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

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

_____ Andrei Ciobanu

"___"_____2025

Curriculumul modular
S.05.O.020 Operațiuni de securitate cibernetică
S.01.O.020 Operațiuni de securitate cibernetică
P.01.O.014 Operațiuni de securitate cibernetică

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 10.05.2025 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:

Josan Liudmila, grad didactic superior, Colegiul Politehnic din Bălți
Dermenji Vasilii, grad didactic întâi, Centrul de Excelență în Informatică și Tehnologii Informaționale
Siminițchi Gheorghe, grad didactic doi, Colegiul Politehnic din Bălți

Recenzenți:

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

Cuprins

I. Preliminarii

Unitatea de curs „Operațiuni de securitate cibernetică” are ca scop dezvoltarea competențelor necesare identificării, evaluării și aplicării măsurilor de protecție a datelor, sistemelor și comunicațiilor digitale împotriva amenințărilor cibernetice. Disciplina abordează concepte fundamentale de securitate a informației, tipologii de atacuri cibernetice, principii ale confidențialității, integrității și disponibilității (CIA), precum și tehnici de apărare precum criptarea, autentificarea, controlul accesului și răspunsul la incidente.

Scopul studierii acestei unități este de a pregăti elevii pentru a înțelege și aplica principii de securitate în contexte reale, contribuind astfel la protejarea infrastructurilor informatice personale și organizaționale, asigurând continuitatea și reziliența acestora în fața amenințărilor digitale.

Pentru a aborda cu succes unitatea de curs „Operațiuni de securitate cibernetică”, elevii trebuie să dețină următoarele cunoștințe și abilități prealabile:

- Cunoștințe de bază despre rețele de calculatoare și funcționarea componentelor (ex. calculatoare, routere, switch-uri);
- Noțiuni fundamentale despre modelul OSI, protocolul TCP/IP și funcționarea adresării IP;
- Utilizarea sistemelor de operare (Windows sau Linux) și rularea unor comenzi simple în linia de comandă;
- Capacitatea de a configura o rețea locală simplă (LAN) și de a testa conectivitatea;
- Familiarizare cu concepte precum fișier, utilizator, cont, parolă, permisiuni;
- Gândire logică și atenție la detalii în lucrul cu structuri de date, parole sau scenarii de acces.

Aceste pre-aciziții sunt esențiale pentru înțelegerea și aplicarea corectă a măsurilor de protecție cibernetică, precum și pentru rezolvarea scenariilor de lucru propuse în cadrul activităților teoretice și practice.

II. Motivaţia, utilitatea unității de curs pentru dezvoltarea profesională

Motivația pentru studierea unității de curs „Operațiuni de securitate cibernetică” derivă din creșterea exponențială a amenințărilor informatice care afectează utilizatorii, companiile și instituțiile publice. Într-o lume digitalizată, în care datele circulă rapid și infrastructurile informatice sunt interconectate, protecția informației devine o prioritate. Elevii sunt motivați de nevoia reală de a învăța cum să identifice, să prevină și să răspundă eficient la atacuri cibernetice, dezvoltând competențe valoroase și căutate pe piața muncii. Acest curs le oferă satisfacția aplicării cunoștințelor în contexte practice, cum ar fi detectarea phishingului, criptarea datelor sau configurarea controalelor de acces, contribuind astfel la securitatea infrastructurilor IT și la protejarea utilizatorilor.

Utilitatea unității de curs „Operațiuni de securitate cibernetică” se reflectă în pregătirea elevilor pentru ocuparea unor poziții cheie în domeniul IT, cum ar fi tehnician în securitate, administrator de sistem sau specialist în protecția datelor. Pe parcursul cursului, elevii dobândesc abilități concrete precum aplicarea criptării, folosirea semnăturilor digitale, analiza traficului de rețea și implementarea politicilor de acces. Aceste competențe sunt esențiale în contextul actual, în care organizațiile își dezvoltă echipe de securitate și implementează măsuri de apărare cibernetică la toate nivelurile. De asemenea, unitatea de curs contribuie la dezvoltarea abilităților transversale, precum gândirea critică, responsabilitatea digitală și capacitatea de reacție în situații de criză, pregătind elevii pentru adaptarea rapidă la schimbările tehnologice și pentru evoluția într-un domeniu dinamic, cu o cerere tot mai mare de specialiști calificați.

