Azərbaycan Respublikası Elm və Təhsil Nazirliyi
Lənkəran Dövlət Universiteti

"Təsdiq edirəm"
Tədris məsələləri üzrə prorektor v.i.e:
dos. Zaur Məmmədov
"07" yanvar 2026-cı il

Fənn sillabusu

İxtisasın şifri və adı: 6006017-İnformasiya təhlükəsizliyi
Fakultə: Aqrar və mühəndislik
Kafedra: Texnologiya və texniki elmlər

I. Fənn haqqında məlumat:
Fənnin adı: S.F.Mobil və simsiz avadanlıqların təhlükəsizliyi ("S.F.Mobil və simsiz avadanlıqların təhlükəsizliyi" işçi fənn proqramı,Lənkəran Dövlət Universitetinin Texnologiya və texniki elmlər kafedrasının 07.01.2026-cı il 5 №-li protokoluna əsasən)
Kodu: ATMTMOF-B08
Tədris ili: III tədris ili (2025/2026)
Semestr: VI (yaz)
Tədris yükü: 60 (30 saat mühazirə, 30 saat laboratoriya)
Təhsilalma forması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 6 kredit

II. Müəllim haqqında məlumat:
Adı, soyadı, elmi dərəcəsi və elmi adı:
Mühazirə müəllimi: **Dəmirov Asəf Ağacəfər oğlu, t.ü.f.d.,dosent.**
Laboratoriya müəllimi:**Məlikzadə Tural Tofiq oğlu, müəllim.**
Kafedranın ünvanı: Lənkəran şəhəri Füzuli 170 a, LDU-nun 1 saylı tədris binası
Məsləhət saatı: V gün saat 12^{20} -13^{55} , V gün saat 12^{20} -13^{55}
E-mail ünvanı: asef.demirov@gmail.com, tural1996t@gmail.com

III.Tövsiyyə olunan dərsliklər və dərs vəsaitləri:

Əsas ədəbiyyat
1.**"Wireless Networks & Security: Next Generation Networks"**, Dr. Cory Beard – Simli & simsiz təhlükəsizlik konseptləri.
2.**"Hacking Exposed Wireless"**, Johnny Cache, Joshua Wright, Vincent Liu – Simsiz hücumlar və müdafiə təcrübələri.
3.**"Mobile Application Security"**, Himanshu Dwivedi – Mobil tətbiq təhlükəsizliyi üzrə praktik nümunələr.
Kurslar & Resurslar
4.**OWASP Mobile Security Project** – Mobil təhlükəsizlik kateqoriyaları, test checklistləri.
5.**Wireshark University / Aircrack-ng Docs** – Snifing və analiz alətləri üçün rəsmi sənədlər.
6.**CVE & NIST NVD Database** – Zəifliklərin standart təsnifatı və risk qiymətləndirilməsi.
Standartlar
7.**IEEE 802.11 Security Standards** – Wi-Fi təhlükəsizlik spesifikasiyaları.
8.**ISO/IEC 27001** – Ümumi informasiya təhlükəsizliyi sistemi.

9.Mühazirələr.S.F.Mobil və simsiz avadanlıqların təhlükəsizliyi.Dəmirov Asəf Ağac oğlu, t.ü.f.d.,dosent.LDU-2026

IV. Prerekvizit fənlər: Fənnin tədrisi üçün öncədən başqa bir fənnin tədrisinə zərurət yoxdur..

V. Korekvizit fənlər: Fənnin tədrisi ilə eyni zamanda başqa fənnin tədrisinə ehtiyac yoxdur.

VI. Fənnin təsviri və məqsədi:

S.F. "Mobil və simsiz avadanlıqların təhlükəsizliyi" fənni tələbələrə mobil və simsiz şəbəkə sistemlərinin arxitekturasını, zəifliklərini, hücum növlərini, müdafiə mexanizmlərini və təhlükəsizlik tədbirlərini praktiki olaraq öyrətməyi hədəfləyir.

