UOT: 004.9:351

Cəfərov Z.Ə.
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
c.zafar@mail.ru

TELEKOMMUNİKASİYA SİSTEMLƏRİNİN İNFORMASİYA TƏHLÜKƏSİZLİYİ ARXİTEKTURU

Məqalədə mühafizə olunmuş informasiya xidmətlərinin təqdim edilməsinə imkan verən telekommunikasiya sistemlərinin informasiya təhlükəsizliyi arxitekturu təhlil olunur. Bu arxitektur mühafizə funksiyalarının çoxlu sayda kombinasiyalarının tətbiqi hesabina mühafizə olunmuş müxtəlif informasiya xidmətlərinin təqdim edilməsinə imkan verir. Təhlükəsizlik funksiyalarının tətbiqi üçün kriptoprovayder modullarından istifadə olunur.

Açar sözlər: *informasiya təhlükəsizliyi, telekommunikasiya sistemləri, kriptoprovayder, təhlükəsizlik arxitekturu.*

Giriş

Dövlət orqanları ilə təsərrüfat subyektləri və vətəndaşlar arasında qarşılıqlı kiber əlaqələrin – elektron dövlətin (e-dövlətin) yaradılması informasiya cəmiyyətinin ən vacib, prioritet istiqamətlərindən biridir. Bu əlaqələr "dövlət-dövlət", "dövlət-biznes", "dövlət-vətəndaş" , "biznes-biznes" və "biznes-vətəndaş" kimi qarşılıqlı ictimai münasibətlərdə təzahür olunur. E-dövlət - informasiya emalı, mübadiləsi və yayılmasının elektron vasitələrinə əsaslanan dövlət idarəetmə sistemidir. Onun yaradılmasında başlıca məqsəd vətəndaşlara, müəssisə və təşkilatlara dövlət orqanlarının bütün növ informasiya xitmətlərinin təqdim olunması prosedurlarının sadələşdirilməsi, xidmət müddətinin qısaldılması və keyfiyyətinin yüksəldilməsi, inzibati xərclərin azaldılması, həmin orqanların fəaliyyəti haqqında informasiya açıqlığının və şəffaflığının təmin olunmasıdır [1].

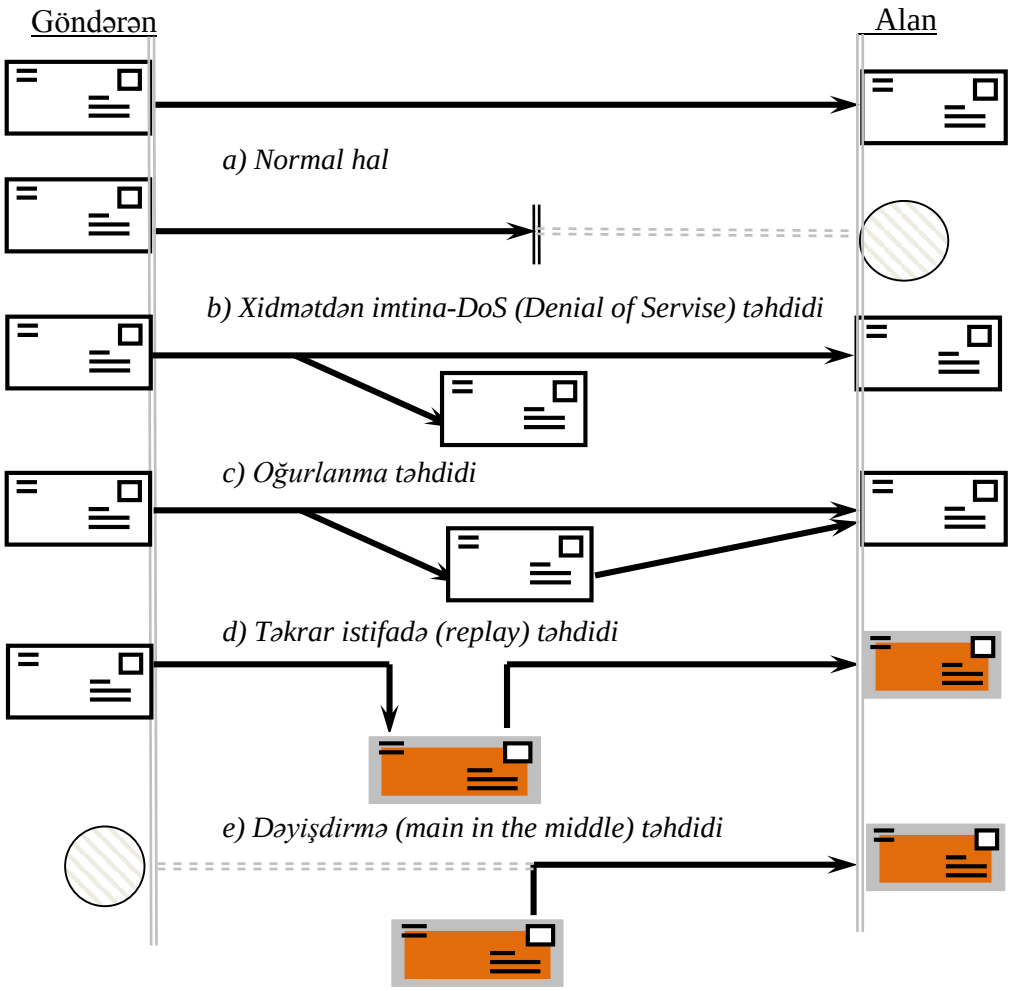
Telekommunikasiya sistemləri e-dövlət konsepsiyasının vacib, informasiya təhlükəsizliyi cəhətinə görə isə ən zəif elementi hesab edilir [2]. E-dövlət konsepsiyasının tam funksionallıqla reallaşdırılması üçün vacib şərtlərdən biri informasiya sistemlərinin texnoloji bazasına malik olan bütün dövlət orqanlarının bir-biri ilə və istənilən növ abunəçilərlə (vətəndaşlar, müəssisə və təşkilatlarla) əlaqə yaratmasına imkan verən təhlükəsiz telekommunikasiya infrastrukturunun təşkil olunmasıdır [3].

