**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: 050632 – "İnformasiya texnologiyaları və sistemləri mühəndisliyi"**

**Təhsil pilləsi: Bakalavr**

**Təhsil müddəti: 4 il**

**"Kompüter təhlükəsizliyinin nəzəri əsasları və təşkili"**
fənnin

# PROQRAMI

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

**AKT fakültəsinin Elmi Şurasında təsdiq edilmişdir: ____ saylı protokol**
**«___»_____2014-cü il**

**Kafedra müdiri:_____ V.H.Musayev**

**AKT fakültəsinin dekanı:____H.T.Qurbanov**

**Bakı-2014**

# TEMATİK PLAN

| Böl-mələr | Mövzular | Auditoriya saatlarının miqdarı | | | | |
|---|---|---|---|---|---|---|
| | | Ümumi saat | Müh. | Məşğ | Lab. | Kurs işi |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1. | 1. Giriş. İnformasiyanın mühafizəsinin və təhlükəsizliyinin əsas anlayışı, məqsədi və vəzifəsi. | 4 | 2 | | 2 | |
| 2. | Mühafizə obyekti və predmeti.<br>2.1. Mühafizə predmeti<br>2.2. İnformasiya mühafizəsi obyekti. | 4 | 2 | | | |
| 3. | Kompüter sistemlərində (KS) informasiya təhlükəsizliyinin mənbələri.<br>3.1. Təsadüfi təhlükələr.<br>3.2. Bilərəkdən (qəsdən) təhlükələr. | 4 | 2 | | 2 | |
| 4. | KS-də informasiya mühafizəsinin hüquqi və təşkilati üsulları.<br>4.1. İnformasiya təhlükəsizliyi sahəsində hüquqi tənzimlənmə.<br>4.2. KS-də informasiya mühafizəsinin təşkili üsullarının ümumi xarakteriztikası. | 4<br>4 | 2<br>2 | | 2<br>2 | |
| 5. | KS-də təsadüfi həmlələrdən informasiya mühafizəsi.<br>5.1. İnformasiyanın təkrarlanması.<br>5.2. KS-də etibarlılıq anlayışı və onun riyazi əsasları.<br>5.3. Səhv əməliyyatların blakirovka edilməsi.<br>5.4. KS-də istifadəçilərin və xidməti heyyətin qarşılıqlı hərəkətlərinin optimallaşdırılması.<br>5.5. Qəza və fövqəladə hallardan itkilərin minimum-laşdırılması. | 4<br>4 | 2<br>2 | | 2<br>2 | |
| 6. | KS-də icazəsiz müdaxilələrdən informasiyanın mühafizəsi.<br>6.1. KS-də informasiyaya müdaxilənin məhdudlaşdırılması.<br>6.2. Proqram vasitələrinin nüsxələşdirilmədən (kopyalanması) və tədqiq edilmədən mühafizəsi. | 5 | 2 | | 3 | |
| 7. | İnformasiya mühafizəsinin kriptoqrafiki təşkili.<br>7.1. İnformasiyanın kriptoqrafiki çevirmə üsullarının əsas təsnifatı.<br>7.2. Şifrələmə. Əsas anlayışlar. Onların riyazi əsasları.<br>7.3. Simmetrik açarla şifrələmə üsulları.<br>7.4. Açıq açarla şifrələmə sistemləri.<br>7.5. Şifrələmə standartları və alqoritmləri<br>7.6. KS-də informasiyanın kriptoqrafik mühafizənin istifadə edilnə perespektivləri.<br>7.7. Deşifrələmə. Əsas anlayışlar onların riyazi | 6<br>2<br>4 | 2<br>2 | 2<br>2 | 2<br>2 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | əsasları.<br>7.8. Asimmetrik açarla şifrələmə üsulları və alqoritmləri.<br>7.9. Deşifrələmə standartları və alqoritmlər. | | | | | |
| 8. | Paylanmış kompüter sistemlərdə (PKS) informasiya mühafizəsinin təşkili.<br>8.1. Paylanmış KS-in arxitekturası.<br>8.2.PKS-də informasiya mühafizəsinin məxsusi xüsusiyyətləri.<br>8.3 PKS-in OSI səviyyəsində informasiya mühafizəsi.<br>8.4. Əlaqə kanallarında informasiya mühafizəsi.<br>8.5. Verilənlər bazasında informasiya mühafizəsinin məxsusi xüsusiyyətləri.<br>8.6. Kriptoqrafiki protokollar, əsas anlayışları və növləri.<br>8.7. Audit və protokollaşdırma. Konfidensialllıq və onun parametrləri. | 4<br>2<br>4 | 2<br><br>2 | <br>2<br> | 2<br><br>2 | |
| 9. | İnformasiya mühafizəsi sistemləri kompleksinin qurulmasının təşkili.<br>9.1. Mühafizə olunan KS-in yaradılması, (təşkili) konsepsiyası.<br>9.2. İnformasiya mühafizəsi sistemləri kompleksinin yaradılması mərhələləri.<br>9.3. İnformasiya mühafizəsi sistemləri kompleksinin modelləşdirilməsi.<br>9.4. Kompüter sistemlərində informasiya mühafizəsinin səmərəlilik göstəricilərinin və kriptoqrafiyaların seçilməsi.<br>9.5. İnformasiya mühafizəsi sistemləri kompleksinin yaradılması (işlənməsi) məsələlərinin riyazi qoyuluşu.<br>9.6.İMSK-in səmərəliliyinin qiymətləndirilməsi.<br>9.7.İMSK-inin təşkilinin strukturunun qurulması. | 6<br>4<br>2 | 2<br>2<br> | 2<br>2<br>2 | 2<br>2<br> | |
| 10. | Məxfi sistemlərin təşkili.<br>10.1. Məxfi sistemin riyazi modeli.<br>10.2. Məxfi sistemlərin təşkili prinsipləri.<br>10.3. Məxfi sistemlərin yeni istiqamətləri və növləri. | | 2 | | 2 | |
| . | Kompüter şəbəkələrində təhlükəsizliyin təmini təşkili.<br>11.1. Kompüter şəbəkələr, növləri və qurulma prinsipləri. Kompüter şəbəkələrində də təhlükəsizliyin riyazi əsasları.<br>11.2. Kompüter şəbəkələrində təhlükəsizliyin təminində ekranlaşdırma, şlüzlər və kriptomarşrutlayıcılar.<br>11.3. Kriptoserver, növləri və təşkili. Server və işçi stansiyaların təhlükəsizliyinin təmini. | | 2 | | 2 | |

