UOT 004.4

Təranə Vəliyeva
Azərbaycan Əmək və Sosial Münasibətlər Akademiyası
e-mail:tarana 055@mail.ru

MÜƏSSİSƏNİN İNFORMASİYA TƏHLÜKƏSİZLİYİ QARŞISININ ALINMASI YOLLARI

Məqalədə müəssisənin informasiya təhlükələrinin yaranma səbəbləri-informasiya sisteminə ziyan vuran proqram təminatının daxil olması, sistem üzərində nəzarətin əldə edilməsi, rabitə xətlərindən və ötürmə resurslarından verilənlərin ələ keçirilməsi, informasiya daşıyıcılarının və sənədlərin oğurlanması və s., həmçinin onların aradan qaldırılması məsələləri tədqiq edilmişdir. Eyni zamanda, müəssisələrdə informasiya təhlükəsizliyi siyasətinin tərkibi, təhlükəsizlik mexanizmləri kompleksi və informasiya təhlükəsizliyini təmin edən sistemlərin əsas xüsusiyyətləri qeyd edilmiş, informasiya təhlükəsizliyinin qarşısının alınmasını təmin etməyin mühüm şərtləri göstərilmişdir.

Məqsəd **–** müəssisədə informasiyanın təhlükəsizliyinin təmin olunması məqsədilə gözlənilən təhlükələrin qarşısının alınmasıdır.

Metodologiya **–** məqalədə müəssisəni informasiya təhlükəsindən qorumaq üçün xüsusi təhlükəsizlik tədbirlərinin tətbiq olunması metodlarından istifadə edilmişdir.

Tədqiqatın nəticələri **–** müəssisənin informasiya təhlükəsizliyi siyasətinin təmin edilməsi üçün məlumatların müdafiə edilməsi, rəhbərliyin qeyri-qanuni işlərlə məşğul olmaq istəyənlər barədə operativ şəkildə məlumatlandırılması, zərərli proqramların tətbiq olunmasının qarşısının aınması üçün qabaqlayaıcı tədbirlərin görülməsidir.

Açar sözlər: *təhlükəsizlik, informasiya təhlükəsizliyi, təhlükəsizlik siyasəti, müəssisə cinayətkarlığı, qabaqlayıcı tədbirlər*

Giriş

Müasir informasiya texnologiyalarının inkişafı informasiya təhlükəsizliyiin ən vacib xarakteristikalarından birini təşkil edir və informasiya emalı sisteminin işlənməsi zamanı təhlükəsizlik amili birinci dərəcəli rol oynayır.

Dünya üzrə bütün sahələri əhatə edən İnternet qlobal şəbəkəsindən istifadə olunmaqla bir çox cinayətlər törədilir və bu mənfi hallar sürətlə yayılır. Buraya aiddir: qeyri qanuni informasiya mənbələrinə daxil olmaq, viruslar yaymaq, banklardan ”elektron pul oğurlamaq”, parnoqrafiya, “elektron şpionluq” və s. Bunların qarşısını almaq, təhlükəsizliyi qorumaq üçün informasiya həm hüquqi, həm texniki tərəfdən mühafizə olunur və mükəmməl qanunlar işlənib hazırlanır. Bu qanunlarda informasiyaların oğurlanmasının, itirilməsinin, dəyişdirilməsinin, qeyri-qanuni məhv edilməsinin, surətinin götürülməsinin qarşısının alınmasının təmin edilməsi, müxtəlif xidməti qürumların informasiyalarının tam təhlükəsizliyinin müəyyənləşdirilməsi əks olunur. Təhlükəsizliyin təmin edilməsi zəruri bir vəzifə olaraq qəsdən və bilərəkdən müdaxilə, informasiyanın oğurlanması və icazəsiz alınması cəhdlərindən qorunmanı ifadə edir. İnformasiya təhlükəsizliyini pozmaq üçün idarəetmə sisteminin aparat-proqram vasitələrindən icazəsiz istifadə edilir, onların dağılmasına səbəb olan hadisə və hərəkətlər törədilir. Ən qorxulu informasiya təhlükələri informasiya sisteminə ziyan vuran proqram təminatının daxil olması, proqram və ya verilənlərin dəyişdirilməsi, dağıdılması, sistem üzərində nəzarətin əldə edilməsi, rabitə xətlərində və ötürmə sistemlərində verilənlərin ələ keçirilməsi, hesablama sistemlərinin resurslarından

icazəsiz istifadə edilməsi, informasiya daşıyıcılarının və sənədlərin oğurlanması səbəblərindən yaranır.

