TEXNİKA ELMLƏRİ

TECHNICAL SCIENCES

https://doi.org/10.36719/2663-4619/107/49-55

Ramazan Eyyubov
Odlar Yurdu Universiteti
riyaziyyat üzrə fəlsəfə doktoru
eyyubov54@mail.ru
Əsmər Qaraxanlı
Azərbaycan Kooperasiya Universiteti
esmercabbarlı95@gmail.com
Həqiqət Əşirova
Odlar Yurdu Universiteti
haqiqatashirova@gmail.com

Kompüter təhlükəsizliyi

Xülasə

İyirmi birinci əsrin başlanğıcı elmin inkişafının bütün sahələrində informasiya texnologiyalarının sürətli inkişafı ilə əlamətdardır. Eyni zamanda informasiya getdikcə daha çox strateji resursa, məhsuldar qüvvəyə və bahalı əmtəəyə çevrilir. Kompüter sistemləri və şəbəkə texnologiyaları çox sürətlə inkişaf edir. Müvafiq olaraq, informasiyanı qorumaq üçün yeni üsullar da sürətlə ortaya çıxır. İnformasiyanın qorunması və onun təhlükəsizliyinin etibarlı təminatı problemi dövrümüzün ən mühüm problemlərindən biridir. Buna görə də mövzu çox aktualdır.

Kompüter sistemlərinin unifikasiyası, qlobal şəbəkələrin yaradılması və informasiya resurslarının çıxış imkanlarının genişləndirilməsinə səbəb olur. Proqram təminatının mürəkkəbliyinin artması və bununla əlaqədar onların etibarlılığının azalması və zəifliklərin sayının artmasına səbəb olur. Kompüter şəbəkələri, spesifik təbiətinə görə, sadəcə olaraq, informasiya təhlükəsizliyi problemlərinə məhəl qoymadan normal fəaliyyət göstərə və inkişaf edə bilməyəcəklər.

Açar sözlər: *kompüter, şəbəkə, təhlükəsizlik, informasiya texnologiyaları, təhdid, kompüter sistemi, məlumat, kompüter sisteminə hücum*

Ramazan Eyyubov
Odlar Yurdu University
Doctor of Philosophy in Mathematics
eyyubov54@mail.ru
Asmar Garakhanli
Azerbaijan Cooperation University
esmercabbarlı95@gmail.com
Hagigat Ashirova
Odlar Yurdu University
haqiqatashirova@gmail.com

Computer Security

Abstract

The beginning of the twenty-first century is marked by the rapid development of information technologies in all areas of scientific development. At the same time, information is increasingly becoming a strategic resource, a productive force, and an expensive commodity. Computer systems and network technologies are developing very rapidly. Accordingly, new methods for protecting

information are also emerging rapidly. The problem of information protection and reliable provision of its security is one of the most important problems of our time. Therefore, the topic is very relevant.

The unification of computer systems leads to the creation of global networks and expansion of access to information resources. The increase in the complexity of software leads to a decrease in their reliability and an increase in the number of vulnerabilities. Computer networks, due to their specific nature, simply cannot function and develop normally without ignoring information security issues.

Keywords: *computer, network, security, information technology, threat, computer system, information, computer system attack*

Giriş

İnformasiya təhlükəsizliyi probleminin formalaşdırılması hazırda bir sıra xüsusiyyətlərə malikdir:

- birincisi, informasiyanın hərtərəfli mühafizəsi məsələsi qaldırılır;
- ikincisi, informasiyanın mühafizəsi obyektlər kütləsi (böyük və kiçik, dövlət və qeyri-dövlət) üçün getdikcə aktuallaşır;
- üçüncüsü, qorunmalı olan məlumatların çeşidi (dövlət, sənaye, kommersiya, şəxsi və s.) kəskin şəkildə genişlənir.

