UDC 004.056
DOI https://doi.org/10.52171/herald.347

Development and Preparation of Information Security Methods

U.K. Sadigov
Azerbaijan Technical University (Baku, Azerbaijan)

For correspondence:
Ulfat Sadigov / e-mail: sadigov.ulfet@gmail.com

Abstract

The article examines relevant aspects of the problem of protecting confidential information within organizational information systems. The main objective of the study is to develop a comprehensive set of information security measures aimed at managing user access, strengthening authentication mechanisms, and ensuring the integrity of information resources. To address the stated problem, user access rights were classified by security levels, and mechanisms for physical and logical access control, two-factor authentication, cryptographic protection tools, network security systems, and antivirus software were analyzed. The effectiveness of data protection methods based on the GOST 28147-89 cryptographic algorithm, as well as specialized security software, was evaluated. The results of the analysis demonstrate that the integrated implementation of technical and organizational security measures significantly reduces the risk of unauthorized access to information resources, ensures data confidentiality and integrity, and creates conditions for the effective enforcement of the organization's information security policy.

Keywords: information security, cybercrime, two-factor authentication, cryptographic protection, antivirus systems, security policy

Submitted *28 December 2025*
Published *12 January 2026*

For citation:
U.K. Sadigov
[Development and Preparation of Information Security Methods]
Herald of the Azerbaijan Engineering Academy, 2026, *ONLINE*
ISSN 2789-8245*, *CC BY-NC 4.0 *https://creativecommons.org/licenses/by-nc/4.0/*

İnformasiya təhlükəsizliyi metodlarının işlənib hazırlanması

Ü.K. Sadıqov
Azərbaycan Texniki Universiteti (Bakı, Azərbaycan)

Xülasə

Məqalədə təşkilatın informasiya sistemlərində məxfi məlumatların qorunması probleminin aktual aspektləri araşdırılmışdır. Tədqiqatın əsas məqsədi istifadəçi girişlərinin idarə edilməsi, autentifikasiya mexanizmlərinin gücləndirilməsi və informasiya resurslarının bütövlüyünün təmin edilməsi üçün kompleks informasiya təhlükəsizliyi tədbirlərinin işlənib hazırlanmasıdır. Problemin həlli məqsədilə istifadəçi hüquqlarının səviyyələr üzrə bölgüsü, fiziki və məntiqi girişə nəzarət mexanizmləri, iki faktorlu identifikasiya, kriptoqrafik mühafizə vasitələri, şəbəkə təhlükəsizliyi sistemləri və antivirus proqram təminatlarının tətbiqi təhlil edilmişdir. Məlumatların qorunması üçün ГОСТ 28147-89 kriptoqrafik alqoritminə əsaslanan şifrələmə üsullarının, eləcə də ixtisaslaşmış təhlükəsizlik proqramlarının səmərəliliyi qiymətləndirilmişdir. Aparılmış təhlillər nəticəsində müəyyən edilmişdir ki, texniki və təşkilati təhlükəsizlik tədbirlərinin kompleks şəkildə tətbiqi informasiya resurslarına icazəsiz giriş risklərini əhəmiyyətli dərəcədə azaldır, məlumatların məxfiliyini və bütövlüyünü təmin edir, həmçinin təşkilatda informasiya təhlükəsizliyi siyasətinin effektiv icrasına şərait yaradır.

Açar sözlər: informasiya təhlükəsizliyi, kibercinayətkarlıq, iki faktorlu identifikasiya, kriptoqrafik mühafizə, antivirus sistemləri, təhlükəsizlik siyasəti

---

Разработка и подготовка методов информационной безопасности

У.К. Садыгов
Азербайджанский технический университет (Баку, Азербайджан)

Аннотация

В статье рассматриваются актуальные аспекты проблемы защиты конфиденциальной информации в информационных системах организации. Основной целью исследования является разработка комплекса мер информационной безопасности, направленных на управление пользовательским доступом, усиление механизмов аутентификации и обеспечение целостности информационных ресурсов. Для решения поставленной задачи проведена классификация прав доступа пользователей по уровням безопасности, а также проанализированы механизмы физического и логического контроля доступа, двухфакторной аутентификации, средства криптографической защиты, системы сетевой безопасности и антивирусное программное обеспечение. Оценена эффективность методов защиты данных, основанных на криптографическом алгоритме ГОСТ 28147-89, а также специализированных программных средств безопасности. Результаты проведённого анализа показывают, что комплексное применение технических и организационных мер безопасности позволяет существенно снизить риски несанкционированного доступа к информационным ресурсам, обеспечить конфиденциальность и целостность данных, а также повысить эффективность реализации политики информационной безопасности в организации.

Ключевые слова: информационная безопасность, киберпреступность, двухфакторная аутентификация, криптографическая защита, антивирусные системы, политика безопасности

Giriş

Elektron sənədlərin və məxfi informasiyanın gündəlik emalı zamanı bütövlüyü pozan müxtəlif risk və təhdidlər meydana çıxır. Təşkilatın sahib olduğu məxfi informasiyanın həcmi artdıqca, həmin məlumatların dəyəri də yüksəlir. Müasir dövrdə informasiya təhlükəsizliyi və məlumatların qorunması çoxsaylı və getdikcə mürəkkəbləşən təhlükələrlə üz-üzədir. Kibercinayətkarlar məqsədlərinə çatmaq üçün istifadə etdikləri üsul və alətləri daim yeniləyir və təkmilləşdirirlər. Kibercinayətkarlıq kontekstində informasiya artıq bir əmtəə kimi qiymətləndirilir və məlumat nə qədər yeni və aktual olarsa, onun bazar dəyəri də bir o qədər yüksək olur. Müasir dövrdə kibercinayətkarlıq təkcə informasiya resurslarına qarşı məsafədən həyata keçirilən texniki hücumlarla məhdudlaşmır. Bu sahədə sosial mühəndislik üsulları getdikcə daha geniş tətbiq olunmağa başlayıb və məlumatın ələ keçirilməsi üçün əlverişli şərait yaratmağa yönəlib. Bu yanaşmalar əsasən hədəf şəxslərin psixoloji xüsusiyyətlərindən istifadə edilməsinə əsaslanır.