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.
CP9. Utilizarea software pentru configurarea echipamentelor de rețea.
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.
RÎ9. Configura echipamentele active de rețea prin aplicații software dedicate, implementând setările necesare pentru funcționarea optimă a rețelei conform cerințelor specificate, normele de securitate și compatibilitate.
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 principalele tipuri de amenințări, vulnerabilități și atacuri cibernetice care afectează utilizatorii, rețelele și organizațiile.
RÎ2. Aplice principiile de confidențialitate, integritate și disponibilitate în evaluarea și proiectarea măsurilor de protecție cibernetică.
RÎ3. Configureze metode de protecție a datelor și comunicațiilor, utilizând criptare, autentificare, control al accesului și măsuri de ascundere a datelor.
RÎ4. Evalueze nivelul de disponibilitate al serviciilor IT și aplică planuri de continuitate, răspuns la incidente și recuperare în caz de dezastru.
RÎ5. Respecte legislația și normele etice specifice domeniului securității cibernetice și contribuie la promovarea unei culturi a securității în organizație.

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			
V	90	30	30	30	Examen	3

Învățământ clasic (2 ani)

Semestrul	Numărul de ore				Forma de evaluare	Numărul de credite
	Total ore	Contact direct		Studiu individual		
		Teorie	Laborator			
I	120	30	30	60	Examen	4

Învățământ dual (2 ani)

Semestrul	Numărul de ore					Forma de evaluare	Numărul de credite
	Total ore	Contact direct			Studiu individual		
		T	IT	IP			
I	60	30	0	30	30	Examen	2

V. Repartizarea orientativă a orelor pe unităţi de învăţare

Învățământ clasic (4 ani)

Nr. crt.	Unități de învățare	Numărul de ore			
		Total ore	Contact direct		Studiu individual
			Teorie	Laborator	
1.	Domeniul securității cibernetice.	10	4	4	2
2.	Principiile de bază în securitatea informației.	14	4	4	6
3.	Amenințări cibernetice, vulnerabilități și atacuri.	14	4	6	4
4.	Protejarea confidențialității și a integrității datelor.	16	6	6	4
5.	Continuitatea operațională și răspunsul la incidente.	16	4	6	6
6.	Protecția infrastructurii și cadrul de reglementare.	20	8	4	8
Total		**90**	**30**	**30**	**30**

Învățământ clasic (2 ani)

Nr. crt.	Unități de învățare	Numărul de ore			
		Total ore	Contact direct		Studiu individual
			Teorie	Laborator	
1.	Domeniul securității cibernetice.	14	4	2	8

2.	Principiile de bază în securitatea informației.	20	4	4	12
3.	Amenințări cibernetice, vulnerabilități și atacuri.	22	6	6	10
4.	Protejarea confidențialității și a integrității datelor.	20	6	6	8
5.	Continuitatea operațională și răspunsul la incidente.	22	4	6	12
6.	Protecția infrastructurii și cadrul de reglementare.	22	6	6	10
Total		**120**	**30**	**30**	**60**

Învățământ dual (2 ani)

Nr. crt.	**Unități de învățare**	**Numărul de ore**			
		Total ore	**Contact direct**		**Studiu individual**
			IT	**IP**	
1.	Domeniul securității cibernetice.	6	0	4	2
2.	Principiile de bază în securitatea informației.	10	0	4	6
3.	Amenințări cibernetice, vulnerabilități și atacuri.	10	0	6	4
4.	Protejarea confidențialității și a integrității datelor.	10	0	6	4
5.	Continuitatea operațională și răspunsul la incidente.	12	0	6	6
6.	Protecția infrastructurii și cadrul de reglementare.	12	0	4	8
Total		**60**	**0**	**30**	**30**

