

**AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ
LƏNKƏRAN DÖVLƏT UNİVERSİTETİ**

“Təsdiq edirəm”
Tədris məsələləri üzrə prorektor
vəzifəsini icra edən:
 dos.Z.I.Məmmədov
12 sentyabr 2025-ci il

Fənn sillabusu

Fakültə: Aqrar və mühəndislik

İxtisas : 060631- Kompüter sistemləri və şəbəkələri

Kafedra: Texnologiya və texniki elmlər

I.Fənn haqqında məlumat:

Fənnin adı: İnformasiyanın təhlükəsizliyi

Kodu: MISF-B051

Tədris ili: II (2025-2026), III semestr

Tədris yükü: Cəmi: 30 saat (15 saat müəhazirə, 15 saat laboratoriya)

Tədris forması: Əyani

Tədris dili: Azərbaycan dili

AKTS üzrə kredit: 5 kredit

II.Müəllim haqqında məlumat:

Vəzifəsi, adı, atasının adı, soyadı: tex.ü.f.d.,dosent, Muradova Vüsalə Xudaşirin qızı

Məsləhət saati: II gün saat 12⁰⁰ – 13⁰⁰

Kafedranın ünvanı: Lənkəran ş. Füzuli 170 a

E-mail ünvanı: vusala.muradoav@lsu.edu.az

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.

Əlavə

4. Сырецкий Г.А. Информатика. Фундаментальный курс. “Основы информационной и вычислительной техники” БХВ-Петербург, 2005
5. “İnformatika” Dərslik, S. Q. Kərimov, S. B. Həbibullayev, T. İ. İbrahimzadə, Bakı 2011

IV.Prekrivizitlər: “İnformasiya təhlükəsizliyi” fənni üzrə təhsil alan bakalavrlara, kibertəhlükəsizlikdə hücumlar, təhdidlər və zəifliklərin öyrənilməsi, təhlükəsiz şəbəkənin arxitekturası, dizaynı, insidentlərə cavab tədbirləri, kibertəhlükəsizlik risklərinin idarə edilməsinin metodları və vasitələrinin öyrənilməsi və istehsalatla əlaqələndirilməsi nəzərdə tutulmuşdur.

V.Korekvizitlər: İnformasiya təhlükəsizliyinin əsas anlayışları, kompüter sistemlərində və şəbəkələrində informasiya hədələri haqqında məlumat, onların təhlil

51
51-
IX. L
qaydalarını

edilməsi tutarlı səviyyədə verilir. Təhlükəsizlik siyasətinin baza anlayış müəyyənləşdirilir. Kriptografik üsullarla yanaşı kompüter informasiyasının müdafiə alqoritminə baxılır.

VI. Fənnin təsviri və məqsədi: Informasiya sistemlərinin təhlükəsizliyinin təminatında kriptografiyası və rabitə kanallarının tətbiqi, informasiyanın məxfiliyyətinin və qorunmasının yüksək keyfiyyətlə həyata keçirilməsinə yönəlmişdir. Simmetrik və assimetrik şifrələmənin 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, Kriptografiyanın 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 buraxılır, 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 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 dərinədən başa düşür, cavabı dəqiq və hərtərəflidir;
- 9 bal - tələbə keçilmiş material tam başa düşür, cavabı dəqiqdir və mövzunun mətnini tam əhatə edir;
- 8 bal - tələbə cavabında ümumi xarakterli bəzi qüsurlara yol verir;
- 7 bal - tələbə keçilmiş material başadüşür, lakin nəzəri cəhətdən bəzi məsələləri əsaslandırma 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 əsaslandırma bilmir;
- 1-2 bal - tələbənin mövzudan qismən xəbəri 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 imtahana qədərki 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 görülməkdir.