İnformasiya təhlükəsizliyi siyasətinin həyata keçirilməsi məsuliyyəti yalnız informasiya təhlükəsizliyi üzrə mütəxəssisin deyil, həm də təşkilatın rəhbərlərinin, şöbə müdirlərinin və onların tabeliyində olanların üzərinə düşür. Hər bir işçidən birbaşa iş vəzifələrinin bir hissəsi olaraq informasiya təhlükəsizliyi siyasətinin tələblərinə riayət etmək tələb olunur.

İşin məqsədi

Məqalənin məqsədi təşkilat daxilində informasiya resurslarının qorunmasını təmin etmək üçün istifadəçi hüquqlarının idarə olunması, identifikasiya və autentifikasiya mexanizmləri, eləcə də kriptoqrafik və antivirus vasitələrinin tətbiqinin əsaslandırılmasıdır.

Məslənin qoyuluşu

Müasir informasiya sistemlərində istifadəçi girişlərinin, məxfi məlumatların və şəbəkə rabitə kanallarının qorunması əsas təhlükəsizlik problemlərindən biridir. Məqalədə bu problemlərin kompleks şəkildə həlli üçün texniki və təşkilati təhlükəsizlik tədbirlərinin tətbiqi zəruriliyi qoyulur.

Məsələnin həlli

Hazırlanan informasiya təhlükəsizliyi siyasəti məlumatları qorumaq üçün nəzərdə tutulmuş aparat və proqram təminatının siyahısını əhatə edir.

Aparat və proqram təminatı sistemi aparat və proqram təminatının birləşməsidir. Aparat təminatına işçi identifikasiya cihazları; məlumatların şifrələnməsi cihazları; elektron kilidlər və blokerlər daxil ola bilər. Proqram təminatı həmçinin proqram təminatı sistemi kimi istifadə edilə bilər. Bu proqram təminatı sistemi məlumatların qorunmasını təmin etməyə və girişi məhdudlaşdırmağa kömək edə bilər. Bunun üçün ilk öncə aşağıdakı kimi proqramları nəzərdən keçirmək lazımdır:

- istifadəçi identifikasiyası proqramları (proqram təminatı bunu təmin edərsə, standart alətlərdən istifadə edilə bilər);
- informasiyaya giriş nəzarəti proqramları; kriptoqrafik qoruma proqramları;

virus infeksiyasının qarşısının alınması proqramları;

- müdaxilə və ya giriş aşkarlama proqramları.

Modernləşdirmə tələb edən ilk amil əməliyyat sisteminin yenilənməsidir. Microsoft hazırda istifadədə olan əməliyyat sistemi olan Windows 7 üçün dəstəyin bitdiyini elan etdiyindən, əməliyyat sistemini Windows 10-a yüksəltmək lazımdır. İnformasiya təhlükəsizliyi vasitələrini seçərkən, müəyyən bir məlu-

matların qorunması vasitəsinin Texniki və İxrac Nəzarəti üzrə Xidmət tərəfindən sertifikatlaşdırılıb-sertifikatlaşdırılmadığını nəzərə almaq vacibdir [1].

Aparılan təhlil zamanı müəyyən edilən əsas məsələlərdən biri məlumatlara giriş hüquqlarının məhdudlaşdırılmasıdır. Əvvəlcə yerli şəbəkədə işləmək üçün məlumatlara giriş məhdudlaşdırılmalıdır. Bu növ qoruma istifadəçiləri qruplara bölməklə və onlara aşağıdakı hüquqları verməklə həyata keçirilə bilər:

1. Administrator – şəbəkə administratorları informasiya təhlükəsizliyi siyasətlərini yarada və dəyişdirə, şəbəkəni və avadanlıqları konfiqurasiya edə bilərlər, lakin məlumatlara girişdə məhdudiyyətlər ola bilər. Giriş məhdudiyyətləri məlumatların sızmasının qarşısını almaq üçün tətbiq olunur.

2. Root – məhdud giriş hüquqlarına malik hesab; bu hesabın tam hüquqları var və heç bir məhdudiyyət yoxdur.

3. İstifadəçi – bir sıra məhdudiyyətlərə (proqram təminatının quraşdırılmasına qadağa, resurslara və məlumatlara məhdud giriş) malik standart istifadəçi hesabı.

4. Qonaq – ciddi şəkildə məhdud hüquqlara malik qonaq istifadəçilər üçün hesab (bu hesab üçüncü tərəf təşkilatlarının işçiləri tərəfindən giriş üçün istifadə olunur).

Cədvəl 1-də istifadəçi qrupu hüquqlarının siyahısı təqdim edilir.

