Kurs: Elektron imzanın tətbiqləri

Kursun müddəti: 2 gün (16 saat)

Kursun proqramı

Modul 1. Elektron sənəd dövriyyəsi və rəqəmsal imza (Rİ). Rİ-nin informasiya sistemlərində istifadəsinin təşkilati-texniki və hüquqi əsasları (4 saat)

- **Əsas anlayışlar, tərifl ər və Rİ-nın xassələri.** Rİ-nin açıq və məxfi açarları. Rİ-nin alqoritmləri və sxemləri. Rİ vasitələri. Əl imzası analoqunun kriptoqrafik növü kimi Rİ-nin xüsusiyyətləri. Rİ elektron sənəd dövriyyəsinin iştirakçıları arasında cavabdehliyin hüquqi qüvvəyə malik bölgüsünün təmin olunması vasitəsi kimi.
- **İdarəetmə, sənəd dövriyyəsi və elektron kommersiya sistemlərində təhlükəsizliyin təmin olunmasında Rİ və digər kriptoqrafik texnologiyaların rolu və yeri.** İnformasiyanın kriptoqrafik mühafizə vasitələrinin (İKMV) həll etdiyi məsələlər: qarşılıqlı əlaqədə olan tərəflərin autentifikasiyası, ötürülən verilənlərin konfidensiallığının, tamlığının və autentikliyinin təmin olunması, cavbdehliyin bölgüsü (boyun qaçırmamanın xassəsi əsasında). Mümkün istifadə nümunələri (dövlət proqramları, elektron kommersiya, korporativ AS-lərin mühafizəsi).
- **Rİ-nin istifadəsinin zəruri texniki və təşkilati şərtləri.** İmzalanan elektron sənədin qavrayışı və təsvirinin birmənalılığı. Elektron sənədlərin vaxt nişanları sistemi (Digital Timestamping Service, DTS). İstifadəçinin mühafizəli iş yerində qurulmuş xüsusi proqram və aparat təminatına əsas tələblər. İstifadəçinin hərəkətlərinin reqlamentləşdirilməsi. Məxfi açarların, istifadəçilərin və sertifikasiya mərkəzlərinin açıq açarlarının sertifikatlarının saxlanması. Açarların istifadə olunan sertifikatların həqiqiliyinin yoxlanması, Rİ-lı sənədlərin arxivləşdirilməsi, imzalanan sənədlərin hüquqi qüvvəsinin təmin olunması.
- **Tərəflərin Rİ-nı onlar arasında ənənəvi kağız sənəd şəklində əvvəlcədən müqavilə imzalanmadan istifadə etməsi.** Açıq açarın qeydiyyatdan keçmiş sertifikatı və məxfi açar istifadəçinin elektron vəsiqəsi kimi. Sertifikasiya mərkəzlərinə inam problemi (reqistrasiya və açarların sertifikasiyası mərkəzlərinə).
- **Rİ və İMKV-nin Azərbaycanda tətbiqinin hüquqi məsələləri.** Elektron qarşılıqlı əlaqəsi iştirakçılarının maraqlarının hüquqi müdafiəsi. Qarşılıqlı əlaqə iştirakçıları arasında münaqişələrin həlli. Elektron sənədlərin hüquqi qüvvəsi. Rİ ilə imzalanmış sənədlərin sübut kimi qəbul olunması şərtləri. "Elektron imza və elektron sənəd haqqında" qanun və onun əsas müddəaları. Rİ və İKMV-nin istifadə olunmasının hüquqi bazasını təmin edən AR qanunları, AR Prezidentinin Fərmanları, hökumətin qərarları, standartlar və digər hüquqi sənədlər. Fəaliyyətin liseziyalaşdırılması, vasitələrin sertifikasiyası, sistemlərin attestasiyası. Normativ və rəhbərlik üçün sənədlərin kriptoqrafik sistemlərə qoyduğu tələblər.

Modul 2. AAİ-nin əsasları (8 saat)

- **Açıq açarlar infrastrukturu konsepsiyası.** AAİ-nin arxitekturası, əsas komponentləri, onların funksiyaları və qarşılıqlı əlaqələri (sertifikasiya orqanları, reqistrasiya orqanları, sertifikatların sahibləri, klient proqram təminatı, informasiya anbarı və s.). İnam modelləri. Sertifikatlar zənciri və sertifikasiya yolları. AAİ-nin realizəsi məsələləri (təşkilati, texniki, sosial). AAİ-də alqoritmlərin, sxemlərin, verilənlər strukturlarının, protokolların və s. unifikasiyasının zəruriliyi. AAİ-nin əsas standartları (PKCS, X.509, RFC). AAİ-də informasiyanın arxivləşdirilməsi.
- **X.509 standartının elektronnıy sertifikatı.** Sertifikatın əsas hissəsinin və onun genişlənmələrinin strukturu. Sahələrin təyinatı və sertifikat şablonları.
- **Sertifikatların formalaşdırılması, imzalanması və istifadəsi.** Açarlanın generasiyası. Sertifikatların paylanması, istifadəsi və geri çağırılması. Sertifikatların geri çağırılması və

fəaliyyətinin dayandırılmasının mümkün səbəbləri. Geri çağırılmış sertifikatların siyahısı (CRL).

- **Sertifikatın statusu haqqında informasiyanın AAİ-da yayımlanması.** Saxlancların təşkili və AAİ ilə əlaqədar informasiyanın nəşri. Geri çağırılmış sertifikat siyahılarının yayım nöqtələri. Geri çağırılmış sertifikat siyahılarının dövri nəşrinin mexanizmləri və protokolları.

Modul 3. Sertifikatların idarə olunması bazasında təhlükəsizliyin korporativ infrastrukturunun yaradılmasının praktik aspektləri (4 saat)

- **AAİ qurulması üçün ən geniş yayılmış məhsulların qısa xülasəsi** (Entrust, Baltimore, RSA, Microsoft, KriptoPro və b.).
- **Microsoft sertifikatlər xidməti (Certificate Services) bazasında açıq açarlar infrastrukturu.** Özək və köməkçi sertifikasiya mərkəzlərinin köməyi ilə sertifikatların idarəolunmasının korporativ iyerarxik infrastrukturunun yaradılması. Açıq açarların korporativ infrastrukturunda kriptoqrafik xidmətlər provayderlərinin istifadə olunması. "Offline" və "online" recimlərində sertifikat mərkəzlərinin sertifikatlarının formalaşdırılması və müxtəlif tətbiqi proqramlar üçün kliyent sertifikatlarının buraxılması. Açar informasiyasının və sertifikatların saxlanması üçün e-Token aparat vasitələrindən istifadə olunması. Geri çağırılmış sertifikatlar siyahılarının yoxlanması xüsusiyyətləri. WEB serverlə mühafizəli SSL/TLS birləşməsinin və mühafizəli elektron poçtun (MS Outlook/Outlook Express) təşkili. Faylların rəqəmsal imzası üçün kliyent proqram təminatının istifadə olunması.