Ministerul Educaţiei al Republicii Moldova
Centrul de Excelenţă în Informatică şi Tehnologii Informaţionale

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

Vitalie Zavadschi

20 decembrie 2016

Curriculumul modular
S.07.O.024 Asistenţă în securitatea reţelelor de calculatoare

Specialitatea: 61230 Reţele de calculatoare
Calificarea: Tehnician pentru reţele de calculatoare

Chişinău 2016

Curriculumul a fost elaborat în cadrul Proiectului
"Parteneriate pentru calitatea şi relevanţa învăţământului profesional tehnic
din Republica Moldova",
implementat de Centrul Educațional PRO DIDACTICA
în parteneriat cu Asociaţia Naţională a Companiilor din Domeniul TIC/ATIC,
cu sprijinul financiar al Agenţiei Austriece pentru Dezvoltare/ADA și al Guvernului României

Autori:

Nicşan Adrian,	Centrul de Excelenţă în Informatică şi Tehnologii Informaţionale;
Zavadschi Vitalie,	grad didactic superior, Centrul de Excelenţă în Informatică şi Tehnologii Informaţionale.

Aprobat de:

Consiliul metodico-ştiinţific al Centrului de Excelenţă în Informatică şi Tehnologii Informaţionale.

Director _____
Vitalie Zavadschi

20 decembrie 2016

Recenzenţi:

1. Asociaţia Naţională a Companiilor din Domeniul TIC/ATIC, adresa: str. Maria Cibotari 28, mun. Chișinău, director executiv Chirița Ana.
2. „EBS Integrator" SRL, adresa: str. Ion Inculeţ 33, mun. Chișinău, director Aremesu Vitalie.

Adresa Curriculumului în Internet:

Portalul naţional al învăţământului profesional tehnic
http://www.ipt.md/ro/produse-educationale

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.

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

S.05.O.019 Arhitectura reţelelor de calculatoare;
F.02.O.013 Administrarea sistemelor de operare;
F.03.O.014 Programarea calculatorului;
S.06.O.021 Mentenanța rețelelor de calculatoare;
S.07.O.023 Asistență în administrarea protocoalelor.

II. Motivaţia, utilitatea modulului pentru dezvoltarea profesională

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

Beneficiile unei asistenţe bune în securitatea rețelelor de calculatoare sunt:

- reducerea probabilităţilor de atacuri în rețea;
- securizarea rețelelor de calculatoare;
- securizarea stațiilor de lucru;
- funcţionarea stabilă şi fiabilă a reţelelor.

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. Competenţele profesionale specifice modulului

Competenţele 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			
VIII	150	30	60	60	Examen	5

V. Unităţile de învăţare

Unităţi de competenţă	Unităţi de conţinut	Abilităţi
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 aplicațiilor de tip 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. Monitorizarea echipamentelor 6. Utilizarea funcțiilor automate	A6. Setarea accesului la echipamente. A7. Monitorizarea echipamentelor. A8. Activarea serviciilor la echipamente. A9. Dezactivarea serviciilor la echipamente . A10. Utilizarea funcțiilor automate la echipamente. A11. Monitorizarea traficului. A12. Scanarea porturilor.
3. Implementarea i-Barierilor (FIREWALLS)		
UC3. Setarea i-Barierilor	7. Liste de control al accesului 8. Filtrarea pachetelor	A13. Setarea serviciului Firewall pe echipamente. A14. Setarea regulilor pentru filtrarea traficului.

