AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

TƏSDİQ TDİRƏM

AzTU-nun tədris işləri üzrə
prorektoru **X.M.Yahudov**
"____"_____2014-cu il

"Kompüter sistemləri və şəbəkələri" kafedrası

İxtisas: *050631* – "Kompüter mühəndisliyi"

Təhsil pilləsi: Bakalavr

Təhsil müddəti: 4 il

"**Kriptoqrafik mühafizənin təşkili**"
fənn

PROQRAMI

Kafedra iclasında təsdiq edilmişdir:____ saylı protokol «____» _____ 2014-cu il

Kafedra müdiri:
prof. V.H.Musayev

AHT fakültəsinin Elmi Şurasında təsdiq edilmişdir:__saylı protokol «___»_____ 2014-cu il

AKT fakültəsinin dekanı:
dos. H.T.Qurbanov

Bakı-2014

Müqəddimə

Əvvəlcə kompüter şəbəkələrinin əsas anlayışları, topologiyası, informasiyanın qorunma üsulları, tarixən informasiyanın qorunma üsulları, müasir informasiya mühafizə metodları, şifrləmə alqoritmləri, aydınlaşdırılacaq və buna əsaslanaraq onun təsnifatı, növləri və arxitekturasına aydınlıq gətiriləcək, sonra isə baza komponentləri və kommunikasiya avadanlıqlarına baxılacaqdır. Yəni, fiziki mühitdə istifadə olunan əlaqə xətlərinin növləri (eşilmiş naqil çütləri, koaksial kabellər, optik lifli kabellər və s.), əlaqələndirici avadanlıqların (adapterlər, işçi stansiyalar, serverlər və s.) rolu, vəzifə və funksiaları, istifadə olunma üsulları göstəriləçəkdir.

Əsasən şifrləmə alqoritmləri kriptoqrafiyanın riyazi əsasları, Evklit alqoritmi, Deff-Helman alqoritmi haqqında məlumat veriləcəkdir. Verilənlərin şifrlənməsi üçün Sezar şifrləmə alqoritmi, Vijiner şifrləmə alqoritmi, Pleyfer şifrləmə alqoritmi haqqında ətraflı məlumat veriləcəkdir.

TEMATİK PLAN

Bölmələr	Mövzunun adları	Auditoriya saatların miqdarı			
		Ümumi	Müh	Lab.	Məşğ.
1	2	3	4	5	6
I 1.1	Giriş. İnformasiya təhlükəsizliyi anlayışı. İnformasiya təhlükəsizliyinin əsas tərkib hissələri.	2	2		
1.2.	İnformasiya təhlükəsizliyi problemin vacibliyi və mürəkkəbliyi. İnformasiya təhlükəsizliyinə obyektyönümlü yanaşma. İnformasiya təhlükəsizliyinə ənənəvi yanaşmanın mənfi cəhəti.	2	2		
1.3.	Ən geniş yayılmış təhlükələr. Təhlükələrin əsas təyini və təsnifat kriteriləri. İnformasiya mühafizəsinin nəzəri modeli. Təhlükələtin əsas növləri və əlamətləri.	2	2		
	Bölmə üzrə cəmi	**6**	**6**		
II	Kompüter şəbəkələrində informasiya təhlükısizliyinin təmim olunması. Kompüter virusları və onun növləri.	2	2		
2.1.	İnformasiya mühafizəsində biometrik autentifikasiya məsələləri. Ekranlaşdırma.	2	2		
2.2.	İnformasiya təhlükəsizliyi. Dünya dövlətlərində informasiya təhlükəsizliyinin tarixi inkişaf istiqamətləri.	2	2		
2.3.	İnformasiya mühafizəsinin metod və vasitələri. İnformasiya mühafizəsinin aparat-proqram metodu.	2	2		
2.4.	İnformasiyanın müasir mühafizə olunma üsulları. Kriptoqrafiya. Kriptoqrafiyanın əsas anlayışları. Kriptoqrafiyanın məqsədi.	2	2		
	Bölmə üzrə cəmi	**10**	**6**		
III.	Kriptoqrafiyanın riyazi əsasları. Ədədlər nəzəriyəsi. Sadə və mürəkkəb ədədlər. Ən böyük ortaq bölünən. Evklid alqoritmi.	2	2		
3.1.	Kriptoqrafik sistemlərə qoyulan tələblər. Şifr. Şifrlərin təsnifatı. Şifrlərin formal modeli. Şifrlərin dözümü.	2	2		
	Bölmə üzrə cəmi	4	6		
IV.	Klassik kriptoqrafiya. Şifrləmə üsulları-yerdəyişmə, əvəzetmə, qammalama və blok şifrləri.	2	2		
4.1.	Şifrləmə alqoritmiləri. Deff-Helman alqoritmi, Sezar şifrləmə alqoritmi. Vijiner şifrləməsi. Şifrləmə alqoritmlərin təsnifatı.	2	2		
4.2.	Pleyfer şifrləmə alqoritmi və onun əsasları. Biqrammalar.	2	2		
4.3.	Kriptosistemlər haqqında ümumi məlumatlar. Şifrləmə və deşifrləmə. Simmetrik və asimmetrik üsullar.	2	2		