X. Təqvim mövzu planı: Mühazirə – 15 saat, seminar – 15 saat, Cəmi 30 – saat.

S/ s	Mühazirə mövzuları		
	Mövzunun adı və məzmunu	Saat	Tarix
1.	İnformasiyanın təhlükəsizliyi fənninə giriş. İnformasiya təhlükələrinin təsnifatı Plan: 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.	2	
2.	Pozucunun qeyri-formal modeli. Təhlükəsizlik hədələrinə qarşı tədbirlər Plan: 1. Pozucunun modeli; 2. Pozucunun modelinin fərziyyələri. 3. Qanunvericilik müdafiə tədbirləri; 4. İnzibati müdafiə tədbirləri; 5. Prosedur və program texniki müdafiə tədbirləri.	2	
3.	Təhlükəsizlik modelləri. Bella-Lapadula və Əlçatanlığa nəzarətin rol modelləri Plan: 1. Təhlükəsizlik modelinin təyinatı və anlayışı; 2. Diskresion əlçatanlıq modeli. 3. Bella-Lapadula təhlükəsizlik modelinin təsviri; 4. Bella-Lapadula təhlükəsizlik modelinin tətbiqi; 5. Əlçatanlığa nəzarətin rol modelinin təsviri (RBAC).	2	
4.	Əlçatanlığa nəzarətin rol modelinin üstünlükləri və hədd qoyma sistemləri Plan: 1. Əlçatanlığa nəzarətin rol modelinin üstünlükləri; 2. Əlçatanlığa hədd qoyma sistemləri; 3. Əlçatanlıq matrisi.	2	
5.	Kriptoqrafiya və Şifrələmə üsulları. Çoxhərflə şifrələmə Plan: 1. Kriptoqrafiyanın əsas anlayışları; 2. Kriptoqrafiyanın bölmələri. 3. Şifrələmə anlayışı; 4. Simmetrik şifrələmə 5. Çoxəlifbəli şifrə; 6. Qronsfeld şifrəsi; 7. Sezar və Qronsfeld şifrələmə üsullarının çatışmazlıqları. 8. Pleyfeyer şifrələnməsi; 9. Hill şifri.	2	
6.	Müasir simmetrik şifrələmə alqoritmləri. Açıq açarlar şifrələmə	2	

	Plan: 1. DES alqoritmi; AES alqoritmi; 2. Simmetrik alqoritmlərin problemləri. 3. Açıq açarla şifrələmə alqoritmi; 4. Açıq açarla şifrələmə alqoritminin şərtləri; RSA alqoritmi		
7.	Parolun köməyi ilə müdafiə. Kompüter virusları və onlarla mübarizə Plan: 1. Parola hücum üsulları. Parolun təhlükəsizliyinin təmini 2. Ümumi əlçatan yerlərdə saxlanılan parolların toplanması 3. Sosial injirinq və fişinq 4. Kompüter viruslarının təsnifatı və meydana gəlməsinin qısa tarixi 5. Polimorfizm – virusların mutasiyası və təhlükəsizliyə qarşı virus hədələrinin tipləri 6. Antivirus proqramlarının yaradılması, inkişafı və viruslarla mübarizə	2	
8.	Şəbəkələrin informasiya təhlükəsizliyi problemləri. Əməliyyat sisteminin təhlükəsizliyinin təmini Plan: 1. Şəbəkənin informasiya təhlükəsizliyinin təmin edilməsi 2. Informasiya təhlükəsizliyinin təmin edilmə üsulları 3. Əməliyyat sisteminin təhlükəsizliyinin təmin edilməsi problemləri 4. Əməliyyat sisteminin təhlükəsizliyinə hədələr və müdafiə olunma anlayışı	1	
Cəmi:		15	
Laboratoriya işləri mövzuları			
S/ s	Mövzunun adı	Saa t	Tarix
1.	Nmap ilə şəbəkə analizi	2	
2.	Wireshark analizatoru ilə paketlərin izlənməsi	2	
3.	Windows parollarının sındırılması	2	
4.	Burp Suite ilə "Session Hijacking" hücumunun yerinə yetirilməsi	2	
5.	Aircrack-ng ilə Wi-Fi parollarının tapılması	2	
6.	Kriptografiya. Şifrələmə. Şifrələmə üsulları. Çoxhərflə şifrələmə	2	
7.	Müasir simmetrik şifrələmə alqoritmləri. Açıq açarla şifrələmə	2	
8.	Parolun köməyi ilə müdafiə	2	
Cəmi:		15	

XI. Fənn üzrə tələblər, tapşırıqlar:

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

"İnformasiya təhlükəsizliyi" fənninin tədrisi zamanı tələbələrə kompüterin strukturuna aid olan müxtəlif bölmələrinin və praktik tətbiqini öyrədilməsi fənn üzrə qoyulan əsas tələblərdən biridir: "İnformasiya təhlükəsizliyi" fənninin tədrisi zamanı qoyulan tələblər aşağıdakı kimidir:

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

- İnformasiya texnologiyalarının fənn ilə əlaqələndirmək;
- İnformasiya kommunikasiya texnologiyalarından istifadə edərək informatika dərində bilik və bacarıqlara yiyələnmək.

