Azərbaycan Respublikası Təhsil Nazirliyi
Bakı İdarəetmə və Texnologiya Kolleci

“İnformasiya sistemlərində təhlükəsizliyin təmini”

fənninin

PROQRAMI

040546 - “Avtomatlaşdırılmış sistemlərin və hesablama texnikasının proqram təminatı”
040545- “Kompüter şəbəkələri və hesablama texnikasının təmiri və servis xidməti”
040543- “Kompüter şəbəkələri”
040547- “İnformasiya işlənməsinin və idarəetmənin avtomatlaşdırılmış sistemləri”
040548 – “İnformasiya texnologiyası sistemləri

Azərbaycan Respublikası Təhsil Nazirliyi Bakı İdarəetmə və Texnologiya Kollecinin Metodiki şurasının 15 sentyabr 2017-ci il tarixli iclasının qərarı ilə təsdiq edilmişdir.
(Protokol № 1)

BAKI-2017

Tərtib edən:

Bakı İdarəetmə və Texnologiya Kollecinin ixtisas müəllimi — Əliyeva Elnarə Elman

Redaktor:

Bakı İdarəetmə və Texnologiya Kollecinin ixtisas müəllimi — Ədilzadə Zeynəb Həsən

Rəy verənlər:

Bakı İdarəetmə və Texnologiya Kollecinin ixtisas müəllimi — 1.Əliyeva Vüsalə İsmayıl

Azərbaycan Texniki Universiteti Professor, texniki elmlər doktoru — 2.Musayev Vidadi Həsən

Azərbaycan Texniki Universiteti baş müəllim — 3.Qəmbərov Mübariz Məmmədəli

İZAHAT VƏRƏQİ

İnformasiya sistemlərində təhlükəsizliyin təmini fənn proqramının tədrisi 60 saat nəzərdə tutulmuşdur: 30 saat mühazirə və 30 saat məşğələ.

Tədris proqramının məqsədi tələbələrə informasiya təhlükəsizliyinin təmin olunması probleminin vacibliyini və aktuallığını, informasiya istifadəçilərinə ziyan vurmağa səbəb olan təbii və ya süni xarakterli təsadüfi yaxud qəsdli təsirlərdən informasiyanın mühafizə olunmasını öyrətməkdir.

Tədris proqramında informasiyanın mühafizəsi anlayışı, kompyuter sistemlərində və şəbəkələrində təhlükələrin təsnifatı, əsas növləri və əlamətləri, təhlükəsizliyin təmin olunmasının texnoloji aspektləri, informasiyanın kriptoqrafik müdafiəsi prinsipləri və s. mövzular açıqlanır.

Cəmiyyətin və dövlətin həyatında informasiyanın, informasiya resurslarının və texnologiyalarının rolunun artması informasiya təhlükəsizliyi məsələlərini ön plana çıxarır.

MÖVZULAR ÜZRƏ SAATLARIN PAYLANMASI

№	Mövzuların adı	Mühazirə	Seminar
1	İnformasiya təhlükəsizliyi anlayışı. Kompyuter sistemləri və şəbəkələrində təhlükələrin təsnifatı	2	2
2	Kompyuter sistemlərində təhlükələrin əsas növləri və əlamətləri	2	2
3	Kompyuter sistemlərində informasiya təhlükəsizliyi və mühafizəsinin üsulları və vasitələri	2	2
4	İnformasiya mühafizəsi aparat vasitələrinin təyinatı və xarakterləri	2	2
5	İnformasiya mühafizəsini təmin edən proqram vasitələri	2	2
6	Təhlükəsizliyin və mühafizənin təşkilində protokollaşdırma və audit	2	2
7	Ziyanverici proqramalar(virus,soxulcan,məntiqi bombalar troyan obyektlər, backdoor)	2	2
8	Elektron rəqəmsal imza. Heş-funksiya	2	2
9	Təhlükəsizlik siyasəti. Kompyuter cinayətkarlığı	2	2
10	Şəbəkələrin informasiya təhlükəsizliyinin təmin olunması	2	2
11	Əməliyyat sistemlərində təhlükəsizliyin təminatı	2	2
12	Kriptoqrafiya. İnformasiyanın kriptoqrafik müdafiəsinin prinsipləri	2	2
13	İnformasiya təhlükəsizliyinin və mühafizəsinin biometrik məsələləri	2	2
14	Protokollar vasitəsilə ötürülmüş verilənlərin müdafiəsi	2	2
15	Virtual lokal şəbəkələrdə təhlükəsizliyin təşkili	2	2
Cəmi: 60 saat			