VI. Unităţile de învăţare

Unităţi de competenţă	Unităţi de conţinut	Abilităţi
1. Domeniul securității cibernetice		
UC1. Analiza contextului securității cibernetice.	1. Caracteristici ale lumii cibernetice. 2. Diferențele între atacatori și specialiști. 3. Tipuri de amenințări și consecințele acestora. 4. Factori care favorizează criminalitatea cibernetică. 5. Profiluri și roluri profesionale în domeniu.	A1. Identificarea principalelor amenințări cibernetice (phishing, malware, spam etc.). A2. Clasificarea actorilor implicați: utilizatori, atacatori, specialiști în securitate. A3. Analiza factorilor sociali, tehnici și economici care favorizează atacurile. A4. Asocierea amenințărilor cu consecințele asupra individului, firmei, statului. A5. Identificarea funcțiilor specialiștilor în cybersecurity.
2. Principiile de bază în securitatea informației		
UC2. Aplicarea principiilor fundamentale ale securității informaționale.	1. Triada CIA: confidențialitate, integritate, disponibilitate. 2. Stările datelor: în repaus, în utilizare, în tranzit. 3. Măsuri de contracarare. 4. Modele de securitate: McCumber Cube, ISO.	A6. Aplicarea principiilor CIA în scenarii concrete (ex. parole, criptare, backup). A7. Corelarea între stările datelor și tipurile de protecție necesare. A8. Compararea modelelor de securitate McCumber și ISO. A9. Aplicarea principiului „defense-in-depth” în cadrul triadei CIA. A10. Explicarea modului în care compromiterea unui principiu afectează securitatea globală.
3. Amenințări cibernetice, vulnerabilități și atacuri		
UC3. Identificarea și clasificarea atacurilor și a vulnerabilităților.	1. Tipuri de malware și coduri malițioase. 2. Tehnici de inginerie socială. 3. Vectori și metode de atac.	A11. Clasificarea malware-ului: virus, troian, ransomware, spyware. A12. Identificarea indicatorilor specifici pentru fiecare tip de malware. A13. Simularea unui scenariu de atac de tip phishing. A14. Recunoașterea diferitelor forme de inginerie socială. A15. Clasificarea atacurilor: DoS, spoofing, injection etc. A16. Identificarea punctelor vulnerabile într-o rețea sau sistem.

Unităţi de competenţă	Unităţi de conţinut	Abilităţi
4. Protejarea confidențialității și a integrității datelor		
UC4. Aplicarea tehnicilor de protecție a datelor.	1. Criptografie: noțiuni, scopuri, algoritmi de bază. 2. Controlul accesului. 3. Semnături și certificate digitale. 4. Protejarea bazelor de date.	A17. Utilizarea criptării simetrice (AES) și asimetrice (RSA). A18. Crearea și aplicarea regulilor de control al accesului (ACL, RBAC). A19. Utilizarea semnăturilor digitale în validarea datelor. A20. Verificarea certificatelor digitale (ex. SSL). A21. Aplicarea măsurilor de protecție a bazelor de date (backup, hashing, tranzacții). A22. Detectarea modificărilor neautorizate asupra datelor.
5. Continuitatea operațională și răspunsul la incidente		
UC5. Asigurarea disponibilității și rezilienței serviciilor IT.	1. Conceptul de disponibilitate ridicată („Five Nines”). 2. Măsuri de redundanță și prevenire. 3. Planuri de răspuns la incidente. 4. Planuri de recuperare în caz de dezastru.	A23. Explicarea conceptului de „uptime 99.999%”. A24. Proiectarea unui sistem cu redundanță hardware/software. A25. Elaborarea unui plan de răspuns la incidente. A26. Documentarea corectă a unui incident. A27. Realizarea unui plan de recuperare în caz de dezastru (DRP). A28. Testarea planului DRP într-un scenariu de simulare.
6. Protecția infrastructurii și cadrul de reglementare		
UC6. Apărarea infrastructurii informatice și respectarea cadrului legal.	1. Măsuri de securizare a sistemelor și rețelelor (hardening). 2. Securitatea fizică și ambientală. 3. Etica profesională și legislația în domeniul securității informației. 4. Oportunități de carieră și certificare.	A29. Configurarea unui server securizat prin „hardening”. A30. Aplicarea măsurilor de protecție fizică (acces controlat, CCTV etc.). A31. Respectarea principiilor etice în activitatea profesională. A32. Identificarea legilor relevante (GDPR, NIS, Legea 161/2003 etc.). A33. Documentarea unui caz de încălcare a eticii profesionale. A34. Realizarea unui plan individual de formare continuă în domeniul cybersecurity.

