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
Fakultə: Aqrar və mühəndislik
Kafedra: Texnologiya və texniki elmlər

I. Fənn haqqında məlumat:
Fənnin adı: **Korporativ şəbəkə(informasiya) sistemlərinin təhlükəsizliyi**
("Korporativ şəbəkə(informasiya) sistemlərinin təhlükəsizliyi" işçi fənn proqramı, Lənkəran Dövlət Universitetinin Texnologiya və texniki elmlər kafedrasının 07.01.2026-cı il 5 №-li protokoluna əsasən)
Kodu: ATMTMOF-B03
Tədris ili: II tədris ili, (2025-2026)
Semestr: IV (yaz)
Tədris yükü: 60 (30 saat mühazirə, 30 saat laboratoriya)
Təhsilalma forması: Əyani
Tədris dili: Azərbaycan dili
AKTS üzrə kredit: 6 kredit

II. Müəllim haqqında məlumat:
Adı, soyadı, elmi dərəcəsi və elmi adı:
Mühazirə müəllimi: **Dəmirov Asəf Ağacəfər oğlu, t.ü.f.d.,dosent.**
Laboratoriya müəllimi: **İsmayılova Ülviyyə Şahəddin , müəllim.**
Məsləhət saatı: V gün saat 12^{20} -13^{55} ,II gün 8^{30}-10^{05}
E-mail ünvanı: asef.demirov@gmail.com, iulviyye70@gmail.com
Kafedranın ünvanı: Lənkəran şəhəri Füzuli 170 a, LDU-nun 1 saylı tədris binası

III.Tövsiyyə olunan dərsliklər və dərs vəsaitləri:

Əsas ədəbiyyat

1.İbrahim-zadə T., Abdullayev V.H. **Korporativ informasiya sistemində informasiyanın mühafizəsi** – Dərs vəsaiti, 425 s.
2.İnformasiya təhlükəsizliyi üzrə beynəlxalq standartlar (ISO/IEC 27000 seriyası)
3.William Stallings – *Network Security Essentials*
4.Charles Pfleeger – *Security in Computing*
5.ISO/IEC 27001 Standartı
6.NIST SP 800 seriyası
7.Cisco Network Security Manuals
8.Mühazirələr. Korporativ şəbəkə(informasiya) sistemlərinin təhlükəsizliyi. Dəmirov Asəf Ağacəfər oğlu , t.ü.f.d.,dosent.2026.

yoxdur.

VI. Fənnin təsviri və məqsədi:

"Korporativ şəbəkə(informasiya) sistemlərinin təhlükəsizliyi" fənninin məqsədi tələbələrdə korporativ şəbəkə və informasiya sistemlərinin təhlükəsizliyinin təmin edilməsi, risklərin idarə olunması, mühafizə mexanizmlərinin layihələndirilməsi və tətbiqi üzrə nəzəri bilik və praktik bacarıqlar formalaşdırmaqdan ibarətdir.

Tələbələrə informasiya sistemləri və şəbəkələrdə təhlükəsizlik boşluqlarının müəyyənləşdirilməsi və qiymətləndirilməsi həyata keçirmə yollarını aşılamaqdan ibarətdir.Mövzular üzrə məqsədlər aşağıdakılardır:

1.İnformasiya təhlükəsizliyinin əsas anlayışlarını formalaşdırmaq.
2.Korporativ İS-in quruluşunu öyrənmək.
3.İnformasiya resurslarının qorunma səviyyələrini anlamaq
4.Təhlükə mənbələrini müəyyənləşdirmək
5.Hücum mexanizmlərini öyrənmək
6.Risklərin qiymətləndirilməsi bacarığı formalaşdırmaq.
7.Təhlükəsizlik siyasətinin hazırlanmasını öyrənmək
8.Texniki təhlükəsizlik mexanizmlərini izah etmək
9.Kriptoqrafiyanın əsaslarını öyrənmək
10.Məlumatın bütövlüyünü qoruma üsullarını öyrənmək
11.Şəbəkə mühafizəsini öyrənmək
12.DB mühafizəsini təmin etməyi öyrənmək
13.Hüquqi tələbləri mənimsətmək
14.Fövqəladə hallara hazır olmaq
15.Gələcək təhlükəsizlik çağırışlarını dərk etmək

Fənnin vəzifələri:

İnformasiya təhlükəsizliyi anlayışlarını sistemli şəkildə izah etmək
Risk və zəiflik anlayışlarını təhlil etmək
Təhlükəsizlik qiymətləndirmə nəticələrinin sənədləşdirilməsi bacarığı formalaşdırmaq
Etik və hüquqi məsuliyyət şüurunu aşılamaqdan ibarətdir.