## Məşğələlərin siyahısı və adları

| Bölmələr | Ишин ады | Məş | |
|---|---|---|---|
| 1 | KS-də mühafizə məsələləri<br>1.1 KS-nin arxitekturası.<br>1.2 Paylanmış KS- də informasiya mühafizəsinin xüsusiyyətləri.Verilənlər bazasında informasiya mühafizəsinin riyazi xüsusiyyətləri.<br>1.3 Kompüter sistemlərində informasiya təhlükəsizliyinin təşkili və qurulmasının kompleks tədbirləri. | 2 | |
| 2 | Kompüterlərdə təhlükəsizliyin təmininin riyazi və müasir tələbləri.<br>2.1 Təhlükəsizliyin mənbələri kriptoqrafiya.<br>2.2 Kriptoqrafiyanın riyazi əsasları.<br>2.3 Şifrələmə və deşifrələmə alqoritmləri.<br>2.4 RSA, DES, İDEA, QOSZ- 28147- 89 standartları və iş prinsipləri. | 2 | |
| 3 | Kriptoqrafiki protokollar, əsas anlayışlar.<br>3.1 Audit və protokollar, Təhlükəsizliyin təminində istifadə edilən protokolların növləri.<br>3.2 Konfidensialllıq və onun papametrləri, Risk və onun hesablanması. | 2 | |
| 4 | Kompüter sistemlərində təhlükəsizliyin təmini.<br>4.1 KS-də baş verən təhlükə mənbələri. KS-də kriptoqrafiki açarlar və onların idarə edilməsi.<br>4.2.KS-də təhlükəsizliyin təşkilində hüquqi əsaslar və tədbirlər. KS-də mühafizənin proqram və texniki vasitələri. | 2 | |
| 5. | Kompüter şəbəkələrində təhlükəsizliyin təmini prinsipləri<br>5.1 Kompüter şəbəkələrinin təsadüfi təhlükələrdən mühafizəsi. Kompüter şəbəkələrində təhlükəsizliyin təminində ekranlaşdırma. Əlaqə kanalları səviyyəsində təhlükəsizliyin təmini.<br>5.2 İnternet və ya LKŞ-də olan hücumlardan mühafizə vasitələri və üsulları.<br>5.3.İşçi stansiyaların təhlükəsizliyinin təmini. Serverin təhlükəsizliyinin təmini NİS, Portmap, FTP, NFS, HTTP-mühafizə. | 2<br>2<br>1<br>2 | |
| | **Bölmə üzrə cəmi** | **30** | |