E-dövlət xidmətləri üzrə informasiya təhlükəsizliyi şərtləri

E-dövlət konsepsiyasına görə, məlumatların nizamlanmış hərəkəti elektron sənəd dövriyyəsi sistemində təşkil olunur. Bu sistemdə istifadə olunan proqramlar, texniki vasitələr və texnologiyalar e*lektron sənəd dövriyyəsi vasitələri* adlanır. Elektron sənəd dövriyyəsi vasitəçisi istisna olmaqla, özü tərəfindən və ya adından elektron sənəd göndərilən fiziki və ya hüquqi şəxs e*lektron sənədi göndərən* (Göndərən), elektron sənədin ünvanlandığı şəxs isə *elektron sənədi alan* (Alan) adlanır [4].

Şəxsən, habelə başqasının adından çıxış etmək səlahiyyəti olan şəxs tərəfindən göndərilmiş və ya özünün proqramlaşdırdığı qaydada fəaliyyət göstərən informasiya sisteminin avtomatik ötürdüyü elektron sənəd Göndərən tərəfindən göndərilmiş hesab edilir. Tərəflər arasındakı müqavilədə başqa hallar müəyyən edilməmişdirsə, Alan qəbul etdiyi elektron sənədin həqiqiliyinin təsdiqlənməsi nəticəsində onu Göndərənin yolladığına əmin olur və istənilən, o cümlədən avtomatik vasitələrlə alınmanı birmənalı təsdiq edən qaydada Göndərəni məlumatlandırır.

Məlumdur ki, mühafizə olunmamış telekommunikasiya şəbəkələrində elektron sənəd mübadiləsi zamanı müxtəlif təhdidlər baş verə bilər (Şəkil 1) [5].



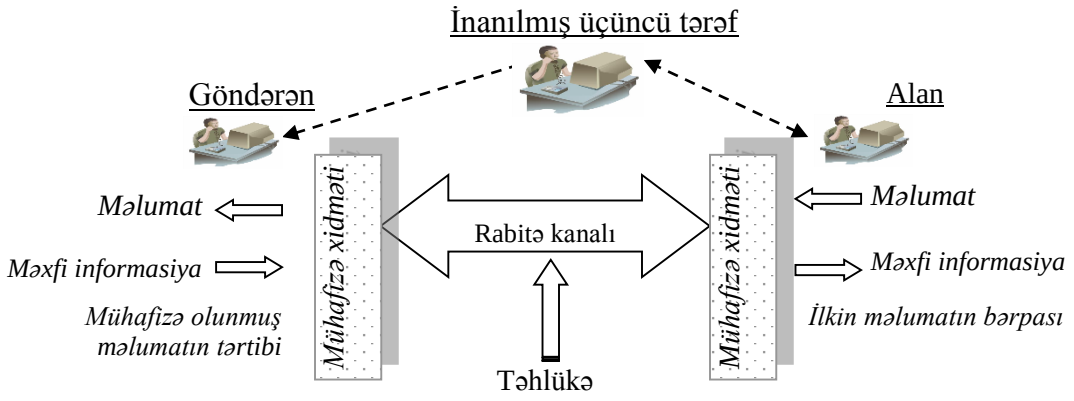
Şəkil1. Eelektron sənəd mübadiləsi zamanı baş verən təhdidlər