VII.Davamiyyətə verilən tələblər: Fənn üzrə semestr ərzində buraxılmış auditoriya saatlarının ümumi sayı LDU-nun Elmi Şurasının 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: Fənn üzrə tələbələrin biliyi 100 ballıq sistemlə qiymətləndirilir.Yəni tələbənin fənn üzrə toplaya biləcəyi balın maksimum miqdarı 100-ə bərabərdir.

Bu balın yarısı (50 balı) tələbənin semestr müddətində fəaliyyətinin nəticəsinə (cari qiymətləndirmə), digər yarısı isə (digər 50 balı) imtahanın nəticəsinə (aralıq qiymətləndirmə) görə verilir.

Fənn üzrə cari qiymətləndirmənin nəticəsinə görə verilən maksimum 50 bala aşağıdakılar daxildir:

- 20 bal - seminar dərslərində fəaliyyətinə görə;
- 30 bal - kollokviumların nəticələrinə görə.

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

İmtahanda qazanılan balların maksimum miqdarı 50-dir. İmtahan yazılı şəkildə aparılır və imtahan biletinə bir qayda olaraq fənn üzrə tədris olunan mövzulara aid 5 sual daxil edilir. Hər sual maksimum 10 bal olmaqla qiymətləndirilir (aşağıda qeyd olunan qiymət meyarına əsasən) ki, bu da toplamda fənn üzrə aralıq qiymətləndirmənin nəticəsinə görə verilən maksimum 50 balı təşkil edir.

Qiymət meyarları aşağıdakılardır:

- 10 bal - tələbə keçilmiş materialı dərindən başa düşür, cavabı dəqiq və hərtərəflidir;
- 9 bal - tələbə keçilmiş materialı tam başa düşür, cavabı dəqiqdir və mövzunun məzmununu tam açа bilir;
- 8 bal - tələbə cavabında ümumi xarakterli bəzi qüsurlara yol verir;
- 7 bal - tələbə keçilmiş materialı yaxşı başa düşür, lakin nəzəri cəhətdən bəzi məsələləri əsaslandıra bilmir;
- 6 bal - tələbənin cavabı əsasən düzgündür;
- 5 bal - tələbənin cavabında çatışmazlıqlar 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 - cavab yoxdur.

Tələbənin fənn üzrə aralıq qiymətləndirmə balının (imtahanda topladığı balın) miqdarı 17-dən az olmamalıdır. Əks təqdirdə tələbənin fənn üzrə aralıq qiymətləndirmə balı cari qiymətləndirmə balına (semestr ərzində tədris fəaliyyəti nəticəsində topladığı bala) əlavə olunmur.
Fənn üzrə cari və aralıq qiymətləndirmənin ümumi nəticəsinə görə tələbənin biliyi yekun olaraq aşağıdakı kimi qiymətləndirilir:

Bal aralığı (göstərilən ballar daxil olmaqla)	Hərflə işarəsi	Sözlə yazılışı
91-100 bal	A	əla
81-90 bal	B	çox yaxşı
71-80 bal	C	yaxşı
61-70 bal	D	kafi
51-60 bal	E	qənaətbəxş
51-baldan aşağı	F	qeyri-kafi

IX. Davranış qaydalarının pozulması:
Tələbə Universitetin Daxili intizam qaydalarını pozduqda onun barəsində mövcud qanunvericilik çərçivəsində müvafiq tədbir görüləcəkdir.