MÖVZULAR VƏ ONLARIN İZAHI

Mövzu 1. **İnformasiyanin təhlükəsizliyi anlayışı. Kompyuter sistemləri və şəbəkələrində təhlükələrin təsnifatı. – 4 saat**

İnformasiya təhlükəsizliyi, informasiyanın mühafizəsi və onu dəstəkləyən infrastrukturun istənilən təsadüfı və ya qanunauyğun təsirlərdən qorunması, lazım olan kompleks tədbirlər. Təhlükəsizliyin aktuallığı və vacibliyi. İnformasiyanın konfidensiallığının pozulmasına yönələn təhlükələr. İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr. Əlyetənliyin pozulmasına yönələn təhlükələr .

Mövzu 2. **Kompyuter sistemlərində təhlükələrin əsas növləri və əlamətləri. – 4 saat**

HS-in resurslarından icazəsiz istifadə edilməsi. HS-in resurslarından düzgün istifadə edilməməsi. Proqram və aparat vasitələrində səhvlərin aşkar edilməsi. Rabitə xətlərində və ötürmə sistemlərində verilənlərin ələ keçirilməsi. Elektromaqnit şüalanmaların icazəsiz qeydə alınması. Hesablama sistemi qurğularının, informasiya daşıyıcılarının və sənədlərin oğurlanması. Hesablama sistemi komponentlərinin, informasiyanın ötürülmə vasitələrinin tərkibinin icazəsiz dəyişdirilməsi və ya sıradan çıxarılması.

Mövzu 3. **Kompyuter sistemlərində informasiya təhlükəsizliyi və mühafizəsinin üsulları və vasitələri. – 4 saat**

İnformasiya mühafızəsinin üsulları:

- Fiziki mühafizə üsulu ilə informasiya təhlükəsizliyi;
- Aparat mühafizə üsulu ilə informasiya təhlükəsizliyi;
- Proqram mühafizə üsulu ilə informasiya təhlükəsizliyi ;
- Təşkilati mühafizə üsulu ilə informasiya təhlükəsizliyi üsullar.

Mövzu 4. **Informasiya mühafizəsi aparat vasitələrinin təyinatı və xarakterləri. – 4 saat**

Təhlükəsizliyi təmin edən aparat proqram vasitələrini beş əsas qrupa bölmək olar:

Birinci qrup: sistemin identifikasiya və autentifikasiya sistemləri

İkinci qrup: sitemin təhlükəsizliyini yüksək səviyyədə təmin edən disk verilənlərinin şifrələnməsi sistemi

Üçüncü qrup: kompyuter şəbəkəsi ilə ötürülən verilənlərin şifrələnməsi sistemi

Dördüncü qrup: mühafizə vasitələrini elektron verilənlərin autentifikasiya sistemi

Beşinci qrup: ən məxfi informasiyaların idarəetmə vasitələri.

Mövzu 5. **İnformasiya mühafizəsini təmin edən proqram vasitələri. – 4 saat**

Proqram mühafizə vasitələrinə mühafizə funksiyasını yerinə yetirən və verilənlərin emalı sisteminin proqram təminatı tərkibinə daxil olan xüsusi proqramlar (antiviruslar və s.). Antivirusların fəaliyyətlərindən asılı olaraq antivirus proqramlarının sinifləri:

- detektorlar
- doktorlar
- müfəttişlər
- doktor-müfəttişlər
- süzgəclər
- vaksinlər
- immunizatorlar

Mövzu 6. **Təhlükəsizliyin və mühafizənin təşkilində protokollaşdırma və audit. – 4 saat**

