Azərbaycan Respublikası Elm və Təhsil Nazirliyi
Lənkəran Dövlət Universiteti

"Təsdiq edirəm"
Tədrisin təşkili və təlim
texnologiyalari üzrə prorektor
vəzifəsini icra edən:
dos.Z.İ.Məmmədov
07 Fevral 2025.

Fənn sillabusu

İxtisas: 050615 İnformasiya təhlükəsizliyi
Kafedra: Texnologiya və texniki elmlər
I. Fənn haqqında məlumat:
Fənnin adı: Korporativ şəbəkə sistemlərinin təhlükəsizliyi
Kodu ATMTMOF B03
Tədris ili: II tədris ili, (2024-2025) Semestr: II
Tədris yükü: Auditoriya saatı 60 (30 saat mühazirə, 30 saat laboratoriya)
Tədris forrması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 6 kredit
Auditoriya N: 215
Saat: 9^{30} ,14^{40} , 11^{20}
II. Müəllim haqqında məlumat:
Adı, soyadı, elmi dərəcəsi və elmi adı: Vüsalə Muradova Xudaşirin qızı, t.ü.f.d., dosent
Məsləhət saatı: IV gün saat 12^{20} -13^{30}
E-mail ünvanı: vusala.muradoav@lsu.edu.az
Kafedranın ünvanı: Lənkəran şəhər Fizuli 170 a Tədris korpusu
III. Tövsiyyə olunan dərsliklər və dərs vəsaitləri:

Əsas ədəbiyyat

1. Aidə Mustafayeva. Şəbəkə təhlükəsizliyi. Dərs vəsaiti, 2024
2. Musayev V.H., Qənbərov M.M., Qənbərova G.T., Əliyeva Ş.X. «İnformasiya təhlükəsizliyi və kompyuter şəbəkələri», Bakı, 2015.
3. Musayev V.H. Qənbərov M.M., Kompüter sistemlərində təhlükəsiz aparat və proqram vasitələri, Baki, 2015.

Əlavə ədəbiyyat

4. Əliquliyev R.M., İmamverdiyev Y.N., İnformasiya təhlükəsizliyi insidentləri. Bakı: İnformasiya texnologiyaları, 2012, 212 s.
5. Charles J.B, Christoper G., Philip A.C., Donald S., Cybersecurity Essentials. "Sybex", 2018, 784 s.
6. Ozkaya E., Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity. Packt Publishing, 2019, 396 p.
7. https://tryhackme.com/

VI. Prekvizitlər: Fənnin tədrisi üçün öncədən şəbəkə təhlükəsizliyi problemi və onu xarakterizə edən amillərin tədrisi vacibdir.

V. Korekvizitlər: Bu fənnin tədrisi ilə eyni vaxtda başqa fənlərin də tədris olunmasına zərurət yoxdur.

VI. Fənnin təsviri və məqsədi: "Korporativ şəbəkə sistemlərinin təhlükəsizliyi" fənninin tədrisi zamanı tələbələrə kompüter şəbəkələrini müxtəlif təhlükə və hücumlardan qorumaq üçün lazımi bilik, bacarıq və vərdişlərin verilməsidir. Bura şəbəkə təhlükəsizliyi prinsipləri, zəifliklərin təhlili, hücumların aşkarlanması və qarşısının alınması üsulları, kriptoqrafiya, təhlükəsizlik siyasəti, risklərin idarə edilməsi və bir çox digər aspektlər üzrə nəzəri və praktiki tapşırıqlar yerinə yetirilir.

VII. Davamiyyətə verilən tələblər:

Fənn üzrə semestr ərzində buraxılmış auditoriya saatlarının ümumi sayı Elmi Şuranın 16 may 2024-cü il tarixli qərarına uyğun olaraq davamiyyət meyarları nəzərə alınmaqla müəyyən olunmuş həddən yuxarı olduğu halda tələbə həmin fəndən imtahana buraxılmır, onun həmin fənn üzrə akademik borcu qalır.