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

Mühazirə mövzuları			
S/s	**Mövzunun adı və məzmunu**	**Saat**	**Tarix**
1.	**Mövzu №1. Giriş: Mobil və simsiz mühitin təhlükəsizliyi** Plan: 1.Mobil və simsiz sistemlərin növləri, 2.Risk mühiti, əsas prinsiplər, tələbələrin gözləntiləri. **Mənbə:9** [1-10]	2	
2.	**Mövzu №2. Şəbəkə modelləri və simsiz protokollar** Plan: 1.OSI/TCP-IP, Wi-Fi (802.11), Bluetooth, 2.ZigBee, LTE/5G və onların təhlükəsizlik aspektləri. **Mənbə:9** [11-20]	2	
3.	**Mövzu № 3. Kriptoqrafiya əsasları** Plan: 1.Simmetrik/asimmetrik şifrələmə, 2. Hash, digests, açar idarəetməsi. **Mənbə:9** [21-30]	2	
4.	**Mövzu №4. Mobil cihaz təhlükəsizliyi** Plan: 1.iOS/Android arxitekturası, 2.sandboxing, app icazələri, jailbreak/root riskləri. **Mənbə:9** [31-40]	2	
5.	**Mövzu №5. Simsiz şəbəkələrdə şifrələmə protokolları** Plan: 1.WEP, WPA/WPA2/WPA3, 2.TKIP, AES-CCMP – müqayisə və zəifliklər. **Mənbə:9** [41-50]	2	
6.	**Mövzu № 6. Autentifikasiya və icazə nəzarəti** Plan:	2	

	1.802.1X, EAP növləri. 2.RADIUS/AAA infrastrukturu. **Mənbə:9** [51-60]		
7.	**Mövzu № 7. Saldırılar və zəiflik növləri (Simli vs Simsiz)** Plan: 1.Sniffing, spoofing. 2.DoS, evil-AP, man-in-the-middle. **Mənbə:9** [61-70]	2	
8.	**Mövzu №8. Mobil tətbiq təhlükəsizliyi** Plan: 1.Təhlükəsiz kodlaşdırma prinsipləri. 2.statik/dinamik analiz giriş. **Mənbə:9** [71-80]	2	
9.	**Mövzu №9. Mobil kommunikasiya hücumları** Plan: 1.SMS/SS7 zəiflikləri. 2.IMSI catcher (Stingray), VoLTE riskləri. **Mənbə:9** [81-90]	2	
10	**Mövzu № 10.Simsiz şəbəkə monitorinqi və təhlükə aşkarlanması** Plan: 1.IDS/IPS, anomaliya aşkarlanması. 2.Traffic analiz. **Mənbə:9** [91-100]	2	
11.	**Mövzu № 11. Kripto analiz və simsiz protokollarda zəiflikləri** Plan: 1.Kripto analizin mexanizmləri. 2.Re-keying problemləri. **Mənbə:9** [101-110]	2	
12.	**Mövzu № 12. Təhlükəsizlik siyasətləri və uyğunluq** Plan: 1.BYOD, MDM/EMM. 2.ISO/IEC 27001 tələbləri simsiz şəbəkələr üçün. **Mənbə:9** [111-120]	2	
13.	**Mövzu №13. Mobil Ödəniş Sistemləri və təhlükəsizlik** Plan: 1.NFC ödəniş protokolları riskləri 2.Tokenizasiya ödəniş protokolları riskləri. **Mənbə:9** [121-130]	2	
14.	**Mövzu № 14. Cloud və Edge inteqrasiyalı mobil təhlükəsizlik** Plan: 1.Cloud cihaz qorunması. 2.API təhlükəsizlik, konteynerləşmə. **Mənbə:9** [131-140]	2	
15.	**Mövzu № 15. Gələcək texnologiyalar & trendlər** Plan: 1.5G/6G təhlükəsizlik. 2.IoT, AI-based hücum/müdafiə sistemləri **Mənbə:9** [141-150]	2	
	Cəmi mühazirə:		**30 s.**
S/s	**Laboratoriya mövzusunun adı**	**Saat**	**T**