Elektron sənəd mübadiləsi zamanı aşağıdakı şərtlərin təmin olunması vacibdir:

- məlumatı qəbul edən tərəf (Alan) məlumat mənbəyinin (Göndərənin) əsilliyinə əmin olmalı;
- Alan qəbul etdiyi məlumatin əsilliyinə əmin olmalı;
- müəllif göndərdiyi məlumatın əsil Alana çatdırıldığına əmin olmalı;
- müəllif müsahibinə göndərdiyi əsil məlumatın çatdırıldığına əmin olmalı;
- Göndərən və Alan məlumatın kənar şəxslərin əlinə keçib oxunmamasına əmin olmalıdır.

Rabitə kanallarının kriptomühafizəsi

Şəkil 2-də şəbəkənin qarşılıqlı əlaqə təhlükəsizliyinin ümumi modeli təsvir olunmuşdur. Şəbəkə əlaqələrində iştirak edən istifadəçilərin servis profillərini üçüncü tərəf (məsələn, inzibatçı) xüsusi verilənlər bazasında yerləşdirir. Servis profilində istifadəçilərin identifikatoru, qeydiyyat verilənləri, məxsusi xidmətlərinin cari parametrləri və s. aktual xarakteristikaları əks etdirilir [6]. İstifadəçinin identifikatoru iki: fərdi (*Private user identities*) və açıq (*Public user identities*) koddan ibarət olur. İstifadəçinin üçüncü tərəfin təyin etdiyi fərdi kodu, qeydetmə və avtorizasiya prosedurlarında istifadə edilir. Açıq kod isə onun sahibi ilə digər istifadəçilərin rabitə seansları təşkil etməsi üçün tətbiq olunur [7]



Şəkil 2. Şəbəkə əlaqələrinin təhlükəsizlik modeli

Açıq açar texnologiyası vasitəsilə mühafizə olunmuş rabitə kanallarının təşkili

Fərz edək ki, DOC göndərənin alana təqdim edəcəyi sənəddir. Müəllif bu məlumatı alana göndərən zaman şifrələyir [8]: $EDOC=E\{K2_A, E\{K1_M, DOC\}\}$.

Şifrələmə prosesində istifadə edilir: şifrələmə proseduru - E(Encryption); göndərənin məxfi açarı - ($K1_M$); alanınn açıq açarı - ($K2_A$)

Alan bu şifrələnmiş məlumatı oxumaq üçün onu əvvəlcə özünün ($K2_M$) məxfi açarının vasitəsi ilə, sonra isə bu sənədi göndərənin ($K1_A$) açıq açarı və D (Dencryption) proseduru ilə deşifrələyərək açıq mətni əldə edir:

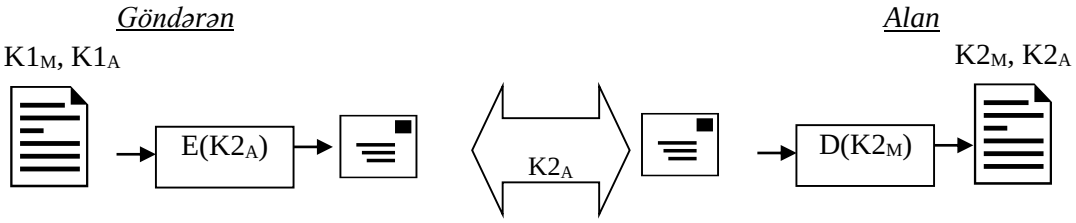
$$DOC = D\{K1_A, D\{K2_M, EDOC\}\}.$$

Bu kriptosxem elektron sənəd mübadiləsi zamanı ödənilməli şərtlərin təmin olunmasına imkan verir [9].

Məxfi açarın yalnız Göndərənə mənsub olduğu təsdiq edilərsə, o bu məlumatdan (imzadan) imtina edə bilməz.

Bədniyyətli şəxs məxfi açarı bilmədən, nəinki göndərən adından sənəd tərtib etmək və hətta rabitə kanalında mübadilə olunan məlumatın məzmununda dəyişiklik apara bilməz [9] .

