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
Fakültə: Aqrar və mühəndislik
Kafedra: Texnologiya və texniki elmlər

I. Fənn haqqında məlumat:

Fənnin adı: Elektronika və İot cihazlarının təhlükəsizliyi ("Elektronika və İot cihazlarının təhlükəsizliyi" işçi fənn proqramı, Lənkəran Dövlət Universitetinin Texnologiya və texniki elmlər kafedrasının 07.01.2026-cı il 5 №-li protokoluna əsasən)
Kodu: İPF-B21
Tədris ili: III tədris ili, (2025-2026)
Semestr: VI (yaz)
Tədris yükü: 45 (30 saat mühazirə, 15 saat laboratoriya)
Təhsilalma forması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 5 kredit

II. Müəllim haqqında məlumat:

Soyadı, adı, ata adı, elmi dərəcəsi və elmi adı:
Mühazirə müəllimi: Məlikzadə Tural Tofiq oğlu
Laboratoriya müəllimi:Əmənullayev Mahir Qabil oğlu
Kafedranın ünvanı: Lənkəran şəhəri Füzuli 170 a, LDU-nun 1 saylı tədris binası
Məsləhət günləri və saatı:
E-mail ünvanı: tural1996t@gmail.com, zamanliaman@mail.ru

III. Tövsiyə olunan dərslik, dərs vəsaiti və metodik vəsaitlər:

1. Dr. Asif Qanbayev, Rəşad Əliyev, Elektronika və IoT cihazların təhlükəsizliyi fənni üzrə mühazirələr toplusu (Bakı, 2025).
2. Orucəliyev A., Kriptoqrafiyanın əsasları (Bakı, 2019).
3. Prof. Yadigar İmamverdiyev, Kriptoqrafiyanın əsasları (Bakı, 2019).
4. Məmmədov F.H., Orucova M.Y., İnformasiya təhlükəsizliyi və təminatı (Bakı, 2022). əlavə
5. Paar C., Pelzl J., Understanding Cryptography (Springer, 2020).
6. Stallings W., Cryptography and Network Security (9th Ed., 2024).
7. İnternet resursları

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:

Bu kurs çərçivəsində tələbələr ənənəvi kritoqrafiyanın yaranması ve inkişafına dair qısa tarixi, aktuallığını. tətbiq sahələrini və mövcud problemlərini, həmçinin müasir kriptosistemlər və şifrləmə üsulları ilə birlikdə kriptoqrafiyanın informasiya təhlükəsizliyinin hansı prinsiplərini necə təmin etdiyini öyrənirlər. Kursda blok, axın və açıq açarlı şifrləmə

alqoritmaları ilə yanaşı qabaqcıl kriptoqrafik alqoritmlər icmal edilir, bu alqoritmlərin prak... tətbiqləri ilə əlaqəli məlumatlar verilir.

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: 15 saat; **Cəmi: 45 saat.**

№	Tədris olunan mövzuların məzmunu	Saat	Tarix
		Mühazirə	
1.	**Mövzu № 1. IoT Texnologiyasının Əsasları və İnkişafı** Plan 1. Əşyaların İnterneti anlayışı və əsas komponentləri 2. IoT sistemlərinin tarixi təkamül mərhələləri 3. Müasir cəmiyyətdə IoT-nin tətbiq sahələri Mənbə:1,4,7	2	
2.	**Mövzu № 2. IoT Sistemlərinin Memarlıq Qatları** Plan 1. Məlumatların toplandığı sensor (qavrama) qatı 2. Şəbəkə ötürücüləri və məlumat transferi prosesi 3. İstifadəçi tətbiqləri və idarəetmə interfeysləri Mənbə:1,3,5,6	2	
3.	**Mövzu № 3. IoT-də Rabitə Standartları və Protokollar** Plan 1. Cihazlararası ünsiyyəti təmin edən əsas protokollar (MQTT, CoAP) 2. Aşağı enerji istehlakı ilə işləyən şəbəkə texnologiyaları 3. Simsiz sensor şəbəkələrində standartlaşdırmanın rolu Mənbə:1,2,4,6	2	
4.	**Mövzu № 4. IoT Ekosistemində Kibertəhlükəsizlik Riskləri** Plan 1. Cihazlara qarşı yönələn müasir hücum növləri 2. Şəbəkə və tətbiq səviyyəsindəki təhlükəsizlik boşluqları 3. Məlumat sızmalarının qarşısının alınması yolları Mənbə:1,4,5	2	
5.	**Mövzu № 5. Sənaye IoT Sistemlərinin Müdafiəsi** Plan 1. Sənaye sahələrində istifadə olunan IoT həlləri 2. Kritik infrastrukturun təhlükəsizlik arxitekturası 3. IoT sistemlərində risklərin qiymətləndirilməsi Mənbə:1,4,5,6	2	