Tədqiqat

İnformasiyanın mühafizəsi tədbirlərinin həyata keçirilməsi geniş yayılmışdır. Bu problemə çoxlu sayda müxtəlif profilli mütəxəssislər cəlb edilmişdir. Lakin onların miqyasını nəzərə alaraq, bu fəaliyyətlərin uğurla həyata keçirilməsi yalnız müvafiq problemlərin həlli üçün metod və vasitələr şəklində yaxşı alətlər olduqda mümkündür.

Kvalifikasiya işinin əsas məqsədi şəbəkələrdə məlumatların mühafizəsi üsul və vasitələrini öyrənmək və təhlil etməkdir.

Bu məqsədə çatmaq üçün bir sıra problemləri həll etmək lazımdır:

- ✓ Təhlükəsizlik təhdidlərini və onların təsnifatını nəzərdən keçirin;
- ✓ Şəbəkədə informasiyanın mühafizəsi üsul və vasitələrini, onların təsnifatını və tətbiqi xüsusiyyətlərini xarakterizə etmək;
- ✓ KS-də fiziki, texniki və proqram təminatının informasiya təhlükəsizliyi vasitələrinin imkanlarını üzə çıxarmaq, onların üstünlüklərini və çatışmazlıqlarını müəyyən etmək;
- ✓ Hərtərəfli informasiya təhlükəsizliyi sisteminin məqsədini nəzərdən keçirmək.

KS təhlükəsizliyinə qəsdən təhdidlərin növləri

Passiv təhdidlər, əsasən, şəbəkə informasiya ehtiyatlarının fəaliyyətinə təsir etmədən icazəsiz istifadəyə yönəlib. Məsələn, verilənlər bazasına icazəsiz daxil olmaq, rabitə kanallarını dinləmək və s.

Aktiv təhlükələr şəbəkənin komponentlərini hədəfə alaraq onun normal fəaliyyətini pozmaq məqsədi daşıyır. Aktiv təhlükələrə, məsələn, kompüterin və ya onun əməliyyat sisteminin sıradan çıxması, verilənlər bazasında məlumatların təhrif edilməsi, kompüter proqramlarının məhv edilməsi, rabitə xətlərinin pozulması və s. Aktiv təhlükələr pakerlərdən, zərərli proqramlardan və s. (Metody zashchity informatsii v KS, 2013, s. 30).

Qəsdən təhdidlər daxili və xarici olaraq iki qrupa bölünür.

Xarici mənbələrdən verilən məlumata görə, sənaye casusluğu geniş vüsət alıb. Bu, kommersiya sirri təşkil edən məlumatların onun sahibi tərəfindən icazə verilməyən şəxs tərəfindən qanunsuz toplanması, mənimsənilməsi və ötürülməsi kommersiya sirri sahibinə ziyan vurur.

İnformasiya təhlükəsizliyinə və şəbəkənin normal işləməsinə əsas təhdidlərə aşağıdakılar daxildir:

- ✓ məxfi məlumatların sızması,
- ✓ məlumatın kompromisi,
- ✓ informasiya ehtiyatlarından icazəsiz istifadə,
- ✓ informasiya resurslarından səhv istifadə,

- ✓ abunəçilər arasında icazəsiz məlumat mübadiləsi,
- ✓ məlumatdan imtina,
- ✓ informasiya xidmətlərinin pozulması,
- ✓ imtiyazlardan qeyri-qanuni istifadə.

Məxfi məlumatın sızması məxfi məlumatın iş prosesində etibar edildiyi və ya iş zamanı məlum olduğu şəbəkədən və ya istifadəçilərin dairəsindən kənara nəzarətsiz buraxılmasıdır.

Məlumatın sahibi tərəfindən açıqlanması vəzifəli şəxslərin və istifadəçilərin qəsdən və ya ehtiyatsız hərəkətləridir, xidməti və ya iş yolu ilə müəyyən edilmiş qaydada müvafiq məlumatların kimə həvalə edildiyi, bu məlumatlarla çıxışına icazə verilməyən şəxslərin onunla tanış olmasına səbəb olmuşdur.