Unităţi de competenţă	Unităţi de conţinut	Abilităţi
	9. Monitorizarea conexiunilor 10. Sistemul de translatare a adreselor	A15. Inspectarea fluxului de date. A16. Configurarea server proxy. A17. Setarea serviciului NAT. A18. Utilizarea instrumentelor de verificare a serviciului Firewall.
4. Securizarea rețelelor locale de calculatoare		
UC4. Securizarea LAN	11. Securizarea stațiilor de lucru 12. Securizarea echipamentelor Wireless și VoIP 13. Configurarea opțiunilor de securitate a comutatoarelor	A19. Instalarea programelor de tip antivirus. A20. Setarea serviciului Firewall pe stațiile de lucru. A21. Setarea protocoalelor de acces protejat la echipamente wireless. A22. Limitarea conexiunilor la echipamente wireless. A23. Utilizarea cheilor de criptare. A24. Setarea filtrului dupa MAC adrese.
5. Implementarea Criptografiei		
UC5. Criptarea datelor	14. Serviciul criptografic 15. Semnăturile digitale 16. Criptarea simetrică și asimetrică	A25. Folosirea protocoalelor de criptare. A26. Utilizarea semnăturilor digitale. A27. Criptarea și decriptarea informației. A28. Utilizarea cheilor de criptare. A29. Semnarea documentelor electronice. A30. Gestionarea cheilor publice.

Unităţi de competenţă	Unităţi de conţinut	Abilităţi
6. Implementarea rețelelor private virtuale		
UC6. Configurarea VPN-urilor	17. VPN-urile 18. Componentele și operațiile IPSec 19. Implementarea accesului la distanță prin VPN 20. Implementarea VPN-urilor SSL	A31. Construirea rețelelor private virtuale. A32. Setarea protocoalelor de tunelare. A33. Crearea tunelurilor. A34. Configurarea serviciului IPSec. A35. Configurarea accesului la distanță. A36. Configurarea mecanismului de autentificare.
7. Administrarea rețelei de calculatoare securizată		
UC7. Utilizarea politicilor de securitate	21. Ciclu de viață a unei rețele de calculatoare securizată 22. Construirea politicilor de securitate	A37. Utilizarea listelor de acces la echipamente active deja existente în rețea. A38. Analiza istoricului a fișierilor cu log-uri. A39. Folosirea sistemelor de alertă în caz de atacuri.

VI. Repartizarea orientativă a orelor pe unităţi de învăţare

Nr. crt.	Unităţi de învăţare	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	Modalităţi de evaluare	Termeni de realizare
1. Amenințările de securitate într-o rețea			
Metodologia atacurilor	Prezentare	Comunicare	Săptămâna 2
2. Securizarea echipamentelor de rețea			
Monitorizarea echipamentelor	Prezentare	Comunicare	Săptămâna 4
Securizarea accesului la echipamente și fișiere	Proiect individual	Susţinerea proiectului	Săptămâna 5
3. Implementarea i-Barierilor (FIREWALLS)			
Sistemul de translatare a adreselor (NAT)	Prezentare	Comunicare	Săptămâna 6
Filtrarea pachetelor	Proiect individual	Susţinerea proiectului	Săptămâna 7

Materii pentru studiul individual	Produse de elaborat	Modalităţi de evaluare	Termeni de realizare
4. Securizarea rețelelor de calculatoare locale			
Securizarea echipamentelor Wireless și VoIP	Prezentare	Comunicare	Săptămâna 8
Configurarea opțiunilor de securitate a comutatoarelor	Proiect individual	Susţinerea proiectului	Săptămâna 9
5. Implementarea Criptografiei			
Serviciul criptografic	Prezentare	Comunicare	Săptămâna 10
Criptarea simetrică și asimetrică	Prezentare	Comunicare	Săptămâna 11
6. Implementarea rețelelor private virtuale			
Componentele și operațiile IPSec	Prezentare	Comunicare	Săptămâna 12
Implementarea accesului la distanță prin VPN	Proiect individual	Susţinerea proiectului	Săptămâna 13
7. Administrarea rețelei de calculatoare securizată			
Construirea politicilor de securitate	Proiect individual	Susţinerea proiectului	Săptămâna 14

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 competenţele ce trebuie formate şi dezvoltate în procesul de formare profesională. Acestea vor fi formate prin organizarea eficientă a procesului de instruire. Pentru aceasta sunt necesare două condiţii:

1. Organizarea activităţilor. Pentru buna organizare a procesului didactic ambii participanţi necesită de a-şi organiza activităţile. De modul cum sunt organizate acestea depinde în mare măsură nivelul de formare a competenţelor. În această ordine de idei, în procesul de organizare a activităţilor se vor asigura:

- condiţii optime pentru buna colaborare dintre elev şi profesor;
- un set de procese care duc la îmbunătăţirea relaţiilor dintre părţi;
- un nivel de implicare a părţilor acţionând în baza unor reguli şi acţiuni prestabilite.