Cədvəl 1 – İstifadəçi qrupu hüquqlarının siyahısı
Table 1 – User Group Rights

Əməliyyatlar	**Administrator**	**Root**	**User**	**Guest**
İstifadəçilərin yaradılması və bloklanması	+	+	-	-
İstifadəçi qruplarının yaradılması və redaktə edilməsi	+	+	-	-
Şəbəkə qurulması	+	+	-	-
Kompüterin şəbəkəyə qoşulması	+	+	-	-
Server parametrlərinin dəyişdirilməsi	-	+	-	-
Kataloqlara və ehtiyat nüsxələrə giriş hüquqlarının konfiqurasiyası	+	+	-	-
İnternetdən faylların yüklənməsi	+	+	+	-
Proqram təminatının quraşdırılması	+	+	-	-
Məlumatların yazılması	+	+	-	-
Məlumatların saxlanması	+	+	+	-
Xarici yaddaşın qoşulması	+	+	+	-
CD/DVD-ROM sürücüləri	+	+	-	-
FTP girişi	+	+	+	-
POP3 girişi	+	+	+	-
SMTP girişi	+	+	+	-
SSL girişi	+	+	-	-
SOCKS girişi	+	+	-	-

İstifadəçi hüquqlarının dəyişdirilməsi lazım gələrsə, administratorun yeni giriş hüquqlarını dəyişdirmək və ya yaratmaq hüququ var. Binaya girişi təşkil etmək üçün kağız buraxılışlar elektron buraxılışlarla əvəz edilməlidir. Bu tədbir binaya daxil olduqda işçinin şəxsiyyətini müəyyən etməyə imkan verəcək. Elektron buraxılışların tətbiqi aşağıdakılara imkan verəcək:

- işçilərin gəliş və gediş vaxtlarını izləmək;
- işdən çıxarılan, müvəqqəti olaraq dayandırılan və ya məzuniyyətdə olan işçilərin girişini məhdudlaşdırmaq;
- binaya daxil olan şəxsin şəxsiyyətini müəyyən etmək.

Buraxılışda aşağıdakı məlumatlar olmalıdır:

- tam adı;
- işçinin şəkli;
- şöbə/bölmə/ofis mənsubiyyəti; işçinin işlədiyi ofis;
- gəlmə vaxtı; gediş vaxtı.

Giriş nəzarətindən danışarkən, elektron kombinasiya kilidinin quraşdırılmasına ehtiyac olduğunu qeyd etmək lazımdır. Bu tədbir məxfi məlumatların emal edildiyi və ya məlumatların saxlanıldığı sahələrə, məsələn, server otaqlarına tətbiq edilməlidir.

Kombinasiya kilidlərinə əlavə olaraq, identifikasiya və giriş nəzarəti metodlarına iki faktorlu identifikasiya əlavə edilə bilər. Məsələn, RUTOKEN-dən iki faktorlu identifikasiya. İki faktorlu identifikasiyada birinci amil istifadəçinin sahib olduğu bir şey, ikincisi isə istifadəçinin bildiyi bir şeydir. İki faktorlu identifikasiya etibarlılığı ilə fərqlənir.

Birincisi, bir insanın sahib olmalı olduğu bir əşyanı kopyalamaq mümkün deyil. Çıxarılmayan kriptoqrafik açarlar yarada bilən ağıllı kartlar və USB tokenləri bu rol üçün xüsusilə uyğundur. Yaradıldıqdan sonra bu açar onu tərk etmədən ağıllı kartda və ya token çipində istifadə olunur. Bu açar çıxarıla bilmədiyi üçün ağıllı kartı kopyalamaq da mümkün deyil.

İkinci amil hesab edilən bilik – obyektlə ayrılmaz şəkildə əlaqəli olmalıdır. Ağıllı kartlar üçün bu amil PIN-dir.

Aparat birdəfəlik parol generatorları və ya OTP tokenləri tez-tez iki faktorlu identifikasiya vasitəsi kimi təşviq olunur. Aparat birdəfəlik parol generatorlarının çoxsaylı tətbiqləri mövcuddur. Aydındır ki, hər bir cihaz unikal kod xarakterizə edir və bu, identifikasiyanın birinci amilinin meyarını ödəyir. Lakin, PIN adətən birdəfəlik parolu oxumaq üçün istifadə edilmir. Bu o deməkdir ki, birinci və ikinci amillərin əlaqələndirilməsi şərti yerinə yetirilmir və bu cür cihazlardan istifadə edərək həyata keçirilən identifikasiya həqiqətən iki faktorlu deyil. İstisna, PIN daxil edildikdən sonra birdəfəlik parolların oxunmasına imkan verən cihazlardır, lakin bunlar olduqca nadirdir.

Biometriya həmçinin identifikasiyanın ikinci amil kimi istifadə edilə bilər. Məsələn, Match-On-Card və oxşar texnologiyalar PIN girişinin barmaq izi analizi ilə əvəz edilməsinə imkan verir ki, bu da PIN-i yadda saxlamaq və daxil etmək ehtiyacını aradan qaldıraraq istifadə rahatlığını artırır.

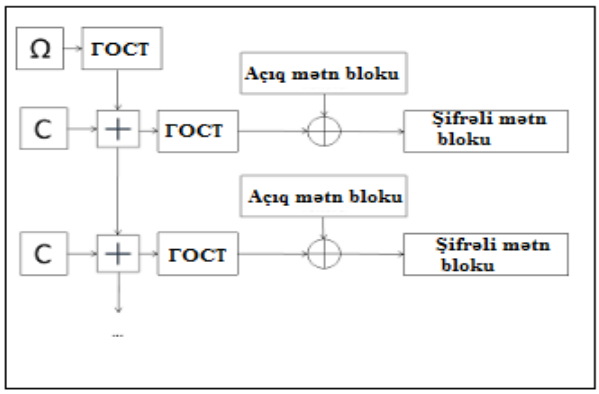
İki addımlı doğrulamaya bənzər, lakin fərqli bir rabitə kanalı üzərindən doğrulamanın baş verməsi ilə fərqlənən zolaqdan kənar identifikasiya.