İcazəsiz giriş qorunan məlumatlara daxil olmaq hüququ olmayan şəxs tərəfindən məxfi məlumatın qanunsuz olaraq qəsdən əldə edilməsidir (Domarev, 2012).

İnformasiyaya icazəsiz girişin ən çox yayılmış üsulları bunlardır:

- ✓ elektron şüalanmanın tutulması;
- ✓ parazit daşıyıcı modulyasiyasını əldə etmək üçün rabitə xətlərinin məcburi elektromaqnit şüalanması (işıqlandırılması);
- ✓ dinləmə cihazlarından (əlfəcinlərdən) istifadə;
- ✓ uzaqdan çəkiliş;
- ✓ akustik şüalanmanın tutulması və printer mətninin bərpası;
- ✓ icazə verilən sorğuları yerinə yetirdikdən sonra sistem yaddaşında qalıq məlumatların oxunması;
- ✓ təhlükəsizlik tədbirlərini aşaraq yaddaş daşıyıcılarının surətinin çıxarılması;
- ✓ qeydiyyatdan keçmiş istifadəçi kimi maskalanmaq;
- ✓ sistem sorğuları kimi maskalanmaq;
- ✓ proqram tələlərindən istifadə;
- ✓ proqramlaşdırma dillərinin və əməliyyat sistemlərinin çatışmazlıqlarından istifadə etmək;
- ✓ informasiyaya çıxışı təmin edən xüsusi hazırlanmış texniki vasitələrin avadanlıq və rabitə xətlərinə qanunsuz qoşulma;
- ✓ mühafizə mexanizmlərinin zərərli şəkildə söndürülməsi;
- ✓ şifrələnmiş informasiyanın xüsusi proqramlar vasitəsilə deşifrə edilməsi;
- ✓ informasiya infeksiyaları (Biyachuyev, 2012, s. 39).

Məxfi məlumatı sızdırmaq üçün istənilən vasitə həm şəbəkənin fəaliyyət göstərdiyi təşkilata, həm də onun istifadəçilərinə əhəmiyyətli maddi və mənəvi ziyan vura bilər.

Zərərli proqram təminatı

Hücumların həyata keçirilməsinin ən təhlükəli üsullarından biri hücuma məruz qalan sistemlərə zərərli proqram təminatının daxil edilməsidir.

Paylanma mexanizminə görə onlar ayırd edirlər:

Məntiqi – məlumatı təhrif etmək və ya məhv etmək üçün daha az istifadə olunur, oğurluq və ya fırıldaqçılıq üçün istifadə olunur;

Məntiq bombası manipulyasiyası adətən təşkilatı tərk etməyi planlaşdıran narazı işçilər tərəfindən edilir, lakin bunu məsləhətçilər, müəyyən siyasi əqidəsi olan işçilər də edə bilər.

Məntiqinin əsl nümunəsi: işdən bombanı gözləyən bir proqramçı iş haqqı proqramında dəyişikliklər edir, adı şirkətin kadr məlumatı dəstindən itdikdən sonra işə minməyə başlayır.

Troyan atı, əsas, yəni tərtib edilmiş və sənədləşdirilmiş hərəkətlərə əlavə olaraq, sənədlərdə təsvir olunmayan əlavə funksiyaları həyata keçirən proqramdır. Qədim Yunan Troya atı ilə bənzətmə haqlıdır – hər iki halda təhlükə, şübhəsiz, bir qabıqda gizlənir. Troyan atı bu və ya digər şəkildə orijinal zərərsiz proqrama daxil edilmiş, sonradan şəbəkə istifadəçilərinə ötürülən (bağışlanan, satılan, dəyişdirilən) əlavə əmrlər blokudur. Bu əmrlər bloku ola bilər müəyyən bir vəziyyət yarandıqda (tarix, vaxt, xarici əmrlə və s.) tetikler. Belə bir proqramı işə salan hər kəs həm öz fayllarını, həm də bütövlükdə bütün KS fayllarını təhlükə qarşısında qoyur. Troyan atı adətən bir istifadəçinin səlahiyyətləri çərçivəsində, lakin başqa istifadəçinin və ya hətta şəxsiyyətini müəyyən etmək bəzən qeyri-mümkün olan yad birinin maraqları üçün fəaliyyət göstərir. Troyan atı, onu işə

