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

Fənn sillabusu

Fakültə: Aqrar və mühəndislik
İxtisas: 050616 Informasiya texnologiyaları
Kafedra: Texnologiya və texniki elmlər

I.Fənn haqqında məlumat:

Fənnin adı: İnformasiyanın təhlükəsizliyi
Kodu: İPF-B15
Tədris ili: III (2024-2025), VI semestr
Tədris yükü: Cəmi: 60 saat (60 saat mühazirə, 30 saat seminar)
Tədris forması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 6 kredit

II.Müəllim haqqında məlumat:

Vəzifəsi, adı, atasının adı, soyadı: dosent, Muradova Vüsalə Xudaşirin qızı
Məsləhət saatı: II gün saat $12^{00} - 13^{00}$
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. Фундаменталный курс. "Основы информационной и вычеслительной техники" БХВ-Петербург, 2005
5. "İnformatika" Dərslik, S. Q. Kərimov, S. B. Həbibullayev, T. İ. İbrahimzadə, Bakı 201

IV.Prekrivizitlər: "İnformasiya təhlükəsizliyi" fənni üzrə təhsil alan bakalavrlara kibertəhlükəsizlikdə hücumlar, təhdidlər və zəifliklərin öyrənilməsi, təhlükəsiz şəbəkən arxitekturası, dizaynı, insidentlərə cavab tədbirləri, kibertəhlükəsizlik risklərinin idar edilməsinin metodları və vasitələrinin öyrənilməsi və istehsalatla əlaqələndirilmə nəzərdə tutulmuşdur.

V.Korekvizitlər: Informsiya təhlükəsizliyinin əsas anlayışları, kompüter sistemlərində və şəbəkələrində informasiya hədələri haqqında məlumat, onların təhlil edilməsi tutarlı səviyyədə verilir. Təhlükəsizlik siyasətinin baza anlayışları müəyyənləşdirilir. Kriptoqrafik üsullarla yanaşı kompüter informasiyasının müdafiə alqoritminə baxılır.

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 qərarina 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 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)

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; 3. Əlçatanlıq matrisi.	2	
9	**Kriptoqrafiya və Şifrələmə** Plan:	2	

	1. Kriptoqrafiyanın əsas anlayışları; 2. Kriptoqrafiyanın bölmələri. 3.Şifrələmə anlayışı; 4. Simmetrik şifrələmə		
10.	**Şifrələmə üsulları. Çoxhərfli şifrələmə** Plan: 1. Çoxəlifbalı şifr; 2. Qronsfeld şifrəsi; 3. Sezar və Qronsfeld şifrələmə üsullarının çatışmazlıqları. 4. Pleyfeyer şifrələnməsi; 5. Hill şifri.	2	
11.	**Müasir simmetrik şifrələmə alqoritmləri. Açıq açarla şifrələmə** Plan: 1. DES alqoritmi; AES alqoritmi; 2. Simmetrik alqoritmlərin problemləri. 3. Açıq açarla şifrələmə alqoritmi; 4. Açıq açarla şifrələmə alqoritminin şərtləri; RSA alqoritmi	2	
12.	**Elektron rəqəmsal imza** Plan: 1. Rəqəmsal imzanın yaranması; Elektron imza.	2	
13	**Parolun köməyilə müdafiə** Plan: 1. Parola hücum üsulları. Parolun təhlükəsizliyinin təmini 2. Ümumi əlçatan yerlərdə saxlanılan parolların toplanması 3. Sosial injiring və fişinq	2	
14	**Kompüter virusları və onlarla mübarizə** Plan: 1. Kompüter viruslarının təsnifatı və meydana gəlməsinin qısa tarixi 2. Polimorfizm – virusların mutasiyası və təhlükəsizliyə qarşı virus hədələrinin tipləri 3. Antivirus proqramlarının yaradılması, inkişafı və viruslarla mübarizə	2	
15	**Şəbəkələrin informasiya təhlükəsizliyi problemləri. Əməliyyat sisteminin təhlükəsizliyinin təmini** Plan: 1. Şəbəkənin informasiya təhlükəsizliyinin təmin edilməsi 2. İnformasiya təhlükəsizliyinin təmin edilmə üsulları 3. Əməliyyat sisteminin təhlükəsizliyinin təmin edilməsi problemləri 4. Əməliyyat sisteminin təhlükəsizliyinə hədələr və müdafiə olunma anlayışı	2	
Cəmi:		**30**	

Laboratoriya işləri mövzuları

S/s	Mövzunun adı	Saat	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	4	
5.	Aircrack-ng ilə Wi-Fi parollarının tapılması	4	
6.	Kriptoqrafiya. Şifrələmə. Şifrələmə üsulları. Çoxhərfli şifrələmə	4	
7	Müasir simmetrik şifrələmə alqoritmləri. Açıq açarla şifrələmə	4	

6.	Kriptoqrafiya. Şifrələmə. Şifrələmə üsulları. Çoxhərfli şifrələmə	4	
7	Müasir simmetrik şifrələmə alqoritmləri. Açıq açarla şifrələmə	4	
8.	Elektron rəqəmsal imza.	2	
9.	Parolun köməyilə müdafiə	2	
10.	Kompüter virusları və onlarla mübarizə	4	
Cəmi:		30	

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 komunikasiya texnologiyalarından istifadə edərək informatika dərsində bilik və bacarıqlara yiyələnmək.

XII. Təlimin nəticələri

-Kibertəhlükəsizlik konsepsiyaları
-Kibertəhlükəsizlikdə hücumlar
-Təhdidlər və boşluqların öyrənilməsi
-Informasiya tamlığının və əlçatanlığının təmin edilməsi
-Təhlükəsizlik modelinin tətbiqi
-Kriptoqrafiyanın əsas anlayışları
-Şəbəkənin qurulması üzrə lazımi biliklər

XIII. Tələbələrin fənn haqqqında fikrin öyrənilməsi:

XIV.Birinci kollekvium 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;
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;

XV. Ikinci kollekvium sualları

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

XVI. Fənnin imtahan sualları:

I ci 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.
9. Qanunvericilik müdafiə tədbirləri;

II ci blok

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

III ci blok

1. Əlçatanlığıa nəzarətin rol modelinin təsviri (RBAC).
2. Əlçatanlığa nəzarətin rol modelinin üstünlükləri;
3. Əlçatanlığa hədd qoyma sistemləri;
4. Əlçatanlıq matrisi.
5. Kriptoqrafiyanın əsas anlayışları;
6. Kriptoqrafiyanın bölmələri.
7. Şifrələmə anlayışı;
8. Simmetrik şifrələmə
9. Çoxəlifbalı 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. Rəqəmsal imzanın yaranması; Elektron imza.

V ci Blok

1. Parola hücum üsulları. Parolun təhlükəsizliyinin təmini
2. Ümumi əlçatan yerlərdə saxlanılan parolların toplanması
3. Sosial injiring 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
7. Şəbəkənin informasiya təhlükəsizliyinin təmin edilməsi
8. İnformasiya təhlükəsizliyinin təmin edilmə üsulları
9. Əməliyyat sisteminin təhlükəsizliyinin təmin edilməsi problemləri
10. Əməliyyat sisteminin təhlükəsizliyinə hədələr və müdafiə olunma anlayışı

Fənnin sillabusu 050631 – **"İnformasiya texnologiyalarının"** 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 № 06).

Fənn müəllimi: **dos. V.X. Muradova**

Kafedra müdiri: **dos. R.F. Əliyev**