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;

bal - kollokviumların nəticələrinə görə.
mətləndirmə zamanı LDU-nun Elmi Şurasının 16 may 2024-cü il tarixli qərarına
ğun olaraq qiymətləndirmə meyarları nəzər alınır.
imtahanda 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 –30 saat, Cəmi 60 – saat.

Mühazirə mövzuları			
S/s	Mövzunun adı və məzmunu	Saat	Tari
1.	**Mühazirə 1. Korporativ şəbəkə sistemlərinə giriş. İnformasiya təhlükəsizliyinin əsasları** **Plan:** 1.Korporativ şəbəkə anlayışı 2.İnformasiya təhlükəsizliyinin məqsədi və vəzifələri 3.CIA triadası (Məxfilik, Bütövlük, Əlçatanlıq)	2	

	4.Təhlükəsizlik problemlərinin yaranma səbəbləri 5.Müasir korporativ şəbəkələrdə təhlükəsizlik tələbləri **Mənbə:8** [1-10]			
2.	**Mühazirə 2. Korporativ informasiya sistemlərinin strukturu və arxitekturası** **Plan:** 1.İnformasiya sistemlərinin növləri 2.Müştəri–server arxitekturası 3.Mərkəzləşdirilmiş və paylanmış sistemlər 4.Şəbəkə səviyyələri və onların təhlükəsizlik rolu 5.Arxitektur zəifliklər **Mənbə:8** [11-20]	2		
3.	**Mühazirə 3.Təhlükə modelləri və risklərin qiymətləndirilməsi** **Plan:** 1.Təhlükə, zəiflik və risk anlayışları 2.Təhlükə mənbələrinin təsnifatı 3.Risk analizi metodları 4.Risklərin qiymətləndirilməsi mərhələləri 5.Risklərin azaldılması yolları **Mənbə:8** [21-30]	2		
4.	**Mühazirə 4. Şəbəkə hücumları və zərərli fəaliyyətlərin növləri** **Plan:** 1.Aktiv və passiv hücumlar 2.Daxili və xarici hücumlar 3.DoS/DDoS hücumları 4.Man-in-the-Middle hücumu 5.Sosial mühəndislik hücumları **Mənbə:8** [31-40]	2		
5.	**Mühazirə 5. Təhlükəsizlik siyasəti və normativ sənədlər** **Plan:** 1.Təhlükəsizlik siyasəti anlayışı 2.Təhlükəsizlik siyasətinin strukturu 3.Girişə nəzarət siyasəti 4.Beynəlxalq standartlar (ISO/IEC 27001) 5.Təhlükəsizlik siyasətinin tətbiqi problemləri **Mənbə:8** [41-50]	2		
6.	**Mühazirə 6. Şəbəkə təhlükəsizlik protokolları** **Plan:** 1.Təhlükəsiz rabitə anlayışı 2.SSL/TLS protokolu 3.IPsec protokolu 4.HTTPS və onun üstünlükləri 5.Protokol səviyyəsində təhlükəsizlik riskləri **Mənbə:8** [51-60]	2		
7.	**Mühazirə 7. Firewall sistemləri və filtrasiya mexanizmləri** **Plan:** 1.Firewall anlayışı və funksiyaları 2.Paket filtrasiya firewall-ları 3.Stateful inspection firewall-ları 4.Application-level firewall-lar 5.Firewall-ların korporativ şəbəkədə yerləşdirilməsi **Mənbə:8** [61-70]	2		

