İNFORMASİYANIN MÜHAFİZƏSİ VƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN ƏSAS ANLAYIŞLARI

UOT 338:004; 330.47; 338:002.6
DOI:10.30546/3006-0346.2024.1.79.183

TURAL HƏSƏNOV
Azərbaycan Texniki Universiteti
E-mail: pm.turalhasanov@gmail.com

İnformasiyanın mühafizəsinin effektivliyi informasiyanın mühafizəsi nəticələrinin məqsədə uyğunluq dərəcəsidir. İnformasiyanın sızmadan qorunması mühafizə olunan məlumatın açıqlanmasından nəzarətsiz yayılmasının, qorunan məlumatlara icazəsiz daxil olmasının və mühafizə olunan məlumatların təcavüzkarlar tərəfindən alınmasının qarşısının alınması üzrə fəaliyyətdir [2].

Məlumatın açıqlanmasından qorunması - qorunan məlumatların nəzarətsiz sayda məlumat alıcılarına icazəsiz ötürülməsinin qarşısını almaq üçün fəaliyyətlərdir.

İnformasiyanın icazəsiz daxil olmaqdan mühafizəsi qanuni sənədlərlə müəyyən edilmiş hüquqları pozmaqla maraqlı subyekt tərəfindən və ya məlumat sahibi və ya mühafizə olunan informasiyaya daxil olmaq hüququ və ya qaydaları ilə qorunan informasiyanın alınmasının qarşısının alınması üzrə fəaliyyətdir [3].

Qorunan məlumatlara həyata keçirən maraqlı subyekt dövlət, hüquqi şəxs, fiziki şəxslər qrupu, o cümlədən ictimai təşkilat, fiziki şəxs ola bilər. İnformasiya təhlükəsizliyi sistemi - informasiya təhlükəsizliyi üzrə müvafiq hüquqi, təşkilati, inzibati və normativ sənədlərlə müəyyən edilmiş qaydalara uyğun olaraq təşkil edilmiş və fəaliyyət göstərən orqanlar və (və ya) icraçıların, onların istifadə etdiyi informasiya təhlükəsizliyi texnologiyasının, habelə təhlükəsizlik obyektlərinin məcmusudur [4].

İnformasiya təhlükəsizliyi dedikdə məlumatın qeyri-qanuni əldə edilməsindən, çevrilməsindən və məhv edilməsindən, habelə informasiya ehtiyatlarının onların fəaliyyətini pozmağa yönəlmiş təsirlərdən mühafizəsi başa düşülür. Bu təsirlərin təbiəti çox müxtəlif ola bilər.

Məlumatların məxfiliyi məlumatlara verilən statusdur və tələb olunan qorunma dərəcəsini müəyyən edir. Məxfi məlumatlara, məsələn, aşağıdakılar daxil ola bilər:

- ❖ istifadəçilərin şəxsi məlumatları;
- ❖ hesablar (adlar və parollar);
- ❖ kredit kartı məlumatları;
- ❖ inkişaf məlumatları və müxtəlif daxili sənədlər;
- ❖ mühasibat uçotu məlumatları.

Məxfi məlumat yalnız sistemin səlahiyyətli və yoxlanılmış (səlahiyyətli) subyektlərinə (istifadəçilər, proseslər, proqramlar) məlum olmalıdır.

Sistemin digər subyektləri üçün bu məlumat naməlum olmalıdır. Qorunan informasiyanın (mühafizə obyektinin) qorunmasının əhəmiyyətinin dərəcələrinin müəyyən edilməsi qorunan informasiyanın təsnifatı adlanır.

İnformasiyanın bütövlüyü dedikdə, ötürülmə və saxlanma prosesində onun strukturunu və ya məzmununu saxlamaq üçün məlumatın mülkiyyəti başa düşülür [4].

Sistemdəki məlumatlar mənbə sənədlərdəki məlumatlardan semantik cəhətdən fərqlənmədikdə, yəni təsadüfən və ya qəsdən təhrif edilmədikdə və ya məhv edilmədikdə informasiyanın bütövlüyü təmin edilir.