Cəmiyyətin bütün sahələrində informasiya təhlükəsindən qorunmaq üçün müdafiə vasitələrinin tətbiqi siyasəti ilə məşğul olma yeni informasiyaların işlənib hazırlanmasında, informasiyanın mövcud mühafizə üsulları və vasitələrinin təkmilləşdirilməsində böyük əhəmiyyətə malikdir. İnformasiyanı təhlükədən xilas etmək üçün mənfi-neqativ halların yayılmasının qarşısını almaq, onu qorumaq, proqram və aparat vasitələrinin mühafizəsi problemini həll etmək, xüsusi təhlükəsizlik tədbirlərinin tətbiq olunmasını təmin etmək mühüm şərt hesab olunur.

1. Müəssisənin informasiya təhlükəsizliyi siyasəti

Müasir texnologiyalar cəmiyyətin bütün sahələrində məsafədən asılı olmadan qarşılıqlı əlaqələrin təşkilində böyük qüvvəyə malikdir və informasiya emalı proseslərini təmin edən sistemlərin əsasını təşkil edir. İstənilən müəssisənin fəaliyyətində idarəetmə prinsipləri informasiya ilə təmin olunduğundan funksional məsələlərin həlli informasiya texnologiyaları vasitəsi ilə həyata keçirilir. Müəyyən informasiya texnologiyaları informasiyanın bütövlüyünün pozulmasına yönələn təhlükələrin qarşısını almaq üçün tədbirlər kompleksini təşkil edir. Belə tədbirlər kompleksi informasiyanıın təbii və ya süni xarakterli təsirlərdən mühafizə olması toplusudur və informasiya təhlükəsizliyi anlamını verir (şəkil 1). İnformasiya təhlükəsizliyi – informasiyanın icazəsiz əldə olunmasının və ötürülməsinin qarşısını alaraq, informasiya obyektlərini və informasiya istifadəçilərini müxtəlif zərərlərdən mühafizə etməklə, mənfi təsirlərin qarşısını alır [3, s.25-30].

Şəkil 1. İnformasiya təhlükəsizliyi və dövlət maraqları
Mənbə: **Ordu.az**

Ümumilikdə, təhlükəsizlik- şəxsiyyətin, dövlətin və cəmiyyətin maraqlarının daxili və xarici təhdidlərdən, yəni, hədd qoymalardan mühafizə olunması olub, vətəndaşların konstitusiya və beynəlxalq normalara uyğun olaraq hüquqlarını təmin edir. Onun qorunması təhlükəsizlik sisteminin səmərəli fəaliyyəti nəticəsində mümkündür. Təhlükəsizliyin obyektləri kimi, cəmiyyətin maddi və mənəvi dəyərləri, dövlət və onun konstitusion quruluşu, suverenliyi və ərazi bütövlüyü götürülür.

Müasir təhlükəsizlik anlayışı "maddi dünyanın və insan cəmiyyətinin müxtəlif növlü neqativ təsirlərdən qorunması" anlamını verir və onun ictimai həyat sahələri üzrə bir neçə tipləri var: siyasi, sosial, qlobal, beynəlxalq, iqtisadi, informasiya, hərbi, demoqrafik, ekoloji, ərzaq, enerji, psixoloji, mənəvi-əxlaqi və s.

Təhlükəsizlik bir siyasət olmaqla, əsasən idarəetmə strategiyasının və onun resurs-

larının miqdarını müəyyən edir. Siyasət özü isə, fəaliyyətin məqsədləri, hüquqi tələbləri və normalarını təmin etmək, idarə etmək üçün təsdiq edilmiş qaydalar toplusudur [1].

Amerikalı dövlət xadimi, diplomat və beynəlxalq əlaqələr üzrə mütəxəssis Henri Kissincerin fikrincə, təhlükəsizlik siyasəti cəmiyyətin bütün fəaliyyətini əhatə edir və belə fəaliyyət zamanı cəmiyyət öz həyati mənafelərini təmin etməyə səy göstərir [2].

Hər hansı bir müəssisənin təhlükəsizlik siyasəti nəyin müdafiə edilməsini, müdafiə qanunlarından hansıların əsas olmasını müəyyən edir və informasiya sistemi üçün müdafiə strategiyası kimi xarakterizə olunur. Müdafiə strategiyasında informasiya təhlükəsizliyini təmin edən proqram tərtib edilərək, onun yerinə yetirilmə ardıcıllığı müəyyən edilir, proqrama uyğun olaraq resurslar ayrılır və bu resurslara məsul şəxslər seçilir. Ümumilikdə, müəssisənin informasiya sisteminin təşkili kompüter vasitəsilə həyata keçirilir, daha doğrusu, təhlükəsizlik siyasəti kompüter mühitində istifadə edilir və təşkilatın spesifik təminatını (müəyyən məqsədləri təmin edən faktoru) əks etdirir. Spesifik tələbata müxtəlif xüsusiyyətli aparat və proqram təminatlarının öz aralarında lazımi səviyyədə işləmələrinin uyuşa bilməsi, kompüterlər, əməliyyat sistemləri, şəbəkə vasitələri, verilənlər bazalarının idarəetmə sistemlərinin bir-biri ilə razılaşdırılmaları aiddir [3, s.63-65].