İstifadəçi və administratorların hesabat verməsinin olmasını təmin etmək. İnformasiya təhlükəsizliyini pozma cəhdlərinin aşkar olunması.Problemlərin aşkar olunması və analizi üçün informasiyanın təqdim olunması.Təhlükəsizlik sisteminin auditi – təhlükəsizlik sisteminə aid informasiyanın tanınması, qeydə alınması, saxlanması və analizi

Mövzu 7. **Ziyanverici proqramlar (virus,soxulcan,məntiqi bombalar ,troyan obyektlər, backdoor). – 4 saat**

Ziyanverici proqramlara aiddir:

- kompüter virusları;
- soxulcanlar;
- məntiqi bombalar;
- troyan obyektlər;
- backdoor (“Xəlvəti giriş”) proqramları;
- kompüter sistemlərinə icazə verilməmiş daxilolma əldə etməkdən ötrü proqram vasitələri;

Kompüter sistemlərinə icazə verilməmiş daxilolma əldə etməkdən ötrü proqram vasitələri:phishing, spyware proqramları, adware proqramları, klaviatura casusu.

.

Mövzu 8. **Elektron rəqəmsal imza. Heş-funksiya. – 4 saat**

Elektron sənədlər ilə mübadiləni yerinə yetirdikdə alınmış sənədin müəllifinin, onun doğru olub-olmamasını və informasiyanın bütöv olmasının quraşdırılması. Elektron imza.

Rəqəmli sertifikat- səlahiyyətli orqan tərəfindən imzalanmış məlumat.Kompüter sisteminin istifadəçilərinin parollarını şifrləmək və elektron imza yaratmaqdan ötrü heşləmə funksiyasından geniş istifadə olunması.

Mövzu 9. **Təhlükəsizlik siyasəti. Kompyuter cinayətkarlığı. – 4 saat**

Security policy (təhlükəsizlik siyasəti) − əsasında konfidensial informasiyanın idarə edilməsi, yayılması və mühafizəsi təşkil olunan qanunlar, qaydalar və praktiki təcrübələr. "Narıncı kitabda" etibarlı sistemi " giriş hüququnu pozmadan müxtəlif məxfilik dərəcəsinə malik informasiyanın istifadəçilər qrupu tərəfindən eyni zamanda emalını təmin etmək üçün yetərli aparat və proqram təminatı istifadə edən “sistem" kimi müəyyən edilməsi. Kibercinayətkarlıq. Hakerlər. Proqram təminatı piratçılığı.

Mövzu 10**. Şəbəkələrin informasiya təhlükəsizliyinin təmin olunması. – 4 saat**

İstifadəçilərin identifikasiyası və autentifikasiyası vasitələri. Kompyuterdə saxlanılan və şəbəkə ilə ötürülən informasiyanın şifrləmə vasitələri. Şəbəkəarası ekranlar.

Şəbəkələrin idarəetmə sistemlərinin əsas komponenti (təşkiledicisi), informasiyanın təhlükəsizliyi sistemi. Sistem aşağıdakıları yerinə yetirməlidir:

- Şəbəkə təhlükəsizliyi vasitələrinə mərkəzləşdirilmiş və operativ idarəetmə təsiri göstərmək;
- Operativ qərarlar qəbul etmək üçün informasiya təhlükəsizliyinin vəziyyəti haqqında obyektiv informasiya əldə etməyə imkan verən audit və monitorinq keçirmək.

Mövzu 11**.Əməliyyat sistemlərində təhlükəsizliyin təminatı. – 4 saat**

Əməliyyat sisteminin effektiv və etibarlı müdafiəsinin təşkili. Əməliyyat sistemlərinin hədələrdən təhlükəsizliyinin onların istifadə edilmə baxımından təsnifləndirilməsi:

- Hücumun məqsədinə görə;
- Əməliyyat sisteminə etdiyi təsirin xarakterinə görə;
- Əməliyyat sisteminə təsir prinsipinə görə;
- Bədniyyətli insan tərəfindən müdafiənin pis vəziyyətə salınması növünə görə.