VII. Studiu individual ghidat de profesor

Învățământ clasic (4 ani)
Învățământ dual (2 ani)

Materii pentru studiul individual	Produse de elaborat	Modalităţi de evaluare	Număr de ore
RÎ1. Identifice principalele tipuri de amenințări, vulnerabilități și atacuri cibernetice care afectează utilizatorii, rețelele și organizațiile.			
Configurarea echipamentelor active (switch-uri, routere)	Studiu de caz: analiza unui atac real (ex. phishing, ransomware) și documentarea vectorilor de atac, impactului și măsurilor de prevenție.	Prezentare individuală. Evaluare pe baza fișei de analiză: structură logică, relevanță, aplicabilitate.	10
RÎ2. Aplice principiile de confidențialitate, integritate și disponibilitate în evaluarea și proiectarea măsurilor de protecție cibernetică.			
Instalarea cablurilor de rețea conform standardelor	Studiu aplicat: proiectarea unei politici CIA pentru un sistem IT. Raport de testare a integrității datelor folosind hash (ex. SHA256)	Prezentare a scenariului CIA și justificarea măsurilor. Verificarea practică a rezultatelor hash.	10
RÎ3. Configureze metode de protecție a datelor și comunicațiilor, utilizând criptare, autentificare, control al accesului și măsuri de ascundere a datelor.			
Configurarea calculatoarelor pentru acces la resurse partajate	Ghid practic de criptare și decriptare a unui fișier. Raport privind semnarea digitală a unui document.	Testare practică individualăRaport scris detaliat.	10

Învățământ clasic (2 ani)

Materii pentru studiul individual	Produse de elaborat	Modalităţi de evaluare	Număr de ore
RÎ1. Identifice principalele tipuri de amenințări, vulnerabilități și atacuri cibernetice care afectează utilizatorii, rețelele și organizațiile.			
Configurarea echipamentelor active (switch-uri, routere)	Studiu de caz: analiza unui atac real (ex. phishing, ransomware) și documentarea vectorilor de	Prezentare individuală. Evaluare pe baza fișei de analiză: structură logică, relevanță, aplicabilitate.	20

Materii pentru studiul individual	Produse de elaborat	Modalităţi de evaluare	Număr de ore
	atac, impactului și măsurilor de prevenție.		
RÎ2. Aplice principiile de confidențialitate, integritate și disponibilitate în evaluarea și proiectarea măsurilor de protecție cibernetică.			
Instalarea cablurilor de rețea conform standardelor	Studiu aplicat: proiectarea unei politici CIA pentru un sistem IT. Raport de testare a integrității datelor folosind hash (ex. SHA256)	Prezentare a scenariului CIA și justificarea măsurilor. Verificarea practică a rezultatelor hash.	20
RÎ3. Configureze metode de protecție a datelor și comunicațiilor, utilizând criptare, autentificare, control al accesului și măsuri de ascundere a datelor.			
Configurarea calculatoarelor pentru acces la resurse partajate	Ghid practic de criptare și decriptare a unui fișier. Raport privind semnarea digitală a unui document.	Testare practică individualăRaport scris detaliat.	20

VIII. Lucrările practice recomandate

1. Stabilirea profilului de atacator și specialist în cybersecurity.
2. Construirea unei hărți de amenințări cibernetice.
3. Aplicarea modelului CIA asupra unei rețele simulate.
4. Analizarea stărilor datelor și aplicarea contramăsurilor.
5. Detectarea și blocarea atacurilor de tip phishing.
6. Scanarea și clasificarea malware-ului într-un sandbox.
7. Realizarea unei simulări de inginerie socială și apărare.
8. Criptarea și decriptarea fișierelor folosind OpenSSL.
9. Configurarea controalelor de acces și permisiuni în Linux.
10. Semnarea digitală a documentelor și verificarea semnăturii.
11. Verificarea certificatelor SSL/TLS ale site-urilor web.
12. Configurarea unei soluții simple de backup automat.
13. Crearea și aplicarea unui plan de răspuns la incident.
14. Evaluarea riscurilor fizice într-un spațiu IT și propunerea de soluții.
15. Apărarea unei infrastructuri IT simulate.