2. Müəssisənin informasiya təhlükəsizliyi siyasətinin tərkib elementləri

Hazırda, ən geniş yayılan təhlükələrdən biri müəssisə cinayətkarlığıdır. Bu cinayətkarlıq məlumatların səlahiyyəti olmayan şəxs və ya şəxslər tərəfindən qanunsuz toplanması, mənimsənilməsi, ötürülməsi, məqsədyönlü təsir göstərilməsi əməliyyatlarıdır. Əksər hallarda isə, icazə olmadan eşitmə qurğularının tətbiqi, məsafədən şəkil çəkmə, yaddaşda qalmış informasiyanın oxunması, informasiya daşıyıcılarının surətinin çıxarılması, qurğuların qeyri-qanuni rabitə xəttlərinə qoşulması, məxsusi proqramlar vasitəsilə qadağaların açılması və s. əməliyyatlar cinayət əmələri olur [4, s.32-35]. Müəssisənin informasiya təhlükəsizliyi siyasərinin təmin olunmasını rəhbərliyin informasiya təhlükəsizliyi üzrə idarəçilik və dəstəyinin müvafiq qanunlara və normativlərə uyğun olaraq təşkili əhatə edir (şəkil 2).

Şəkil 2. Məlumatların qanunsuz toplanmasının qarşısının alınması
Mənbə: İŞƏTSQ

Bu siyasət vacib resursların, məsələn, kompüter sistemlərinin və verilənlərin mühafizəsinə məqsədləri, məsuliyyəti və ümumi tələbləri təsvir edərək, təhlükəsizlik mexanizmləri kompleksinin köməyi ilə realizə olunur. Təhlükəsizlik mexanizmləri kimi, şəbəkələrarası ekranlar, antivirus sistemləri, video-nəzarət sistemləri və s. götürülür. İnformasiya təhlükəsizliyi siyasətinə daxil olan sənədlər iyerarxik şəkildə bu cür təsvir edilir:

1. Umumi informasiya təhlükəsizliyi siyasəti – rəhbərliyin münasibəti bildirilərək informasiya təhlükəsizliyinin idarə edilməsinə yanaşma, nəzarətin məqsədləri və mexa-

nizmləri müəyyən edilir;

2. Xüsusi informasiya təhlükəsizliyi siyasəti – antivirus proqramlarına müraciət, paroldan istifadə, İnternetin tətbiqi və s.təmin olunur;

3. İstismar üzrə təlimatlar yaradılır;

4. Vəzifələr üzrə təlimatlar yaradılır [1].

Müəssisənin informasiya təhlükəsizliyi siyasətinin tərkibinə aşağıdakı bölmələr daxildir:

- informasiya risklərinin idarə edilməsi;
- giriş hüquqlarının verilməsi;
- informasiya resurslarının auditi;
- elektron poçtdan istifadə;
- informasiya təhlükəsizliyi insidentlərinə cavabvermə;
- informasiya təhlükəsizliyinin monitorinqi;
- məsafədən giriş;
- fiziki təhlükəsizlik;
- informasiyanın kriptoqrafik mühafizəsi;
- şəxsi heyətin təhlükəsizliyi;
- şəbəkə təhlükəsizliyi;
- ehtiyat surətçıxarma;
- resursların təkrar istifadəsi, məhv edilməsi və s.

3. Müəssisənin informasiya təhlükəsizliyi problemləri və onun həlli yolları

Müəssisənin informasiya təhlükəsizliyi, adətən, sənəd formasında tərtib olunur və bu sənəddə müəssisənin problemləri izah olunur, bütün sahələr üzrə problemlərin həlli həyata keçirilir. Müəssisənin problemlərinə aşağıdakılar aid edilə bilər:

- müəssisənin müəyyən məqsədə çatması üçün görüləcək işlərin formalaşdırılması, bu məqsəd naminə ümumi istiqamətin müəyyənləşdirilməsi;
- İnformasiya təhlükəsizliyinin təmin edilməsi proqramının formalaşdırılması və proqramın yerinə yetirilməsində məsul şəxslərin müəyyən edilməsi;
- qayda-qanunların həyata keçirilməsi üçün material bazasının tərtib olunması;
- idarəedicilik qərarlarını yerinə yetirmək üçün proqram təminatının düzgün istifadə edilməsi.

Müəssisədə təhlükəsizlik siyasətinə baza təhlükəsizliyi, xüsusiləşdirlmiş təhlükəsizlik və təhlükəsizlik prosedurları aiddir.