	Mühazirə 8. IDS/IPS sistemləri və şəbəkə monitorinqi **Plan:** 1.IDS və IPS anlayışları 2.Anomaliya əsaslı aşkarlama 3.İmza əsaslı aşkarlama 4.IDS/IPS arxitekturası 5.Monitorinq sistemlərinin əhəmiyyəti **Mənbə:8** [71-80]	2	
9.	**Mühazirə 9. Autentifikasiya, avtorizasiya və identifikasiya** **Plan:** 1.AAA modeli 2.Şifrəyə əsaslanan autentifikasiya 3.Çoxfaktorlu autentifikasiya 4.Rol əsaslı giriş nəzarəti 5.Korporativ identifikasiya sistemləri **Mənbə:8** [81-90]	2	
10	**Mühazirə 10. Kriptoqrafik üsulların şəbəkə təhlükəsizliyində tətbiqi** **Plan:** 1.Kriptoqrafiyanın əsas anlayışları 2.Simmetrik və asimmetrik şifrələmə 3.Rəqəmsal imza 4.Hash funksiyaları 5.Açarların idarə olunması **Mənbə:8** [91-100]	2	
11.	**Mühazirə 11. VPN texnologiyaları və təhlükəsiz əlaqə** **Plan:** 1.VPN anlayışı və məqsədi 2.Site-to-Site VPN 3.Remote Access VPN 4.VPN protokolları 5.VPN təhlükəsizlik problemləri **Mənbə:8** [101-110]	2	
12.	**Mühazirə 12. Korporativ server və xidmətlərin təhlükəsizliyi** **Plan:** 1.Server təhlükəsizliyi anlayışı 2.Əməliyyat sistemlərinin mühafizəsi 3.Xidmətlərin təhlükəsiz konfiqurasiyası 4.Giriş hüquqlarının idarə olunması 5.Ehtiyat nüsxələmə və bərpa **Mənbə:8** [111-120]	2	
13.	**Mühazirə 13.Virtualizasiya və bulud mühitlərində təhlükəsizlik** **Plan:** 1.Virtualizasiya texnologiyaları 2.Bulud xidmət modelləri 3.Virtual mühitlərdə risklər 4.Bulud təhlükəsizlik mexanizmləri 5.Korporativ bulud siyasəti **Mənbə:8** [121-130]	2	
14.	**Mühazirə 14. Təhlükəsizlik insidentlərinin idarə olunması** **Plan:**	2	

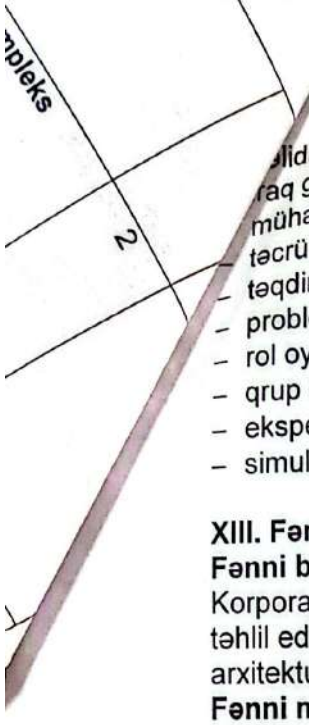
	1.Təhlükəsizlik insidenti anlayışı 2.İnsidentlərin aşkarlanması 3.Reaksiya və cavab mərhələləri 4.Zərərin qiymətləndirilməsi 5.Hadisədən sonra təhlil **Mənbə:8** [131-140]		
15.	**Mühazirə 15. Korporativ şəbəkə sistemlərində kompleks təhlükəsizlik modeli** **Plan:** 1.Kompleks təhlükəsizlik anlayışı 2.Texniki və təşkilati tədbirlər 3.Təhlükəsizlik arxitekturasının qurulması 4.Risk əsaslı yanaşma 5.Fənnin yekunu və ümumiləşdirmə **Mənbə:8** [141-150]	2	
	Cəmi mühazirə:	**30 s.**	
S/s	**Laboratoriya mövzusunun adı**	**Saat**	**Tarix**
1.	**Şəbəkə təhlükəsizliyi üzrə laboratoriya mühiti ilə tanışlıq**	**2**	
2.	**Şəbəkə topologiyasının qurulması və təhlükəsizlik analizi**	**2**	
3.	**Təhlükələrin identifikasiyası və risklərin hesablanması**	**2**	
4.	**Şəbəkə trafikinə nəzarət və analiz (Wireshark)**	**2**	
5.	**Firewall konfiqurasiyası**	**2**	
6.	**Paket filtrasiya və NAT tətbiqi**	**2**	
7.	**IDS sisteminin qurulması (Snort və s.)**	**2**	
8.	**Autentifikasiya mexanizmlərinin tətbiqi**	**2**	
9.	**VPN bağlantısının yaradılması**	**2**	
10.	**Şəbəkədə şifrələmə mexanizmləri**	**2**	
11.	**Server təhlükəsizliyinin təmin edilməsi**	**2**	
12.	**Virtual mühitlərdə təhlükəsizlik ssenariləri**	**2**	
13.	**Hücum ssenarilərinin modelləşdirilməsi**	**2**	
14.	**Təhlükəsizlik insidentinin aşkarlanması və cavab**	**2**	
15.	**Yekun laboratoriya işi – kompleks təhlükəsizlik layihəsi**	**2**	
Cəmi laboratoriya:		**30 s.**	
Fənn üzrə cəmi:		**60 s.**	