6.	**Mövzu № 6. Kriptoqrafik Üsullarla Məlumatın Qorunması** Plan 1. IoT cihazlarında tətbiq edilən şifrələmə metodları 2. Cihazların autentifikasiyası (doğrulanması) prosesi 3. Rəqəmsal sertifikatların istifadə qaydaları Mənbə:1,3,7	2	
7.	**Mövzu № 7. Bulud Texnologiyaları və IoT İnteqrasiyası** Plan 1. Məlumatların bulud sistemlərində emalı və analizi 2. Bulud mühitində kiber müdafiə mexanizmləri 3. Amazon AWS və Microsoft Azure IoT təhlükəsizlik həlləri Mənbə:1,3,5,7	2	
8.	**Mövzu № 8. Duman Hesablamaları (Fog Computing) və Üstünlükləri** Plan 1. Duman hesablamalarının IoT şəbəkəsində rolu 2. Kənar emal (Edge computing) ilə gecikmələrin azaldılması 3. Duman qovşaqlarının təhlükəsizlik infrastrukturunun qurulması Mənbə:1,3,4	2	
9.	**Mövzu № 9. Süni İntellektlə Anomaliyaların Aşkarlanması** Plan 1. Təhlükəsizlik monitorinqində maşın öyrənməsinin tətbiqi 2. Zərərli proqramların davranış analizi metodu ilə tapılması 3. Süni intellekt əsaslı avtomatik cavab sistemləri Mənbə:1,3,5,6	2	
10.	**Mövzu № 10. Blokçeyn Texnologiyasının IoT-yə Tətbiqi** Plan 1. Mərkəzləşdirilməmiş şəbəkələrdə məlumat bütövlüyü 2. Ağıllı müqavilələr vasitəsilə təhlükəsiz cihaz idarəetməsi 3. Blokçeyn əsaslı cihaz identifikasiya sistemləri Mənbə:1,5,6,7	2	
11.	**Mövzu № 11. İnsidentlərin İdarə Edilməsi və Bərpa Prosesi** Plan 1. Kiber insidentlərin qeydə alınması və təhlili 2. Hücumdan sonra sistemin bərpası üçün görülən tədbirlər	2	

	3. Müdafiə strategiyalarının təkmilləşdirilməsi Mənbə:1,4,5,6		
12.	**Mövzu № 12. IoT Cihazlarının Aparat Təminatı Səviyyəsində Analizi** Plan 1. Fiziki interfeyslər (UART, JTAG) vasitəsilə cihaza qoşulma 2. Donanım komponentlərinin təhlükəsizlik yoxlaması 3. Cihaz daxili portların bağlanması və qorunması Mənbə:1,2,4,7	2	
13.	**Mövzu № 13. Mikroproqramların (Firmware) Təhlükəsizlik Təhlili** Plan 1. Firmware fayl sisteminin çıxarılması və deşifrə edilməsi 2. Mikroproqramlardakı proqram kodlarının zəiflik analizi 3. Firmware-in təhlükəsiz yenilənməsi (Update) prosesi Mənbə:1,2,3,4	2	
14.	**Mövzu № 14. Praktik Sızma Testləri (Penetration Testing)** Plan 1. IoT cihazları üçün sızma testi metodologiyaları 2. OWASP standartları əsasında təhlükəsizlik yoxlaması 3. Zəifliklərin aşkarlanması üçün istifadə olunan alətlər Mənbə:1,2,3,4	2	
15.	**Mövzu № 15. IoT-də Şəbəkə Trafikinin Analizi və Monitorinq** Plan 1. Şəbəkə paketlərinin ələ keçirilməsi və təhlili (Wireshark) 2. İcazəsiz qoşulmaların və trafik sıçrayışlarının izlənilməsi 3. DoS və digər şəbəkə hücumlarının simulyasiyası Mənbə:1,4,7	2	
Cəmi		**30 saat**	