4.4.	Müasir şifrləmə alqoritmləri və onların nəzəri əsasları.	2	2		
	Bölmə üzrə cəmi	**10**			
V.	Şifrləmə standartı. DES alqoritmi. DES şifrləmə standartı.	2	2		
5.1.	Faylların blok-blok simmetrik şifrlənməsi. Feyştel şəbəkəsi, TEA alqoritmi. İnformasiyanın bit-bit şifrlənməsi.	2	2		
5.2.	Açıq və gizli açarlı kriptosistemlər. RSA alqoritmi.	2	2		
5.3.	RSA şifrləmə sistemi. Evklid alqoritmi.	2	2		
5.4.	RSA alqoritmin tətbiqi. Həticələr.	2	2		
5.5.	Elektron imza texnologiyası. Elektron imza haqqında məlumat. Elektron imzaya qoyulan tələblər.	2	2		
5.6.	Rəqəm imzası sxemləri. RSA imza sxemi.	2	2		
5.7.	Autentifikasiya, protokollar. Müəlliflik hüquqlarının müdafiəsi.	1	1		
	Bölmə üzrə cəmi	**15**	**15**		
	Fənn üzrə cəmi	**45**	**45**		

1. Məşğələ dərslərinin mövzuları

İnformasiyanın mühafizə olunma üsulları. Kriptoqrafiya haqqında ümumi məlumat.	**2**
Kriptoqrafiyanın əsas terminləri və anlayışları. Kriptoqrafiya və kriptoanaliz.	**2**
Kriptoqrafiyanın riyazi əsasları. Ədədlər nəzəriyəsi. Sadə və mürəkkəb ədədlər.	**2**
Faylların kodlaşması və dekodlaşması.	**2**
Simmetrik kriptosistem. Faylların skremblerlə bit-bit şifrlənməsi.	**2**
Faylların blok-blok şifrlənməsi. Feyştel şəbəkəsi. DES şifrləmə standartı.	**2**
Asimmetrik kriptosistem. RSA alqoritmi. Açıq və gizli açarlı yaradılması.	**2**
Elektron imza texnologiyası. Elektron imza haqqında məlumat.	**2**
Fənn üzrə cəmi	**15**

2. Sərbəst işlərin mövzuları

İnformasiya təhlükəsizliyi anlayışı. İnformasiya təhlükə-sizliyinin əsas tərkib hissələri
İnformasiya mühafizəsinin nəzəri modeli. Təhlükələtin əsas növləri və əlamətləri
İnformasiyanın müasir mühafizə olunma üsulları. Kriptoqrafiya.
Kriptoqrafiyanın riyazi əsasları. Evklid alqoritmi
Klassik kriptoqrafiya. Şifrləmə üsulları
Şifrləmə alqoritmiləri və şifrləmə üsulları- Sezar, Vijiner, Pleyfer, Vernam.
Şifrləmə stan dartı. DES alqoritmi. DES şifrləmə standartı.
Faylların bib-bit və blok-blok şifrlənməsi.
Açıq və gizli açarlı kriptosistemlər. RSA alqoritmi
Elektron imza haqqında məlumat. Elektron imzaya qoyulan tələblər

ƏDƏBIYYAT

1. R.M.Əliquliyev, Y.N.İmamverdiyev “Kriptoqrafiyanın tarixi”, “İnformasiya texnologiyaları mətbəsi” Bakı-2006 il.

2. R.M.Əliquliyev, Y.N.İmamverdiyev “Kriptoqrafiyanın əsasları”, “İnformasiya texnologiyaları mətbəsi” Bakı-2007 il.

3. İ.J.İbrahimzadə, M.A.İsmayılov, Y.B. Sərdarov “Kompüter sistemlərində mühafizənin təşkili” I və II cild, Bakı-2007 il.

4. Э.Таненбаум “Компютерные сети” издательство “Питер ”, 2005 год.

5. Yaşenko V.V. “Kriptoqrafiyanın əsas anlayışları”, Riyazi maarif. 1998.

Əyani və digər tədris-metodiki vəsaitlərin, metodiki materialların siyahısı

s/s	Adı	Mövzu planı üzrə mövzunun şifri	Miqdarı
1.	Slaydlar		Elektron
2.	Fənnin öyrənilməsinə dair metodiki göstərişlər		Elektron və çap nüsxəsi

“Kriptoqrafik mühafizənin təşkili” fənninin sillabusu “AKT –fakültəsinin” (şifr --------) ixtisasının tədris planı və “İnformasiya mühafizəsi” fənninin proqramı əsasında tərtib olunmuşdur.

Sillabus “Kompüter sistemləri və şəbəkələri” kafedrasının iclasında müzakirə olunmuşdur.

(“__ ”_____2012 il tarixli iclas “ __ ” N-li protokol)

Kafedra müdiri, t.e.d. Musayev V.H.