Mövzu 12. **İnformasiyanın kriptoqrafik müdafiəsinin prinsipləri. – 4 saat**

Verilənlərin dəyişdirilməsi və onların müdafiəsinə istiqamətləndirilməsi.Qeyri - qanuni istifadəçilərdən qorunma. Məlumatların şifrələnməsi . Şifrləmənin simmetrik(şifrləmə alqoritmlərindən DES, 3-DES, IDEA, FEAL, Skipcack, RC2, RC4, RC5, CAST, Blowfish

kimi blok şifrləri və bir sıra axın şifrləri) və asimmetrik üsulları. Əvəz etmə ilə şifrləmə.Yerlərini dəyişdirmək üsulu ilə şifrləmə.Açarlardan istifadə edən şifrləmə üsulları.

Mövzu 13. **İnformasiya təhlükəsizliyinin və mühafizəsinin biometrik məsələləri. – 4 saat**

İnformasiya təhlükəsizliyi və mühafizəsində biometrik audentifikasiya məsələləri.

Audentifikasiya − identifikasiya olunan (tanınan) subyektin kim olduğunu təsdiq edən parol (Parol [password], yalnız verilənlərdən istifadə etmək hüququ olan şəxsin bildiyi simvollar yığını), biometrik parametrlər (barmaq izlərinə görə identifikasiya, gözün qüzehli qişasının şəklinə görə identifikasiya, nitqin özəlliklərinə görə identifikasiya, üzün təsvirinə görə identifikasiya, ovucun cizgilərinə görə identifikasiya) və s. kimi məlumatların subyektdən əldə edilməsi.

Mövzu 14. **Protokollar vasitəsilə ötürülmüş verilənlərin müdafiəsi. – 4 saat**

Verilənlərin IP-də təhlükəsiz ötürülməsi. İP təhlükəsizliyini təmin edən protokollar. Verilənlərin İP -də təhlükəsiz ötürülməsi. AH(Authcntication Hcader) və ESP(Encapsulating Security Payload) protokolları vasitəsilə otürülmüş verilənlərin müdafiəsi. Naqilsiz şəbəkənin təhlükəsizliyi

Mövzu 15**. Virtual lokal şəbəkələrdə təhlükəsizliyin təşkili. – 4 saat**

VPN-başqa bir şəbəkənin üzərində yaradılmış (qurulumş) məntiqi şəbəkə (əsasəndə internet) . VPN-in iki əsas sinfi: müdafiə olunan və etibarlı .Texniki məsələlərin həll edilmə arxitekturasına görə VPN-in sinifləri :

1.Korporativ daxili.

2.Uzaqlaşdırılmış əlçatanlığı olan VPN.

3.Korporativarası VPN (extranet VPN).

ƏDƏBİYYAT

1.Барабанова М.И.Кияев “Информационные технологии системы, сети, безопасность в системах и сетях”.

2.С.И.Макаренко “Информационная безопасность”.

3.В.Шаньгин “Компьютерная безопасность информационных систем”.

Bakı İdarəetmə və Texnologiya Kollecinin ixtisas fənn müəllimi Əliyeva Elnarə Elman qızının orta ixitsas müəssisələrində təhsil alan tələbələr üçün "İnformasiya sitemlərində təhlükəsizliyin təmini" fənnindən hazırladığı proqrama

Rəy

"İnformasiya sistemlərində təhlükəsizliyin təmini" fənni üzrə tərtib olunmuş proqram 60 saatı əhatə edir. Bura həm nəzəri, həm də praktiki saatlar daxildir.

Mövzularda informasiya təhlükəsizliyinin aktuallığı, təhlükəsizliyin təmin olunmasının proqram və texniki vasitələri, biometrik mühafizə vasitələri İstifadəçilərin identifikasiyası və autentifikasiyası vasitələri; Kompyuterdə saxlanılan və şəbəkə ilə ötürülən informasiyanın sifrələmə vasitələri, şəbəkəarasi ekranlar, virtual şəxsi şəbəkələr və s. haqqında məlumat açıqlanmışdır.

Müəllim Əliyeva Elnarə Elman qızının "İnformasiya sistemlərində təhlükəsizliyin təmini " fənni üzrə tərtib etdiyi proqramın tədrisini mümkün hesab edirəm.

Bakı İdarəetmə və Texnologiya Kollecinin ixtisas müəlimi **Əliyeva Vüsalə İsmayıl**