Azərbaycan Respublikası Elm və Təhsil Nazirliyi
Lənkəran Dövlət Universiteti

«Təsdiq edirəm»
Tədris məsələləri
üzrə prorektor vəzifəsini icra edən
dos Z.İ.Məmmədov:

"12" sentyabr 2025-ci il

Fənn sillabusu

Fakültə: Aqrar və mühəndislik
İxtisas: 050615- İnformasiya təhlükəsizliyi
Kafedra: Texnologiya və texniki elmlər
I.Fənn haqqında məlumat:
Fənnin adı: İnformasiyanın təhlükəsizliyinin əsasları
Kodu: İPF-B02
Tədris ili: I (2025-2026), I semestr
Tədris yükü: Cəmi: 60 saat (30 saat mühazirə, 30 saat seminar)
Tədris forması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 6 kredit
II.Müəllim haqqında məlumat:
Adı, soyadı, elmi dərəcəsi: m. Məlikzadə Tural Tofiq oğlu
Məsləhət saatı: I – gün saat 10^{30} -11^{30}- da.
Kafedranın ünvanı: Lənkəran ş. Füzuli 170 a
E-mail ünvanı: tural1996t@gmail.com
III.Tövsiyyə olunan dərsliklər və dərs vəsaitləri:

Əsas

1. "İnformasiya təhlükəsizliyi" Dərslik Əlizadə M. N., Bayramov H. M., Məmmədov Ə. S., Bakı-2016
2. Namazov F.H. "İnformasiya sistemlərində təhlükəsizliyin təmini" Bakı. 2015.
3. İbrahimzadə T.İ. "İnformatika sistemlərində təhlükəsizliyin təmini" Bakı, Elm, 2012.
4. Сырецкий Г.А. Информатика. Фундаменталный курс. "Основы информационной и вычеслительной техники" БХВ-Петербург, 2005

Əlavə

5. "İnformatika" Dərslik, S. Q. Kərimov, S. B. Həbibullayev, T. İ. İbrahimzadə, Bakı 2011

IV. Prerekrevizitlər: Bu gün informasiya cəmiyyətinə kecid şəraitində Azərbaycan təhsil sisteminin qarşısında duran ən əsas vəzifələrdən biri kimi innovasiya texnologiyalarını dərindən bilən, onları öz işinə tətbiq etməyi bacaran və yeni iqtisadi münasibətlər şəraitində əmək bazarının tələblərini ödəyə biləcək mürəkkəb iqtisadi münasibətlər şəraitində rəqabətə davamlı kadrların – şəxsiyyətlərin yetişdirilməsidir.

V.Korekreviztilər: Müstəqil və qrup şəklində fəaliyyət göstərmək bacarıqlarına yiyələnmək; Zəruri informasiyanı axtarıb tapmaq və ondan sistemləşdirilmiş formada istifadə etmək və qorumaq

VI.Fənnin təsviri və məqsədi: İnformasiya sistemlərinin təhlükəsizliyinin təminatında kriptoqrafiyası və rabitə kanallarının tətbiqi, informasiyanın məxfiçiliyinin və qorunmasının yüksək keyfiyyətlə həyata keçirilməsinə yönəlmişdir. Simmetrik və assimetrik şifrəlmənin müxtəlif üsulları, müasir alqoritmləri, informasiya sisteminin təhlükəsizliyini təmin edilməsində əsas vasitədir; elektron rəqəmsal imza.
Fənin tədrisində əsas məqsəd tələbələrə informasiya və kompüter sistemlərində informasiya təhlükəsizliyinin səviyyələrini, beynəlxalq standartlarını, qanun vericilik tədbirlərini, texniki mühafizəsinin təşkilini, Kriptoqrafiyanın əsas prinsiplərini, simmetrik və assimetrik şifrələmə üsullarını öyrətməkdən ibarətdir.

