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: "Əməliyyat sistemlərinin təhlükəsizliyi" ("Əməliyyat sistemlərinin təhlükəsizliyi " işçi fənn proqramı, Lənkəran Dövlət Universitetinin Texnologiya və texniki elmlər kafedrasının 07.01.2026-cı il 5 №-li protokoluna əsasən)
Kodu:ATMTMOF-B07
Tədris ili: III tədris ili, (2025-2026) Semestr: VI
Tədris yükü: Auditoriya saatı 60 (30 saat mühazirə, 30 saat laboratoriya)
Tədris forması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 6 kredit
II. Müəllim haqqında məlumat:
Soyadı, adı, ata adı, elmi dərəcəsi və elmi adı:
Mühazirə müəllimi:b/m Ələskərov Nadir Hüseynoğlu,
Laboratoriya müəllimi:Nuruzadə Arzu Əli qızı
Kafedranın ünvanı: Lənkəran şəhər Fizuli 170 a 1 saylı tədris korpusu
Məsləhət günləri və saatı: II- gün saat 11^{40} -12^{30}, V- gün saat 08^{30} -10^{05}
E-mail ünvanı: nadir.alaskarov @ gmail.com arzu.nuruzade 96 @ gmail.com

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

1. Əlizadə Nətləb nuruş oğlu,Bayramov Hafiz məhərrəm oğlu "İnformasiya təhlükəsizliyi", Dərslik, Bakı-2016
2. Abbasov Ə.M,ƏlizadəM.N "İnformatika və kompüterləşmənin əsasları"Dərslik-2012
3. Z.M.Məmmədov, Y.P. Dursunov, F.H.Namazov, "İnformasiya sistemlərində təhlükəsizliyin təmini" Baki-2015
4. Salayev Oktay Ağacan Ağayev Munir Qəribağa "ƏMƏLİYYAT SİSTEMLƏRİ" BAKI – 2022
5. Aidə Mustafayeva. Şəbəkə təhlükəzisliyi. Dərslik, Bakı-2024
6. "Linux for Beginners" Mark Hoebeke, Jean-Michel Aroumougom Mark Hoebeke, Jean-Michel Aroumougom. Linux for Beginners. Licence. Station Biologique de Roscoff, France. 2022.
7. 4.S.Q.Kərimov, S.B. Həbibullayev, T.İ.İbrahimzadə. İnformatika. Bakı, 2011.
8. 5. Основы организации сетей Cisco. Том 1. Москва-Санкт-Петербург-Киев, 2002.

Əlavə ədəbiyyat

9. İNTERNET saytları.
10. Mühazirə konspekt materialları.

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.

VII. **Fənnin təsviri və məqsədi:** Bu fənn tələbələrə əməliyyat sistemlərinin təhlükəsizliyini təmin etmək üçün nəzəri biliklər və praktik bacarıqlar qazandırır. Fənn çərçivəsində tələbələr əməliyyat sistemlərinə yönəlmiş təhlükələri və məlumatların saxlanması zamanı yaranan riskləri müəyyən etməyi, şəbəkə və mobil sistemlərdə təhlükəsizlik tədbirlərini öyrənməyi bacarırlar. Həmçinin, müxtəlif əməliyyat sistemlərində (MS-DOS, Linux, UNIX, Windows, Android və iOS) istifadəçi hesablarının, şifrələrin, fayl və verilənlərin qorunmasını, müdafiə mexanizmlərinin tətbiqini və audit prosedurlarını praktik şəkildə həyata keçirə bilirlər.

Fənnin məqsədi tələbələrə əməliyyat sistemlərinin təhlükəsizliyinin təmin olunması ilə bağlı əsas anlayışları mənimsətmək və onları praktik fəaliyyətlər vasitəsilə tətbiq etmə bacarığı qazandırmaqdır. Tələbələr əməliyyat sistemlərinə yönəlmiş təhlükələri və riskləri müəyyən edə, müdafiə mexanizmlərini qurub konfiqurasiya edə, istifadəçi identifikasiyası ilə autentifikasiyanı tətbiq edə, təhlükəsizlik siyasətini hazırlayıb həyata keçirə və audit prosedurlarını tətbiq edə bilirlər. Həmçinin fayl və verilənlərin qorunması, arxivləşdirilməsi və bərpasını təmin edə, şəbəkə və mobil əməliyyat sistemlərində təhlükəsizlik tədbirlərini tətbiq edə və laboratoriya məşğələləri vasitəsilə nəzəri biliklərini praktik olaraq sınaya bilirlər.