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

Simularea şi modelarea. Simularea este utilizată pentru prezentarea la faza iniţială a unor concepte, oferind posibilitatea de ghidare a activităţii studentului în bază de situaţii practice. Prin intermediul acestei metode se pot reda, prin analogie, diverse situaţii, raţionamente, care pot să reprezinte relaţii dintre obiecte, fenomene, procese etc. Această metodă se recomandă pentru predarea-învăţarea-evaluarea următoarelor unităţi de conţinut:

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

Problematizarea mai poate fi denumită şi predare prin rezolvare de probleme sau predare productivă de probleme. Conform acestei metode instruitul este pus în faţa unor dificultăţi create în mod deliberat şi prin depăşirea lor învaţă ceva nou. „Punctul forte" al metodei îl constituie situaţia-problemă. Din această cauză este necesar de a formula corect situaţia. La crearea situaţiei de tip problemă se va ţine cont de următoarele caracteristici:

A. Situaţia trebuie să prezinte o dificultate pentru instruit, iar pentru a găsi soluţia, acesta se va confrunta cu efort de gândire;

B. Situaţia trebuie să prezinte interes, astfel încât acesta să acţioneze spre a rezolva problema;

C. Situaţia trebuie să orienteze activitatea instruitului spre a rezolva problema şi de al cointeresa pe acesta de a dobândi noi cunoştinţe;

D. Rezolvarea situaţiei nu va fi posibilă fără a apela la resursele recent dobândite.

Prin intermediul situaţiei 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 situaţia 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 soluţiei – 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 soluţiei;

4. Obţinerea rezultatului final – se analizează rezultatul obţinut şi formate anumite concluzii.

Această metodă se recomandă pentru predarea-învăţarea-evaluarea următoarelor unităţi de conţinut:

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

Instruirea asistată de calculator este o metodă didactică care valorifică principiile de modelare şi analiză cibernetică. Prin intermediul calculatorului se pune la dispoziţia elevului un set de probleme, care necesită a fi analizate, completate sau elaborate. Utilizarea metodei va oferi posibilitatea de organizare a informaţiei conform cerinţelor programei adaptabile la capacităţile fiecărui student; stimularea cognitivă a studentului prin secvenţe didactice şi întrebări ce vizează depistarea unor lacune, probleme, situaţii-problemă; rezolvarea sarcinilor didactice prezentate anterior prin reactivarea sau obţinerea informaţiilor necesare de la resursele informatice apelate prin intermediul calculatorului; realizarea unor sinteze recapitulative după parcurgerea unor teme, module de studiu, lecţii; asigurarea unor exerciţii suplimentare de stimulare a creativităţii studentului.

Această metodă se recomandă pentru predarea-învăţarea-evaluarea următoarelor unităţi de conţinut:

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

Metoda studiul de caz valorifică o situaţie reală care se analizează şi se rezolvă. Sunt cazuri când este necesar de a prezenta studentului probleme deja rezolvate. Avantajul metodei, constă în faptul că fiecare student 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-învăţarea-evaluarea următoarelor unităţi de conţinut:

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

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:

- Implementarea Criptografiei.

- Amenințările de securitate într-o rețea modrenă.

X. Sugestii de evaluare a competenţelor profesionale

Axarea procesului de învăţare-predare-evaluare pe competenţe presupune efectuarea evaluării pe parcursul întregului proces de instruire. Evaluarea continuă va fi structurată în evaluări formative şi evaluări sumative (finale) ce ţin de interpretarea creativă a informaţiilor şi de capacitatea de a rezolva situaţiile de problemă.