XI.Fənn üzrə tələblər:

Korporativ şəbəkə təhlükəsizliyinin əsas anlayışlarını mənimsəməlidir.Təhlükə, zəiflik və riskləri müəyyənləşdirməlidir.Şəbəkə təhlükəsizlik arxitekturası qurmağı öyrənməlidir.Təhlükəsizlik texnologiyalarını tətbiq etməlidir.Təhlükəsizlik insidentlərini idarə etməlidir.Informasiya təhlükəsizliyinin mahiyyətini öyrənməlidir.KİS arxitekturasını təsvir etməyi bilməlidir.Resursları təsnif etməlidir.Təhlükə mənbələrini fərqləndirməlidir.Hücum növlərini tanımalıdır.Risk analizi aparmalıdır.Siyasət sənədi hazırlamalıdır.Texniki vasitələri müqayisə etməlidir.Sifrələmə üsullarını bilməlidir.ERİ-nin iş prinsipini bilməlidir.Şəbəkə mühafizəsi tədbirləri təklif etməlidir.DB təhlükəsizliyini qiymətləndirməlidir.Normativ sənədləri tanımalıdır..İnsident planı hazırlamalıdır.Müasir riskləri təhlil etməlidir.

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



lidir. İstifadə edilə biləcək tədris və öyrənmə üsullarına aşağıdakıları nümunə raq göstərmək olar:

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

XIII. Fənn üzrə təlimin nəticələri:

Fənni bitirən tələbə:

Korporativ şəbəkə təhlükəsizliyi konsepsiyalarını izah edir.Təhlükə, zəiflik və riskləri təhlil edir.Şəbəkə təhlükəsizlik texnologiyalarını tətbiq edir.Təhlükəsizlik siyasəti və arxitekturası hazırlayır.Təhlükəsizlik insidentlərinə cavab tədbirləri görür.

Fənni mənimsəyən tələbə:

Korporativ şəbəkə təhlükəsizliyinin əsas anlayışlarını izah edir.Təhlükə, zəiflik və riskləri müəyyənləşdirir.Şəbəkə təhlükəsizlik arxitekturası qurur.Təhlükəsizlik texnologiyalarını tətbiq edir.Təhlükəsizlik insidentlərini idarə edir.Informasiya təhlükəsizliyinin mahiyyətini izah edir.KİS arxitekturasını təsvir edir.Resursları təsnif edir.Təhlükə mənbələrini fərqləndirir.Hücum növlərini tanıyır.Risk analizi aparır.Siyasət sənədi hazırlayır.Texniki vasitələri müqayisə edir.Sifrələmə üsullarını izah edir.ERİ-nin iş prinsipini izah edir.Şəbəkə mühafizəsi tədbirləri təklif edir.DB təhlükəsizliyini qiymətləndirir.Normativ sənədləri tanıyır.İnsident planı hazırlayır.Müasir riskləri təhlil edir.