## Laborotoriya işlərinin siyahısı və adları

| Bölmələr | Ишин адı | Lab. | |
|---|---|---|---|
| 1. | 2 | 3 | 4 |
| 2. | Təhlükəsizliyin obyekti və sahələri. Təhlükəsizlik mənbələri və növləri. | 2 | |
| 3. | Paylanmış KS-də mühafizə məsələləri, Paylanmış KS-nin arxitekturası və mühafizəsinin xüsusiyyətləri.<br>Verilənlər bazasında informasiya mühafizəsinin riyazi xüsusiyyətləri, informasiya təhlükəsizliyinin təşkili və qurulmasının kompleks tədbirləri. | 2<br>3 | |
| 4. | KS-də mühafizənin proqram və texniki vasitələri. | 2 | |
| 5. | Simmetrik və asimmetrik sistemlər. | 2 | |
| 6. | KS-də icazəsiz müdaxilələrdən informasiyanın mühafizəsi. | 2 | |
| 7. | Kompüterlərdə təhlükəsizliyin təmininin riyazi və müasir tələbləri.<br>Təhlükəsizliyin mənbələri kriptoqrafiya, Kriptoqrafiyanın riyazi əsasları.<br>Şifrələmə və deşifrələmə alqoritmləri.<br>RSA, DES, İDEA, QOSZ- 28147- 89 standartları və iş prinsipləri. | 2<br>2 | |
| 8. | Kriptoqrafiki protokollar, əsas anlayışlar.<br>Audit və protokollar. Təhlükəsizliyin təminində istifadə edilən protokolların növləri.<br>Konfidensialllıq və onun papametrləri. Risk və onun hesablanması. | 2<br>2 | |
| 9. | Kompüter sistemlərində təhlükəsizliyin təmini. KS-də baş verən təhlükə mənbələri. KS-də kriptoqrafiki açarlar və onların idarə edilməsi, hüquqi əsaslar və tədbirlər. | 2 | |
| 10. | Məxfi sistemlərin təşkili. Məxfi sistemin riyazi modeli və təşkili prinsipləri.<br>Kompüter şəbəkələrinin təsadüfi təhlükələrdən mühafizəsi və təhlükəsizliyin təminində ekranlaşdırma.<br>İnternet və ya LKŞ-də olan hücumlardan mühafizə vasitələri və üsulları. Serverin təhlükəsizliyinin təmini | 2<br>3 | |
| | **Bölmə üzrə cəmi** | **30** | |

**Mövzu 1. Təhlükəsizliyin təşkilinin məqsədi və vəzifəsi. Mühafizə obyekti və predmeti.**

Təhlükəsizliyin təşkilinin məqsədi, vəzifələri, **m**ühafizə predmeti, informasiya mühafizəsi obyekti və s. kimi məsələlər nəzərdən keçrləcəkdir.

Paylanmış KS-də mühafizə məsələləri, paylanmış KS-nin arxitekturası və mühafizəsinin xüsusiyyətləri haqqında mılumatlar veriləcək və onlarda təhlükəsizlik məsələlərinə baxılacaqdır. Verilənlər bazasında informasiya mühafizəsinin riyazi xüsusiyyətləri, informasiya təhlükəsizliyinin təşkili və qurulmasının kompleks tədbirləri haqqında məlumat verilməsi nəzərdə tutulur.

**Mövzu 2.. Kompüter sistemlərində informasiya təhlükəsizliyinin mənbələri.**

Paylanmış KS-də mühafizə və təhlükə mınbılıri məsələləri, onun növləri, təsadüfi təhlükələr və bilərəkdən (qəsdən) yaradılan təhlükələr haqqında izhat veriləcək. İnformasiya təhlükəsizliyi sayəsətinin hüquqi tənzimlənmə, KS-də informasiya mühafizəsinin təşkili üsullarının ümumi xarakteriztikası veriləcəkdir.

