Kurs: İnformasiya təhlükəsizliyinin əsasları

Kursun müddəti 4 gün (32 saat)

Kursun proqramı

Modul 1. Informasiya təhlükəsizliyinin əsas anlayışları (2 saat)
Informasiya təhlükəsizliyinin tərifi. Informasiya mühafizəsinin predmeti və obyekti. Informasiya təhlükəsizliyinin üç aspekti. Dövlət sirri. Konfidensial informasiya və onun növləri. İnformasiya təhlükəsizliyi təhdidləri və onların təsnifatı.

Modul 2. Kompüter şəbəkələrinə hücumlar (4 saat)
Protokol analizatorları ilə trafikin dinlənilməsi və analizi. Məsafədəki qovşaq, şəbəkə barəsində informasiyanın toplanması. nmap proqramından istifadə
Qarşılıqlı əlaqə tərəflərindən birini əvəzləmək üçün şəbəkə infrastrukturuna hücumlar. ARP-spufinq. DNS-spufinq. ICMP vasitəsi ilə qovşağa yalançı marşrutun qəbul etdirilməsi. TCP birləşməsində tərəflərdən birinin əvəzlənməsi.
Xidmətdən imtina hücumları. Paylanmış xidmətdən imtina (DDoS) hücumları.
DDoS hücumların üçsəviyyəli və dördsəviyyəli modeli.

Modul 3. Informasiya təhlükəsizliyinin təmin edilməsi üsulları (2 saat)
Informasiya təhlükəsizliyinin təmin edilməsinə kompleks yanaşma. Informasiya təhlükəsizliyi sahəsində Azərbaycan Respublikası qanunvericiliyi. Təşkilatı tədbirlər. İnformasiya təhlükəsizliyi xidməti. Fiziki mühafizə. Mühəndis-texniki tədbirlər. Antivirus proqramlar. İdentifikasiya və autentifikasiya. Avtorizasiya. Protokollaşdırma və audit. Ekranlaşdırma.

Modul 4. Autentifikasiya metodları. Biometrik identifikasiya (2 saat)
Parollar. Sorğu-cavab protokolları. Sıfır bilik verməklə isbat. Fiat-Şamir protokolu. Biometrik texnoloiyaların növləri. Biometrik sistemlərin əsas parametrləri. Barmaq izinə görə identifikasiya. Biometrik pasportlar.

Modul 5. Kriptoqrafiyanın əsas elementləri (4 saat)
Kriptoqrafiyanın həll etdiyi məsələlər. Kriptoqrafiyanın əsas anlayışları. Kriptoqrafiyanın inkişaf mərhələləri. Klassik şifrlər: yerdəyişmə və əvəzetmə şifrləri. Kriptoqrafik hücumların növləri. Blok şifrləri. Feystel şəbəkələri. DES standartı. AES standartı. Axın şifrləri. Açarların idarə edilməsi. Açarların iyerarxiyası. Informasiyanın tamlığına nəzarət – heş funksiyalar. SHA-1 alqoritmi.

Modul 6. Açıq açarlı kriptosistemlər. Rəqəmsal imza. Açıq Açarlar İnfrastrukturu (2 saat)
Açıq açarlı şifrləmə konsepsiyası. Diffi-Hellman açar mübadiləsi sxemi. RSA kriptosistemi. Elektron imza və rəqəmsal imza. Rəqəmsal imza sxemləri. ElGamal imza sxemi. Açıq açar sertifikatı və onun formatı. Açıq Açarlar İnfrastrukturu (AAİ, PKİ). AAİ-nin komponentləri. AAİ-nin arxitekturası.

Modul 7. Şəbəkə təhlükəsizliyinin kriptoqrafik protokolları. Virtual xüsusi şəbəkələr (4 saat)
İPSec protokollar steki. SSL/TLS protokolu. PPTP, L2F və L2TP protokolları. PAP, CHAP və EAP protokolları. RADIUS, TACACS+ və Kerberos autentifikasiya protokolları. LDAP kataloqlar xidməti. HTTPS protokolu. Elektron poçtu mühafizə metodları.

Modul 8. Şəbəkələrarası ekranlar. Hücumların aşkarlanması sistemləri (2 saat)
Şəbəkələrarası ekranların növləri. Şəbəkələrarası ekranların əsas komponentləri.
Şəbəkələrarası ekranların əsasında şəbəkə mühafizəsinin əsas sxemləri.
Şəbəkələrarası ekranların tətbiqi üzrə tipik həllər.
Müdaxilələrin aşkarlanması sistemlərinin təsnifatı Müdaxilələrin aşkarlanması sistemlərinin arxitekturası və komponentləri. İnformasiyanın siqnatur və statistik analizi metodları. Doğru və yalan işədüşmələr.

Modul 9. Əməliyyat sistemlərinin təhlükəsizliyi (qısa xülasə). Verilənlər bazalarının təhlükəsizliyi (qısa xülasə) (4 saat)
Əməliyyat sistemlərinə təhdidlərin təsnifatı Təhlükəsiz əməliyyat sistemlərinin yaradılması prinsipləri Əməliyyat sistemlərinin mühafizə mexanizmləri. UNIX əməliyyat sistemi. Windows əməliyyat sistemi. Linux əməliyyat sistemi
Verilənlər bazası mühafizəsinin xüsusiyyətləri. Verilənlər bazasının istifadəçiləri. Verilənlər bazasına spesifik təhdidlər.

Modul 10. İnformasiya təhlükəsizliyi insidentlərinə cavabvermə (2 saat)
İnformasiya təhlükəsizliyi insidentləri. İnformasiya təhlükəsizliyi insidentləri üzrə standartlar. İnsidentə cavabvermə komandaları. İnsidentə cavabvermə prosesinin mərhələləri. İnsidentlərinə cavabvermə prosedurları. İnsidentin təhqiqatı

Modul 11. İnformasiya təhlükəsizliyi sahəsində standartlar (2 saat)
Narıncı kitab. Əsas anlayışlar. Təhlükəsizlik mexanizmləri. Təhlükəsizlik sinifləri. «Narıncı kitab»ın şəbəkə üçün interpretasiyası.
Paylanmış sistemlərin informasiya təhlükəsizliyi. X.800 tövsiyələri. Şəbəkə təhlükəsizlik servisləri. Şəbəkə təhlükəsizlik mexanizmləri.
İSO/İEC 15408 İnformasiya texnologiyalarının təhlükəsizliyini qiymətləndirmə meyarları. Funksional tələblər. Zəmanət tələbləri.

Modul 12. İnformasiya təhlükəsizliyinin idarə edilməsi (2 saat)
İSO 2700x standartları. Informasiya təhlükəsizliyini idarəetmə mərhələləri. Informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi. Informasiya təhlükəsizliyi siyasəti. Informasiya təhlükəsizliyi siyasətinin qurulması metodikası. Informasiya təhlükəsizliyini idarəetmə sisteminin auditi