Baza təhlükəsizliyi-müəssisədə təhlükəsizliyin məqsədini və strukturunu açıqlayır, kimin nəyə cavab verməsini müəyyənləşdirir, edilmiş dəyişikləri vaxt çərçivəsində müəyyən edir, icazə verilən və verilməyən fəaliyyətləri müəyyən edir. Eyni zamanda müəssisənin özünə aid olan informasiyanı təhlil etməsinə, təhlükəsizlik sisteminin yaradılması üçün vacib olan işlərin bütünlükdə yerinə yetirilməsinə imkan verir.

Xüsusiləşdirilmiş təhlükəsizlik-müəssisədə təhlükəsizliyin cari vəziyyətini araşdırmağa şərait yaratmaqla müəyyən sayda istifadəçilərin maraqlarını və əlçatanlıq siyasətinilarını təmin edir. Əlçatanlıq dedikdə, elektron avadanlıqlardan və müəssisə ilə əlaqəli şirkətlərin servislərindən düzgün istifadə edilməsi üçün standart normaların müəyyən edilməsi, işçilərin onlara məxsus informasiyaların və korporativ resursların təhlükəsizliyinin qorunması nəzərdə tutulur. Əks halda, müəssisə virusların hücumu, şəbəkə sisteminin və servisin etibardan düşməsi kimi risklərlə qarşılaşa bilir. Əlçatanlıq siyasəti isə, işçinin ona məxsus informasiyanı kompüterdə saxladıqdan sonra, qoruması üçün, məsuliyyət daşımasını, işçinin ona aid olmayan, lakin istifadəsi üçün icazə verilən faylları oxumağa,

surətlərinin çıxarılmasına səlahiyyətlərinin olmasını, elektron poçtdan istifadə imkanının verilməsini əhatə edir.

Təhlükəsizlik prosedurları – təhlükəsizlik siyasətini yerinə yetirən mexanizmi, yəni, sxemi hansı formada müdafiə etməyi müəyyən edir. Prosedur – müəssisədə icra olunan məsələlərin həllini həyata keçirən təlimatdır. Bu təlimata aiddir: müəssisəyə aid informasiyaların məxfi saxlanması üçün parolların qurulması, müdafiə olunması, dəyisdirilməsi, ehtiyat üçün surəti çıxarılmış material və vəsaitlərin müdafiə olunmaqla yaddaşda saxlanılması, login və istifadəçi parolunun arxivləşdirilməsi, işçi işdən çıxarıldıqda ona məxsus parolun ləğv edilməsi və s. (şəkil 3).

Şəkil 3. Təhlükəsizlik prosedurları
Mənbə: Texniki Yardım

Müəssisədə bəzən, baş vermiş qayda-qanun pozuntularına cavab vermək mümkün olmur, lakin, elə pozuntular da vardır ki, baş verməmiş onların qarşısını almaq olur. Təhlükəsizlik pozuntularının qarşısını almaq üçün aşağıdakı qaydalara əməl etmək mühüm hesab edilir:

- “xidmətdən imtina” hücumunu vaxtında yoluna qoymaq;
- işçilərə vəzifə prinsiplərinin icrasını yerinə yetirməli olduqlarını izah etmək;
- işlənəcək informasiyanı izləmək; tədqiqatları təhlil etmək və qəflətən edilən hücumları araşdırmaq;
- informasiyanı müəssisədən kənara yaymağı ehtimal olunan işçini xəbərdar etmək;
- müəssisədə yerinə yetiriləcək işlərin təhlillərinə rəhbərlik edən şəxsin məsuliyyətini və bu işdə iştirak edənlərin kimliyini yoxlamaq və s.

Müəssisənin iİnformasiya təhlükəsizliyinin idarəedilməsinin elementlər bir neçə qrup üzrə standartlaşdırılır:

1. Təhlükəsizliyin təmin edilməsi–müəssisənin rəhbərliyi tərəfindən informasiya təhlükəsizliyi sahəsində siyasətin dəstəklənməsi;
2. İnformasiya təhlükəsizliyinin təşkili – müəssisədə informasiya təhlükəsizliyi sisteminin iş qabiliyyətini təmin edəcək təşkilati strukturun yadradılması;
3. Resursların idarə edilməsi – informasiya resurslarının dəyər dərəcələrinə görə məsuluyyətin paylanması;
4. İşçilərin təhlükəsizliyi – insan səhvləri riskinin, oğurluğun və avadanlığın qanunsuz istifadəsinin azaldılması;
5. Fiziki təhlükəsizlik – avtorizə olunmamış girişin və təşkilatın informasiya sisteminin işinin pozulmasının qarşısının alınması;
6. Kommunikasiyanın və əməliyyatların idarə edilməsi – qurğuların və şəbəkələrin təhlükəsiz fəaliyyətinin təmin edilməsi;
7. Müəssisənin informasiya sisteminin yaradılması – bu sistemin inkişafı zamanı

informasiya təhlükəsizliyi tələblərinin yerinə yetirilməsi;
8. Tətbiqi proqramların və verilənlərin təhlükəsizliyinin dəstəklənməsi;
9. İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi;
10. Müəssisənin fasiləsiz fəaliyyətinin idarə edilməsi – fövqəladə hallarda fasiləsiz fəaliyyətin təmin edilməsi üçün fəaliyyət planının hazırlanması.