XIV. Tələbələrin fənn haqqında fikrinin öyrənilməsi:

XV. Kollokvium sualları

I Kollokvium sualları

1.Korporativ şəbəkə anlayışı
2.İnformasiya təhlükəsizliyinin məqsədi və vəzifələri
3.CIA triadası (Məxfilik, Bütövlük, Əlçatanlıq)
4.Təhlükəsizlik problemlərinin yaranma səbəbləri
5.Müasir korporativ şəbəkələrdə təhlükəsizlik tələbləri
6.İnformasiya sistemlərinin növləri
7.Müştəri–server arxitekturası
8.Mərkəzləşdirilmiş və paylanmış sistemlər
9.Şəbəkə səviyyələri və onların təhlükəsizlik rolu
10.Arxitektur zəifliklər
11.Təhlükə, zəiflik və risk anlayışları
12.Təhlükə mənbələrinin təsnifatı
13.Risk analizi metodları
14.Risklərin qiymətləndirilməsi mərhələləri
15.Risklərin azaldılması yolları

II Kollokvium sualları

16.Aktiv və passiv hücumlar
17.Daxili və xarici hücumlar
18.DoS/DDoS hücumları
19.Man-in-the-Middle hücumu

20.Sosial mühəndislik hücumları
21.Təhlükəsizlik siyasəti anlayışı
22.Təhlükəsizlik siyasətinin strukturu
23.Girişə nəzarət siyasəti
24.Beynəlxalq standartlar (ISO/IEC 27001)
25.Təhlükəsizlik siyasətinin tətbiqi problemləri
26.Təhlükəsiz rabitə anlayışı
27.SSL/TLS protokolu
28.IPsec protokolu
29.HTTPS və onun üstünlükləri
30.Protokol səviyyəsində təhlükəsizlik riskləri

XVI. İmtahan sualları:

1.Korporativ şəbəkə anlayışı
2.İnformasiya təhlükəsizliyinin məqsədi və vəzifələri
3.CIA triadası (Məxfilik, Bütövlük, Əlçatanlıq)
4.Təhlükəsizlik problemlərinin yaranma səbəbləri
5.Müasir korporativ şəbəkələrdə təhlükəsizlik tələbləri
6.İnformasiya sistemlərinin növləri
7.Müştəri–server arxitekturası
8.Mərkəzləşdirilmiş və paylanmış sistemlər
9.Şəbəkə səviyyələri və onların təhlükəsizlik rolu
10.Arxitektur zəifliklər
11.Təhlükə, zəiflik və risk anlayışları
12.Təhlükə mənbələrinin təsnifatı
13.Risk analizi metodları
14.Risklərin qiymətləndirilməsi mərhələləri
15.Risklərin azaldılması yolları
16.Aktiv və passiv hücumlar
17.Daxili və xarici hücumlar
18.DoS/DDoS hücumları
19.Man-in-the-Middle hücumu
20.Sosial mühəndislik hücumları
21.Təhlükəsizlik siyasəti anlayışı
22.Təhlükəsizlik siyasətinin strukturu
23.Girişə nəzarət siyasəti
24.Beynəlxalq standartlar (ISO/IEC 27001)
25.Təhlükəsizlik siyasətinin tətbiqi problemləri
26.Təhlükəsiz rabitə anlayışı
27.SSL/TLS protokolu
28.IPsec protokolu
29.HTTPS və onun üstünlükləri
30.Protokol səviyyəsində təhlükəsizlik riskləri
31.Firewall anlayışı və funksiyaları
32.Paket filtrasiya firewall-ları
33.Stateful inspection firewall-ları
34.Application-level firewall-lar
35.Firewall-ların korporativ şəbəkədə yerləşdirilməsi
36.IDS və IPS anlayışları
37.Anomaliya əsaslı aşkarlama
38.İmza əsaslı aşkarlama

DS/IPS arxitekturası
Monitorinq sistemlərinin əhəmiyyəti
11.AAA modeli
42.Şifrəyə əsaslanan autentifikasiya
43.Çoxfaktorlu autentifikasiya
44.Rol əsaslı giriş nəzarəti
45.Korporativ identifikasiya sistemləri
46.Kriptoqrafiyanın əsas anlayışları
47.Simmetrik və asimmetrik şifrələmə
48.Rəqəmsal imza
49.Hash funksiyaları
50.Açarların idarə olunması

"Korporativ şəbəkə(informasiya) sistemlərinin təhlükəsizliyi" fənninin sillabusu bakalavr pilləsi üzrə 6006017-İnformasiya təhlükəsizliyi ixtisası üçün olan təhsil proqramı, tədris planı və bu fənnin 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: dosent, A. A. Dəmirov.

m, Ü. Ş. İsmayılova.

Kafedra müdiri: dosent, R. F. Əliyev