VIII. Qiymətləndirmə:

Qiymətləndirmə zamanı Elmi Şuranın 16 may 2024-cü il tarixli qərarına uyğun olaraq qiymətləndirmə meyarları nəzər alınır.

Tələbələrin biliyi 100 ballı sistemlə qiymətləndirilir. Bundan 50 balı tələbə semestr ərzində, 50 balı isə imtahanda toplayır. Semestr ərzində toplanan 50 bala aşağıdakılar aiddir: 30 bal kollokviuma görə, 20 bal seminar və ya laboratoriya dərslərində fəaliyyətinə görə. İmtahanda qazanılan balların maksimum miqdarı 50-dir. İmtahan biletinə bir qayda olaraq fənni əhatə edən 5 sual daxil edilir.

Qiymət meyarları aşağıdakılardır:

-10 bal- tələbə keçirilmiş materialları dərindən başa düşür, cavabı dəqiqdir və hərtərəflidir.

- 9 bal - tələbə keçirilmiş materialları tam başa düşür, cavabı dəqiqdir və mövzunun mətnini tam açа bilir.

- 8 bal - tələbə cavabında ümumi xarakterli bəzi qüsurlara yol verir.

- 7 bal - tələbə keçirilmiş materialları başa düşür, lakin nəzəri cəhətdən bəzi məsələləri əsaslandıra bilmir.

- 6 bal - tələbənin cavabı əsasən düzgündür.

- 5 bal - tələbənin cavabında çatışmamazlıqlar var, mövzunu tam əhatə edə bilmir.

- 4 bal - tələbənin cavabı qismən doğrudur, lakin mövzunu izah edərkən bəzi səhvlərə yol verir.

- 3 bal - tələbənin mövzudan xəbəri var, lakin fikrini əsaslandıra bilmir.

-1-2 bal - tələbənin mövzudan qismən xəbəri var.

- 0 bal - suallara cavab yoxdur.

Tələbənin imtahanda topladığı balın miqdarı 17-dən az olmamalıdır. Əks təqdirdə tələbənin imtahan göstəriciləri semestr ərzində tədris fəaliyyəti nəticəsində topladığı bala əlavə olunmur.

Semestr nəticələrinə görə yekun qiymətləndirmə (imtahan və imtahana qədərki ballar əsasında)

51 baldan aşağı "qeyrikafi" -F,
51 - 60 bal "qənaətbəxş" -E,
61 - 70 bal "kafi" -D,
71 - 80 bal "yaxşı" -C,
81 - 90 bal "çoxyaxşı" -B,
91 - 100 bal "əla" -A kimi qiymətləndirilir.

IX. Davranış qaydalarının pozulması: Tələbə Universitetin daxili nizam-intizam qaydalarını pozduqda əsasnamədə nəzərdə tutulan qaydada tədbir görüləcək.