Məlumatların bütövlüyünün təmin edilməsi informasiya təhlükəsizliyinin mürəkkəb vəzifələrindən biridir. İnformasiyanın etibarlılığı onun mənbəyi olan subyektə və ya bu məlumatın alındığı subyektə ciddi mənsubiyyətlə ifadə olunan məlumatın xassəsidir.

İnformasiyanın hüquqi əhəmiyyəti informasiya daşıyıcısı olan sənədin hüquqi qüvvəyə malik olması deməkdir.

İstifadəçi məlumatlarla yalnız ona çıxışı olduqda işləyə bilər. İnformasiya əldə etmək - subyektin informasiya ilə, o cümlədən texniki vasitələrin köməyi ilə tanış olmaq imkanı əldə etməsi, informasiya əldə etmək subyekti informasiya proseslərində hüquqi münasibətlərin iştirakçısıdır.

İnformasiyaya çıxışın səmərəliliyi informasiyanın və ya bəzi informasiya ehtiyatının onun əməliyyat ehtiyaclarına uyğun olaraq son istifadəçi üçün əlçatan olması qabiliyyətidir [5].

Qanunvericilik aktlarına görə İnformasiya sahibi istifadə, sahiblik, sərəncam vermək səlahiyyətlərini tam formada reallaşdıran subyektdir.

İnformasiya sahibi - informasiyaya sahib olan və ondan istifadə edən, qanunla müəyyən edilmiş hüquqlar çərçivəsində sərəncam vermək səlahiyyətini həyata keçirən subyekt və ya məlumat sahibidir.

İnformasiya istifadəçisi (istehlakçısı) - onun sahibindən, mülkiyyətçisindən və ya vasitəçidən müəyyən edilmiş hüquq və məlumat əldə etmək qaydalarına uyğun olaraq alınmış məlumatdan və ya onların pozulması ilə istifadə edən subyektdir.

İnformasiya əldə etmək hüququ hüquqi sənədlərlə və ya məlumat sahibi və ya sahibi tərəfindən müəyyən edilmiş məlumat əldə etmək üçün qaydalar məcmusudur.

İnformasiya əldə etmək qaydası subyektin informasiyaya və onun daşıyıcılarına çıxış qaydasını və şərtlərini tənzimləyən qaydalar məcmusudur. İnformasiyaya icazəli giriş, girişə nəzarətin müəyyən edilmiş qaydalarını pozmayan məlumatların əldə edilməsidir.

Sistem komponentlərinə giriş hüququnu tənzimləmək üçün girişə nəzarət qaydaları istifadə olunur.

İnformasiyaya icazəsiz girişi həyata keçirən şəxs və ya proses girişə nəzarət qaydalarını pozandır. Mühafizə inzibatçısı kompüter sistemini informasiyaya icazəsiz daxil olmağın qarşısını almağa görə cavabdehdir.

Mövcud olan məlumatın həmçinin kompüter sisteminin resursunun və ya komponentinin, yəni komponentin və ya resursun mülkiyyətinin sistemin qanuni subyektləri üçün əlçatan olmasını nəzərdə tutur.

Mövcud ola biləcək resursların göstərici siyahısına aşağıdakılar daxildir:

- ❖ printerlər,
- ❖ serverlər,
- ❖ iş stansiyaları,
- ❖ istifadəçi məlumatları,
- ❖ əməliyyat üçün tələb olunan istənilən kritik məlumatlar.

Sistemin resursunun və ya komponentinin bütövlüyü, təsadüfi və ya qəsdən təhriflər və ya dağıdıcı təsirlər şəraitində sistemin işləməsi zamanı semantik olaraq dəyişməz qalma xüsusiyyətidir.

İdentifikasiya, autentifikasiya, avtorizasiya kimi mühüm anlayışlar qrupu informasiya və sistem resurslarına çıxışla bağlıdır.

Sistemin (şəbəkə) hər bir subyekti mövzunu müəyyən edən bəzi məlumatlarla (rəqəm, simvol sətri) əlaqələndirilir.