4. İnformasiya təhlükəsizliyi siyasətinin təmin olunmasının kompleks tədbirləri

Ümumilikdə, informasiya təhlükəsizliyi siyasətinin təmin olunması problemi kompleks yanaşma tədbirlərini tələb edir. Bu tədbirlərə aiddir:

- Qanunvericilik tədbirləri;
- İnzibati tədbirlər;
- Təşkilati tədbirlər;
- Proqram-texniki tədbirlər.

Qanunvericilik tədbirləri müvafiq qanunları, normativ aktları, standartları və s. əhatə etməklə, informasiya təhlükəsizliyinin pozucularına qarşı neqativ münasibəti dəstəkləyir.

İnzibati tədbirlər təşkilatlarda informasiya təhlükəsizliyi sahəsində tədbirlər proqramını formalaşdırır və onun yerinə yetirilməsini zəruri resurslar ayırmaqla və işlərin vəziyyətinə nəzarət etməklə yerinə yetirir.

Təşkilati tədbirlər informasiya mühafizəsinin səmərəli vasitələrindən biri olmaqla, qurulan bütün mühafizə sistemlərinin əsasını təşkil edir. Mühafizə sistemləri bunlardır:

- şəxsi heyətin idarə olunması;
- sistemin iş qabiliyyətinin saxlanması;
- təhlükəsizlik rejiminin pozulmasına reaksiya;
- bərpa işlərinin planlaşdırılması.

Proqram – texniki tədbirlər identifikasiya (istifadəçinin öz adının bildirməsi) və autentikasiya (istifadəçi adının təsdiqlənməsi), icazələrin idarə olunması, protokol-laşdırma və audit, kriptoqrafiya, ekranlaşdırma proseslərinin icra olunmasına imkan verir.

Autentikasiyanın ən geniş yayılmış növü paroldur. Daxil edilmiş parol və istifadəçi üçün əvvəlcədən verilmiş parol müqayisə edilir. Onlar üst-üstə düşdükdə istifadəçinin həqiqiliyi təsdiqlənmiş sayılır. Bəzən parollar elektron ələ keçirilə bilir. Bu zaman çıxış yolu rabitə xətləri ilə ötürülməzdən əvvəl parolların kriptoqrafik şifrələnməsidir. Parolların etibarını artırmaq üçün ona hərf, rəqəm, durğu işarələri olmaqla texniki məhdudiyyətlər qoyulur, fəaliyyət müddətləri vaxtaşırı dəyişdirilir, sistemə lazımsız daxilolma cəhdləri məhdudlaşdırılır və digər müvafiq metodlar tətbiq edilir.

İcazələrin idarə edilməsi istifadəçi və proseslərin informasiya və kompyuter resursları üzərində yetinə yetirdikləri əməliyyatları müəyyən etməyə və onlara nəzarət etməyə imkan verir. Bu idarə edilmə proqram vasitələri ilə realizə olunur və informasiya təhlükəsizliyi sahəsində ən mürəkkəb mövzu hesab olunur.

Protokollaşdırma informasiya sistemində baş verən hadisələr haqqında məlumatın qeyd edilməsi və toplanması, *audit* isə, toplanan informasiyanın analizidir. Protokollaşdırma və audit prosesi əsasən istifadəçi və administratorların hesabat verməsini təmin edir və informasiya təhlükəsizliyini pozma cəhdlərini aşkarlayır.

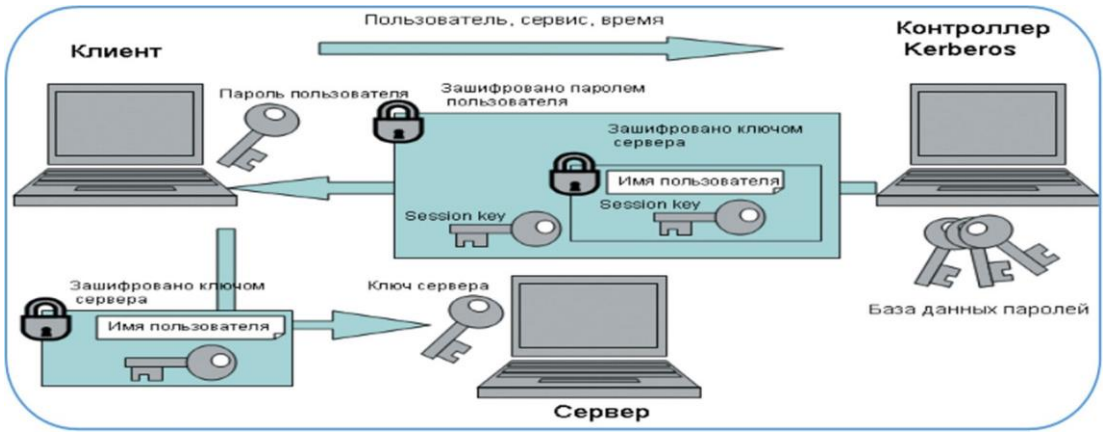
Kriptoqrafiya (yunan dilində “gizli yazı”) informasiyanı mənfi əməllərdən mühafizə etmək üçün istifadə edilən informasiya çevirməsidir-şifrləmədir. Bu əməliyyat müəyyən alqoritmdən və açardan istifadəni nəzərdə tutur.