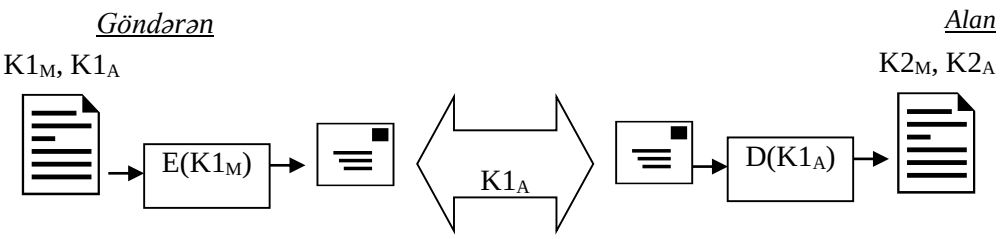
Məlumat mübadiləsinin iştirakçıları açıq açarlarını ($K1_A$, $K2_A$) mübadilə edərək öz aralarında istiqamətli rabitə kanalı yarada bilərlər. Göndərən Alanın açıq açarı ilə məlumatı şifrələyib göndərəcək, şifrələnmiş bu məlumatı yalnız və yalnız Alan öz məxfi açarı ilə deşifrələyərək məlumatın tam məxfiliyini, yəni autentifikasiyasını təmin edəcək (Şəkil 3).



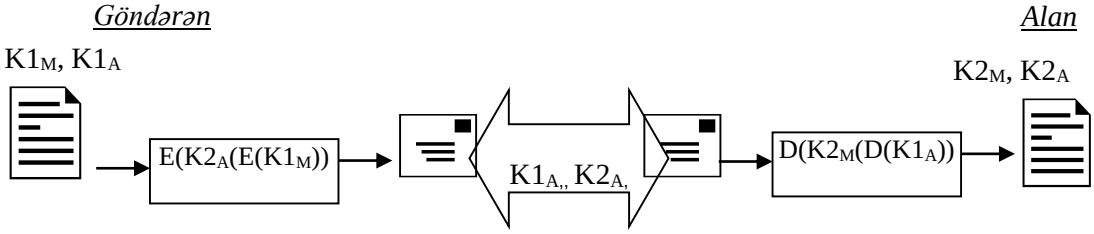
Şəkil 3. İstiqamətli kanalların yaradılması sxemi

Müəllif məlumatı öz məxfi açarı ilə şifrələyib göndərəcək, müsahib isə müəllifin açıq açarı ilə deşifrələyərək məlumatın həmin açıq açarın sahibi tərəfindən hazırlanıb göndərilməsinə əmin olacaqdır. Bu müəllifin identifikasiyasını təmin edir (Şəkil 4).

Əvvəlcə Göndərənin məxfi açarı ilə, sonra Alanın açıq açarı ilə məlumatın ikiqat ardıcıllıqla şifrələnməsi iki istiqamətli mühafizə olunmuş rabitə kanalı yaratmağa imkan verir (Şəkil 5).



Şəkil 4. Göndərənin identifikasiyası sxemi



Şəkil 5. Mühafizə olunmuş rabitə kanalı

Telekommunikasiya sistemlərinin təhlükəsizlik arxitekturu

Telekommunikasiya sistemlərinin təhlükəsizlik arxitekturu səviyyə (lay) və müstəvi kimi iki anlayışla müəyyən olunur (Şəkil 6) .