Bu məlumat sistemin (şəbəkə) subyektinin identifikatorudur. Qeydiyyatdan keçmiş identifikatoru olan subyekt hüquqi (hüquqi) subyektdir [1].

Subyektin identifikatoru ilə tanınması subyektin identifikasiyası prosedurudur. Bu proses sistemə (şəbəkəyə) daxil olmağa çalışdıqda həyata keçirilir. Autentifikasiya sistemin subyektlə qarşılıqlı əlaqəsində digər addımıdır [5]. Mövzunun autentifikasiyası subyektin verilmiş şəxsiyyətlə autentifikasiyasıdır. Doğrulama proseduru subyektin iddia etdiyi şəxs olub-olmadığını müəyyən edir.

Subyektin identifikasiyası və autentifikasiyası aparıldıqdan sonra avtorizasiya proseduru həyata keçirilir. Subyektin avtorizasiyası sistemin (şəbəkənin) müvafiq səlahiyyətləri və mövcud resursları ilə eyniləşdirmə və autentifikasiyadan uğurla keçmiş qanuni subyektin verilməsi prosedurudur.

Təhlükəsizliyə dəyən zərər sistemdə (şəbəkədə) olan və emal olunan məlumatların təhlükəsizlik vəziyyətinin pozulmasını bildirir.

Təhlükəsizlik anlayışı kompüter sisteminin (şəbəkə) zəifliyi anlayışı ilə əlaqədardır. Kompüter sistemindəki zəiflik, təhlükənin həyata keçirilməsinə səbəb ola biləcək sistemin xas olan uğursuz xüsusiyyətidir.

Kompüter sisteminə hücum hücumçu tərəfindən bu və ya digər sistem zəifliyinin axtarışı, yaxud da istifadəsidir.

Təhlükəsizlik təhdidlərinə qarşı mübarizə kompüter sistemlərini və şəbəkələrini qorumaq məqsədi daşıyır. Təhlükəsiz sistem təhlükəsizlik təhdidlərinə uğurla və effektiv şəkildə müqavimət göstərən təhlükəsizlik xüsusiyyətlərinə malik sistemdir [5].

İnformasiyanın mühafizəsi metodu - informasiyanın mühafizəsinin müəyyən prinsip və vasitələrinin tətbiqi qaydası və qaydaları. İnformasiya təhlükəsizliyi aləti - informasiyanın mühafizəsi üçün nəzərdə tutulmuş və ya istifadə edilən texniki, proqram aləti, maddə və/yaxud materialdır [3].

İnformasiya təhlükəsizliyi texnologiyası - informasiya təhlükəsizliyi vasitələri, informasiya təhlükəsizliyinin effektivliyinə nəzarət vasitələri, idarəetmə vasitələri və informasiya təhlükəsizliyini təmin etmək üçün nəzərdə tutulmuş sistemlərdir.

Korporativ şəbəkələr məlumatı emal edən paylanmış avtomatlaşdırılmış sistemlərə (AS) aiddir.

Nəticə

AS-nin təhlükəsizliyinin təmin edilməsi AS-nin işləmə prosesinə hər hansı icazəsiz müdaxiləyə, habelə onun komponentlərini dəyişdirmək, oğurlamaq, sıradan çıxarmaq və ya məhv etmək cəhdlərinə qarşı mübarizənin təşkilini, yəni AS-nin bütün komponentlərini - aparat vasitələrini, proqram təminatı (proqram təminatı), məlumat və personalı təşkil edir.

Təhlükəsizlik siyasəti kompüter sisteminin müəyyən təhlükələrdən qorunmasının işini tənzimləyən normalar, qaydalar və praktiki tövsiyələr toplusudur.

ƏDƏBİYYAT SİYAHISI:

1. Abbasov Ə.M., Əlizadə M.N., Seyidzadə E.V., Musayev İ.K. İnformatika və kompüterləşmənin əsasları, Dərslik, Yeni işlənmiş nəşri, RS "Poliqal" nəşriyyatı, 2012, 932 səh.