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) imtahanin 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

XI.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

№	Tədris olunan mövzuların məzmunu	Saat	Tarix
		Mühazirə	
1.	**Mövzu 1 .**Əməliyyat sistemlərinin təhlükəsizliyinin təmin edilməsi problemləri Plan: 1.Əməliyyat sistemlərinin təhlükəsizliyinə hədələr. 2.Əməliyyat sismlərinin hucumlara məruz qalması. Mənbə:1,2,3	2	
2.	**Mövzu 2.**Əməliyyat sisteminin müdafiə olunma anlayışı. Plan: 1.Əməliyyat sisteminin müdafiə olunmasına yanaşma. 2.Müdafiənin inzibatı tədbirləri. Mənbə:1,2,3	2	
3.	**Mövzu 3..**Adekvat təhlükəsizlik siyasəti. Plan: 1.Təhlükəsizlik siyasətinin optimal adekvatlığı 2.Təhlükəsizlik siyasətinin həyata keçirilməsi Mənbə:1,2,3	2	

4.	**Mövzu 4.**Əməliyyat sisteminin müdafiə olunma altsisteminin arxitekturası. Plan: 1. Əməliyyat sisteminin müdafiə olunma altsisteminin əsas funksiyaları 2.Əlçatanlıq subyektlərinin identifikasiyası və autentifikasiyası. Mənbə:1,2,3	2	
5.	**Mövzu 5.**Əməliyyat sistemləri obyektinə əlçatanlığın məhdudlaşdırılması. Plan: 1.Obyektə və subyektə əlçatanlıq metodu. 2.Əlçatanlığın məhdudlaşdırılması qanunları Mənbə:1,2,3	2	
6.	**Mövzu 6.**Əlçanlığın seçməklə məhdudlaşdırılması Plan: 1.Obyektlərə daxil olma imkanı. 2.Əlçatanlığnı seçməklə məhdudlaşdırılması.. Mənbə:1,2,3	2	
7.	**Mövzu 7.**Əlçatanlığın müvəkkil məhdudlaşdırılmasının informasiya axınına nəzarəti. Plan: 1.Əməliyyat sisteminə audit prosedurunun tətbiqi. 2.Auditə qoyulan tələbat. 3.Audit siyasəti. Mənbə:1,2,3	2	
8.	**Mövzu 8.**Şəbəkə təhlükəsizliyi vasitələrilə idarəetmə üsulları. Plan: 1. Şəbəkə təhlükəsizliyi vasitələrilə idarəetmə məsələləri. 2.Sisistemin təhlükəsizlik monitorinqi. Mənbə:1,2,3	2	
9.	**Mövzu 9.**Şəbəkə təhlükəsizliyi vasitələrilə idarəetmə arxitekturası. Plan: 1.Əsas anlayışlar. 2.Monitorinq və audit hadisələrinin protokollaşdırılması. Mənbə:1.2,4	2	
10.	**Mövzu 10.** MS-DOS sistemində məlumatların saxlanması və risklər Plan 1. MS-DOS nədir və necə işləyir 2. FAT fayl sistemi haqqında sadə məlumat	2	