"Dürüst" iki faktorlu identifikasiya adətən asimmetrik kriptoqrafiyanı tətbiq edən aparat cihazlarının istifadəsinə əsaslanır. Bu halda ilk identifikasiya amili istifadəçinin şəxsi açarını xarakterizə edən aparat cihazının özüdür. Dublikat yaradılmasının qarşısını almaq üçün şəxsi açar çıxarılmayan olmalıdır. İkinci amil PIN-dir, onun biliyi istifadəçiyə cihazdan istifadə etməyə imkan verir. PIN ilə cihaz arasındakı əlaqə çox vacibdir - biri digəri olmadan istifadə edilə bilməz.

Məxfi məlumatları emal edən kompüterlərdə, parol identifikasiyasına əlavə olaraq, rəqəmsal imza kimi açarla açılan elektron kilid quraşdırılmalı və açılmalıdır. Elektron kilid yalnız cihazı açarla açmır, həm də aparatı yoxlayır. Yoxlama kompüterin hər hansı bir komponentinin dəyişdirilib-dəyişdirilmədiyini və ya dəyişdirilmədiyini müəyyən edir. Yoxlama uğursuz olarsa, giriş bloklanacaq. Bu təhlükəsizlik tədbiri kompüterin işinə fiziki müdaxilənin, məsələn, yaddaş cihazının oğurlanmasının qarşısını almaq üçün nəzərdə tutulmuşdur.

Sistemdəki zəifliyi, xüsusən də rabitə kanalının təhlükəsizliyini təmin etməyi həll etməliyik. Bu zəifliyi aradan qaldırmaq üçün Continent-AP təhlükəsizlik sistemindən istifadə etməliyik. Bu sistem, ГОСТ 28147-89 standartına uyğun olaraq, açıq rabitə kanalları üzərindən ötürülən məlumatların kriptoqrafik qorunması üçün nəzərdə tutulmuşdur.

Digər vacib amil şəbəkə müdaxilələrindən qorunmadır. Şəbəkə müdaxilələrindən qorunmanın təmin edilməsi olduqca mürəkkəb bir işdir və ilk növbədə, ən azı müdaxiləni izləyə bilmək lazımdır. Continent-AP sistemi ictimai şəbəkələrdən müdaxilələrdən qorunma təmin etməyə qadirdir. Hücum aşkarlama rejimində sistem imza və evristik metodlardan istifadə edərək şəbəkə hücumlarını aşkarlaya, sistem idarəetmə mərkəzi və elektron poçt vasitəsilə aşkar edilmiş hücumlar barədə administratora real vaxt rejimində məlumat verə və sistemin işləməsi zamanı sistemdə aşkar edilmiş hücumlar barədə qrafik hesabatlar yarada bilər [2]. Daha sonra biz digər zəifliyi də aradan qaldırmalıyıq, yəni məlumatların və açar faylların şifrələnməsini təmin etməliyik. Kompüterdəki məxfi məlumatlar ГОСТ 28147-89 kriptoqrafik alqoritmindən istifadə edərək şifrələnmiş şəkildə saxlanılır. Şəkil 1-də oyunlaşdırma rejimində ГОСТ 28147-89-un diaqramı göstərilir [3].



Şəkil 1 – Qamma rejimində işləmə sxemi
Figure 1 – Gamma Mode Operation Scheme

İşçinin kompüterində saxlama üçün fayl şifrələməsi CRYPTO ARM istifadə etməklə həyata keçirilə bilər. CryptoARM, faylları şifrələmək və elektron imzalamaq üçün hazırlanmış bir proqramdır. Bu proqram korporativ məlumatların qorunma səviyyəsini əhəmiyyətli dərəcədə artırır. Bu məlumat internet, elektron poçt və ya çıxarıla bilən media vasitəsilə ötürülə bilər [4].

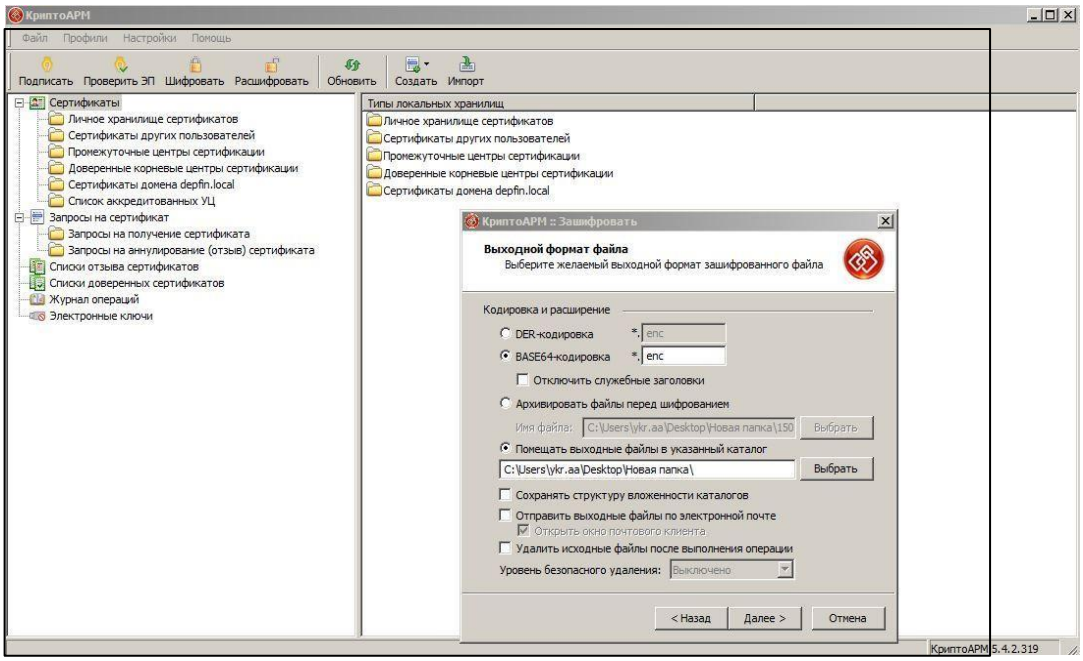
Şifrələmə zamanı həm şifrəni açmaq üçün istifadə olunan sertifikatları (Şəkil 3), həm də istifadə olunan şifrələmə alqoritmini seçə bilərik [5]