salan istifadəçinin geniş imtiyazlar dəsti varsa, ən təhlükəli hərəkətləri edə bilər. Bu halda, Troyan atını yaradan və təqdim edən və özü bu imtiyazlara malik olmayan təcavüzkar səhv əllərlə icazəsiz imtiyazlı funksiyaları yerinə yetirə bilər.

Virus, daha çoxalma qabiliyyətinə malik olan dəyişdirilmiş nüsxəni daxil etməklə digər proqramları yoluxdura bilən proqramdır (Goshko, 2014, s. 93).

Virusun iki əsas xüsusiyyətlə xarakterizə olunduğu güman edilir:

- özünü çoxaltma qabiliyyəti,
- hesablama prosesinə müdaxilə etmək bacarığı.

Son viruslarla mübarizə problemi çox aktuallaşıb, buna görə də bir çox insan bunun nəticəsində işləyir. Müxtəlif təşkilati tədbirlər tətbiq edilir, yeni antivirus proqramlarından istifadə edilir və bütün bu təbliğat aparılır. Son zamanlar yoluxma və məhv edilmə miqyasını az və ya çox məhdudlaşdırmaq mümkün olmuşdur. Lakin canlı təbiətdə olduğu kimi bu mübarizədə tam uğur qazandı.

Qurd şəbəkə vasitəsilə yayılan və özünün surətini maqnit mühitində qoymayan proqramdır. Qurd hansı hostun yoluxmuş ola biləcəyini müəyyən etmək üçün şəbəkə dəstək mexanizmlərindən istifadə edir. Daha sonra eyni mexanizmlərdən istifadə edərək bədənini və ya bir hissəsini bu düyünə köçürür və ya işə salır, ya da bunun üçün uyğun şərtləri gözləyir. Bu sinfin ən məşhur nümayəndəsi, 1988-ci ildə interneti yoluxduran Morris virusudur. Qurdun yayılması üçün uyğun mühit, bütün istifadəçilərin dost hesab edildiyi, bir-birinə güvəndiyi və qoruyucu mexanizmlərin olmadığı bir şəbəkədir. Özünüzü bir qurddan qorumağın ən yaxşı yolu şəbəkənizə icazəsiz girişə qarşı tədbir görməkdir. Şifrə oğurlayanlar parolları oğurlamaq üçün xüsusi olaraq hazırlanmış proqramlardır. İstifadəçi sistem terminalına daxil olmağa çalışdıqda, iş sessiyasını bitirmək üçün lazım olan məlumat ekranda göstərilir. Daxil olmağa cəhd edərkən istifadəçi işğalçının sahibinə göndərilən ad və parol daxil edir, bundan sonra səhv mesajı göstərilir və giriş və idarəetmə əməliyyat sisteminə qaytarılır (Grishina).

Parolunu yazarkən səhv etdiyini düşünən istifadəçi yenidən sistemə daxil olur və sistemə giriş əldə edir. Lakin onun adı və şifrəsi artıq işğalçı proqramının sahibinə məlumdur. Parolun ələ keçirilməsi başqa yollarla da mümkündür. Bu təhlükənin qarşısını almaq üçün sistemə daxil olmamışdan əvvəl adı və şifrəni başqasına deyil, xüsusi olaraq sistem daxiletmə proqramına daxil etdiyinizə əmin olmalısınız.

Bundan əlavə, parollardan istifadə və sistemlə işləmək qaydalarına ciddi riayət etməlisiniz. Əksər pozuntular ağıllı hücumlara görə deyil, sadə səhlənkarlığa görə baş verir. Parollardan istifadə üçün xüsusi hazırlanmış qaydalara riayət etmək etibarlı qorunmanın zəruri şərtidir (Mostovoy, 2010).

