UOT 504.064.47

Ağayev B.S.[1], Mehdiyev Ş.A. [2], Əliyev T.S.[3]
[1,2,3]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1,3] depart6@iit.ab.az, [2]depart11@iit.ab.az

ELEKTRON MƏLUMAT DAŞIYICILARI İNFORMASİYA TƏHLÜKƏSİZLİYİNİN OBYEKTİ KİMİ

Məqalədə bir sıra məlumat daşıyıcılarının informasiya təhlükəsizliyi və mühafizə problemləri araşdırılır. Elektron tullantıların daşıyıcılarında və kağızda saxlanılan məxfi və dövlət sirri daşıyan məlumatların qorunması, ehtiyat nüsxələrinin yaradılması, utilizasiyası, bərpa metodları və qurğuları analiz edilir. Məlumat daşıyıcılarının idarə edilməsi sisteminin yaradılması məsələsi nəzərdən keçirilir.

Açar sözlər: *elektron tullantılar, elektron tullantıların utilizasiyası, elektron məlumat daşıyıcıları, informasiya təhlükəsizliyi, informasiya mühafizəsi, maqnit-optik daşıyıcılar, strimmerlər.*

Giriş

İnsanların istənilən sahədə əmək fəaliyyəti prosesində maddi nemətlər və xidmətlərlə yanaşı, tullantılar da yaranır. Tullantılar insan sağlamlığına təhlükə yaratmaqla bərabər, ətraf mühiti də çirkləndirir. Eyni zamanda, tullantılar sənaye üçün mühüm material-xammal və istilik-energetik xammal resurslarıdır. Tullantılar insan sağlamlığına və ətraf mühitə vurduğu ziyana və ya yaratdığı təhlükəyə görə kəskin fərqlənirlər: onlar ziyansız və ya çox ziyanlı (təhlükəli) ola bilər.

Elektron tullantılar - tullantıların bir növüdür və yaratdığı təhlükəyə görə III qrupa (təhlükəli) aid edilir. Beynəlxalq Standartlaşdırma İttifaqının təsnifatına görə, elektron tullantılar qrupuna elektron cihaz, qurğu və avadanlıqlar, o cümlədən kompüter avadanlıqları ilə bərabər, elektrotexniki (elektrik) avadanlıqları da daxildir və qısaca olaraq *WEEE* (*Waste Electrical and Electronic Equipment* – Elektrik və Elektron Avadanlıqların Tullantıları) kimi işarələnir.

Avropa İttifaqının elektron tullantılar haqqında 2012/19/EU saylı Direktivində 10 qrupda toplanmış 600 adda elektrik və elektron avadanlıqlarının tullantıları elektron tullantıya aid edilir [1]. Telekommunikasiya və şəbəkə avadanlıqları təsnifatın üçüncü qrupunu təşkil edir.

Digər tərəfdən, tarix boyu informasiya insanın və cəmiyyətin keyfiyyətli fəaliyyətini təmin edən mühüm aminlərdən biri olmuşdur. Bir tərəfdən, insanların həyat keyfiyyətini yüksəldən vasitə kimi informasiyanın əhəmiyyəti artsa da, digər tərəfdən, informasiya cəmiyyətinin formalaşdığı müasir dövrdə onun yarada biləcəyi təhlükə və ziyanın kəmiyyət və keyfiyyət göstəriciləri də yüksəlir. Məlumatların itirilməsi, bədniyyətli tərəfindən qərəzli məqsədlərlə əldə keçirilməsi nəticəsində, məxfilik və sirlilik dərəcəsindən asılı olaraq, bu ziyan az və ya çox ola bilər. İnformasiya təhlükəsizliyi və onun mühafizə metodlarının inkişafı paralel olaraq sızma kanallarının genişlənməsi, oğurlanması (əldə keçirilməsi) üçün istifadə edilən texnika və texnologiyaların daha yüksək inkişaf səviyyəsi ilə müşayiət edilir. Araşdırmalar göstərir ki, zaman keçdikcə informasiya təhlükəsizliyinin təmin edilməsi məsələlərinin aktuallığı daha da artır. Ona görə də hazırda hər bir ciddi təşkilat məlumatların informasiya təhlükəsizliyi və mühafizəsi məsələlərinə çoxfaktorlu, çoxməqsədli problem kimi yanaşmalı və effektiv təhlükəsizlik sisteminin: a) təşkilati-hüquqi; b) proqram-aparat; və c) mühəndis-texniki aspektlərinin yerinə yetirilməsinə xüsusi diqqət yetirməlidir.