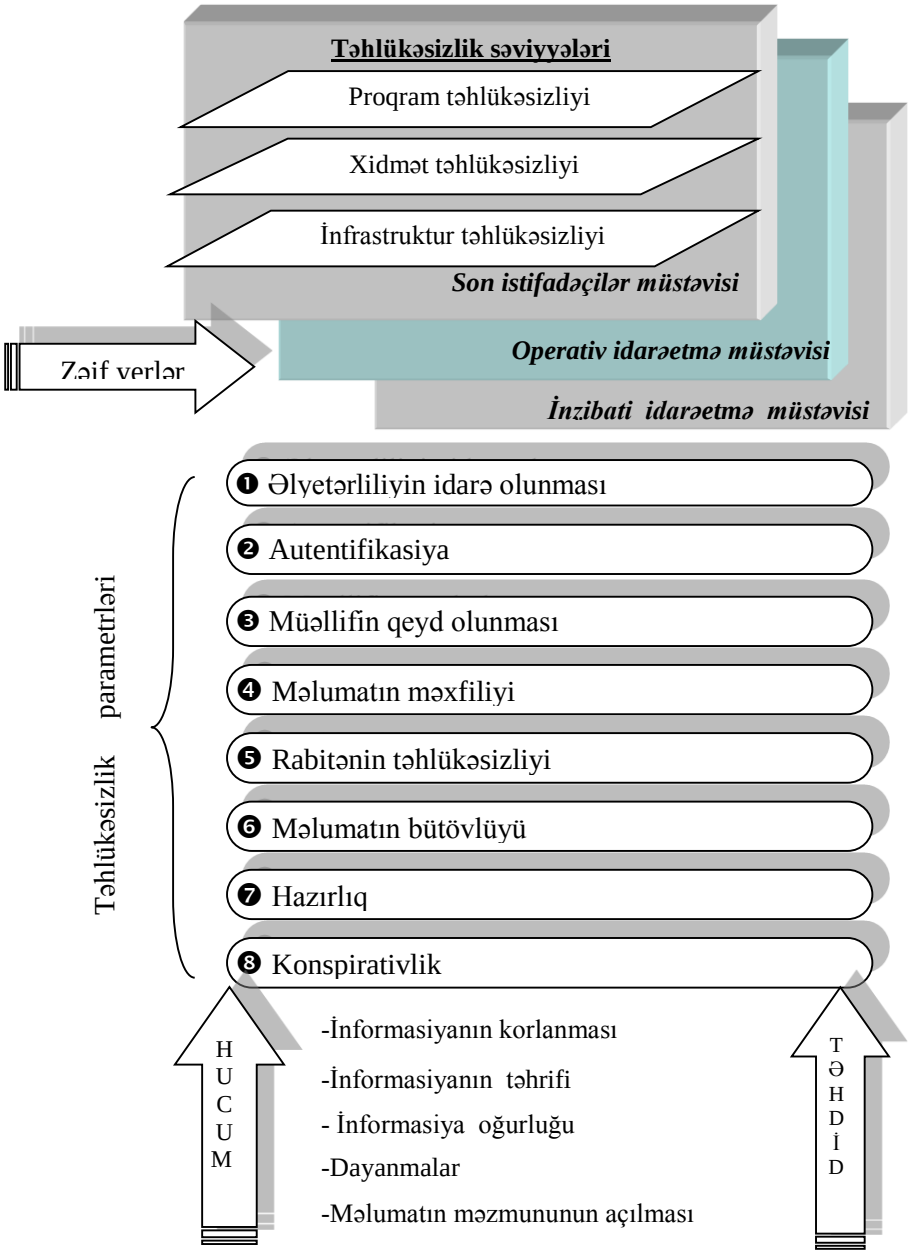
Tətbiqi proqramlar (əlavələr), xidmətlər və infrastrukturdan ibarət 3 *təhlükəsizlik səviyyəsi* şəbəkəni bilavasitə təşkil edən elementlər və sistemlər üzərinə qoyulan tələblərin yerinə yetirilməsi ilə əlaqələndirilir. Bu tələblərin səviyyələr üzrə paylanması zamanı hər bir səviyyənin təhlükəsizliyi hesabına tam mühafizəni təmin etmək məqsədilə iyerarxik yanaşma tətbiq olunur. Təhlükəsizlik arxitekturunun səviyyələrlə təşkilinin üstün cəhətlərindən biri telekommunikasiya sistemlərinin tam mühafizəsini təmin etmək məqsədilə müxtəlif təhlükəsizlik funksiyalarının təkrar tətbiqinin mümkün olmasıdır. Təhdidlərə nəzərən müxtəlif olduqlarına görə hər bir səviyyənin mühafizə tədbirləri onların yerinə yetirdikləri funksiyalara görə müəyyən olunur.

İnfrastruktur səviyyəsi rabitə vasitələrindən və ayrı-ayrı şəbəkə elementlərindən təşkli olunur. Bu səviyyəyə aid marşrutlayıcıları, kommutatorları və onlar arasında rabitə kanallarını nümunə göstərmək olar. *Xidmətlər səviyyəsi* istifadəçilərə təqdim olunan şəbəkə xidmətlərinin təhlükəsizliyini təmin edir. *Tətbiqi proqramlar səviyyəsi* abunəçilərin istifadə etdikləri şəbəkə əlavələrinə tələblərin ödənməsini təmin edir.

Təhlükəsizlik müstəviləri şəbəkənin inzibati idarəçiliyi, şəbəkəni və ya siqnallaşmanı operativ idarəetmə və son istifadəçilərin fəaliyyəti ilə bağlı ayrı-ayrı xüsusi ehtiyaclarını təmin edir.

İnzibati idarəetmə müstəvisi istismar, inzibatçılq, texniki xidmət və təminat funksiyaları ilə bağlıdır. *Operativ idarəetmə müstəvisi* şəbəkə mühiti və texnologiyasından asılı olmayaraq rabitə seansların təşkili üzrə siqnallaşma məsələləri ilə əlaqəlidir. *Son istifadəçilər müstəvisi* istehlakçıların şəbəkəyə təhlükəsiz daxil olmalarını və istifadə etmələrini təmin edir. Bu müstəvi həm də son istifadəçi məlumatlarını mühafizə edir.

