelor presupune respectarea normelor de siguranță electrică și a procedurilor specifice pentru configurarea rețelelor, iar întreținerea implică actualizarea periodică a software-ului, verificarea conexiunilor fizice și curățarea componentelor hardware. Spațiul trebuie să fie dotat cu o rețea electrică stabilă, ventilație adecvată și acces la internet de mare viteză, esențial pentru simulări și testări în timp real.

Standardul de dotare a laboratoarelor

Suprafața totală a laboratorului – min. 30 m²
Suprafața pentru un elev – min. 2 m²
Numărul locurilor de lucru – min. 15

Nr. crt.	Denumirea	Cantitatea per elev	Cantitatea per atelier
a) Echipamente			
1.	Calculator (PC cu procesor i5, 16 GB RAM, SSD)	1	15
2.	Monitor LED 24"	1	15
3.	Router de rețea (ex. Cisco/Juniper/Mikrotik)	-	2
4.	Switch gestionabil (24 porturi)	-	2
5.	Access Point Wi-Fi	-	1
6.	Firewall hardware	-	1
b) Mobilier și tehnică sanitară			
7.	Masă de lucru	1	15

8.	Scaun ergonomic reglabil	1	15
9.	Dulap pentru echipamente	-	2
c) Utilaj tehnologic			
10.	Simulator de rețea (ex. Packet Tracer instalat pe PC)	1(software)	25(licențe)
11.	Server de testare (pentru simulări)	-	1
d) Instrumente și dispozitive			
12.	Cablu de rețea UTP (cu conectori RJ45)	2	30
13.	Cleste sertizare RJ45	1	15
14.	Tester de cablu rețea	1	15
e) Inventar și ustensile			
15.	Șurubelniță set (pentru PC-uri)	1	15
16.	Kit curățare echipamente (spray aer comprimat)	1	15
17.	Cablu de alimentare suplimentar	1	15
18.	Organizator cabluri	-	10

1. **Echipamentele** (PC-uri, routere, switch-uri) sunt esențiale pentru simularea și configurarea rețelelor, iar specificațiile tehnice (ex. 16 GB RAM) asigură funcționarea fluentă a aplicațiilor de securitate și simulare.
2. **Mobilierul** este dimensionat pentru a oferi fiecărui elev un spațiu de lucru individual, iar chiuveta este inclusă pentru igiena mâinilor după manipularea cablurilor sau echipamentelor.
3. **Utilajele tehnologice** includ software precum Cisco Packet Tracer, necesar pentru învățarea practică, și un server pentru teste avansate.
4. **Instrumentele** (clești, testere) permit elevilor să construiască și să diagnosticheze rețele fizice.
5. **Inventarul** asigură mentenanța și organizarea echipamentelor.

XII. Resursele didactice recomandate elevilor

Nr. crt.	Denumirea resursei	Locul în care poate fi consultată/ accesată resursă
1.	Chappell, Laura. Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide. Universitatea Chappell, 2012	Biblioteca
2.	A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996	https://cacr.uwaterloo.ca/hac/
3.	Lyon, Gordon. Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.Com, LLC, 2008.	Biblioteca
4.	IPSec Virtual Private Network Fundamentals	Biblioteca
5.	Curs Online ”Network Security”	https://www.netacad.com/courses/network-security?courseLang=en-US