IX. Sugestii metodologice

Unitatea de curs „Operațiuni de securitate cibernetică” are ca obiectiv dezvoltarea competențelor practice și teoretice esențiale pentru proiectarea, configurarea și mentenanța infrastructurilor de rețea în

condiții de securitate. Pentru a asigura un proces educațional eficient și relevant, metodologia didactică propusă îmbină armonios elemente teoretice, activități practice și scenarii aplicative inspirate din situații reale, adaptate nivelului elevilor și cerințelor actuale ale industriei IT. Mai jos sunt prezentate câteva sugestii metodologice recomandate pentru desfășurarea cursului:

Abordare teoretic-practică integrată

- **Prelegeri interactive**: Introduceți concepte-cheie precum principiile CIA (confidențialitate, integritate, disponibilitate), tipuri de atacuri cibernetice, metode de protecție și modele de securitate (ISO 27001, McCumber Cube). Completați explicațiile cu exemple reale de incidente de securitate.
- **Demonstrații live**: Arătați practic cum funcționează o criptare simetrică, cum se verifică o semnătură digitală sau cum se detectează un atac de tip phishing folosind unelte specifice (OpenSSL, Wireshark, browsere, antivirus).

Învățare bazată pe simulare

- **Laboratoare practice**: Organizați sesiuni în care elevii aplică măsuri de securitate asupra sistemelor sau fișierelor (ex. criptare, semnături, ACL), analizează comportamentul codurilor malițioase în sandbox, identifică vulnerabilități.
- **Exerciții de depanare**: Propuneți situații simulate în care elevii trebuie să identifice atacuri sau erori de configurare (ex. parole slabe, lipsa backup-ului) și să aplice contramăsuri adecvate.

Metoda proiectului

- **Proiecte de grup**: Împărțiți elevii în grupuri și oferiți-le sarcina de a crea un plan de securitate pentru o instituție fictivă (școală, clinică, companie). Elevii vor proiecta soluții pentru controlul accesului, criptarea datelor, backup și răspuns la incidente.
- **Prezentări finale**: Echipele își vor prezenta soluția tehnică, explicând alegerile făcute (tipuri de atacuri anticipate, măsuri de protecție, simularea unui incident și răspunsul asociat).

Studiul de caz

- Prezentați exemple de incidente de securitate din companii reale (ex. atacuri ransomware, breșe de date, phishing masiv). Discutați cauzele, impactul și modul de remediere.
- Rugați elevii să propună o versiune adaptată a studiului de caz pentru un alt tip de organizație (ex. școală, ONG, firmă mică), ajustând politicile de protecție.

Învățare prin rezolvarea problemelor

- **Scenarii deschise**: Formularea unor cerințe fără soluție unică, cum ar fi: „Concepeți o politică de backup și restaurare pentru o rețea locală în care se procesează date confidențiale”.
- **Simulări de incidente**: Exerciții în care elevii trebuie să reacționeze la un incident (ex. detecție malware, pierdere de integritate, alertă firewall), urmărind pașii unui plan de răspuns.

Utilizarea resurselor tehnologice

- **Simulatoare și software**: Utilizați Cisco Packet Tracer pentru simularea rețelelor atacate, GNS3 pentru infrastructuri mai avansate, Wireshark pentru analiza traficului și OpenSSL pentru criptare/semnături.
- **Platforme de învățare online**: Furnizați acces la materiale complementare (video, ghiduri de configurare, demonstrații) prin Google Classroom, Moodle etc., pentru învățare autonomă.

Încurajarea autonomiei și cercetării

- **Documentare suplimentară**: Recomandați elevilor resurse tehnice oficiale (Cisco, MikroTik, NIST), ghiduri de bune practici sau forumuri comunitare pentru rezolvarea unor sarcini concrete de configurare și apărare.
- **Sarcini de cercetare**: Încurajați elevii să cerceteze soluții moderne precum autentificarea multifactor (MFA), SD-WAN sau zero trust, și să prezinte impactul acestora asupra securității.

Feedback și reflecție

- **Feedback regulat**: După fiecare activitate practică, oferiți elevilor feedback punctual despre punctele tari și erorile comise, însoțite de sugestii de îmbunătățire.
- **Jurnal de învățare**: Încurajați elevii să țină evidența provocărilor întâmpinate și a soluțiilor găsite, pentru a reflecta asupra progresului lor individual în domeniul securității cibernetice.

Recomandări generale:

- Asigurați un echilibru între teorie și practică, alocând cel puțin 60% din timp activităților hands-on.
- Adaptați nivelul de complexitate al sarcinilor la progresul elevilor, începând cu configurații simple și avansând spre rețele mai complexe.
- Încurajați colaborarea, dar și responsabilitatea individuală, prin combinarea activităților de grup cu cele individuale.