Xarici müdaxilədən qorunma ixtisaslaşmış proqram təminatının quraşdırılması və konfiqurasiyası ilə əldə edilə bilsə də, mövcud olan çoxlu sayda seçim və metod səbəbindən daxili fəaliyyətin qarşısını almaq və izləmək daha çətindir. Mənbəyi müəyyən etmək üçün qeydiyyat aktivləşdirilə bilər; bu, məsələn, məlumatı yaddaş qurğusuna fiziki olaraq yükləyərkən məlumatların itirilməsinin qarşısını almayacaq.

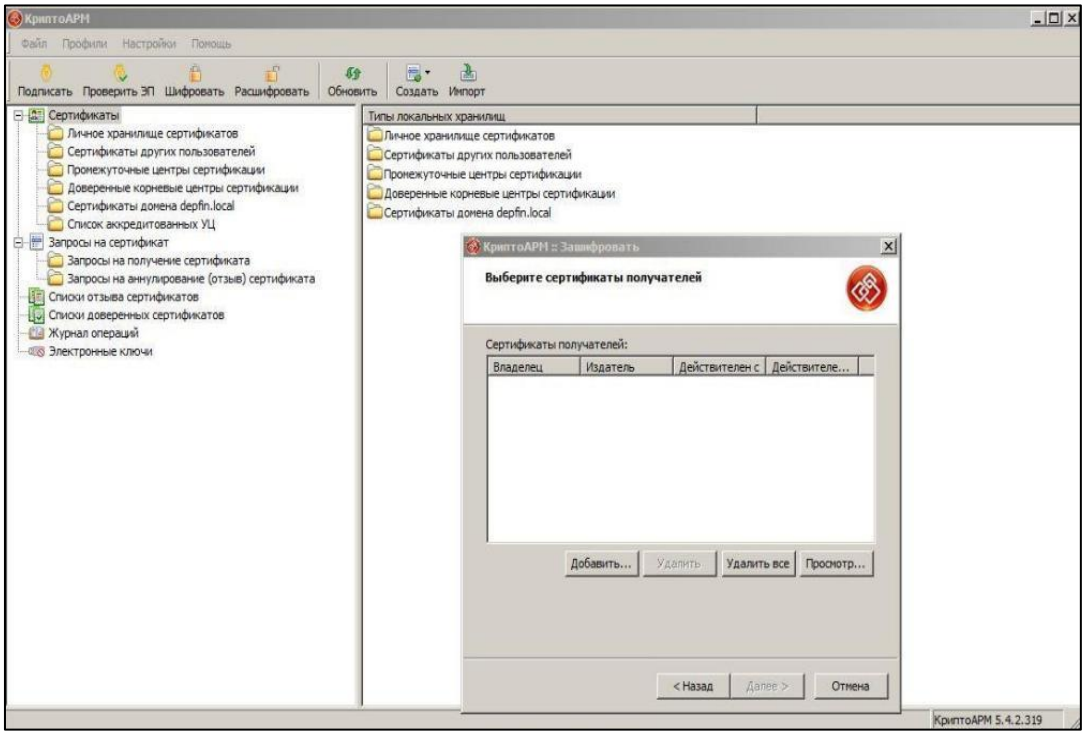
Bu tədbir hansı istifadəçinin hansı hərəkətləri etdiyini aşkar edə bilər ki, bu da öz növbəsində məlumat sızmasının mənbəyini və ya məlumat güzəştinin törədicisini müəyyən etməyə kömək edə bilər.

Həssas məlumatlara malik kompüterlər kiber hücumçuların əsas hədəfi olduğundan, bu cür kompüterlərdə sızmalarla bağlı had-

isələri araşdırmaq üçün məlumatların kölgələndirilməsi həyata keçirilməlidir. Bu həll standart əməliyyat sistemi alətlərindən istifadə etməklə tətbiq oluna bilər və müəyyən edilmiş zəifliyi aradan qaldırır.



Şəkil 2 – CryptoARM şifrələmə pəncərəsi
Figure 2 – CryptoARM encryption window



Şəkil 3 – CryptoARM alıcısının seçim pəncərəsi
Figure 3 – CryptoARM recipient selection window

Antivirus proqram təminatı kompüteri qorumağın əsas vasitəsidir; hazırda İT bazarı geniş çeşiddə antivirus həlləri təklif edir. Antivirus proqram təminatının seçilməsi təhlil tələb edir.

Tədqiqat üçün ümumi zərərli proqram axınında müəyyən edilmiş doqquz texnoloji cəhətdən əhəmiyyətli virus nümunəsi seçilmişdir.

Cədvəl 2-dəki müqayisədən göründüyü kimi, sistemin performans göstəriciləri təxminən eyni olaraq qalır, lakin texniki dəstək baxımından əhəmiyyətli bir fərq var. Dəstəkdəki fərq ondadır ki, hər iki laboratoriya şübhəli faylları qəbul edə, onları zərərli proqram təminatı bazasına əlavə edə və real vaxt rejimində tövsiyələr verə bilər. Bundan əlavə, Kaspersky və Dr.Web laboratoriyaları yerlidir və FSTEC uyğunluq sertifikatlarına malikdir.