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 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 keçilmiş material dərindən başa düşür, cavabı dəqiq və hərtərəflidir;
-9 bal - tələbə keçilmiş material tam başa düşür, cavabı dəqiqdir və mövzunun mətnini tam açabilir;
-8 bal - tələbə cavabında ümumi xarakterli bəzi qüsurlara yol verir;
-7 bal - tələbə keçilmiş material başadüşür, lakin nəzəri cəhətdən bəzi məsələləri əsaslandıra bilmir;
-6 bal - tələbənin cavabıəsasəndüzgündür;
-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 - tələbəninmövzudanqismənxəbəri var;
-0 bal - suala 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 nəticəsinə görə yekun qiymətləndirmə (imtahan və imtahanaqədərki ballar əsasında)***

91-100 bal - əla (A)
81-90 bal - çox yaxşı (B)
71-80 bal - yaxşı (C)

61-70 bal - kafi (D)

51-60 bal – qənaətbəxş (E)

51-baldan aşağı - qeyri-kafi (F)

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.

Mühazirə mövzuları			
S/s	**Mövzunun adı və məzmunu**	**Saat**	**Tarix**
1.	**İnformasiyanın təhlükəsizliyi fənninə giriş** Plan: 1. İnformasiya mühafizəsi və konfidensiallığı; 2. İnformasiya tamlığının və əlçatanlığının təmin edilməsi; 3. İnformasiya təhlükəsi anlayışı.	2	
2.	**İnformasiya təhlükələrinin təsnifatı** Plan: 1. Təhlükələrin siyahısı; 2. Sistemin sıradan çıxması halları; 3. İnformasiyanın azalma kanalları.	2	
3.	**Pozucunun qeyri-formal modeli** Plan: 1. Pozucunun modeli; 2. Pozucunun modelinin fərziyyələri.	2	
4.	**Təhlükəsizlik hədələrinə qarşı tədbirlər** Plan: 1. Qanunvericilik müdafiə tədbirləri; 2. İnzibati müdafiə tədbirləri; 3. Prosedur və proqram texniki müdafiə tədbirləri.	2	
5.	**İnformasiya təhlükəsizliyinin məsələləri, kriteriləri və prinsipləri** Plan: 1. İnformasiya təhlükəsizliyi sistemlərinin məsələləri; 2. İnformasiya texnologiyalarının təhlükəsizliyinin qiymətləndirilməsinin ümumi kriteriləri; 3. Avtomatlaşdırılmış informasiya sistemlərinin müdafiə sisteminin qurulmasının əsas prinsipləri.	2	
6.	**Təhlükəsizlik modelləri** Plan: 1. Təhlükəsizlik modelinin təyinatı və anlayışı; 2. Diskresion əlçatanlıq modeli.	2	
7.	**Bella-Lapadula və Əlçatanlığa nəzarətin rol modelləri** Plan: 1. Bella-Lapadula təhlükəsizlik modelinin təsviri; 2. Bella-Lapadula təhlükəsizlik modelinin tətbiqi; 3. Əlçatanlığa nəzarətin rol modelinin təsviri (RBAC).	2	
8	**Əlçatanlığa nəzarətin rol modelinin üstünlükləri və hədd qoyma sistemləri** Plan: 1. Əlçatanlığa nəzarətin rol modelinin üstünlükləri; 2. Əlçatanlığa hədd qoyma sistemləri;	2	