XII. Təlimin nəticələri

“İnformasiya təhlükəsizliyi” ixtisası üzrə təhsil alan məqistrlara əsas kibertəhlükəsizlik konsepsiyaları, kibertəhlükəsizlikdə hücumlar, təhdidlər və boşluqların öyrənilməsi, informasiya tamlığının və əlçatanlığının təmin edilməsi, qanunvericilik müdafiə tədbirləri, təhlükəsizlik modelinin tətbiqi, kriptografiyanın əsas anlayışları, rəqəmsal imzanın yaranması, elektron imza, təhlükəsiz şəbəkənin qurulması üzrə lazımi biliklərin verilməsini təmin etmək və praktika ilə əlaqələndirilməsini nəzərdə tutur. Fənnin mənimsənilməsi, tələbələrin müstəqil tədqiqat və təcrübəyə əsaslanan təcrübəyə nail olmasına nail olur. Bu fənn, gələcəkdə informasiya təhlükələrinin qarşısını almağa nail olan nəzəri və təcrübi bilikləri təmin edir.

XIII. Tələbələrin fənn haqqında fikrin öyrənilməsi:

XIV. Birinci kollektivium 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. Qanunvericilik müdafiə tədbirləri;
10. İnzibati müdafiə tədbirləri;

XV. İkinci kollektivium sualları

1. Prosedur və proqram texniki müdafiə tədbirləri;
2. İnformasiya təhlükəsizliyi sistemlərinin məsələləri;
3. İnformasiya texnologiyalarının təhlükəsizliyinin qiymətləndirilməsinin ümumi kriteriləri;
4. Avtomatlaşdırılmış informasiya sistemlərinin müdafiə sisteminin qurulmasının əsas prinsipləri;
5. Təhlükəsizlik modelinin təyinatı və anlayışı;
6. Diskresion əlçatanlıq modeli;
7. Bella-Lapadula təhlükəsizlik modelinin təsviri;
8. Bella-Lapadula təhlükəsizlik modelinin tətbiqi;
9. Əlçatanlığa nəzarətin rol modelinin təsviri (RBAC);
10. Əlçatanlığa nəzarətin rol modelinin üstünlükləri;

XVI. Fənnin imtahan sualları:

I ci blok

1. İnformasiya mühafizəsi və konfidensiallığı;

2. İnformasiya təhlükəsizliyinin 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 ci blok

1. Qanunvericilik müdafiə tədbirləri;
2. İnzibati müdafiə tədbirləri;
3. Prosedur və proqram texniki müdafiə tədbirləri
4. Təhlükəsizlik modelinin təyinatı və anlayışı;
5. Diskresion əlçatanlıq modeli.
6. Bella-Lapadula təhlükəsizlik modelinin təsviri;
7. Bella-Lapadula təhlükəsizlik modelinin tətbiqi;
8. Əlçatanlığa nəzarətin rol modelinin təsviri (RBAC).

III ci blok

1. Əlçatanlığa nəzarətin rol modelinin üstünlükləri;
2. Əlçatanlığa hədd qoyma sistemləri;
3. Əlçatanlıq matrisi.
4. Kriptografiyanın əsas anlayışları;
5. Kriptografiyanın bölmələri.
6. Şifrələmə anlayışı;
7. Simmetrik şifrələmə
8. Çoxəlifbəli şifr;

VI ci blok

1. Qronsfeld şifrəsi;
2. Sezar və Qronsfeld şifrələmə üsullarının çatışmazlıqları.
3. Pleyfeyer şifrələnməsi;
4. Hill şifri.
5. DES alqoritmi; AES alqoritmi;
6. Simmetrik alqoritmlərin problemləri.
7. Açıq açarla şifrələmə alqoritmi;
8. Açıq açarla şifrələmə alqoritminin şərtləri; RSA alqoritmi
9. Parola hücum üsulları. Parolun təhlükəsizliyinin təmini

V ci Blok

1. Ümumi əlçatan yerlərdə saxlanılan parolların toplanması
2. Sosial injiring və fişinq
3. Kompüter viruslarının təsnifatı və meydana gəlməsinin qısa tarixi
4. Polimorfizm – virusların mutasiyası və təhlükəsizliyə qarşı virus hədələrinin tipləri
5. Antivirus proqramlarının yaradılması, inkişafı və viruslarla mübarizə
6. Şəbəkənin informasiya təhlükəsizliyinin təmin edilməsi
7. İnformasiya təhlükəsizliyinin təmin edilmə üsulları
8. Əməliyyat sisteminin təhlükəsizliyinin təmin edilməsi problemləri
9. Əməliyyat sisteminin təhlükəsizliyinə hədələr və müdafiə olunma anlayışı

Fənnin sillabusu : **060632** informasiya texnologiyaları və sistem mühəndisliyi
ixtisasının tədris planı və fənn proqramı əsasında tərtib edilmişdir.

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

Fənn müəllimi:



dos. V.X. Muradova

Kafedra müdiri:



dos. R.F. Əliyev