Ekranlaşdırma iki informasiya sistemini nizamlamaqla istifadəçilərin serverlərə müraciətlərini təmin edir və öz funksiyalarını iki sistem arasındakı bütün informasiya

axınına nəzarət etməklə yerinə yetirir [7].

İnformasiya sistemlərində informasiya təhlükəsizliyini kompleks təşkil etmək üçün bu sistemin yerləşdiyi bütün ərazi tam əhatə olunmalı, sistemin qurgularının və rabitə xətlərinin yerləşdiyi ayrı-ayrı ərazilər nəzarətdə saxlanmalı, informasiya daşıyıcılarının xarici təsirlərdən qorunması təmin olunmalı, informasiyanın saxlanması, emalı və ötürülməsi prosesləri düzgün icra edilməlidir. İnformasiya təhlükəsizliyini təmin etmək üçün bir çox proqram sistemləri mövcuddur. Bu sistemlərdən də ən çox müraciət olunanları “Kerberos” və “Kobra” sistemləridir.

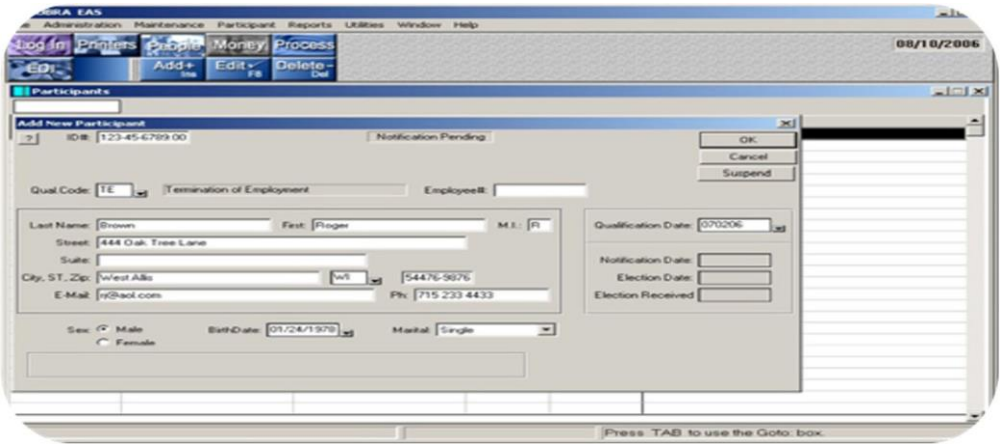
“Kerberos” sistemi – şifrlənmə açarlarının mübadiləsi üçün yaxşı mühafizə olunan mərkəzləşdirilmiş idarəetmə sistemi olub, bir neçə işçi stansiyalara malikdir. Bu işçi stansiyalar mühafizə olunmur və serverlər zəif mühafizə olunur. Sistemdə informasiya şəbəkədə ötürülərək bir neçə dəfə şifrlənirr. Şəbəkədə parollar heç vaxt şifrlənməmiş ötürülmür. Xidməti informasiyanın mübadiləsi zamanı məhdud vaxt ərzində işlək olan və istifadəçinin adından, ünvanından və vaxt qeydiyyatından ibarət olan şifrlənmiş verilənlərdən-autentikatorlardan (authenticator) istifadə edilir (şəkil 4).