Activităţile de evaluare vor fi orientate spre motivarea elevilor şi obţinerea unui feedback continuu, fapt ce va permite corectarea operativă a procesului de învăţare, stimularea autoevaluării şi a evaluării reciproce, evidenţierea succeselor, implementarea evaluării selective sau individuale.

Pentru a eficientiza procesele de evaluare, înainte de a demara evaluările, cadrul didactic va aduce la cunoştinţa elevilor tematica lucrărilor, modul de evaluare (bareme/grile/criterii de notare) şi condiţiile de realizare a fiecărei evaluări.

Evaluarea curentă/formativă se va realiza prin diverse modalităţi: observarea comportamentului elevului, analiza rezultatelor activităţii elevului, discuţia/conversaţia, prezentarea proiectelor individuale de activitate. Prin evaluarea curentă/formativă, cadrele didactice informează elevul despre nivelul de performanţă; îl motivează să se implice în dobîndirea competenţelor profesionale.

Evaluarea sumativă se realizează la finele modulului în baza simulării în atelier a unei situaţii 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 cunoştinţe şi abilităţi. În acest scop, vor fi clar stabiliţi indicatorii şi descriptorii de performanţă 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 şi instrumente de evaluare. Portofoliul, de regulă este realizat pe o perioadă mai îndelungată (în decursul mai multor ore). Conţinutul unui portofoliu este reprezentat de rezultatele la: lucrări practice, studiul individual, investigaţii, referate şi 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 informaţii concludente privind pregătirea, evoluţia, atitudinea elevului) sau chiar de către elev (pe considerente de performanţă, preferinţe etc.). Structurarea evaluării sub forma de portofoliu se dovedeşte deosebit de utilă, atât pentru profesor, cât şi pentru elev sau părinţii acestuia. Pentru a realiza o evaluare pe bază de portofoliu, profesorul:

- va comunica elevilor intenţia de a realiza un portofoliu, adaptând instrumentele de evaluare ce constituie “centrul de greutate” ale portofoliului la specificul unităţii de învăţare;
- va alege componentele ce formează portofoliul, dând şi 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 şi un sistem de criterii pe baza cărora să realizeze evaluarea globală şi finală a portofoliului;
- va pune în evidenţă evoluţia elevului, particularităţile de exprimare şi de raportare a acestuia la aria vizată;
- va integra rezultatul evaluării portofoliului în sistemul general de notare.

În calitate de **produse pentru măsurarea competenţei** se vor folosi, după caz:

- serviciul FIREWALL setat pe echipamente de rețea;
- configurarea echipamentelor pentru filtrarea pachetelor;
- setarea listelor de control al accesului ;
- securizarea stațiilor de lucru;
- configurarea rețelelor VPN.

Criterii de evaluare a produselor pentru măsurarea competenţelor sunt:

- corectitudinea configurării serviciului FIREWALL;
- claritatea în alcătuirea schemei reţelei;
- respectarea cerinţelor la folosirea serviciului FIREWALL;
- corectitudinea schemei de lucru a i-Barierilor.

XI. Resursele necesare pentru desfăşurarea procesului de studii

Cerinţe faţă de sălile de curs	
Pentru orele teoretice	Cabinet de informatică cu 18 calculatoare. Proiector.
Pentru orele de laborator	Laborator de informatică care asigură fiecărui elev un calculator. Rutere ce suportă o configurare avansată.
Cerinţe tehnice	
Parametri tehnici minimi ale calculatorului	Procesor: 2 GHz. Memorie operativă: 4 GB. Unitate de stocare: 500 GB. Afişaj şi grafică: size: 22'', resolution: 1366 × 768. 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 naţional de informatică, Piatra Neamţ	Internet
2.	Banica Ion , Note de Curs: Comunicaţii între Calculatoare. Editura: Teora, 2005	Internet
3.	Răzvan Rughiniş. Reţele locale. Editura PRINTECH, 2012	Internet
4.	Răzvan Rughiniş. Proiectarea Reţelelor de Calculatoare. Editura:PRINTECH, 2014	Internet