Məqalədə, əsasən, elektron tullantıların informasiya daşıyıcılarının informasiya təhlükəsizliyinin proqram-aparat təminatı məsələlərinə baxılacaq.

Elektron informasiya daşıyıcıları haqqında

Son illər informasiya cəmiyyətinin formalaşması ilə əlaqədar olaraq onun xarekterik xüsusiyyətlərini əks etdirən kompüterləşmə, şəbəkələşmə prosesləri geniş vüsət alıb. Bu isə, ilk növbədə, kompüter və şəbəkə avadanlıqlarının sayının sürətlə artması deməkdir. Təkcə Azərbaycan kimi kiçik bir ölkədə, 2014-cü məlumatlarına görə, 1 mln.-dək kompüter və 10 mln-dan çox mobil telefon istifadədə olmuşdur [ ]. Bu istifadəçilərin hər biri üçün sahib olduğu texniki vasitələrin informasiya təhlükəsizliyinin təmin edilməsi əhəmiyyətli məsələdir. Texnika və texnologiyaların müasir inkişaf səviyyəsində istifadə olunan texniki qurğu və avadanlıqların böyük əksəriyyəti elektron yaddaş, element və qovşaqlarına – elektron informasiya daşıyıcılarına malikdir. Ona görə də texniki nöqteyi-nəzərdən, informasiya təhlükəsizliyi dedikdə, ilk növbədə, onların informasiya daşıyıcılarının təhlükəsizliyi məsələləri nəzərdə tutulur.

Məlumat daşıyıcılarının informasiya təhlükəsizliyinin təmin edilməsi məlumatların əks olunduğu maddi daşıyıcıların növündən, onun fiziki, mexaniki, kimyəvi, erqonomik xüsusiyyətlərindən asılı olaraq seçilmiş mühafizə metodları və qaydaları ilə təmin edilir. İnformasiyanın əsas həcmi aşağıda göstərilən maddi daşiyıcılarda yadda saxlanılır.

– bərk və yumşaq maqnit daşıyıcılar (disklər, disketlər);
– maqnit-optik daşıyıcılar (disklər);
– strimmerlər;
– *ZIP*-yaddaş diskləri;
– fləş-yaddaş prinsipi əsasında yaradılmış fləş-disklər – fləş-saxlanclar, fləş-kart;
– kağiz;
– və s.

Bütün bu maddi yaddaş vasitələrində mətn, audio-video materiallar, şəkillər, layihələr, hesablamalar və s. formasında saxlanılan informasiyanın tərkibində məxfi məlumatlar (fərdi, xidməti, kommersiya, məhkəmə-istintaq, peşə, istehsalat və s.) və ya dövlət sirri (xüsusi əhəmiyyətli, tam məxfi və məxfi) ola bilər. Bu fiziki daşıyıcılar məlumatların yazıldığı yerlərdə (ev, iş yerləri, istirahət yerləri və s.) saxlanıla, başqa yerə daşına, başqasına verilə, tullanıla və s. yerdəyişmələrə məruz qala bilər. Aydındır ki, bu daşıyıcıların nəzarətsiz hərəkəti, icazəsiz istifadəsi, itməsi və ya oğurlanması, qərəzli məqsədlə silinməsi, dəyişdirilməsi və s. hallar dövlət maraqları, təşkilatlar, adi vətəndaşlar üçün ziyanlı ola bilər. ABŞ-ın *Identity Theft Resource Center* qeyri-hökumət təşkilatının məlumatına görə, e-tullantıların zərərsizləşdirilməsinin etibarlı metodlarla aparılmaması nəticəsində 2014-cü il ölkənin hökumət və hərbi sektorunda 50 halda, dövlət sirri də daxil olmaqla, sirr daşıyan məlumatların itirilməsi baş vermişdir (2,5 mln. ədəd mətn – fayl şəklində) [2]. Ona görə də informasiya daşıyıcısında yadda saxlanılan məlumatların informasiya təhlükəsizliyinin təmin edilməsi dövlət, təşkilatlar və hər bir şəxs üçün əhəmiyyətli və aktual məsələdir. İnformasiya daşıyıcısından informasiyanın icazəsiz yayılması (sızması), əsasən, aşağıdakı kanallar vasitəsilə həyata keçirilir.