Şəkil 4. “Kerberos” proqram sistemi (Heimdal Kerberosun işləmə prinsipini öyrənirik)
Mənbə: SecurityLab.ru

“Kerberos” sistemində istifadəçi özünün identifikasiya kodunu sistemə daxil edir. Həmin kod kliyent tərəfindən şifrlənir və “icazə almaq üçün icazə” sorğusu kimi identifikasiya serverinə ötürülür. İdentifikasiya serveri verilənlər bazasında icazəli istifadəçilərin parolunu tapıb məlumatı şifrləyir və kliyentə göndərir. Kliyent “İcazəyə icazə” aldıqdan sonra onu açır, oradan parolu götürür və istifadəçidən parolu soruşur. Alınan və daxil edilən parollar uyğun gəlirsə, kliyent tələb olunan şəbəkə resurslarına müraciət ücün serverə şifrlənmiş sorğu tərtib edir. Açılma və yoxlamalar nəticəsində istifadəcinin həqiqiliyinə əmin olduqdan sonra server istifadəçiyə sistemin resurslarından istifadə üçün şifrlənmiş icazə göndərir. Kliyent bu icazənii alıb, şifri açır, şifrlənrniş məlumat vasitəsilə tələb olunan serverlə əlaqə yaradır və istifadəçi resurslara müraciət hüququ əldə edir.

“Kobra” sistemi düzgün mühafizə texnoloqiyasına əsaslanmaqla ən geniş yayılmış və səmərəli sistemlərdən biridir. Bu sistemdə düzgün mühafizə dinamik şifrlənmə üsulunun köməyilə qurulur. Xarici yaddaşa yazılan məxfi informasiya istifadəçinin parolundan asılı olan açara görə avtomatik şifrlənir. Şifrlənən informasiyanın oxunması zamanı şifr avtomatik olaraq açılır. Şifirlənmənin sürətini və etibarlığını artırmaq üçün kriptomühafizə texnoloqiyasından istifadə edilir (şəkil 5) [6, s.142-143].



Şəkil 5. “Kobra” proqram sistemi
Mənbə: /Back/PDF Broghure/Get A Demo/

İnformasiya verilənlər bazasında (VB) saxlanılarkən onların təhlükəsizliyini mühafizə etmək də ən mühüm şərt hesab olunur. Verilənlər bazasında mühafizə vasitələrinə aiddir: parol mühafizəsi, verilənlərin və proqramların şifrlənməsi, VB obyektlərinə müraciət hüququnun təyin edilməsi.

Parol mühafızəsi – VB-yə icazəsiz müraciətin ən sadə mühafizə üsulu olub, istifadəçilər və ya VB administratoru tərəfindən təyin edilir, onun uçotunu və saxlanmasını VBİS yerinə yetirir. Parollar VBİS-in müəyyən sistem fayllarında şifrlənmiş şəkildə saxlanır. Parolu daxil etdikdən sonra istifadəçiyə mühafizə olunan VB ilə işləmək ücün bütün imkanlar verilir.

Verilənlərin şifrlənməsi – VBİS-in formatını bilən digər proqramların bu bazada olan verilənləri oxuya bilməməsi üçün istifadə olunan metoddur. Bu şifrləmədə hər bir kəs VB-nin şifrini aça bilir. Əgər şifrlənmə və şifrin açılması üçün parol tələb olunursa, onda düzgün parol daxil edilərək şifr açılır.

VB obyetlərinə müraciət hüququnun təyin edilməsi-VBİS-in əsas resurslarından istifadə etmək üçündür. Bu müraciət hüquqi obyektlər üzərində bir çox mühüm əməliyyatları-obyektin verilənlərinə baxılması və oxunmasını, verilənlərin redaktə edilməsini, verilənlərin cədvəlinin strukturunun dəyişdirilməsini və s. təyin edir.

Bəllidir ki, informasiyanı İnternet vasitəsi ilə əldə edilməsi İT-nin vacib parameterlərindən biri sayılır. Bu zaman İnternet mühüti hər kəs üçün daha təhlükəsiz edilməli və kibercinayətkarlığa qarşı mübarizə aparılmalıdır. Kibercinayət-informasiya sisteminə bağlı informasiya ehtiyatlarını və informasiya texnologiyalarından istifadə edən istifadəçiləri hədəfə alan, icazəsiz və hüquqa zidd şəkildə daxil olunan və sonra həyata keçirilən əməl və ya cinayətlərdir. Başqa sözlə, kibercinayət əsasən kompüter və internetə bağlı işlənən əməldir. Kibercinayət zamanı insan, onun əmlakı, eyni zamanda istifadə olunan sistemin özü də hədəf seçilir. Məsələn, bir sistemə zərər vermək, bazanı, informasiya ehtiyatını silmək, şifrələmək, ələ keçirmək, sistemin iş prinsipini dayandırmaq, şəxsi həyatın toxunulmazlığını pozmaq, əlaqəni icazəsiz izləmək, qeydə almaq və s. əməllər kibercinayətkarlıq hesab edilir. Kibercinayətkarlıqla mübarizə aparmaq üçün ekspert və mütəxəssislərin təcrübə mübadiləsi aparmasına şərait yaradılmalı, əks-hücumlara hazır olunmalıdır [5, s.34-37].