Məlumatın kompromissi. O, bir qayda olaraq, verilənlər bazasında icazəsiz dəyişikliklər yolu ilə həyata keçirilir, bunun nəticəsində onun istehlakçısı ya ondan imtina etməyə, ya da dəyişiklikləri müəyyən etmək və həqiqi məlumatı bərpa etmək üçün əlavə səylər göstərməyə məcbur olur. Təhlükəli məlumatlardan istifadə edərkən istehlakçı səhv qərarlar vermək riski altındadır.

İnformasiya resurslarından icazəsiz istifadə, bir tərəfdən, onun sızmasının nəticələri və ona güzəşt vasitəsidir. Digər tərəfdən, müstəqil əhəmiyyət kəsb edir, çünki idarə olunan sistemə (tam uğursuzluğa qədər) və ya onun abunəçilərinə böyük ziyan vura bilər.

İcazə verildiyi halda, informasiya ehtiyatlarının səhv istifadəsi qeyd olunan resursların məhvinə, sızmasına və ya güzəştə getməsinə səbəb ola bilər. Bu təhlükə çox vaxt CS-də istifadə olunan proqram təminatındakı səhvlərin nəticəsidir. Abunəçilər arasında icazəsiz məlumat mübadiləsi onlardan birinin ona daxil olması qadağan edilən məlumatı alması ilə nəticələnə bilər. Nəticələr icazəsiz giriş üçün olduğu kimidir (Shan'gin, 2012).

Məlumatdan imtina bu məlumatı alan və ya göndərən tərəfindən onun alınması və ya göndərilməsi faktlarının tanınmamasından ibarətdir.

Bu, tərəflərdən birinə rəsmi şəkildə imtina etmədən bağlanmış maliyyə müqavilələrini texniki yolla ləğv etməyə və bununla da digər tərəfə xeyli ziyan vurmağa imkan verir.

İnformasiya xidmətinin pozulması təhlükədir, onun mənbəyi KS-də istifadə olunan İT-dir. Abunəçiyə informasiya resurslarının verilməsində gecikmə onun üçün ağır nəticələrə səbəb ola bilər.

İstifadəçinin qərar qəbul etmək üçün lazım olan məlumatların vaxtında olmaması onun irrasional hərəkət etməsinə səbəb ola bilər.

İmtiyazlardan qeyri-qanuni istifadə. Hər hansı qorunan sistem fövqəladə hallarda istifadə olunan alətləri və ya mövcud təhlükəsizlik siyasətini pozaraq fəaliyyət göstərə bilən alətləri ehtiva edir. Məsələn, gözlənilməz audit zamanı istifadəçi sistemin bütün dəstlərinə daxil ola bilməlidir.

Bu alətlər adətən administratorlar, operatorlar, sistem proqramçıları və xüsusi funksiyaları yerinə yetirən digər istifadəçilər tərəfindən istifadə olunur.

Əksər təhlükəsizlik sistemləri belə hallarda imtiyaz dəstlərindən istifadə edir, yəni müəyyən funksiyanı yerinə yetirmək üçün müəyyən imtiyaz tələb olunur. Tipik olaraq, istifadəçilərin minimum imtiyazlar dəsti var, idarəçilər isə maksimuma malikdir.

İmtiyaz dəstləri təhlükəsizlik sistemi ilə qorunur. İmtiyazların icazəsiz (qanunsuz) ələ keçirilməsi təhlükəsizlik sistemində səhvlər olduqda mümkündür, lakin ən çox təhlükəsizlik sisteminin idarə edilməsi prosesində, xüsusən də imtiyazlardan ehtiyatsız istifadə edildikdə baş verir (Gatsenko, 2014, s. 113).