Telekommunikasiya sistemlərinin informasiya mühafizəsi arxitekturu daxilində 2 təşkiledici ilə yanaşı, şəbəkə təhlükəsizliyi problemlərinin həlli üçün 8 təhlükəsizlik parametri təyin edilmişdir [10, 11, 12]: 1) Əlyetərliliyin idarə olunması; 2) Autentifika-siya; 3) Müəllifin qeyd olunması; 4) Məlumatın konfidensiallığı; 5) Rabitənin təhlükəsizliyi; 6) Məlumatın tamlığı; 7) Hazırlıq; 8) Konspirativlik (gizlilik).



Şəkil 6. Telekommunikasiya sistemlərinin təhlükəsizlik arxitekturunun elementləri

Autentifikasiya sistemə daxil olmaq üçün təqdim etdiyi identifikatorun ona məxsusluğunun yoxlanması yolu ilə subyekt və ya obyektin əsilliyinin təsdiq olunmasıdır. Hal-hazırda "obyekt" termini təkcə fiziki şəxsləri - istifadəçiləri deyil, qurğuları, xidmət və tətbiqi proqramları da əhatə edir. Autentifikasiya həm də obyektin sistemə qeyri-qanuni müdaxiləyə cəhd etməməsinə və əvvəlki mübadilə olunan məlumatın zəbt edilib təkrar göndərilmədiyinə zəmanət verməlidir. Autentifikasiyanın iki növü mövcuddur: məlumat mənbəyinin autentifikasiyası (rabitə seansı təşkil olunarkən) və rabitə seansının eyni hüquqlu obyektinin (rabitə seansı təşkil etmədən) autentifikasiyası. Şəbəkə rabitə seansını eyni hüquqlu obyektlər arasında təşkil etməli və müraciət olunan Alanın identikliyinə zəmanət verməlidir. Adətən, autentifikasiya identifikasiyadan sonra başlanır.

İdentifikasiya istifadəçinin sistemdə izlənməsi məqsədilə subyekt və ya obyektlərə daxilolma identifikatorunun mənimsənilməsi və ya təqdim edilmiş identifikatorun mövcud identifikatorlar siyahısı ilə müqayisəsi hesab olunur. *İdentifikator* sistemə və ya onun resurslarına müəyyən qayda (icazə) ilə daxil olmaq üçün subyekt və ya obyektlərə bu sistemdə mənimsənilmiş yeganə fərdi kodu təsvir edir.

Autentifikasiyasına görə istifadəçinin səlahiyyətlərinin və ya onun daxil olacağı informasiya resursları və elementlərinin müəyyənləşdirilməsi *avtorizasiya* (ixtiyar vermə) adlanır. Telekommunikasiya şəbəkəsində autentifikasiya, identifikasiya və avtorizasiya üçün istifadə olunan informasiyanın mühafizəsi təmin olunmalıdır.

Göndərənin qeyd olunması istifadəçinin göstərdiyi fəaliyyətdən inkar etməsinin sistem tərəfindən qarşısının alınması bacarığıdır. Bu cür fəalliyyət kimi, kontentlərin yaradılması, çatdırılması, yayımı və qəbulu, məlumat mübadiləsinin, müxtəlif təyinatlı rabitə seanslarının, audio-videokonfransların iştirakçısı və s. nümunə ola bilər. Göndərənin qeyd olunmasının təmin edilməsi üzrə tələbə görə məlumatın göndərişi və (və ya) qəbulu faktının inkar edilməzliyi nəzərdə tutulur ki, Göndərənin qanuni məlumatı göndərməsindən imtinaya və ya müsahibin onu qəbul etməsini danmasına yol verilməsin. Telekommunikasiya şəbəkəsi burada bir və ya iki rejim müəyyən edə bilər: ya məlumat onun mənbəyinin yoxlanması ilə qəbul edilir, ya da Göndərən məlumatın çatdırılması faktını təsdiq edən vasitələrə malik olur ki, nəticədə, Alan məlumat və ya kontentin qəbul olunması faktını inkar edə bilməsin.