№	Tədris olunan mövzuların məzmunu	Saat Laboratoriya	Tarix
1.	**Mövzu № 1.** IoT-nin əsas komponentləri və memarlıq qatlarının analizi	**2**	
2.	**Mövzu № 2.** IoT protokolları və kibertəhlükəsizlik risklərinin simulyasiyası	**2**	
3.	**Mövzu № 3.** Sənaye IoT sistemlərində kriptoqrafik məlumat mühafizəsi	**2**	
4.	**Mövzu № 4.** Bulud və Duman (Fog) hesablamalarında təhlükəsizlik arxitekturası	**2**	

5.	**Mövzu № 5.** Süni intellekt və Blokçeyn əsaslı anomaliya aşkarlama sistemləri	2	
6.	**Mövzu № 6.** İnsidentlərin idarə edilməsi və aparat (Hardware) səviyyəsində analiz	2	
7.	**Mövzu № 7.** Mikroproqramların (Firmware) təhlükəsizlik analizi və sızma testləri	2	
8.	**Mövzu № 8.** Şəbəkə trafikinin monitorinqi və hücum simulyasiyası	1	
Cəmi		**15 saat**	
	Fənn üzrə cəmi	**45**	

XI. Fənn üzrə tələblər:

- Kriptoqrafik Sistemlərin Fərqləndirilməsi: Tələbə klassik və müasir kriptoqrafiyanı, həmçinin simmetrik və asimmetrik şifrləmə sistemlərini bir-birindən fərqləndirməyi bacarmalıdır.
- İnformasiya Təhlükəsizliyi Prinsipləri: Konfidensiallıq, tamlıq, autentifikasiya və inkar edilməməninin kriptoqrafik üsullarla necə təmin olunduğunu dərindən bilməlidir.
- Şifrləmə Alqoritmləri üzrə Biliklər: Blok və axın şifrlərini, onların əsas alqoritmlərini və praktiki tətbiq sahələrini tanımalıdır.
- Açıq Açarlı İnfrastruktur (PKI): Açıq açarlı alqoritmlər və PKI (Public Key Infrastructure) haqqında fundamental biliklərə malik olmalıdır.
- Heş Funksiyaları və Rəqəmsal İmza: Heş funksiyalarının informasiya təhlükəsizliyindəki rolunu və rəqəmsal imzalarda istifadə olunma əhəmiyyətini başa düşməlidir.
- Protokollar barədə Anlayış: Qabaqcıl kriptoqrafik protokolların tətbiq sahələri barədə ümumi anlayışa sahib olmalıdır.

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 təlim nəticələri:

FTN 1 - Əsas elektronika komponentlərini – məntiqi sxemləri, çeviriciləri, rezistor, kondensator, tranzistor, induktiv sarğılar, diodları tanıyır, onlardan istifadə edərək dövrələr qurmağı bacarır.

FTN 2 - Elektronika dövrələrində müşahidə və sınaqlar etmək üçün simulyasiya proqramından istifadə etməyi bacarır.

FTN 3 - Elektrik dövrələrinin əsas kəmiyyətlərini ölçmək üçün ölçmə alətlərindən istifadə edə bilərsiniz.
FTN 4 - Qurğular arasında məlumat mübadiləsi üçün fərqli protokollarla tanış olmalıdır.
FTN 5 - Qurğular arasında simsiz rabitə üçün fərqli texnologiyalar barədə məlumatlı olmalıdır.
FTN 6 - IoT qurğularla bağlı informasiya təhlükəsizliyi məsələlərini öyrənməli, onlara qarşı mümkün kiber-hücumları və hücumlardan müdafiə üsullarını bilməlidir.

XIV. Tələbələrin fənn haqqında fikrinin öyrənilməsi:

XV. Kollokvium sualları:

I. Kollokvium sualları

1. Əşyaların İnterneti anlayışı və əsas komponentləri
2. IoT sistemlərinin tarixi təkamül mərhələləri
3. Müasir cəmiyyətdə IoT-nin tətbiq sahələri
4. Məlumatların toplandığı sensor (qavrama) qatı
5. Şəbəkə ötürücüləri və məlumat transferi prosesi
6. İstifadəçi tətbiqləri və idarəetmə interfeysləri
7. Cihazlararası ünsiyyəti təmin edən əsas protokollar (MQTT, CoAP)
8. Aşağı enerji istehlakı ilə işləyən şəbəkə texnologiyaları
9. Cihazlara qarşı yönələn müasir hücum növləri
10. Məlumat sızmalarının qarşısının alınması yolları