X. Təqvim mövzu planı: Mühazirə 30 saat, seminar 30 saat. Cəmi: 60 saat

№	Keçirilənmühazirə, seminar, məşgələ, laboratoriyavəsərbəstmövzuların məzmunu	Saat	Tarix
1	2	3	4
	Mühazirə mövzuları		
1.	**Mövzu № 1. Şəbəkə cihazları və texnologiyaları** Plan: 1. Aktiv və passiv şəbəkə cihazları 2. Osı və tcp/ ıp modelı 3. Port nömrələrı və şəbəkə protokolları 4. İnternet səviyyəsinin protokollari: ipv4 və ipv6 5. Şəbəkə problemlərinin aradan qaldirilmasi 6. Virtuallaşdırma texnologiyaları 1. Mənbə: 1,3,4	2	
2.	**Mövzu № 2. Şəbəkə topologiyası** Plan: 1. Şəbəkə dizaynı və topologiyalar 2. Fiziki bağlanti problemlərinin aradan qaldirilmasi 3. Ethernet standartlari 4. Naqillərin paylanması texnologiyası Mənbə: 2,3,4	2	
3.	**Mövzu 3. Şəbəkənin idarə edilməsi** Plan: 1. Şəbəkə avadanlıqları 2. Avadanlıq problemlərinin aradan qaldırılması vasitələri 3. Proqram təminatı problemlərinin aradan qaldırılması vasitələri 4. Snmp – syslog – şəbəkə trafikinin təhlili 5. Şəbəkə sənədləri 6. Qos və şəbəkə performansı Mənbə: 1,3, 4	2	
4.	**Mövzu 4. Şəbəkə təhlükəsizliyinə giriş** Plan: 1. Şəbəkə təhlükəsizliyinin əsas məqsədi, predmeti və vəzifələri 2. Şəbəkə təhlükəsizliyinin növləri 3. Şəbəkə təhlükəsızliyi üçün alətlər 4. Ən yaxşı şəbəkə təhlükəsizliyi sertifikatları Mənbə:1,3, 4	2	
5.	**Mövzu № 5. Simsiz (wi-fi) təhlükəsizlik** Plan: 1. Simsiz (wi-fi) təhlükəsizlik üsullari 2. Şifrələmə protokollari 3. Mac ünvan filtrləmə 4. Cihazin yerləşdirilməsi qaydasi və siqnal gücü Mənbə : 2,3,4	2	
6.	**Mövzu № 6. Autentifikasiya, avtorizasiya və şəbəkə təhlükəsizliyi auditi** Plan: 1. Təhlükəsizlik konsepsiyası aaa (authentıcatıon, authorızatıon, accountıng) 2. Şəbəkə təhlükəsizliyi auditi 3. Şəbəkə təhlükəsizliyi auditi alətləri	2	

	Mənbə: 1,3,4.		
7.	**Mövzu № 7. Ümumi təhdidlər və zəifliklər** Plan: 1. Məxfilik, tamlıq və əlçatanlığa yönəlmiş təhdidlər 2. Wi-fi zəifliklər 3. Şəbəkə cihazı zəifliklər 4. Şəbəkə infrastrukturunun zəifliklər 5. Tətbiq zəifliklər 6. Təhdidlərın azaldılması Mənbə: 1,3, 4,	2	
8.	**Mövzu № 8. Firewall- şəbəkələrarası ekranlaşdırma** Plan: 1. Firewall – şəbəkələrarası ekranlaşdırmanın əsas mahiyyəti və vəzifələri 2. Firewall – əsas konfiqurasiyası və işləmə mexanizmi 3. Firewall növləri 4. Proseslərin təftişi və paket filtrləmə 5. Şəbəkə ünvanlarinin translyasiyasi (network address translation -nat) Mənbə: 1,3,4.	2	
9.	**Mövzu 9. İds/ips sistemləri** Plan: 1. İds/ips sistemlərinə giriş 2. İds-in işləmə mexanizmi və növləri 3. Ids ilə ips arasındakı fərq 4. Siem - hadisə və məlumatların təhlükəsiz idarəetmə sistemləri 5. Şəbəkə təhlükəsizliyinin əməliyyat mərkəzi Mənbə: 1,3, 4.	2	
10.	**Mövzu 10. Korporasiya anlayışı və korporasiyanın təşkilində informasiyanın rolu** Plan: Korporasiya anlayışı və korporasiyanın təşkilində informasiyanın rolu Mənbə : 2,3,4	2	
11.	**Mövzu 11. Korporativ şəbəkə anlayışı** Plan: 1.Korporativ şəbəkə anlayışı Mənbə : 1,2,3	2	
12.	**Mövzu 12. Korporativ şəbəkənin əsasları** Plan: 1.Korporativ şəbəkənin əsasları Mənbə : 1,2,3	2	
13.	**Mövzu 13. Korporativ şəbəkələrin çoxsəviyyəli təsviri** Plan: 1. Korporativ şəbəkələrin çoxsəviyyəli təsviri Mənbə : 1,2,3	2	
14.	**Mövzu 14. Korporativ Şəbəkənin Strukturu** Plan: 1. Korporativ Şəbəkənin Strukturu Mənbə: 1,2,3	2	