– insayder və autsorsinq fəaliyyəti;
– elmi tədqiqat və təcrübi konstruktor işləmələri (ETTKİ);
– istehsalat fəaliyyəti;
– kağız və elektron tullantıların məlumat daşıyıcıları.

İnsayder fəaliyyəti (işçilər və ya keçmiş əməkdaşlar, tərəfdaşlar və s. tərəfindən informasiya təhlükəsizliyinin pozulması), eləcə də, autsorsinq fəaliyyəti (təşkilatın işçi, iş yeri, iş funksiyalarının və s. resurslarının başqa təşkilatın xidmətinə verilməsi) prosesində autsorser əməkdaşları tərəfindən informasiya təhlükəsizliyinin pozulması, əsasən, məlumatların qeyri-qanuni əldə edilməsi və digər tərəfə ötürülməsi yolu ilə baş verir. ETTKİ, eləcə də, istehsal prosesində yaranan kağız sənədlər (eskizlər, layihələr, qeydlər, hesablamalar, hesabatlar və s.), maketlər, qovşaqlar, elementlər, məhsul nümunələri və onların tullantıları, çıxdaş məhsulları, istehsalat yerindən ətrafa yayılan axar çirkab sular, hava kütləsi, istifadə edilən radioaktiv elementlərin şüaları və s. müəyyən məxfi və sirli məlumatların daşıyıcıları ola bilər. Bu

mənbələrin informasiya təhlükəsizliyi də mövcud qanunvericilik, təşkilatdaxili hüquqi-normativ sənədlər, təlimatlar, təşkilati qaydalar və s. vasitələrlə təmin edilməlidir.

Texnika və texnologiyaların müasir inkişaf səviyyəsində əsas informasiya daşıyıcıları elektron formadadır. Elektron daşıyıcılardakı məlumatların informasiya təhlükəsizliyinin pozulması hallarının böyük əksəriyyəti saxlanan informasiyanın zəruri hallarda silinməməsi və ya məhv edilməməsi nəticəsində baş verir. Burada "zəruri hal" dedikdə, baş verməsi planlaşdırılan və bu zaman yol verilməyən müdaxilələrə imkan yaranacağı ehtimal olunan əməliyyatlar nəzərdə tutulur. Bu əməliyyatlara, əsasən, aşağıdakılar aiddir:

- istismar müddəti bitmiş elektron və elektrik avadanlıqların balansdan silinməsi (o cümlədən ev təsərrüfatları üçün – atılması) – elektron tullantı halına keçməsi;
- elektron tullantıların idarə edilməsi sisteminin tələblərinə uyğun olaraq, ilkin və təkrar emal məqsədilə tullantı mərkəzlərinə təhvil verilməsi;
- məişət və sənaye tullantıları kimi atılması;
- avadanlıqların təmir məqsədilə başqa təşkilata daşınması;
- elektron tullantıların (məsələn, kompüterlərin) hədiyyə, yardım və ya başqa formada digər təşkilatın balansına keçirilməsi;
- müəyyən məqsədlə daşıyıcıların bir yerdən başqa yerə daşınması (bölmələrdən ofisə, iş yerindən evə, təmir yerlərinə və s.)
- və s.