1.	Virtual test mühiti qurulması	2	
2.	Sniffing və Traffic analiz	2	
3.	WPA/WPA2/WPA3 zəifliklərin yoxlanması	2	
4.	Evil-Twin/AP spoofing testləri	2	
5.	Bluetooth kəşfiyyatı və hücumları	2	
6.	Mobil tətbiq statik analiz	2	
7.	Mobil tətbiq dinamik analiz	2	
8.	SMS/SS7 zəifliklərinin laborator sınağı	2	
9.	IDS/IPS konfiqurasiyası	2	
10.	VPN və şifrələmə protokolları	2	
11.	IoT cihazların simsiz təhlükəsizliyi	2	
12.	BYOD və MDM alətlərinin testləşdirilməsi	2	
13.	Mobil ödəniş sınaq mühiti	2	
14.	Cloud/Edge təhlükəsizlik senariləri	2	
15.	Final laboratoriya: Simulyasiya ssenarisi	2	
Cəmi laboratoriya:		**30 s.**	
Fənn üzrə cəmi:		**60 s.**	

XI. Fənn üzrə tələblər:

Fənni bitirən tələbə:mobil və simsiz avadanlıqların təhlükəsizliyini aparma bacarığı qazanmalıdır.Texniki hesabat hazırlaya bilməlidir

Fənnin sonunda tələbələr mobil və simsiz avadanlıqların təhlükəsizliyinin əsas prinsiplərini anlayan, təhlükəsizlik boşluqlarını müəyyən edib qiymətləndirə bilən və informasiya sistemlərinin qorunmasının gücləndirilməsinə töhfə verən ilkin səviyyəli informasiya təhlükəsizliyi mütəxəssisi kimi formalaşmalıdır.

XII.Fənnin tədrisi üçün nəzərdə tutulan tədris və öyrənmə metodları:

Təlim prosesində fərqli tədris metodlarından istifadə edilməlidir. Bu metodlar tələbəyönümlü yanaşmanı və tələbələrin təlim prosesindəki fəal rol oynamasını təşviq etməlidir. İstifadə edilə biləcək tədris və öyrənmə üsullarına aşağıdakıları nümunə olaraq göstərmək olar:

- mühazirələr,
- təcrübi tapşırıqlar:
- təqdimatlar və müzakirələr,
- problemlərə əsaslanan tədris:
- rol oyunlar, hesabatlar:
- qrup qiymətləndirməsi:
- ekspert metodu;
- simulyasiyalar.

XIII. Fənn üzrə təlimin nəticələri:

Fənni bitirən tələbə:mobil və simsiz avadanlıqların təhlükəsizliyini aparma bacarığı qazanır.Texniki hesabat hazırlaya bilir

Fənnin sonunda tələbələr mobil və simsiz avadanlıqların təhlükəsizliyinin əsas prinsiplərini anlayan, təhlükəsizlik boşluqlarını müəyyən edib qiymətləndirə bilən və informasiya sistemlərinin qorunmasının gücləndirilməsinə töhfə verən ilkin səviyyəli informasiya təhlükəsizliyi mütəxəssisi kimi formalaşırlar.

XIV. Tələbələrin fənn haqqında fikrinin öyrənilməsi:

XV. Kollokvium sualları

I Kollokvium sualları
1.Mobil və simsiz mühitin təhlükəsizliyi
2.Mobil və simsiz sistemlərin növləri,
3.Risk mühiti, əsas prinsiplər, tələbələrin gözləntiləri.
4.Şəbəkə modelləri və simsiz protokollar
5.OSI/TCP-IP, Wi-Fi (802.11), Bluetooth-un təhlükəsizlik aspektləri
6.ZigBee, LTE/5G və onların təhlükəsizlik aspektləri.
7.Kriptoqrafiya əsasları
8.Simmetrik/asimmetrik şifrələmə,
9.Hash, digests, açar idarəetməsi.
10.Mobil cihaz təhlükəsizliyi
11.iOS/Android arxitekturası,
12.sandboxing, app icazələri, jailbreak/root riskləri.
13.Simsiz şəbəkələrdə şifrələmə protokolları
14.WEP, WPA/WPA2/WPA3,
15.TKIP, AES-CCMP – müqayisə və zəifliklər