15.	**Mövzu 15. Korporativ kompüter şəbəkələrinin təşkilində domen mexanizmindən istifadə** Plan: 1. Korporativ kompüter şəbəkələrinin təşkilində domen mexanizmindən istifadə Mənbə: 1,2,3	2	
	Cəmi	**30**	
	Laborator məşqələ mövzuları		
1.	**Şəbəkə cihazları və texnologiyaları**	**4**	
2.	**Şəbəkə topologiyası**	**4**	
3.	**Simsiz (wi-fi) təhlükəsizlik**	**4**	
4.	**Autentifikasiya, avtorizasiya və şəbəkə təhlükəsizliyi auditi**	**4**	
5.	**Ümumi təhdidlər və zəifliklər**	**4**	
6.	**Firewall- şəbəkələrarası ekranlaşdırma**	**4**	
7.	**İds/ips sistemləri**	**4**	
8.	**Korporativ şəbəkələrin çoxsəviyyəli təsviri**	**2**	
	Cəmi	**30**	

XI. Fənn üzrə tələblər, tapşırıqlar:

Fənnin tədrisinin sonunda tələbələr **"Korporativ şəbəkə sistemlərinin təhlükəsizliyi "** kursundan müəyyən biliklərə malik olmalı, o cümlədən fənn haqqında nəzəri və praktik şəkildə fikirlərini əsaslandırmağı bacarmalıdırlar.

"Korporativ şəbəkə sistemlərinin təhlükəsizliyi " fənninin tədrisi zamanı tələbələrə kompüterin strukturuna aıd olan müxtəlif bölmələrinin və praktik tətbiqini öyrədilməsi fənn üzrə qoyulan əsas tələblərdən biridir: " Kibertəhlükəsizliyin əsasları " fənninin tədrisi zamanı qoyulan tələblər aşağıdakı kimidir:

- Mühazirə mətninin hazırlanması,
- test tapşırıqları,
- referat işləri,
- fərdi tapşırıqlar,
- praktiki məsələlər.

XII.Təlimin nəticələri

Fənnin mənimsənilməsi nəticəsində tələbələr bilməlidirlər:

- Kompüter şəbəkələrinə, informasiya resurslarına yönəlmiş təhdidlərin təsnifatını
- Kompüter şəbəkələrində informasiya təhlükəsizliyi baxımından zəif yerlərini
- İnformasiyanın sızmasının və ona icazəsiz girişin əldə olunmasının əsas yollarını
- Hücumların aşkarlanması və qarşısının alınması üçün yeni üsul və vasitələrin seçilməsi
- Təhlükəsizlik sistemlərinin mütəmadi olaraq yenilənməsi rəqəmsal dünyada təhlükəsizliyi qorumaq
- Müdafiə strategiyasını

XIII. Tələbələrin fənn haqqında fikrinin öyrənilməsi:

XIV.Birinci kollekvium sualları

1. Aktiv və passiv şəbəkə cihazları
2. Osı və tcp/ ıp modelı
3. Port nömrələrı və şəbəkə protokolları
4. İnternet səviyyəsinin protokollari: ipv4 və ipv6
5. Şəbəkə problemlərinin aradan qaldirilmasi
6. Virtuallaşdırma texnologiyaları
7. Şəbəkə dizaynı və topologiyalar
8. Fiziki bağlanti problemlərinin aradan qaldirilmasi
9. Ethernet standartlari
10. Naqillərin paylanması texnologiyası
11. Şəbəkə avadanlıqları
12. Avadanlıq problemlərinin aradan qaldırılması vasitələri
13. Proqram təminatı problemlərinin aradan qaldırılması vasitələri
14. Snmp – syslog – şəbəkə trafikinin təhlili
15. Şəbəkə sənədləri