Cədvəl 2 – Antivirusların müqayisəsi, virus aşkarlama yoxlaması
Table 2 – Comparison of antivirus programs: virus detection test

Virus	**Antiviruslar**						
	Panda Internet Security	Kaspersky Internet Security	McAfee Internet Security	Microsoft Security Essentials	Dr. Web Security Space Pro	Norton Security	Avast! Internet Security
APT	+	+	-	+	+	+	+
Cidox	-	+	-	-	+	-	+
Powelix	-	+	-	+	-	+	-
Backboot	-	+	-	-	+	-	+
WMIGhost	-	+	-	-	-	-	-
Stoned	-	+	+	+	+	+	+
Pihar	-	+	-	-	+	-	-
SST	-	+	-	-	+	-	+
Zeroaccess	-	+	-	+	+	+	+
Nəticələr	1/9	9/9	1/9	4/9	7/9	4/9	6/9

Cədvəl 3 – Antivirus funksiyalarının müqayisəsi
Table 3 – Comparison of antivirus functions

Virus	**Antiviruslar**						
	McAfee Internet Security	Panda Internet Security	Norton Security	Kaspersky Internet Security	Avast! Internet Security	Microsoft Security Essentials	Dr. Web Security Space Pro
Tələb üzrə skanlama	+	+	+	+	+	+	+
Real vaxt rejimində qorunma	+	+	+	+	+	+	+
Yükləmə zamanı skanlama	+	+.	+	+	-	-	+
Veb qorunması	+	+	+	+	+	-	+
E-poçt qorunması	+	-	+	+	-	+	+
Onlayn yeniləmələr	+	+	+	+	+	+	+

Cədvəl 3-də göstərildiyi kimi, antivirus proqram təminatının funksionallığı ümumiyyətlə çox oxşar və müqayisə edilə biləndir, lakin pullu antivirus həlləri sınaqdan keçirilmiş bütün xüsusiyyətləri özündə birləşdirir. Yuxarıdakı cədvəllərdəki məlumatları nəzərə alaraq, Dr.Web Lab-ın həllərinin ən üstün olduğunu görürük.

Təhlükəsizlik həllərindən effektiv istifadə etmək üçün kompüteri qoruma səviyyələrinə bölmək lazımdır:

1-ci Səviyyəli kompüter məxfi məlumatların emalı və saxlanması üçün nəzərdə tutulmuş ən təhlükəsiz iş stansiyasıdır.

2-ci Səviyyəli kompüter məxfi olmayan məlumatların gündəlik emalı üçün nəzərdə tutulmuş əsas təhlükəsizlik alətlərinə malik kompüterdir.

Təşkilatdakı bütün kompüterlərdə antivirus proqramı quraşdırılmalı və informasiya təhlükəsizliyinə cavabdeh şəxs tərəfindən vaxtında yenilənməlidir. Aparılan təhlillərə əsasən, Dr.Web və Kaspersky ən çox üstünlük verilən proqramlar kimi görünür. Hər bir məhsulun lisenziya qiyməti nəzərə alınmaqla, Dr.Web seçilib. Bu məhsulun digər bir üstünlüyü, maliyyə şöbələri kimi dövlət təşkilatlarında məlumatların qorunması proqram təminatı seçilərkən çox vacib meyar olan FSTEC sertifikatıdır.

Təşkilatdakı hər bir kompüter qəfil elektrik kəsintilərindən qorunmaq üçün fasiləsiz enerji təchizatı ilə təchiz olunmalıdır. Bu, elektrik kəsintisi halında kompüterdəki iş məlumatlarının qorunub saxlanılmasını təmin edir. Məlumat itkisinin və ya avadanlıqların

sıradan çıxmasının qarşısını almaq üçün server avadanlığı da fasiləsiz enerji təchizatı ilə təchiz olunmalıdır.

Başlamaq üçün təşkilat daxilində istifadə olunan sənədlərin strukturunu müəyyən etmək lazımdır. İnformasiya təhlükəsizliyi siyasəti ən yüksək səviyyəli sənəd olmalıdır. Buna görə də, maliyyə şöbəsində istifadə olunan sənədlərin iyerarxiyası aşağıdakı kimi olmalıdır:

1) Bu informasiya təhlükəsizliyi siyasəti birinci (ən yüksək) səviyyədə informasiya təhlükəsizliyi üzrə daxili tənzimləyici sənəddir.

2) İkinci səviyyəli sənədlərə təşkilatın işçilərinin birinci və ikinci səviyyəli sənədləri tətbiq etmək üçün hərəkətlərini təsvir edən təlimatlar, prosedurlar, qaydalar və digər sənədlər daxildir.

3) Üçüncü səviyyəli sənədlərə yuxarı səviyyəli tələblərin yerinə yetirilməsi barədə hesabat sənədləri daxildir.

Məlumatların qorunmasının uğuruna birbaşa təsir edən növbəti amil, yalnız informasiya resursları ilə işləmə qaydaları və prinsipləri, onları pozmağa görə məsuliyyət və informasiya təhlükəsizliyi siyasəti ilə tanış edən sənəd imzalayan istifadəçilərin informasiya resursları ilə işləməsinə icazə verilməsi tələbidir.