Təhlükəsizlik sisteminin idarə edilməsi qaydalarına ciddi riayət etmək və minimum imtiyazlar prinsipinə riayət etmək bu cür pozuntuların qarşısını almağa imkan verir.

KS təhlükəsizlik tədbirləri

Həyata keçirilmə üsullarına görə kompüter şəbəkələrinin təhlükəsizliyini təmin edən bütün tədbirlər aşağıdakılara bölünür: hüquqi (qanunverici), mənəvi-etik, təşkilati (inzibati), fiziki, texniki (texniki və proqram təminatı) (Kasperskiy, 2009, s. 22).

Hüquqi müdafiə tədbirlərinə ölkədə qüvvədə olan qanunlar, fərmanlar və qaydalar daxildir, informasiya münasibətləri iştirakçılarının onun işlənməsi və istifadəsi prosesində hüquq və vəzifələrini müəyyən edən, habelə bu qaydaların pozulmasına görə məsuliyyət müəyyən edən, bununla da məlumatdan sui-istifadə hallarının qarşısını alan və potensial pozucular üçün çəkindirici vasitə olan məlumatlar.

Mənəvi və etik əks tədbirlərə ənənəvi olaraq ölkədə və ya cəmiyyətdə yayılmış kompüter şəbəkələri kimi formalaşan və ya inkişaf edən davranış normaları daxildir. Bu normalar, qanunvericiliklə təsdiq edilmiş normativ aktlar kimi, əksər hallarda məcburi xarakter daşımır, lakin onların yerinə yetirilməməsi adətən bir şəxsin, bir qrup şəxsin və ya təşkilatın nüfuzunun və nüfuzunun azalmasına səbəb olur.

Əxlaqi normalar həm yazılmamış (məsələn, dürüstlük, vətənpərvərlik və s. ümumi qəbul edilmiş normalar), həm də yazılı ola bilər, yəni müəyyən qaydalar və ya qaydalar toplusunda (nizamnamələrində) rəsmiləşdirilir.

Təşkilati (inzibati) mühafizə tədbirləri məlumatların emalı sisteminin fəaliyyətini, onun resurslarından istifadəni tənzimləyən təşkilati xarakterli tədbirlərdir. Personalın fəaliyyəti, eləcə də təhlükəsizlik təhdidlərinin mümkünlüyünü ən çətinləşdirəcək və ya aradan qaldıracaq şəkildə istifadəçinin sistemlə qarşılıqlı əlaqəsi proseduru. Bunlara daxildir (Yakimenko, 2013):

- ✓ məlumatların emalı sistemlərinin şəbəkələrinin və digər obyektlərinin layihələndirilməsi, qurulması və təchiz edilməsi zamanı həyata keçirilən fəaliyyətlər;
- ✓ istifadəçinin şəbəkə resurslarına çıxışı qaydalarının işlənib hazırlanması üzrə tədbirlər (təhlükəsizlik siyasətinin işlənib hazırlanması);
- ✓ kadrların seçilməsi və hazırlanması zamanı həyata keçirilən tədbirlər;
- ✓ təhlükəsizliyin və etibarlı giriş nəzarətinin təşkili;
- ✓ sənədlərin və informasiya daşıyıcılarının uçotunun, saxlanmasının, istifadəsinin və məhv edilməsinin təşkili;
- ✓ girişə nəzarət detallarının paylanması (parollar, şifrələmə açarları və s.);
- ✓ istifadəçilərin işinə aşkar və gizli nəzarətin təşkili;
- ✓ avadanlıq və proqram təminatının layihələndirilməsi, hazırlanması, təmiri və modifikasiyası zamanı həyata keçirilən fəaliyyətlər və s.

Fiziki qorunma tədbirləri müxtəlif növ mexaniki, elektro- və ya elektron-mexaniki cihazların və strukturların istifadəsinə əsaslanır, potensial pozucuların şəbəkə komponentlərinə və qorunan məlumatlara, habelə vizual müşahidə, rabitə və təhlükəsizlik siqnallarının texniki vasitələrinə mümkün nüfuz və çıxış yollarında maneələr.