**Mövzu 3. Kompüterlərdə təhlükəsizliyin təmininin riyazi və müasir tələbləri.**

Təhlükəsizliyin mənbələri kimi kriptoqrafiya, kriptoqrafiyanın riyazi əsasları haqqında məlumat veriləcəkdir. Şifrələmə və deşifrələmə alqoritmləri, onların təşkili və proqramlarını qurulması haqqında geniş izahat veriləcək. RSA, DES, İDEA, QOST- 28147- 89 və s. kimi alqoritmlər, standartlar və iş prinsipləri haqqında ətraflı izahatlar veriləcəkdir. Bununla yanaşı olaraq təhlükəsizliyin sistemlərdə və şəbəkələrdə kriptoqrafiki protokolların köməyi ilə təşkilinin, audit və protokollarşdırma, Konfidensialllıq və onun papametrləri, risk və onların hesablanması nəzərdən keçriləcəkdir.

**Mövzu 4. Məxfi sistemlərin təşkili. İnformasiya mühafizəsi sistemləri kompleksinin qurulmasının təşkili.**

Məxfi sistemin riyazi modeli. Məxfi sistemlərin təşkili prinsipləri. Məxfi sistemlərin yeni istiqamətləri və növləri**.** Mühafizə olunan KS-in yaradılması, (təşkili) konsepsiyası. İnformasiya mühafizəsi sistemləri kompleksinin yaradılması mərhələləri. İnformasiya mühafizəsi sistemləri kompleksinin modelləşdirilməsi. Kompüter sistemlərində informasiya mühafizəsinin səmərəlilik göstəricilərinin və optimallıq kriptoqrafiyalarının seçilməsi. İnformasiya mühafizəsi sistemləri kompleksinin yaradılması (işlənməsi) məsələlərinin riyazi qoyuluşu. İMSK-in səmərəliliyinin qiymətləndirilməsi. İMSK-ini n təşkili strukturunun qurulması.

**Mövzu 5. Kompüter şəbəkələrində təhlükəsizliyin təmini təşkili**

Kompüter şəbəkələr, növləri və qurulma prinsipləri. Kompüter şəbəkələrində də təhlükəsizliyin riyazi əsasları nəzərdən keçriləcəkdir. Kompüter şəbəkələrində təhlükəsizliyin təminində istifadə edilən aparat və texniki vasitələr, o cümlədən ekranlaşdırıcılar, şlüzlər və kriptomarşrutlayıcılar haqqında məlumatlar veriləcəkdir. Serverlər, işçi stansiyaların, kriptoserver, onların növləri və təşkilində təhlükəsizliyinin təmini veriləcəkdir.

# ƏDƏBİYYAT


1. Т.М. Аскерова. Защита информации и информационная безопасность. Москва, 2201.
2. Э. Таненбаум – «Компьютерные сети», издательство «Питер». 2005г.
3. Т.А. Партыка, И.И. Попов «Информационная безопасность» Москва, 2007.
4. Мельников В. Защита информации в компьютерных системах. – Москва, 1997.
5. Гайкович В., Першин А. Безопасность электронных банковских систем. Москва, 1994.
6. Голотенко В. Информационная безопасность – обзор основных положений.- Москва, 1996.
7. Галатенко В. А. Информационная безопасность. Москва, Финансы и статистика, 1997.
8. А.Д.Смирнов Архитектура вычислительных систем М, 1990.
9. А.Н.Ларионов и др. Вычислительные комплексы, системы и сети М.,1987.
10. V.H.Musayev və başq. Kompüterlərin və sistemlərin arxitekturası Bakı, 2007.

**Proqramı tərtib etdi:**

V.H.Musayev, K.Ə.Əbilov

Proqram "Kompüter sistemləri və şəbəkələri" kafedrasının "__"_____2014-cü il tarixli iclasında (№-__saylı protokol) müzakirə edilmişdir.

Kafedra müdiri: professor V.H.Musayev

Proqram AKT fakültəsinin metodqrupunun "__"_____2014-cü il tarixli iclasında (№__ saylı protokol) müzakirə edilmişdir

Metodqrupun sədri: dos. E.A.Balıyev

Proqram AKT fakültəsənin Elmi Şurasının "__"_____2014-cü il tarixli iclasında (№__saylı protokol) müzakirə edilmişdir.

AKT fakültəsinin dekanı: dos. H.T.Qurbanov