Elektron tullantların informasiya daşıyıcılarının utilizasiyası haqqında

Azərbaycan qanunvericiliyinə görə, işlək vəziyyətindən, mənəvi və ya fiziki aşınma dərəcəsindən asılı olmayaraq, 9 il istismar müddəti bitdikdən sonra (ildə 10,1% amortizasiya şərti ilə) kompüterlər balansdan silinə bilər. Balansdan silinmiş kompüterlər müvəqqəti saxlanma yerinə, məsələn, anbara göndərilir. "İstehsalat və məişət tullantıları haqqında" Azərbaycan Respublikası Qanununa [3] və "Qiymətli metallar və qiymətli daşlar haqqında" Azərbaycan Respublikası Qanununa [4] görə, tərkibində qiymətli metallar (qızıl, gümüş və platin qrupu elementləri) olduğuna görə kompüterlər balansdan silinən andan qiymətli metalların tullantıları hesab edilir. Tərkibindəki qiymətli metalların hasil edilməsi üçün bu tullantılar yaranma yerində xüsusi qaydada emal edilməli və ya bu məqsədlə xüsusi təşkilatlara təhvil verilməlidir. Lakin ölkəmizin qanunvericiliyində "elektron tullantıları", "elektron tullantıların idarə edilməsi" məfhumları olmadığı kimi, bu sinif tullantıların ilkin və təkrar emalı müəssisələri, infrastrukturu da yoxdur [5]. Adətən təşkilatlar qanunun tələbləri ilə ziddiyyət yaratmamaq üçün kompüterlərin, eləcə də, digər elektrik və elektron avadanlıqların balansdan silinməsini uzadır (xüsusilə anbarlaşdırma imkanları məhduddursa), balansdan silib anbarda saxlayır və ya bağışlama, hədiyyə və s. adla uşaq bağçası, orta məktəb və s. təşkilatların balansına keçirir [6]. Bir çox hallarda kompüterlər məişət və istehsalat tullantıları kimi atılır. Eyni sözləri ev təsərrüfatlarına da aid etmək olar. Tullantı poliqonlarına düşən kompüterlər basdırma yolu ilə zərərsizləşdirilir və ya sadəcə atılmış vəziyyətdə qalır.

Aparılmış müşahidələr göstərir ki, bir çox hallarda, istər ev təsərrüfatları, istərsə də, təsərrüfat subyektləri atılmaq üçün nəzərdə tutulmuş kompüterlərin informasiya daşıyıcılarındakı informasiyanı, ümumiyyətlə, silmirlər və ya etibarlı (keyfiyyətli) şəkildə məhv etmirlər. Burada "etibarlı şəkildə məhvetmə" dedikdə, daşıyıcılardan informasiyanın elə silinməsi nəzərdə tutulur ki, həmin məlumatları heç bir üsulla bərpa etmək mümkün olmasın. Əks təqdirdə müəyyən yollarla bədniyyətli tərəfindən əldə edilmiş məlumatlardan qərəzli məqsədlərlə istifadə etmək imkanı yaranır. Təcrübədən məlumdur ki, peşəkar kəşfiyyatçıların məlumatları əldə etmək üçün çox "sevdiyi" mənbələrdən biri tullantı yerləridir (zibilxanalar, poliqonlar). İnformasiya daşıyıcılarındakı informasiyanın silinməsi onlardakı məlumatların məxfilik və sirlilik dərəcəsindən asılı olaraq iki texnologiya üzrə aparılır:

1. informasiyanı daşıyıcıya yazma prinsiplərinə əsaslanan silmə texnologiyaları. Bu texnologiyada, əsasən, iki metoddan istifadə edilir: a) kompüterin əməliyyat sisteminin funksional imkanları ilə silmə; b) xüsusi silmə qurğularından istifadə etməklə məhvetmə.
2. digər mexanizmlərə əsaslanan metodlarla silmə (məhvetmə).

Kompüterin əməliyyat sisteminin proqram vasitələrinin imkanları ilə daşıyıcılardakı informasiyanı etibarlı şəkildə silmək mümkün deyil. Prinsip etibarilə ilə əməliyyat sistemi elə işlənir ki, istifadəçilərin təsadüfi səhv əməliyyatları nəticəsində məlumatlar dönməz şəkildə itməsin, yəni lazım gəldikdə onu bərpa etmək mümkün olsun. Kompüterin aparat həlli də bu şərti nəzərə alır. Bərk və yumşaq maqnit, maqnit-optik disk və disketlərə, eləcə də, maqnit lentlərə (strimmerlərə) yazma (oxuma) prinsiplərinə toxunmadan kompüterlərdən informasiyanın əməliyyat sistemi vasitəsilə silinməsi texnikasını nəzərdən keçirək. Silmə əməliyyatı əsasən üç metodla həyata keçirilir:

– əməliyyat sisteminin "*Delete*" standart silmə komandasından istifadə etməklə;
– silinməsi nəzərdə tutulan informasiyanın üzərinə (daşıyıcıda tutduğu sektora) yeni, informativlik daşımayan məlumatın yazılması ilə;
– daşıyıcını yenidən formatlaşdırmaqla.