Texniki (texniki) mühafizə tədbirləri KS-nin bir hissəsi olan və (müstəqil və ya digər vasitələrlə birlikdə) mühafizə funksiyalarını yerinə yetirən müxtəlif elektron cihazların istifadəsinə əsaslanır (Stolings, 2013).

Proqram təminatının mühafizəsi üsulları üç sahədə məlumatı birbaşa qorumaq üçün nəzərdə tutulub:

a) avadanlıq,

b) proqram təminatı,

c) verilənlər və idarəetmə əmrləri.

Məlumatın ötürülməsi zamanı mühafizəsi üçün məlumatların şifrlənməsinin müxtəlif üsulları adətən onlar rabitə kanalına və ya fiziki mühitə daxil edilməzdən əvvəl, sonradan şifrənin açılması ilə istifadə olunur. Təcrübə göstərir ki, şifrələmə üsulları mesajın mənasını olduqca etibarlı şəkildə gizlədə bilər.

Maşın məlumatlarına girişi idarə edən bütün təhlükəsizlik proqramları suallara cavab vermək prinsipi əsasında fəaliyyət göstərir: kim hansı əməliyyatları və hansı verilənlər üzərində həyata keçirə bilər (Sidorin, 2013).

Giriş aşağıdakı kimi müəyyən edilə bilər:

- ✓ ümumi (hər bir istifadəçiyə qeyd-şərtsiz verilir),
- ✓ imtina (şərtsiz imtina, məsələn, məlumatın silinməsinə icazə),
- ✓ hadisədən asılı (hadisə idarəsi),
- ✓ verilənlərin məzmunundan asılıdır,
- ✓ vəziyyətdən asılı (kompüter sisteminin dinamik vəziyyəti),
- ✓ tezlikdən asılıdır (məsələn, istifadəçiyə girişə yalnız bir dəfə və ya müəyyən sayda icazə verilir),
- ✓ istifadəçinin adı və ya digər xarakteristikası ilə,
- ✓ hakimiyyətdən asılı olan,
- ✓ icazə ilə (məsələn, parolla),
- ✓ prosedura görə.

Həmçinin icazəsiz giriş cəhdlərinə qarşı effektiv tədbirlərə qeydiyyat alətləri daxildir. Bu məqsədlər üçün ən perspektivlisi xarici ölkələrdə geniş istifadə olunan və monitorinq (kompüterin mümkün təhlükələrinin avtomatik monitorinqi) adlanan yeni xüsusi təyinatlı əməliyyat sistemləridir.

Monitorinq əməliyyat sisteminin (ƏS) özü tərəfindən həyata keçirilir və onun vəzifələrinə maşın məlumatlarının daxil edilməsi/çıxışı, emalı və məhv edilməsi proseslərinin monitorinqi daxildir. ƏS icazəsiz giriş vaxtını və daxil olmuş proqram təminatını qeyd edir. Bundan əlavə, o, dərhal kompüter təhlükəsizlik xidmətini təhlükəsizlik pozuntusu barədə xəbərdar edir və zəruri məlumatların eyni vaxtda çapını həyata keçirir. Bu yaxınlarda ABŞ və bir sıra Avropa ölkələrində kompüter sistemlərini qorumaq üçün xüsusi alt proqramlardan da istifadə edilmişdir ki, bu da məxfi məlumatı olan faylın məzmununa icazəsiz baxmaq cəhdi zamanı əsas proqramın özünü məhv etməsinə səbəb olur. "Məntiqi bomba"nın hərəkəti (Vikhorev, 2013).