	3. MS-DOS sistemində təhlükəsizlik çatışmazlıqları və risklər Mənbə:3,4		
11.	**Mövzu 11.**Linux əməliyyat sistemində istifadəçi və şifrə təhlükəsizliyi Plan 1.Linux əməliyyat sistemində İstifadəçi və administrator anlayışı 2.Linux ƏS-də Güclü şifrələrin yaradılması və qorunması 3.Linux əməliyyat sistemində Şifrə dəyişdirmə və istifadəçi bloklama qaydaları Mənbə:4,6	2	
12.	**Mövzu 12.**UNIX sistemində faylların qorunması Plan UNIX əməliyyat sistemində Fayl və qovluq anlayışı, faylların qorunması UNIX sistemində oxuma, yazma və icra icazələri (r, w, x) Mənbə:4,7	2	
13.	**Mövzu 13.**Windows əməliyyat sistemlərinin bütün verilənlərin təhlükəsiz saxlanılmasının təmini imkanları. Plan: 1.Təşkilatın verilənlərinin təhlükəsiz saxlanılmasının əsas cəhətləri. 2. Məlumatların kopyalamasının kölgə texnologiyası. Mənbə:1,2,3	2	
14.	**Mövzu 14.**Windows əməliyyat sistemində verilənlərin bərpası. Plan: 1.Məlumatların arxivləşdirməsi. 2.Windows sistemində daxili bərpa vasitələri Mənbə:1,3	2	
15.	**Mövzu 15.**Mobil əməliyyat sistemlərində sadə təhlükəsizlik qaydaları (Android və iOS) Plan 1.Mobil əməliyyat sistemlərində Ekran kilidi və PIN kod istifadəsi 2.Tətbiq yükləyərkən diqqət edilməli məqamlar 3.Telefonun viruslardan qorunması Mənbə:4	2	
	Cəmi:	**30s**	

№	Tədris olunan mövzuların məzmunu	Saat	Tarix
		Laboratoriya	
1.	**Mövzu 1.**Əməliyyat sistemlərində təhlükəsizlik problemlərinin aşkarlanması və təhlili	2	
2.	**Mövzu 2.**Əməliyyat sistemində müdafiə mexanizmlərinin qurulması və konfiqurasiyası	2	
3.	**Mövzu 3.**Adekvat təhlükəsizlik siyasətinin tətbiqi və həyata keçirilməsi	2	
4.	**Mövzu 4.**Əməliyyat sisteminin müdafiə olunma altsisteminin arxitekturasının öyrənilməsi və istifadəçi identifikasiyası ilə autentifikasiyanın tətbiqi	2	
5.	**Mövzu 5.**Əməliyyat sistemləri obyektinə əlçatanlığın məhdudlaşdırılması metodlarının tətbiqi	2	
6	**Mövzu 6.**Əlçatanlığın seçmə üsulu ilə məhdudlaşdırılması və obyektlərə giriş imkanlarının idarə olunması	2	
7.	**Mövzu 7.**Əlçatanlığın müvəkkil məhdudlaşdırılması və informasiya axınına nəzarətdə audit prosedurlarının tətbiqi	2	
8.	**Mövzu 8.**Şəbəkə təhlükəsizliyi vasitələrilə idarəetmə üsullarının tətbiqi və sistemin təhlükəsizlik monitorinqinin aparılması	2	
9.	**Mövzu 9.**Şəbəkə təhlükəsizliyi vasitələri ilə idarəetmə arxitekturasının qurulması	2	
10.	**Mövzu 10.**MS-DOS əməliyyat sistemində məlumatların saxlanması üsulları və təhlükəsizlik risklərinin tədqiqi	2	
11.	**Mövzu 11.** "Linux əməliyyat sistemində istifadəçi hesablarının yaradılması və şifrə təhlükəsizliyinin yoxlanması	2	
12.	**Mövzu 12.**UNIX əməliyyat sistemində faylların qorunması	2	
13.	**Mövzu 13.**Windows əməliyyat sistemlərində bütün verilənlərin təhlükəsiz saxlanmasının təmin edilməsi	2	
14.	**Mövzu 14.**Windows əməliyyat sistemində verilənlərin bərpası aparılması	2	
15.	**Mövzu 15.**Mobil əməliyyat sistemlərində (Android və iOS) sadə təhlükəsizlik qaydalarının tətbiqi və yoxlanması	2	
Cəmi:		**30 s**	

XI. Fənn üzrə tələblər:Fənnin tədrisinin sonunda tələbələr "Əməliyyat sistemlərinin təhlükəsizliyi " kursundan müəyyən biliklərə malik olmalı, o cümlədən fənn haqqında nəzəri və praktik şəkildə fikirlərini əsaslandırmağı bacarmalıdırlar.