İşə qəbul zamanı işçiyə Maliyyə Departamentinin İnformasiya Təhlükəsizliyi Siyasətində təsvir edildiyi kimi, informasiya resurslarının təhlükəsizliyini təmin etmək üçün hüquq və vəzifələri barədə məlumat verilməlidir və bu məsuliyyətlər onların vəzifə təsvirinə daxil edilməlidir. Brifinq və vəzifə təsviri həm Maliyyə Departamentinin İnformasiya Təhlükəsizliyi Siyasətinin tətbiqi və dəstəklənməsi üçün ümumi məsuliyyətləri, həm də resursların qorunması və təhlükəsizliklə bağlı xüsusi əməliyyatların yerinə yetirilməsi üçün xüsusi məsuliyyətləri əhatə etməlidir.

Yeni işə götürülən bütün işçilər təyin olunmuş məsuliyyətləri qəbul etməli və İnformasiya Təhlükəsizliyi Siyasətinə riayət etmək məsuliyyətlərini müəyyən edən əmək müqavilələrini imzalamalıdırlar. Müqavilədə işçinin Təşkilatın İnformasiya Təhlükəsizliyi Siyasətinə uyğunluğunu yoxlamaq üçün auditlər aparmasına razılığı, eləcə də məxfi məlumatların məxfiliyini qorumaq öhdəliyi olmalıdır. Müqavilədə işçinin İnformasiya Təhlükəsizliyi Siyasətinə əməl etməməsi halında görüləcək tədbirlər göstərilməlidir.

İnformasiya təhlükəsizliyi məsuliyyətləri Təşkilatın hər bir işçisinin vəzifə təlimatlarına daxil edilməlidir.

Bütün yeni işçilər məlumatların siyahısı, müəyyən edilmiş giriş səviyyəsi və bu səviyyəni pozduğuna görə cəzalarla tanış olmalı və imza atmalıdırlar.

Bir işçiyə Təşkilatın informasiya sisteminə giriş imkanı verərkən, onlar informasiya sisteminin istifadəçi təlimatını oxumalı və imza atmalıdırlar.

İnformasiya resursları ilə işləmək səlahiyyəti olan hər bir işçiyə qeydiyyatdan keçməli və informasiya sisteminə daxil olacaqları unikal ad (istifadəçi hesabı) verilməlidir. Lazım gələrsə, bəzi işçilərə birdən çox unikal ad (hesab) verilə bilər. Təşkilatda işləyərkən eyni istifadəçi adından ("qrup adı") istifadə edən birdən çox işçinin olması qadağandır. Bu tələbə əlavə olaraq, qeyd etmək lazımdır ki, informasiya təhlükəsizliyi təlimi müntəzəm olaraq keçirilməlidir. Təlimdən əlavə, istifadəçi bilikləri test alətləri vasitəsilə qiymətləndirilməli və zərurət yarandıqda, onları təkmilləşdirmə kurslarına göndərmək kimi boşluqlar aradan qaldırılmalıdır.

Növbəti addım istifadəçi qeydiyyatıdır. Qeydiyyat proseduru məsul şəxs tərəfindən ərizə kimi sənəd əsasında həyata keçirilməlidir. Bu ərizədə istifadəçi haqqında zəruri məlumatlar, məsələn:

- ✓ Adı, soyadı;
- ✓ vəzifəsi;
- ✓ işçinin xidmət müddəti (əgər işçi müvəqqətidirsə);
- ✓ işçini vəzifəyə təyin edən əmr nömrəsi olmalıdır.

Həmçinin qeyd etmək lazımdır ki, istifadəçinin səlahiyyətlərinə xitam verildikdə, informasiya resurslarına bütün giriş dərhal bloklanmalıdır.

Şifrə təminatı proseduruna xüsusi diqqət yetirilməlidir; bu proses aşağıdakı tələblərə cavab verən rəsmi prosedur kimi təmin edilməlidir:

• bütün istifadəçilər şəxsi və qrup parollarının məxfi saxlanılması tələbi barədə məlumatlandırılmalı və imzalanmalıdır;

• mümkün olduqda, sistem elə konfiqurasiya edilməlidir ki, istifadəçi ilk dəfə müvəqqəti parolla daxil olduqda, sistem dərhal dəyişdirilməsini tələb etsin;

• müvəqqəti parollar istifadəçiyə yalnız şəxsiyyəti müəyyən etdikdən sonra verilməlidir;

• Şifrələri üçüncü tərəflərlə və ya şifrələnməmiş e-poçt vasitəsilə paylaşılmamalıdır;

• Müvəqqəti parolları asanlıqla təxmin etmək və ya istifadəçidən istifadəçiyə təkrarlamaq mümkün olmamalıdır;

• İstifadəçi parolun alınmasını təsdiqləməlidir;

• Parollar yalnız elektron şəkildə təhlükəsiz formatda saxlanılmalıdır;

• Proqram təminatı təchizatçısı tərəfindən təyin edilmiş parollar quraşdırıldıqdan dərhal sonra dəyişdirilməlidir;

• Parolun uzunluğu, simvol dəsti və giriş cəhdlərinin sayı üçün tələblər müəyyən edilməlidir;

• İstifadəçi parolları ən azı 90 gündə bir dəfə dəyişdirilməlidir.

Giriş hüquqları istifadəçinin etimadnaməsinə əsasən verilir, onların hərəkətləri qeyd olunur və işlənmiş məlumatların məxfiliyi təmin edilir.

Eyni etimadnamələrin müxtəlif istifadəçilər tərəfindən istifadəsinə icazə verilmir. Təhlükəsizlik Administratoru istifadəçi hesabı üçün ilkin parol təyin edir, bundan sonra istifadəçi öz parolunu təyin edir.

Maliyyə Departamentinin işçilərinə üçüncü tərəf USB disklərindən istifadə etmək qadağandır. Bu, kompüterin yoluxmasının və ya casus proqram təminatının quraşdırılmasının qarşısını almaq üçündür.