	3. Əlçatanlıq matrisi.		
9	**Kriptoqrafiya** Plan: 1. Kriptoqrafiyanın əsas anlayışları; 2. Kriptoqrafiyanın bölmələri.	2	
10.	**Şifrələmə** Plan: 1. Şifrələmə anlayışı; 2. Simmetrik şifrələmə; 3. Sezar şifri.	2	
11.	**Şifrələmə üsulları** Plan: 1. Çoxəlifbalı şifr; 2. Qronsfeld şifrəsi; 3. Sezar və Qronsfeld şifrələmə üsullarının çatışmazlıqları.	2	
12.	**Çoxhərfli şifrələmə** Plan: 1. Pleyfeyer şifrələnməsi; 2. Hill şifri.	2	
13.	**Müasir simmetrik şifrələmə alqoritmləri** Plan: 1. DES alqoritmi; 2. AES alqoritmi; 3. Simmetrik alqoritmlərin problemləri.	2	
14.	**Açıq açarla şifrələmə** Plan: 1. Açıq açarla şifrələmə alqoritmi; 2. Açıq açarla şifrələmə alqoritminin şərtləri; 3. RSA alqoritmi.	2	
15.	**Elektron rəqəmsal imza** Plan: 1. Rəqəmsal imzanın yaranması; 2. Elektron imza.	2	
Cəmi:		**30**	

Seminar mövzuları

S/s	Mövzunun adı	Saat	Tarix
1.	**İnformasiyanın təhlükəsizliyi fənninə giriş**	2	
2.	**İnformasiya təhlükələrinin təsnifatı**	2	
3.	**Pozucunun qeyri-formal modeli**	2	
4.	**Təhlükəsizlik hədələrinə qarşı tədbirlər**	2	
5.	**İnformasiya təhlükəsizliyinin məsələləri, kriteriləri və prinsipləri**	2	
6	**Təhlükəsizlik modelləri**	2	
7.	**Bella-Lapadula və Əlçatanlığa nəzarətin rol modelləri**	2	
8.	**Əlçatanlığa nəzarətin rol modelinin üstünlükləri və hədd qoyma sistemləri**	2	
9.	**Kriptoqrafiya**	2	
10.	**Şifrələmə**	2	
11.	**Şifrələmə üsulları**	2	

12.	**Çoxhərfli şifrələmə**	2	
13.	**Müasir simmetrik şifrələmə alqoritmləri**	2	
14.	**Açıq açarla şifrələmə**	2	
15.	**Elektron rəqəmsal imza**	2	
Cəmi:		**30**	

XI. Fənn üzrə tələblər, tapşırıqlar:

- İnformasiya texnologiyalarının fənn ilə əlaqələndirmək;
- İnformasiya komunikasiya texnologiyalarından istifadə edərək informatika dərsində bilik və bacarıqlara yiyələnmək.
- İnformasiya mühafizəsi

XII. Fənn üzrə təlimin nəticələri

- İnformasiya mühafizəsi
- Tətbiqi informasiya sistemlərinin qurulması prinsiplərini mənimsəmək
- Çoxtəyinatlı informasiyaların emalı üçün müasir proqram təminatından istifadə etməyi bacarmaq
- Texnologiyalarının təhlükəsizlyinin müasir vəziyyətlərini və inkişaf tendensiyalarını bilməlidirlər.

XIII. Tələbələrin fənn haqqında fikrinin öyrənilməsi:

XIV. Fənnin kollokvium sualları:

Birinci kollekvum sualları.

1. İnformasiya mühafizəsi və konfidensiallığı;
2. İnformasiya tamlığının və əlçatanlığının təmin edilməsi;
3. İnformasiya təhlükəsi anlayışı;
4. Təhlükələrin siyahısı;
5. Sistemin sıradan çıxması halları;
6. İnformasiyanın azalma kanalları;
7. Pozucunun modeli;
8. Pozucunun modelinin fərziyyələri;
9. Təhlükəsizlik hədələrinə qarşı tədbirlər
10. Qanunvericilik müdafiə tədbirləri;
11. İnzibati müdafiə tədbirləri;

12. Prosedur və proqram texniki müdafiə tədbirləri;
13. İnformasiya təhlükəsizliyi sistemlərinin məsələləri;
14. İnformasiya texnologiyalarının təhlükəsizliyinin qiymətləndirilməsinin ümumi kriteriləri;
15. Avtomatlaşdırılmış informasiya sistemlərinin müdafiə sisteminin qurulmasının əsas prinsipləri;