" Əməliyyat sistemlərinin təhlükəsizliyi " fənninin tədrisi zamanı tələbələrə kompüterin strukturuna aıd olan müxtəlif bölmələrinin və praktik tətbiqini öyrədilməsi fənn üzrə qoyulan əsas tələblərdən biridir:

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

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

XIII Fənn üzrə təlimin nəticələri:

- Əməliyyat sistemlərinə yönəlmiş hədələri, hücum növlərini və məlumatların saxlanması zamanı yaranan riskləri müəyyən etmək və təhlil etmək bacarığı.
- Əməliyyat sistemində müdafiə mexanizmlərini qurmaq, konfiqurasiya etmək, müdafiə altsisteminin arxitekturasını öyrənmək, istifadəçi identifikasiyası və autentifikasiyasını tətbiq etmək bacarığı.
- Adekvat təhlükəsizlik siyasətini hazırlamaq, həyata keçirmək, obyektlərə və subyektlərə əlçatanlığı seçmə üsulu ilə məhdudlaşdırmaq və audit prosedurlarını tətbiq etmək bacarığı.
- İstifadəçi hesablarını yaratmaq, idarə etmək, güclü şifrə siyasətini tətbiq etmək, şifrələrin dəyişdirilməsi və bloklanmasını həyata keçirmək bacarığı.
- Fayl və verilənlərin qorunmasını təmin etmək, UNIX və Windows əməliyyat sistemlərində icazələri tətbiq etmək, verilənləri arxivləşdirmək və bərpa mexanizmlərini həyata keçirmək bacarığı.
- Şəbəkə və mobil əməliyyat sistemlərində təhlükəsizlik tədbirlərini tətbiq etmək, monitorinq və audit aparmaq, mobil cihazlarda əsas təhlükəsizlik qaydalarını yoxlamaq bacarığı.

XIV. Tələbələrin fənn haqqında fikrinin öyrənilməsi:

_____

_____

_____

XV. Kollokvium sualları:

I Kollokvium sualları

1.Əməliyyat sistemlərinin təhlükəsizliyinin təmin edilməsi problemləri
2.Əməliyyat sistemlərinin təhlükəsizliyinə hədələr.
3.Əməliyyat sismlərinin hucumlara məruz qalması.
4.Əməliyyat sisteminin müdafiə olunma anlayışı.
5.Əməliyyat sisteminin müdafiə olunmasına yanaşma.
6.Müdafiənin inzibatı tədbirləri.

7.Adekvat təhlükəsizlik siyasəti.
8.Təhlükəsizlik siyasətininoptimaladekvatlığı
9.Təhlükəsizlik siyasətinin həyata keçirilməsi.
10.Əməliyyat sisteminin müdafiə olunma altsisteminin arxitekturası.
11.Əməliyyat sisteminin müdafiə olunma altsisteminin əsas funksiyaları
12.Əlçatanlıq subyektlərinin identifikasiyası və autentifikasiyası.
13.Əməliyyat sistemləri obyektinə əlçatanlığın məhdudlaşdırılması.
14.Obyektə və subyektə əlçatanlıq metodu.
15.Əlçatanlığın məhdudlaşdırılması qanunları

II. Kollokvium sualları

1.Əlçanlığın seçməklə məhdudlaşdırılması
2.Obyektlərə daxil olma imkanı.
3.Əlçatanlığın müvəkkil məhdudlaşdırılmasının informasiya axınına nəzarəti.
4.Əməliyyat sisteminə audit prosedurunun tətbiqi.
5..Auditə qoyulan tələbat.
6.Audit siyasəti.
7.Şəbəkə təhlükəsizliyi vasitələrilə idarəetmə üsulları.
8. Şəbəkə təhlükəsizliyi vasitələrilə idarəetmə məsələləri.
9.Sisistemin təhlükəsizlik monitorinqi.
10.Şəbəkə təhlükəsizliyi vasitələrilə idarəetmə arxitekturası.
11.Əsas anlayışlar.
12.Monitorinq və audit hadisələrinin protokollaşdırılması.
13.MS-DOS nədir və necə işləyir
14. FAT fayl sistemi haqqında sadə məlumat
15. MS-DOS sistemində təhlükəsizlik çatışmazlıqları və risklər