Aceste metodologii sunt concepute pentru a dezvolta atât competențele tehnice, cât și abilitățile transversale ale elevilor, pregătindu-i să aplice măsuri eficiente de securitate cibernetică, să gestioneze incidente și riscuri informatice și să răspundă cerințelor reale ale mediului profesional din industria IT.

X. Sugestii de evaluare

Evaluarea în cadrul unității de curs „Operațiuni de securitate cibernetică” urmărește să reflecte capacitatea elevilor de a înțelege conceptele fundamentale ale securității informaționale și de a aplica în practică măsuri de protecție, analiză, remediere și prevenție a incidentelor cibernetice. Scopul evaluării

este de a verifica atât competențele tehnice, cât și abilitățile de lucru individual și în echipă, cu accent pe situații reale. Mai jos sunt prezentate forme de evaluare recomandate:

Test teoretic scris

- **Format**: Întrebări cu răspunsuri scurte, alegere multiplă sau completare (ex. „Enumerați componentele triadei CIA și explicați rolul fiecăreia în securitatea datelor").
- **Obiectiv**: Verificarea cunoștințelor teoretice despre principii de securitate, tipuri de atacuri, modele conceptuale (CIA, ISO), criptografie, etică și legislație.
- **Criterii de evaluare**: Corectitudinea răspunsurilor, claritatea exprimării, utilizarea terminologiei adecvate.

Probe practice individuale

- **Format**: Elevii primesc o sarcină practică specifică (ex. criptarea unui fișier, configurarea controlului de acces, aplicarea unei semnături digitale, detectarea unei erori de configurare).
- **Obiectiv**: Evaluarea aplicării tehnice a cunoștințelor – identificarea riscurilor, aplicarea de măsuri de securitate, utilizarea uneltelor (OpenSSL, Packet Tracer, Wireshark).
- **Criterii de evaluare**: Funcționalitatea soluției, corectitudinea pașilor executați, interpretarea rezultatelor, respectarea cerințelor.

Proiect de grup

- **Format**: Echipe de 2–4 elevi elaborează un proiect de securitate cibernetică aplicată (ex. elaborarea unui plan de răspuns la incident, proiectarea unei politici de backup pentru o instituție, configurarea și documentarea unui sistem cu protecții de bază).
- **Obiectiv**: Verificarea capacității de colaborare, de documentare, de aplicare integrată a măsurilor de securitate.
- **Criterii de evaluare**: Relevanța soluției, justificarea deciziilor, claritatea raportului/prezentării, funcționalitatea simulării.

Exerciții de depanare (troubleshooting)

- **Format**: Elevii primesc un sistem sau o rețea preconfigurată cu o vulnerabilitate (ex. port deschis inutil, lipsă criptare, configurație incorectă de firewall, dublare de adresă IP) și trebuie să o identifice și să o remedieze.
- **Obiectiv**: Testarea capacității de analiză, diagnostic și remediere – competență critică pentru securitatea cibernetică.
- **Criterii de evaluare**: Rapiditatea și corectitudinea identificării problemei, aplicarea soluției potrivite, justificarea alegerii.

Evaluare continuă

- **Format**: Participare activă la activități practice precum criptarea fișierelor, testarea semnăturilor digitale, identificarea riscurilor, remedierea incidentelor simulate (ex.

detectarea unei configurări greșite de firewall). Completarea de chestionare scurte și reflecții rapide asupra activității.

- **Obiectiv**: Observarea implicării constante și a progresului în aplicarea măsurilor de securitate cibernetică.
- **Criterii de evaluare**: Gradul de implicare, acuratețea soluțiilor propuse, respectarea timpului și corectitudinea execuției.

Portofoliu sau jurnal de activități

- **Format**: Elevii colectează într-un portofoliu/jurnal activitățile practice realizate: configurări, erori identificate, soluții aplicate, interpretări personale. Fiecare activitate este însoțită de o scurtă reflecție asupra lecțiilor învățate și competențelor dobândite.
- **Obiectiv**: Încurajarea autoreflecției, a documentării și a consolidării progresului individual.
- **Criterii de evaluare**: Claritatea explicațiilor, relevanța și calitatea documentării, nivelul de autoanaliză și aplicabilitatea soluțiilor descrise.