İkinci kollekvum sualları

1. Təhlükəsizlik modelinin təyinatı və anlayışı;
2. Diskresion alçatanlıq modeli;
3. Bella-Lapadula təhlükəsizlik modelinin təsviri;
4. Bella-Lapadula təhlükəsizlik modelinin tətbiqi;
5. Əlçatanlığıa nəzarətin rol modelinin təsviri (RBAC);
6. Əlçatanlığa nəzarətin rol modelinin üstünlükləri;
7. Əlçatanlığa hədd qoyma sistemləri;
8. Əlçatanlıq matrisi;
9. Kriptoqrafiyanın əsas anlayışları;
10. Kriptoqrafiyanın bölmələri;
11. Şifrələmə anlayışı;
12. Simmetrik şifrələmə;
13. Sezar şifri;
14. Çoxəlifbalı şifr;
15. Qronsfeld şifrəsi;

XV. Fənnin imtahan sualları:

I blok

1. İnformasiya mühafizəsi və konfidensiallığı;
2. İnformasiya tamlığının və əlçatanlığının təmin edilməsi;
3. İnformasiya təhlükəsi anlayışı;
4. Təhlükələrin siyahısı;
5. Sistemin sıradan çıxması halları;
6. İnformasiyanın azalma kanalları;
7. Pozucunun modeli;
8. Pozucunun modelinin fərziyyələri;

II blok

9. Qanunvericilik müdafiə tədbirləri;
10. İnzibati müdafiə tədbirləri;
11. Prosedur və proqram texniki müdafiə tədbirləri;

12. İnformasiya təhlükəsizliyi sistemlərinin məsələləri;
13. İnformasiya texnologiyalarının təhlükəsizliyinin qiymətləndirilməsinin ümumi kriteriləri;
14. Avtomatlaşdırılmış informasiya sistemlərinin müdafiə sisteminin qurulmasının əsas prinsipləri;
15. Təhlükəsizlik modelinin təyinatı və anlayışı;
16. Diskresion alçatanlıq modeli;

III blok

17. Bella-Lapadula təhlükəsizlik modelinin təsviri;
18. Bella-Lapadula təhlükəsizlik modelinin tətbiqi;
19. Əlçatanlığa nəzarətin rol modelinin təsviri (RBAC);
20. Əlçatanlığa nəzarətin rol modelinin üstünlükləri;
21. Əlçatanlığa həd qoyma sistemləri;
22. Əlçatanlıq matrisi;

IV blok

23. Kriptoqrafiyanın əsas anlayışları;
24. Kriptoqrafiyanın bölmələri;
25. Şifrələmə anlayışı;
26. Simmetrik şifrələmə;
27. Sezar şifri;
28. Çoxəlifbalı şifr;
29. Qronsfeld şifrəsi;
30. Sezar və Qronsfeld şifrələmə üsullarının çatışmazlıqları;
31. Pleyfeyer şifrələnməsi;
32. Hill şifri;

V blok

33. DES alqoritmi;
34. AES alqoritmi;
35. Simmetrik alqoritmlərin problemləri;
36. Açıq açarla şifrələmə alqoritmi;
37. Açıq açarla şifrələmə alqoritminin şərtləri;
38. RSA alqoritmi;
39. Rəqəmsal imzanın yaranması;
40. Elektron imza.

Fənnin sillabusu 050615 – "İnformasiya təhlükəsizliyi" ixtisasının tədris planı və fənn proqramı əsasında tərtib edilmişdir.

Sillabus "Texnologiya və texniki elmlər" kafedrasında müzakirə edilərək, təsdiq edilmişdir (12 sentyabr 2025-cü il, protokol № 01).

Kafedra müdiri: **dos. R. Əliyev**

Fənn müəllimi: **m. T. T. Məlikzadə, A.Ələskərzadə.**