XVI. Fənnin imtahan sualları

1. Əməliyyat sistemlərinin təhlükəsizliyinin təmin edilməsi problemləri
2. Əməliyyat sistemlərinin təhlükəsizliyinə hədələr.
3. Əməliyyat sismlərinin hucumlara məruz qalması.
4. Əməliyyat sisteminin müdafiə olunma anlayışı.
5. Əməliyyat sisteminin müdafiə olunmasına yanaşma.
6. Müdafiənin inzibatı tədbirləri.
7. Adekvat təhlükəsizlik siyasəti.
8. Təhlükəsizlik siyasətininoptimaladekvatlığı
9. Təhlükəsizlik siyasətinin həyata keçirilməsi.
10. Əməliyyat sisteminin müdafiə olunma altsisteminin arxitekturası.
11. Əməliyyat sisteminin müdafiə olunma altsisteminin əsas funksiyaları
12. Əlçatanlıq subyektlərinin identifikasiyası və autentifikasiyası.
13. Əməliyyat sistemləri obyektinə əlçatanlığın məhdudlaşdırılması.
14. Obyektə və subyektə əlçatanlıq metodu.
15. Əlçatanlığın məhdudlaşdırılması qanunları
16. Əlçanlığın seçməklə məhdudlaşdırılması
17. Obyektlərə daxil olma imkanı.
18. Əlçatanlığnı seçməklə məhdudlaşdırılması.
19. Əlçatanlığın müvəkkil məhdudlaşdırılmasının informasiya axınına nəzarəti.
20. Əməliyyat sisteminə audit prosedurunun tətbiqi.

21. Auditə qoyulan tələbat.
22. Audit siyasəti.
23. Şəbəkə təhlükəsizliyi vasitələrilə idarəetmə üsulları.
24. Şəbəkə təhlükəsizliyi vasitələrilə idarəetmə məsələləri.
25. Sisistemin təhlükəsizlik monitorinqi.
26. Şəbəkə təhlükəsizliyi vasitələrilə idarəetmə arxitekturası.
27. Əsas anlayışlar.
28. Monitorinq və audit hadisələrinin protokollaşdırılması.
29. MS-DOS nədir və necə işləyir
30. FAT fayl sistemi haqqında sadə məlumat
31. MS-DOS sistemində təhlükəsizlik çatışmazlıqları və risklər
32. Linux əməliyyat sistemində İstifadəçi və administrator anlayışı
33. Linux ƏS-də Güclü şifrələrin yaradılması və qorunması
34. Linux əməliyyat sistemində Şifrə dəyişdirmə və istifadəçi bloklama qaydaları
35. UNIX əməliyyat sistemində Fayl və qovluq anlayışı, faylların qorunması
36. UNIX sistemində oxuma, yazma və icra icazələri (r, w, x)
37. Windows əməliyyat sistemlərinin bütün verilənlərin təhlükəsiz saxlanılmasının təmini imkanları.
38. Təşkilatın verilənlərinin təhlükəsiz saxlanılmasının əsas cəhətləri.
39. Məlumatların kopyalamasının kölgə texnologiyası.
40. Windows sistemində daxili bərpa vasitələri
41. Məlumatların arxivləşdirməsi.
42. Mobil əməliyyat sistemlərində Ekran kilidi və PIN kod istifadəsi
43. Tətbiq yükləyərkən diqqət edilməli məqamlar
44. Telefonun viruslardan qorunması

" Əməliyyat sistemlərinin təhlükəsizliyi " fənninin sillabusu 6006017-"İnformasiya təhlükəsizliyi" ixtisasının tədris planı və fənn proqramı əsasında tərtib edilmişdir.

Sillabus "Texnologiya və texniki elmlər" kafedrasında müzakirə edilərək, təsdiq edilmişdir (07.01. 2026-ci il, protokol №05).

Fənn müəllimi: b/m N. H. Ələskərov

A.Ə.Nuruzadə

Kafedra müdiri: dos. R.F. Əliyev