Konspirativlik (gizlilik) anlayışı informasiya təhlükəsizliyinin əsas motivləşdirici amillərindən biridir. Adətən, bu termin fiziki şəxsin ona aid hər hansı məlumatın toplanması və saxlanmasına nəzarət və təsir edə bilməsi, həmçinin bu məlumatın məzmunun kim tərəfindən və kimə açılması hüququnu bildirir. Konspirativlik daha geniş mənada informasiyanın kənar şəxslər tərəfindən açıla bilməsinin mümkünsüzlüyünü təmin edən aparat-proqram (məsələn, kriptoqrafiya, steqanoqrafiya və s.) vasitələrilə əlaqələndirilir. Əsasən, konspirativlik (gizlilik) və konfidensiallıq eyni termin kimi istifadə olunur, lakin qeyd etmək lazımdır ki, onların fərqli məna çalarları da mövcuddur. Belə ki, gizlilik istifadəçini və onun fəaliyyətinin identifikasiya məlumatı üzrə assosiasiyasına, konfidensiallıq anlayışı isə məlumatlara icazəsiz daxilolmalardan mühafizəyə aid edilir. Məlumatın konfidensiallığını təmin etmək üçün, adətən, şifrələmə, fayla daxilolma siyahıları və hüquqların idarə edilməsi kimi metodlardan istifadə edilir.

Məlumatın tamlığı onun icazəsiz dəyişdirilməməsinin göstəricisidir. Daha geniş mənada, bu termin informasiyanın icazəsiz yaranmadan, dəyişiklikdən, silinmədən, təkrarlamadan mühafizəsinə zəmanət verməklə, bu cür cəhdlərin baş verməsinin aşkarlanmasını təmin edir.

Konspirativlik, konfidensiallıq, autentifikasiya, müəllifliyin qeyd olunması və məlumatın tamlığı anlayışları ilə yanaşı, təhlükəsizliyin daha üç parametri tətbiq olunur: daxilolmaların (əlyetərliliyin) idarə olunması, rabitə və hazırlıq.

Təhlükəsizliyin *daxilolmaları* (əlyetərliliyi) *idarəetmə* parametri şəbəkə resurslarını icazəsiz (qeyri-qanuni) istifadədən mühafizə edir. Bu parametr şəbəkə elementlərinə, saxlanan və mübadilə olunan informasiyaya, xidmət və tətbiqi proqramlara yalnız səlahiyyətli heyət və qurğuların icazəsinin təqdim olunmasını təmin edir.

Rabitə parametri məlumatın seansın yalnız müvafiq səlahiyyətli iştirakçıları arasında mübadiləsini təmin edir. Bu parametr məlumat mübadiləsi zamanı ünvandəyişmə və zəbtolunma üzrə mühafizə tədbirlərinə aid olunur.

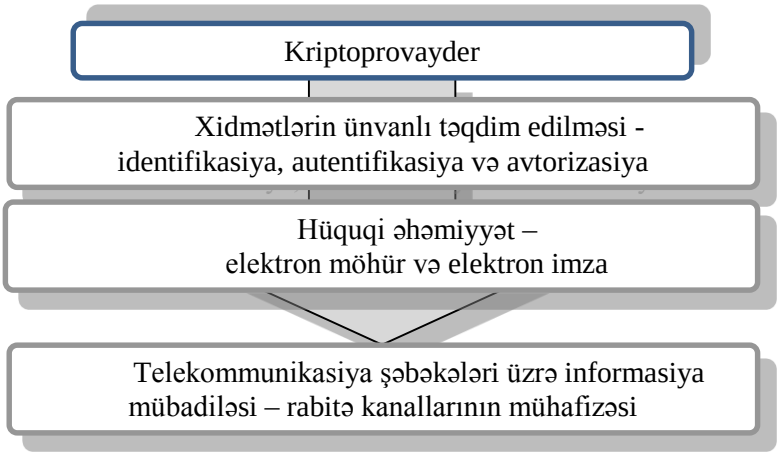
Təhlükəsizliyin *hazırlıq* parametri dayanmalar (fasilələr) zamanı şəbəkə elementlərinə, bazada saxlanan və mübadilə olunan informasiyaya, xidmət və tətbiqi proqramlara heyət və qurğuların səlahiyyətinə görə icazəli istifadəsindən imtina olunmamasını təmin etməkdir. Bu kateqoriyaya şəbəkənin qəzalardan sonra ilkin vəziyyətə gətirilməsi və bərpası tədbirləri aid olunur.

Kriptoprovayder. Telekommunikasiya sistemlərinin informasiya təhlükəsizliyi arxitekturu, elektron sənədlərin mühafizəsi üzrə şərtləri kriptoprovayderlər vasitəsilə təşkil oluna bilər. Kriptoprovayder - kriptoqrafik funksiyalar kitabxanasından təşkil olunmuş standart interfeysə malik ayrıca proqram moduludur [13, 14] (Şəkil 7).

Kriptoprovayder müxtəlif kriptoqrafik alqoritmlərin tətbiqi proqramlarda istifadə olunmasını təmin edir:

- standart interfeysin reallaşdırılması;

- sertifikatlarla işləmə;
- şifrələmə açarları ilə işləmə;
- imza ilə işləmə;
- sənədlərin şifrələnməsi və imzalanması;
- alqoritm sxemlərinə üçüncü tərəfin qarışmasının mümkünsüzlüyü.