Nəticə

İstənilən müəssisədə informasiya təhlükəsizliyi üzrə mükəmməl strategiya tətbiq olunmalıdır. Bu strategiyada informasiya proseslərinin mühafizəsi, sabitliyi, informasiya ehtiyatlarının qorunması, təhdidlərin qarşısının alınması üçün istifadəçilərin fəaliyyətinin əlaqələndirilməsi, kibertəhlükəsizlik sahəsində risklərin qiymətləndirilməsi, idarə olunması və s. kimi mühüm müddəalar gücləndirilməlidir. Müəssisələrin informasiya-telekommunikasiya sistemlərinin və şəbəkələrinin, elektron sənəd dövriyyəsinin, kibertəhlükəsizlik sahəsində hazırlığın artırılması, bu sahədə qabaqlayıcı tədbirlərin həyata keçirilməsi, internet informasiya resurslarının və informasiya sistemlərinin təhlükəsizlik parametrlərinə diqqətin gücləndirilməsi əsas şərt kimi nəzərə alınmalıdır.

Azərbaycanda informasiya təhlükəsizliyi ilə bağlı bütün sahələrdə operativ və çevik fəaliyyət təmin olunaraq antivirus, antihaker proqram məhsullarının tətbiq edilməsi prosesi gedir, dünya tərəfindən qəbul edilmiş ən qabaqcıl və innovativ informasiya təhlükəsizliyinə dair standartların tətbiq edilməsinə dərin zəmin yaradılır. Təhlükəsizlik xidmətlərindən istifadənin diapazonunun günü-gündən genişlənməsi daha müasir texnoloji yeniliklər təklif edir.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT SİYAHISI

1. AzScienceCERT “İnformasiya təhlükəsizliyi siyasəti”. AMEA İnformasiya Texnologiyaları İnstitutu. 2013
2. Rüstəmov (BDU-nun professoru) Milli təhlükəsizlik məsələsi (yazı)
3. V.Ə.Qasımov “İnformasiya təhlükəsizliyinin əsasları”. Dərslik. Bakı, 2009
4. M.Əlizadə, H.Bayramov, Ə.Məmmədov “İnformasiya təhlükəsizliyi”. Dərslik. Bakı. “İqtisad Universiteti“ nəşriyyatı, 2016
5. “İnformasiya sistemlərində təhlükəsizliyin təmini” fənnindən mühazirələr. SDTK. Sumqayıt. 2020
6. M.Məmmədov “İnformasiya iqtisadiyyatı”. Dərs vəsaiti. Kitab Yurdu.org. 2013
7. İnformasiya təhlükəsizliy i/ Kompüter şəbəkələrində informasiya təhlükəsizliyinin təmini.Vikikitab
8. “Kibercinayətkarlıq haqqında” Konvensiyanın Təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, 30 sentyabr 2009-cu il

Тарана Велиева

ПУТИ ПРЕДОТВРАЩЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Резюме

В статье рассмотрены причины возникновения информационных угроз предприятий-проникновение вредоносного программного обеспечения в информационную систему, получение контроля над системой, перехват данных с линий связи и передающих ресурсов, хищение носителей информации и документов и др., а также были исследованы вопросы их устранения. При этом отмечается состав политики информационной безопасности на предприятиях, комплекс механизмов безопасности и основные характеристики систем обеспечения информационной безопасности, указываются важные условия обеспечения предотвращения информационной безопасности.

Цель – предотвращение ожидаемых угроз с целью обеспечения информационной безопасности на предприятии.

Методология **–** в статье использованы методы применения специальных мер безопасности для защиты предприятия от информационной опасности.

Результаты исследования **–** защита информации для обеспечения политики информационной безопасности предприятия заключается в оперативном информировании руководства о желающих заниматься незаконной деятельностью, принятии превентивных мер по предотвращению внедрения вредоносных программ.

Ключевые слова: *безопасность, информационная безопасность, политика безопасности, корпоративная преступность, превентивные меры*

Tarana Valiyeva

THE INFORMATION SECURITY POLICY OF ENTERPRISE

Summary

The article discusses the causes of information threats to enterprises – the penetration of malicious software into the information system, gaining control over the system, interception of data from communication lines and transmitting resources, theft of information carriers and documents, etc., and also investigated the issues of their elimination. At the same time, the composition of the information security policy at enterprises, the complex of security mechanisms and the main characteristics of information security systems are noted, and important conditions for ensuring the prevention of information security are indicated.

Purpose of the research **–** prevention of expected threats in order to ensure information security in the enterprise.

Methodology – the article uses methods of applying special security measures to protect the enterprise from information hazards.

Findings **–** information protection to ensure the information security policy of the enterprise consists in promptly informing the management of those who want to engage in illegal activities, taking preventive measures to prevent the introduction of malicious programs.

Keywords: *безопасность, информационная безопасность, политика безопасности, корпоративная преступность, превентивные меры*