II. Kollokvium sualları

1. Sənaye sahələrində istifadə olunan IoT həlləri
2. Kritik infrastrukturun təhlükəsizlik arxitekturası
3. IoT sistemlərində risklərin qiymətləndirilməsi
4. IoT cihazlarında tətbiq edilən şifrələmə metodları
5. Cihazların autentifikasiyası (doğrulanması) prosesi
6. Məlumatların bulud sistemlərində emalı və analizi
7. Amazon AWS və Microsoft Azure IoT təhlükəsizlik həlləri
8. Duman hesablamalarının IoT şəbəkəsində rolu
9. Kənar emal (Edge computing) ilə gecikmələrin azaldılması
10. Təhlükəsizlik monitorinqində maşın öyrənməsinin tətbiqi

XVI. İmtahan sualları:

1. Əşyaların İnterneti anlayışı və əsas komponentləri
2. IoT sistemlərinin tarixi təkamül mərhələləri
3. Müasir cəmiyyətdə IoT-nin tətbiq sahələri
4. Məlumatların toplandığı sensor (qavrama) qatı
5. Şəbəkə ötürücüləri və məlumat transferi prosesi
6. İstifadəçi tətbiqləri və idarəetmə interfeysləri

7. Cihazlararası ünsiyyəti təmin edən əsas protokollar (MQTT, CoAP)
8. Aşağı enerji istehlakı ilə işləyən şəbəkə texnologiyaları
9. Cihazlara qarşı yönələn müasir hücum növləri
10. Məlumat sızmalarının qarşısının alınması yolları
11. Sənaye sahələrində istifadə olunan IoT həlləri
12. Kritik infrastrukturun təhlükəsizlik arxitekturası
13. IoT sistemlərində risklərin qiymətləndirilməsi
14. IoT cihazlarında tətbiq edilən şifrələmə metodları
15. Cihazların autentifikasiyası (doğrulanması) prosesi
16. Məlumatların bulud sistemlərində emalı və analizi
17. Amazon AWS və Microsoft Azure IoT təhlükəsizlik həlləri
18. Duman hesablamalarının IoT şəbəkəsində rolu
19. Kənar emal (Edge computing) ilə gecikmələrin azaldılması
20. Təhlükəsizlik monitorinqində maşın öyrənməsinin tətbiqi
21. Zərərli proqramların davranış analizi metodu ilə tapılması
22. Süni intellekt əsaslı avtomatik cavab sistemləri
23. Mərkəzləşdirilməmiş şəbəkələrdə məlumat bütövlüyü
24. Ağıllı müqavilələr vasitəsilə təhlükəsiz cihaz idarəetməsi
25. Blokçeyn əsaslı cihaz identifikasiya sistemləri
26. Kiber insidentlərin qeydə alınması və təhlili
27. Hücumdan sonra sistemin bərpası üçün görülən tədbirlər
28. Müdafiə strategiyalarının təkmilləşdirilməsi
29. Fiziki interfeyslər (UART, JTAG) vasitəsilə cihaza qoşulma
30. Donanım komponentlərinin təhlükəsizlik yoxlaması
31. Cihaz daxili portların bağlanması və qorunması
32. Firmware fayl sisteminin çıxarılması və deşifrə edilməsi
33. Mikroproqramlardakı proqram kodlarının zəiflik analizi
34. Firmware-in təhlükəsiz yenilənməsi (Update) prosesi
35. IoT cihazları üçün sızma testi metodologiyaları
36. OWASP standartları əsasında təhlükəsizlik yoxlaması
37. Zəifliklərin aşkarlanması üçün istifadə olunan alətlər
38. Şəbəkə paketlərinin ələ keçirilməsi və təhlili (Wireshark)
39. İcazəsiz qoşulmaların və trafik sıçrayışlarının izlənilməsi
40. DoS və digər şəbəkə hücumlarının simulyasiyası

"Elektronika və İot cihazlarının təhlükəsizliyi fənninin sillabusu **6006017 - "İnformasiya təhlükəsizliyi"** ixtisasının təhsil proqramı, tədris planı və 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: **Tural Məlikzadə, Əmənullayev Mahir**

Kafedra müdiri: **Dos Rəşad Əliyev**