İstifadəçinin kompüteri işə salındıqda hər gün qismən antivirus taramasından, iş həftəsinin sonunda və ya lazım olduqda isə tam taramadan keçməlidir [6, 7].

İşə başlamazdan əvvəl istifadəçi hər hansı bir casus proqramı aşkar etmək üçün iş sahəsini vizual olaraq yoxlamalıdır.

İstifadəçi tərəfindən alınan elektron poçt mesajlarına xüsusi diqqət yetirilməlidir. Şübhəli məzmunlu elektron poçtları əvvəlcə yoxlamadan açmaq qəti qadağandır.

Hər bir istifadəçi informasiya resurslarına daxil olmaq üçün tələb olunan parollarının oğurlanmasının qarşısını almalıdır. Şifrələr də vaxtaşırı dəyişdirilməlidir. İstifadəçi parollarının təhlükəsizliyinə görə məsuliyyət daşıyır.

Kiberhücum təhlükəsi yaranarsa, bütün istifadəçilərə məlumat verilməli və təlimat verilməlidir [8].

İnformasiya təhlükəsizliyi üzrə mütəxəssis (və ya üçüncü tərəf təşkilatı) qorunan informasiya resurslarına icazəsiz giriş əldə etmək üçün mümkün cəhdləri simulyasiya etməklə Təşkilatın informasiya təhlükəsizliyi tədbirlərini vaxtaşırı sınaqdan keçirməlidir.

İnformasiya təhlükəsizliyi üzrə mütəxəssis Təşkilatın əməliyyat sistemlərində və ya proqram təminatında müəyyən edilmiş zəifliklər barədə məlumat toplamalı və təhlil etməlidir. Bu məlumat müxtəlif şirkətlərin, ictimai birliklərin və informasiya təhlükəsizliyi üzrə ixtisaslaşmış digər təşkilatların rəsmi nəşrlərindən əldə edilə bilər.

Mövcud informasiya təhlükəsizliyi siyasətini nəzərdən keçirərkən müəyyən edilmiş çatışmazlıqları da nəzərə almaq lazımdır. Xüsusilə, aşağıdakılar həll edilməlidir:

- İT şöbəsi ilə daimi istifadəçilər arasında ünsiyyət qurulmalı və sənədləşdirilməlidir.

- Tərəflərin məsuliyyət dərəcəsi müəyyən edilməli və sənədləşdirilməlidir.

- İnformasiya təhlükəsizliyi siyasətini pozmaq üçün hər hansı bir meyl və ya niyyəti müəyyən etmək üçün işə namizədlərin test edilməsi və müsahibəsi vacibdir.

- Təşkilatın məlumatların hazırlanması prosesi təmin edilməlidir, xüsusən də informasiya nəzarəti həyata keçirilməlidir.

- Avadanlıqların çatdırılmasını və təmirini ən qısa müddətdə təmin edə bilən bir təşkilatla müqavilə bağlanmalıdır.

Nəticə

Məqalənin əsas elmi nəticəsi ondan ibarətdir ki, hazırlanmış informasiya təhlükəsizliyi siyasəti məlumatların oğurlanması, itirilməsi və ya korrupsiyası kimi potensial riskləri azaldır. Tətbiq olunmuş informasiya təhlükəsizliyi siyasətinin əsas üstünlükləri aşağıdakılardır:

- İşçilərin hərəkətləri üzərində daha böyük nəzarət;
- Daxili hücumlar riskinin azaldılması;
- Binalara giriş nəzarəti;
- Şəxsi identifikasiyanın qismən avtomatlaşdırılması.

Beləliklə, tətbiq olunmuş informasiya təhlükəsizliyi siyasəti geniş tətbiq oluna bilər, onun istifadəsi məlumatların itirilməsi risklərini azaldacaq və iqtisadi baxımdan onun istifadəsi mümkün və effektivdir.

Maraqlar münaqişəsi

Müəllif bu məqalədə araşdırılması tələb olunan maraqlar münaqişəsinin olmadığını qeyd edir.

REFERENCES

1. **Efimushkin V.A., Ositis A.P.** Rol «skvoznyh» cifrovyh tekhnologii v razvitii telekommunikacij // Moskva: Elektrosvyaz. 2021. №1, – s.28-35, DOI: 10.34832/ELSV.2021.14.1.003.
2. **Hertzog R., Roland Mas.** The DEBIAN administrator’s handbook. 2015. – 522 p.

3. **Lachihina A.B.** Modeli protivodejstviya ugrozam narusheniya informacionnoj bezopasnosti pri ekspluatacii baz dannyh v zashchishchennyh korporativnyh informacionnyh sistemah / Lachihina Anastasiya Borisovna – Moskva, 2010.
4. **Luckij S.Ya.** Korporativnoe upravlenie tekhnicheskim perevooruzheniem firm: Uchebnoe posobie / S.Ya. Luckij - M.: Vysshaya shkola, 2003. - 319 s.
5. **İbrahimova S.R., Hüseynzadə İ.M.** Təhlükəsizlik sisteminin təkmilləşdirilməsi üçün modifikasiya edilmiş Vernam şifrləmə alqoritmi. Elmi Məcmuə Cild 27, №3, 2025, DOI: 10.30546/EMNAA.2025.25.03.108
6. Sravnenie Antivirusov 2019, https://www.anti-malware.ru/tests_history
7. Luchshie antivirusy 2026 goda, https://top10antivirusov.com/
8. **Abbasova P.Ə.** Kiberfiziki sistemlerdə təhlükəsizliyin analizi və qiymətləndirilməsi. "Azərbaycan Mühəndislik Akademiyasının Xəbərləri, 2025, 17(3), 111–118 s. https://doi.org/10.52171/herald.303