II Kollokvium sualları
16.Autentifikasiya və icazə nəzarəti
17.802.1X, EAP növləri,
18.RADIUS/AAA infrastrukturu.
19.Saldırılar və zəiflik növləri (Simli vs Simsiz)
20.Sniffing, spoofing,
21.DoS, evil-AP, man-in-the-middle.
22.Mobil tətbiq təhlükəsizliyi
23.Təhlükəsiz kodlaşdırma prinsipləri,
24.statik/dinamik analiz giriş.
25.Mobil kommunikasiya hücumları
26.SMS/SS7 zəifliklər,
27.IMSI catcher (Stingray), VoLTE riskləri.
28.Simsiz şəbəkə monitorinqi və təhlükə aşkarlanması
29.IDS/IPS, anomaliya aşkarlanması,
30.Traffic analiz.

XVI. İmtahan sualları:

1.Mobil və simsiz mühitin təhlükəsizliyi
2.Mobil və simsiz sistemlərin növləri,
3.Risk mühiti, əsas prinsiplər, tələbələrin gözləntiləri.
4.Şəbəkə modelləri və simsiz protokollar
5.OSI/TCP-IP, Wi-Fi (802.11), Bluetooth-un təhlükəsizlik aspektləri
6.ZigBee, LTE/5G və onların təhlükəsizlik aspektləri.
7.Kriptoqrafiya əsasları
8.Simmetrik/asimmetrik şifrələmə,
9.Hash, digests, açar idarəetməsi.
10.Mobil cihaz təhlükəsizliyi
11.iOS/Android arxitekturası,
12.sandboxing, app icazələri, jailbreak/root riskləri.
13.Simsiz şəbəkələrdə şifrələmə protokolları
14.WEP, WPA/WPA2/WPA3,

[illegible] AES-CCMP – müqayisə və zəiflik[illegible]
[illegible] Autentifikasiya və kaza nəzarəti
[illegible] 802.1X. EAP növləri.
[illegible] RADIUS/AAA infrastrukturu.
[illegible] Şəbəkələr və zəiflik növləri (Simli və Simsiz)
20. Sniffing, spoofing.
21. DoS, evil-AP, man-in-the-middle.
22. Mobil tətbiq təhlükəsizliyi
23. Təhlükəsiz kodlaşdırma prinsipləri.
24. statik/dinamik analiz giriş.
25. Mobil kommunikasiya hücumları
26. SMS/SS7 zəifliklər,
27. IMSI catcher (Stingray). VoLTE riskləri.
28. Simsiz şəbəkə monitorinqi və təhlükə aşkarlanması
29. IDS/IPS, anomaliya aşkarlanması,
30. Traffic analiz.
31. Kripto analiz və simsiz protokollarda zəifliklər
32. Kripto analizin mexanizmləri,
33. Re-keying problemləri.
34. Mobil Ödəniş Sistemləri və təhlükəsizlik34
35. NFC ödəniş protokolları riskləri
36. Tokenizasiya ödəniş protokolları riskləri.
37. Cloud və Edge inteqrasiyalı mobil təhlükəsizlik
38. Cloud cihaz qorunması.
39. API təhlükəsizlik,
40. Konteynerləşmə
41. Gələcək texnologiyalar & trendlər
42. 5G təhlükəsizlik.
43. 6G təhlükəsizlik.
44. IoT hücum/müdafiə sistemləri.
45. AI-based hücum/müdafiə sistemləri

S.F.Mobil və simsiz avadanlıqların təhlükəsizliyi fənninin sillabusu bakalavr pilləsi üzrə **6006017-İnformasiya** ixtisasının təhsil proqramı, tədris planı və bu fənnin işçi fənn proqramı əsasında tərtib edilmişdir.
Sillabus **"Texnologiya və texniki elmlər "** kafedrasında müzakirə edilərək təsdiq edilmişdir **(07.01.2026-cı il, protokol № 5).**

Fənn müəllimi: dosent, A. A. Dəmirov.

m, T. T. Məlikzadə.

Kafedra müdiri: dosent, R. F. Əliyev