Şəkil 7. Kriptoprovayder

Kriptoprovayder müxtəlif informasiya sistemlərində tətbiq olunaraq, informasiya mühafizəsinin təminatı üzrə aşağıdakı məsələləri həll edir [15]:

- identifikasiya;
- autentifikasiya;
- avtorizasiya;
- şifrələmə;
- informasiyanın tamlığının yoxlanılması.

Nəticə

Təhlükəsizlik arxitekturu aspektində informasiya təhlükəsizliyi parametrləri mühafizə tədbirləri üçün səviyyə və müstəvilərin təşkil etdiyi 3×3 matrisinin hər bir oyuğuna tətbiq oluna bilir. Telekommunikasiya sistemlərinin təhlil olunan informasiya təhlükəsizliyi arxitekturu mühafizə funksiyalarının çoxlu sayda müxtəlif kombinasiyalarının tətbiqi hesabına mühafizə olunmuş informasiya xidmətlərinin təqdim edilməsinə imkan verir. Təhlükəsizlik funksiyalarının tətbiqi üçün kriptoprovayder modulları istifadə olunur.

Ədəbiyyat

1. Антанович Н.А., Решетников С.В. Высокие технологии в государственном управлении: государственная политика в области информатизации // Проблемы управления, 2004, №4, с.18-23.
2. Устинов Г.Н. Уязвимость и информационная безопасность телекоммуника-ционных технологий, М., Радио и связь, 2003, с.128.
3. Обзор систем электронного документооборота//http://www.ixbt.com/soft/ sed.shtml, 20 декабря 2011г.
4. «Elektron sənəd və elektron imza haqqında» Azərbaycan Respublikasının Qanunu, 9 mart, 2004-cü il, http://www.e-qanun.az
5. Мещеряков Р.В., Шелупанов А.А., Белов Е.Б., Лось В.П. Основы информацион-ной безопасности, М., Горячая линия – Телеком, 2006, 540 с.
6. Конахович, Г. Защита информации в телекоммуникационных системах, М., МК-Пресс, 2005, 356 с.

7. Кулаков В.Г., Андреев А.Б., Заряев А.В. и др. Защита информации в телекоммуникационных системах. Учебник, Воронежский институт МВД России, 2002, 300 с.
8. Əliquliyev R.M., İmamverdiyev Y.N. Rəqəm imzası texnologiyası, Bakı, "Elm", 2003, 132 s.
9. Семенов Г. Цифровая подпись // Открытые системы, 2002, № 07-08, с. 67-78.
10. Игоничкина Е.В. Анализ алгоритмов электронной цифровой подписи / Материалы III Международного конкурса по информационной безопасности "Securitatea informationala – 2006", 14-15 апреля 2006 г.
11. Волчков А. Современная криптография // Открытые системы, 2002, № 07-08, с. 48.
12. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, М., Издательство "ТРИУМФ", 2007, 816 с.
13. Chadwick D. W. "The Use of X.509 in E-Healthcare", Workshop on Standardization in E-health, Geneva, 23-25 May 2003;
14. Euchner M., Probst P-A. "Multimedia Security within Study Group 16: Past, Presence and Future", ITU-T Security Workshop, 13-14 May 2002, Seoul, Korea, http://www.itu.int/itudoc/itu-t/workshop/security/present/s2p3r1.html
15. BS ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management, London, BSI, 2005, 45 c.

УДК: 004.9:351

Джафаров Зафар А.
Азербайджанский Технический Университет, Баку, Азербайджан
c.zafar@mail.ru

Архитектура информационной безопасности телекоммуникационной системы

В данной статье проанализирована архитектура информационной безопасности телекоммуникационной системы, которая позволяет предоставлять защищенные информационные услуги. Данная архитектура дает возможность многократного применения функции информационной защиты для обеспечения межконцевой безопасности различных информационных услуг. Для применения функции информационной защиты используют модули криптопровайдеров.

Ключевые слова: *информационная безопасность, телекоммуникационные системы, криптопровайдер, архитектура безопасности.*

Zafar A. Jafarov
Azerbaijan Technical University, Baku, Azerbaijan
c.zafar@mail.ru

Information security architecture of telecommunication systems

This article analyzes the security architecture of telecommunication systems that is able to provide secure information services. This architecture allows the reuse of application-to-end security for different applications. Crypto modules are used for application of information security functions.

Keywords: *information security, communication systems, encryption provider, security architecture.*