Təhlükəsizlik məqsədləri:

- kriptoqrafik üsullardan istifadə etməklə rabitə kanallarında və verilənlər bazalarında məlumatların mühafizəsi;
- məlumat obyektlərinin və istifadəçilərin həqiqiliyinin təsdiqi (rabitə quran tərəflərin autentifikasiyası);
- məlumat obyektlərinin bütövlüyünün pozulmasının aşkar edilməsi;
- konfidensial məlumatların işləndiyi texniki vasitələrin və binaların yan kanallar vasitəsilə sızmalardan və onlara daxil edilmiş elektron informasiya axtarış cihazlarından mühafizəsinin təmin edilməsi;

- proqram məhsullarının və kompüter avadanlıqlarının onlara proqram viruslarının və əlfəcinlərin daxil edilməsindən mühafizəsinin təmin edilməsi;
- şifrələmə vasitələrindən istifadə etmək səlahiyyəti olmayan, lakin məxfi məlumatı pozmaq və abunə məntəqələrinin işini pozmaq məqsədlərini güdən şəxslərin rabitə kanalı vasitəsilə icazəsiz hərəkətlərdən qorunması;
- məxfi məlumatların təhlükəsizliyini təmin etməyə yönəlmiş təşkilati və texniki tədbirlər.

Nəticə

Bu məqsədə çatmaq üçün aşağıdakı vəzifələri həyata keçirmək lazımdır:

- tədqiq olunan problem üzrə metodiki ədəbiyyatın təhlili əsasında konseptual aparatı müəyyən etmək;
- nəzəri materialların toplanması və sistemləşdirilməsi, informasiya təhlükəsizliyinə təhdidlərin təsnifatı və şəbəkənin qorunması üçün əsas tədbirlər;
- təcrübədə az istifadə olunan informasiya təhlükəsizliyi təhdidlərinin təsnifləşdirilməsi yollarını və şəbəkəni qorumaq üçün əsas tədbirləri nəzərdən keçirin.

Bu işdə aşağıdakı tədqiqat metodlarından istifadə edilmişdir:

- metodoloji ədəbiyyatın öyrənilməsi və təhlili (nəzəri təhlil və sintez);
- informasiya təhlükəsizliyi təhdidləri zamanı insanların fəaliyyətinin monitorinqi; tədqiqat məlumatlarının kəmiyyət və keyfiyyətcə işlənməsi.

Ədəbiyyat

1. Biyachuyev, T. A. (2012). *Bezopasnost' korporativnykh setey* (ucheb. posobiye). Pod red. L. G. Osovetskogo. SPbGU ITMO.
2. Domarev, V. V. (2012). *Zashchita informatsii i bezopasnost' komp'yuternykh system*. Piter.
3. Grishina, N. V. *Organizatsiya kompleksnoy zashchity informatsii*. Citforum.ru. http://citforum.ru
4. Goshko, S. V. (2014). *Entsiklopediya po zashchite ot virusov*. Izd-vo "SOLON-Press".
5. Gatsenko, O. Yu. (2014). *Zashchita informatsii.* Solon-press.
6. Kasperskiy, Ye. (2009). *Komp'yuternyye virusy*. Solon-press.
7. Mostovoy, D. Yu. (2010). *Sovremennyye tekhnologii bor'by s virusami.*
8. Metody zashchity informatsii v KS. (2013). *Komp'yutera*, 2.
9. Shangin, V. (2012). *Zashchita komp'yuternoy informatsii. Effektivnyye metody i sredstva*. DMK – Press.
10. Stolings, V. (2013). *Kriptografiya i zashchita setey: printsipy i praktika*. Izdatel'skiy dom "Vil'yams".
11. Sidorin, Yu. S. (2013). *Tekhnicheskiye sredstva zashchity informatsii*. MGTU im. Baumana.
12. Vikhorev, S. V. (2013). Kak uznat' – otkuda napast' ili otkuda iskhodit ugroza bezopasnosti informatsii. Zashchita informatsii. *Konfident*, 13.
13. Yakimenko, A. S. (2013). *Sredstva zashchity informatsii*. Yuniti.

Daxil oldu: 21.07.2024
Baxışa göndərildi: 20.08.2024
Təsdiq edildi: 05.09.2024
Çap olundu: 20.10.2024