Kurs: Elektron imza infrastrukturunun qurulması

Kursun müddəti: 4 gün (32 saat)

Kursun proqramı

Modul 1. Rəqəmsal imza (6 saat)
Rəqəmsal imza (Rİ) sxemlərinin təsnifatı. Məlumatın əlavəsi ilə və məlumatın bərpası ilə imzalar. Rİ-yə hücumlar. RSA, DSA, ECDSA, QOST P 34.10-2001 imza sxemləri. Rİ-nin praktik tətbiqi aspektləri (XML, ETSI).

Modul 2. Açarların idarə olunması texnikası (2 saat)
Əsasları və baza konsepsiyaları. Rİ və şifrləmə açarlarının idarə olunması problemi (generasiya, saxlama, ötürmə, istifadə etmə, geri çağırma, dəyişdirmə və s.). Açarların idarə olunmasında etibarlı üçüncü tərəflərin xidmətləri. Açarların təsnifatı və onların istifadəsinə məhdudiyyətlər, o cümlədən alqoritmlərin tipinə və sonrakı istifadə sahələrinə görə məhdudiyyətlər. Açıq açarların yayılması üçün texnologiyalar (o cümlədən, AAİ ilə rəqabət aparan texnologiyalar).
Açar materialının həyat tsikli. Açarların idarə olunması siyasəti, məqsədləri, metodları. Açarların həyat tsiklinin müxtəlif mərhələlərində onların mühafizəsinə tələblər. Saxlama və istifadə zamanı açarların mühafizəsinin metod və vasitələri.

Modul 3. Açıq açarlar infrastrukturu konsepsiyası (4 saat)
AAİ komponentləri və onların funksiyaları, onlara tələblər (sertifikasiya orqanları, reqistrasiya orqanları, sertifikatların sahibləri, kliyent proqram təminatı, AAİ informasiyasının saxlancları və s.).
AAİ arxitekturası. Sertifikasiya mərkəzlərinin mürəkkəb sisteminin varlığı halında inam modelləri. Sertifikatlar zənciri və sertifikasiya yolları. AAİ-ın sadə arxitekturları. Təşkilat üçün AAİ-nin arxitekturası. Hibrid arxitekturalar.

Modul 4. Rİ və informasiyanın kriptoqrafik mühafizəsi vasitələri (İKMV) tətbiqinin hüquqi aspektləri (2 saat)
Elektron qarşılıqlı təsirin iştirakçılarının maraqlarının hüquqi müdafiəsi. Qarşılıqlı təsirin iştirakçıları arasında münaqişələrin həlli. Elektron sənədlərin hüquqi qüvvəsi. Rİ imzası ilə imzalanmış sənədlərin sübut kimi qəbul olunması şərtləri. "Elektron imza haqqında" qanun və onun əsas müddəaları. Rİ və İKMV-lərinin istifadə olunmasının hüquqi bazasını təmin edən Azərbaycan Respublikası qanunları, Azərbaycan Respublikası Prezidentinin fərmanları, hökumətin qərarları, standartlar və digər normativ sənədlər. Fəaliyyətin akkreditasiyası, vasitələrin sertifikasiyası, sistemlərin attestasiyası.

Modul 5. X.509 standartının elektron sertifikatı (4 saat)
RFC 3280. Sertifikata əlavələr və onların istifadəsi. Sertifikatın əsas konteksti. Certifikatın və ona əlavələrin strukturu. Sertifikata əlavələrin verdiyi imkanlardan istifadə olunması.
Sertifikatların geri çağırılması. Geri çağırılma metodları. CRL-in istifadəsi. CRL-ə əlavələrin və CRL yazısına əlavələrin istifadəsi. Sertifikatın statusu haqqında informasiyanın bölünməsi. OCSP. Geri çağırılmanın digər imkanları.

Modul 6. AAİ-ın idarə olunması protokolları (4 saat)
AAİ-ın idarəedici tranzaksiyaları. Tranzaksiyaların modeli. AAİ-ın idarə olunması protokollarının müqayisə kriteriləri. PKCS #10. PKCS #10 + SSL (TLS). PKCS #10 + PKCS #7. CMP. SCEP. AAİ-ın idarə olunması protokollarının və tranzaksiya modellərinin seçilməsi.
AAİ-də informasiyanın yayılması. Saxlancların protokolları və atributları. X.500 texnologiyası və LDAP. FTP. HTTP. Elektron poçt. Sərhəd saxlancları.

Modul 7. AAİ qurulması üçün məhsulların qısa xülasəsi (4 saat)
Entrust, RSA, Baltimore, KriptoPro, Microsoft və s. AAİ-ın kliyent proqram təminatı. AAİ-ın fərz olunan kliyenti və abonenti tərəfindən dəstəklənən tranzaksiyaların minimal dəsti.
Microsoft, RSA Keon məhsulları əsasında AAİ-ın realizəsi. Kriptoqrafik xidmət provayderlərinin (Cryptographic Service Provider - CSP) və açar materialının aparat mühafizə vasitələrinin istifadəsi (e-Token və s.).

Modul 8. İKMV-də API-nin istifadəsi (6 saat)
Kriptoqrafik funksiyaların realizəsi üçün istifadə olunan API-ların xülasəsi. GSS-API, JCA API, CDSA, PKCS #11. MS Crypto API 2.0. Dəstəklənən funksiyalar (sertifikatları saxlama funksiyaları, sertifikatları kodlama/dekodlama funksiyaları, kriptoqrafik funksiyalar, aşağı səviyyə funksiyaları və sadələşdirilmiş funksiyalar). Sistem səviyyəli kriptoqrafik provayderlər.