- Combinați metodele de evaluare pentru a obține o imagine completă a competențelor elevilor, punând accent pe latura practică (minimum 60% din evaluare).
- Comunicați clar criteriile de evaluare înainte de fiecare probă și oferiți feedback detaliat după finalizare, evidențiind punctele forte și zonele de îmbunătățit.
- Ajustați nivelul de dificultate al sarcinilor în funcție de progresul elevilor, trecând treptat de la configurații simple la scenarii mai complexe.

Aceste sugestii de evaluare sunt concepute pentru a verifica atât cunoștințele teoretice, cât și abilitățile practice necesare configurării și mentenanței rețelelor de calculatoare, pregătind elevii pentru cerințele reale ale profesiei de administrator de rețea.

XI. Resursele necesare pentru atingerea rezultatelor învățării

Laboratorul destinat desfășurării unității de curs „Operațiuni de securitate cibernetică” trebuie să fie dotat cu echipamente și resurse tehnologice care să permită elevilor aplicarea practică a măsurilor de protecție, detectare, analiză și remediere a incidentelor informatice. Infrastructura trebuie să includă calculatoare performante, conectate într-o rețea locală configurabilă, echipamente de rețea (routere, switch-uri) și unelte specifice pentru monitorizare, testare și depanare.

Este necesară instalarea de software specializat, precum Cisco Packet Tracer, Wireshark, OpenSSL sau aplicații de criptare, semnătură digitală și gestionare a accesului. Mobilierul va fi ergonomic, adaptat lucrului individual sau în echipă, iar spațiile de lucru trebuie să asigure acces facil la echipamente și siguranță operațională.

Condițiile de utilizare includ respectarea normelor de securitate electrică și digitală, gestionarea ordonată a cablurilor și dispozitivelor pentru a preveni accidentele, precum și utilizarea exclusivă de software licențiat. Este esențial ca accesul la internet să fie stabil și securizat, pentru a permite activități de testare în medii simulate sau reale.

Întreținerea laboratorului presupune actualizarea regulată a aplicațiilor de securitate, verificarea stării echipamentelor, curățarea periodică a stațiilor de lucru și înlocuirea componentelor defecte de către personal tehnic autorizat. De asemenea, spațiul trebuie să fie bine ventilat, iluminat adecvat și să permită desfășurarea eficientă a activităților practice în domeniul securității cibernetice.

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 (cu specificații minime: procesor i5, 8 GB RAM, SSD 256 GB)	1	15
2.	Monitor LED 24"	1	15
3.	Router de rețea (ex. Cisco/Juniper)	-	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
10.	Tabla interactivă/whiteboard	-	1
c) Utilaj tehnologic			
11.	Router profesional	-	15
12.	Access Point Wi-Fi securizat	-	15
d) Instrumente și dispozitive			
13.	Software specializat: Cisco Packet Tracer, Wireshark, OpenSSL, antivirus, VPN client	-	15
14.	Platforme educaționale (Moodle, Google Classroom, Netacad.com, etc.)	-	1
e) Inventar și ustensile			
16.	Manuale și ghiduri de programare	1	15
17.	Markere pentru tablă albă	-	4
18.	Burete pentru tablă albă	-	1

XII. Resursele didactice recomandate elevilor

Nr. crt.	Denumirea resursei	Locul în care poate fi consultată / accesată resursa
1.	E-learning platform netacad.com	https://www.netacad.com/
2.	CCNA-Routing-and-Switching-Complete-Study-Guide-Exam-100-105-Exam-200-105-Exam-200-125-PDF.	Server local al instituţiei, format electronic
3.	Donahue, G. Network warrior. – O'Reilly Media, 2011. – 788 p.	Server local al instituţiei, format electronic
4.	Balchunas, Aaron. Cisco CCNA Study Gide. 2014. – 321 p.	Server local al instituţiei, format electronic
5.	Tomai, N.; Silaghi, Gh.C. Tehnologii şi aplicaţii mobile. – Cluj-Napoca: Risoprint, 2012. –	Server local al instituţiei, format electronic
6.	Moise, G.; Constantinescu, Z.; Vlădoiu, M.; Dumitru, M. Networking şi securitate. – Ploiesti: Editura Universității Petrol-Gaze, 2015.	Server local al instituţiei, format electronic