XV. Ikinci kollekvium sualları

1. Qos və şəbəkə performansı
2. Şəbəkə təhlükəsizliyinin əsas məqsədi, predmeti və vəzifələri
3. Şəbəkə təhlükəsizliyinin növləri
4. Şəbəkə təhlükəsızliyi üçün alətlər
5. Ən yaxşı şəbəkə təhlükəsizliyi sertifikatları
6. Simsiz (wi-fi) təhlükəsizlik üsullari
7. Şifrələmə protokollari
8. Mac ünvan filtrləmə
9. Cihazin yerləşdirilməsi qaydasi və siqnal gücü
10. Təhlükəsizlik konsepsiyası aaa (authentıcatıon, authorızatıon, accountıng)
11. Şəbəkə təhlükəsizliyi auditi
12. Şəbəkə təhlükəsizliyi auditi alətləri
13. Məxfilik, tamlıq və əlçatanlığa yönəlmiş təhdidlər
14. Wi-fi zəifliklərı
15. Şəbəkə cihazı zəifliklərı

XVI. Fənnin imtahan sualları:

I ci blok

1. Aktiv və passiv şəbəkə cihazları
2. Osı və tcp/ ıp modelı
3. Port nömrələrı və şəbəkə protokolları
4. İnternet səviyyəsinin protokollari: ipv4 və ipv6
5. Şəbəkə problemlərinin aradan qaldirilmasi
6. Virtuallaşdırma texnologiyaları
7. Şəbəkə dizaynı və topologiyalar
8. Fiziki bağlanti problemlərinin aradan qaldirilmasi
9. Ethernet standartlari

II ci blok

10. Naqillərin paylanması texnologiyası
11. Şəbəkə avadanlıqları
12. Avadanlıq problemlərinin aradan qaldırılması vasitələri
13. Proqram təminatı problemlərinin aradan qaldırılması vasitələri
14. Snmp – syslog – şəbəkə trafikinin təhlili
15. Şəbəkə sənədləri
16. Qos və şəbəkə performansı
17. Şəbəkə təhlükəsizliyinin əsas məqsədi, predmeti və vəzifələri
18. Şəbəkə təhlükəsizliyinin növləri

III cü blok

19. Şəbəkə təhlükəsızliyi üçün alətlər
20. Ən yaxşı şəbəkə təhlükəsizliyi sertifikatları
21. Simsiz (wi-fi) təhlükəsizlik üsulları
22. Şifrələmə protokolları
23. Mac ünvan filtrləmə
24. Cihazin yerləşdirilməsi qaydasi və siqnal gücü
25. Təhlükəsizlik konsepsiyası aaa (authentıcatıon, authorızatıon, accountıng)
26. Şəbəkə təhlükəsizliyi auditi
27. Şəbəkə təhlükəsizliyi auditi alətləri

IV cü blok

28. Məxfilik, tamlıq və əlçatanlığa yönəlmiş təhdidlər
29. Wi-fi zəifliklər
30. Şəbəkə cihazı zəifliklər
31. Şəbəkə infrastrukturunun zəifliklər
32. Tətbiq zəifliklər
33. Təhdidlərın azaldılması
34. Firewall – şəbəkələrarası ekranlaşdırmanın əsas mahiyyəti və vəzifələri
35. Firewall – əsas konfiqurasiyası və işləmə mexanizmi
36. Firewall növləri

V ci blok

37. Ids ilə ips arasındakı fərq
38. Sıem - hadisə və məlumatların təhlükəsiz idarəetmə sistemləri
39. Şəbəkə təhlükəsizliyinin əməliyyat mərkəzi
40. Korporasiya anlayışı və korporasiyanın təşkilində informasiyanın rolu
41. Korporativ şəbəkə anlayışı
42. Korporativ şəbəkənin əsasları
43. Korporativ şəbəkələrin çoxsəviyyəli təsviri
44. Korporativ Şəbəkənin Strukturu
45. Korporativ kompüter şəbəkələrinin təşkilində domen mexanizmindən istifadə

" Korporativ şəbəkə sistemlərinin təhlükəsizliyi " fənninin sillabusu 050631 - "İnformasiya təhlükəsizliyi" ixtisasının tədris planı və fənn proqramı əsasında tərtib edilmişdir.

Sillabus **"Texnologiya və texniki elmlər"** kafedrasında müzakirə edilərək, təsdiq edilmişdir (07 fevral 2025-ci il, protokol № 01).

Fənn müəllimi: **dosent, V. X. Muradova**

Kafedra müdiri: **dosent, R. F. Əliyev**