2. Əilizadə M.N., Seyidzadə E.V., Salmanova M.Ə.

İnformatika (Mövzular, suallar və testlər), dərs vəsaiti, Bakı 2012

3. Fərziyev T. İnformatika (magistraturaya hazırlaşanlar üçün vəsait), Bakı 2012, 322 səh.

4. R. Sahay, W. Meng ve C. D. Jensen, "The application of Software Defined Networking on security computer ağlar: Bir anket," Ağ ve Bilgisayar Uygulamaları Dergisi, cilt. 131, sayfa 28-108, 2019.

5. Paulauskas N. Computer System Attack Classification / N. Paulauskas, E. Garšva // Electronics and Electrical Engineering. – 2020. – № 2(66). – P. 84–87.

XÜLASƏ

İstifadəçilərə ünvanlanan informasiyanın emalı, toplanması və ötürülməsinin müasir üsulları son və ya onlara məxsus olan məlumatların itirilməsi, təhrif edilməsi və açıqlanması ehtimalı ilə bağlı təhlükələrin meydana gəlməsi ilə nəticələnmişdi. Buna görə də kompüter sistemlərinin və şəbəkələrinin informasiya təhlükəsizliyinin təmin edilməsi İT-nin inkişafında aparıcı istiqamətlərdən biridir. İnformasiya təhlükəsizliyi qorunan məlumatın sızmasının, qorunan məlumatlara icazəsiz və qəsdən təsirlərin qarşısını almaq üçün fəaliyyətdir.Mühafizə obyekti məlumatın mühafizəsi məqsədinə uyğun olaraq mühafizənin təmin edilməsi zəruri olan məlumat, informasiya daşıyıcısı və ya informasiya prosesi. İnformasiya təhlükəsizliyinin məqsədi informasiya təhlükəsizliyinin arzuolunan nəticəsidir. İnformasiyanın mühafizəsinin məqsədi informasiyanın mümkün sızması və ya icazəsiz və qəsdən məlumatlara təsir nəticəsində məlumatın sahibinə, istifadəçisinə dəyən ziyanın qarşısını almaq ola bilər.

Açar sözlər: *İnformasiya, kompüter sistemləri, şəbəkə.*

Tural Hasanov
Azerbaijan Technical University
pm.turalhasanov@gmail.com
0009-0006-6719-9730

BASIC CONCEPTS OF INFORMATION PROTECTION AND INFORMATION SECURITY

Summary

Modern methods of processing, collecting and transmitting information addressed to users have resulted in the emergence of threats related to the possibility of loss, distortion and disclosure of information that belongs to users. Therefore, ensuring the information security of computer systems and networks is one of the leading directions in the development of IT. Information security is an activity to prevent the leakage of protected information, unauthorized and intentional effects on protected information. The object of protection is the information, information carrier or information process that needs to be protected in accordance with the purpose of information protection. The goal of information security is the desired outcome of information security. The purpose of information protection may be to prevent damage to the owner, owner, user of information as a result of possible leakage of information and/or unauthorized and intentional impact on information.

Keywords: *Information, computer systems, network.*

Турал Гасанов
Азербайджанский Технический Университет
pm.turalhasanov@gmail.com
0009-0006-6719-9730

ОСНОВНЫЕ ПОНЯТИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Резюме

Современные методы обработки, сбора и передачи информации, адресованной пользователям, привели к появлению угроз, связанных с возможностью утраты, искажения и раскрытия информации, принадлежащей пользователям. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития ИТ. Информационная безопасность - деятельность по предотвращению утечки защищаемой информации, несанкционированного и умышленного воздействия на защищаемую информацию.Объектом защиты является информация, носитель информации или информационный процесс, подлежащие защите в соответствии с целью защиты информации. Целью информационной безопасности является желаемый результат информационной безопасности. Целью защиты информации может быть предотвращение нанесения ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и умышленного воздействия на информацию.

Ключевые слова: *Информация, компьютерные системы, сеть.*