Bu metodlardan heç biri informasiyanın 100% silinməsini təmin etmir. Məsələ ondadır ki, daşıyıcı qurğuların maqnit (maqnit-optik) yazma (silmə) başlıqları elə hesablanmışdır ki, informasiyanı tam silmək üçün kifayət edəcək maqnit (optik sahəsi) intensivliyi yaratmasın. Digər tərəfdən, informasiyanı bərpasə mümkün olmayacaq şəkildə silmək üçün kompüterin yazma-silmə qurğularının (vinçesterin, *CD/DVD-ROM*-ların və s.), maqnit-optik başlıqlarının gücünün (intensivliyinin) lazımi qədər artırılması onların ölçülərinin təxminən 2-3 dəfə böyüdülməsi ilə nəticələnərdi ki, bu da kompüterlərin miniatürləşmə prinsiplərinə (xüsusi ilə mobil kompüterlərdə) ziddir. Yəni xüsusi texniki vasitələrlə daşıyıcıların qalıq maqnitizminə (optik selinə) əsasən, ilkin informasiyanı bərpa etmək mümkündür. Ona görə də bu sadə üsullardan, bir qayda olaraq, məxfi və dövlət sirri daşımayan məlumatların silinməsi üçün istifadə edilir. Qeyd edək ki, bu üç proqram metodundan hər sonrakı əvvəlkinə nisbətən informasiyanı daha etibarlı şəkildə silir. Bəzi məlumatlara görə, əks kəşfiyyat və digər xüsusi orqanlar üçün hazırlanmış müasir qurğular ən mükəmməl silmə vasitələri ilə təmizlənmiş daşıyıcılarda qalan izə görə ilkin məlumatları bərpa edir [7]. Ona görə də yüksək dərəcəli dövlət sirri yazılmış daşıyıcıları etibarlı şəkildə təmizləmək üçün yeganə yol onları yüksək temperaturda əritməkdir. İkinci texnologiya güclü maqnit (optik sahəsi) yaradan qurğulardan istifadə etməklə aşağıdakı hallarda tətbiq edilir:

– adi iş rejimində istifadə üçün (Şəkil 1).

Silinmək üçün nəzərdə tutulan daşıyıcılar kompüterdən çıxarılır və xarici qurğuda yerləşdirilir və qurğu işə salınır. Daşıyıcının tipindən asılı olaraq qurğular müxtəlif konstruksiyalara malikdir. Daşıyıcıların iş yerində silinməsi üçün istifadə edilir.

– təcili hallarda silmək üçün.

Qurğu kompüterin daxilində quraşdırılır. Hüquq-mühafizə, vergi orqanları, rəhbərlik və s. tərəfindən qəflətən müsadirə və ya qarət təhlükəsi və s. hallar yarandıqda təcili silmək məqsədilə istifadə edilir. Qurğunu işə salan düymə, adətən, gizli yerdə quraşdırılır.



a) b) c)

Şəkil 1. Sərt disklər (a), disketlər (b) və *ZIP*-yaddaşlar (c) üçün silmə qurğuları

Müsadirə və ya qarət məqsədilə gələnlər, adətən, əvvəlcə kompüter yerləşən otağın elektrik təchizatını dayandırırlar ki, sahibi daşıyıcıları silə bilməsin. Ona görə də qurğu avtonom qida mənbəyinə, silmə qurğusunu radiokanalla (radiopult, mobil telefon və s. vasitəsilə) işə salmaq imkanına malikdir. Daşıyıcının icazəsiz əldə edilməsi (oğurluq, qarət) məqsədilə kompüter gövdəsinin açılması, yerdəyişməsi və s. halları baş verdikdə qurğunu avtomatik işə salan variantlar da mövcuddur.

– daşınmanın təhlükəsizliyini təmin etmək üçün (Şəkil 2).

Şəkil 2. MD-nin daşınması üçün təhlükəsizlik keysi

Müəyyən məqsədlərlə başqa yerə daşındığı zaman itirilmiş, oğurlanmış daşıyıcıların məlumatlarının məsafədən silinməsi məqsədilə istifadə edilir. Silmə qurğusu "diplomat", attaşe-keys və s. tipli çantalarda quraşdırılır. Disk qurğuda yerləşdirilmiş halda daşınır. Avtonom qidalanma, məsafədən idarəetmə, qutunun açılmasının siqnalizasiyası və s. funksiyaları var.

– daşıyıcıların ehtiyat nüsxələrinin saxlancları üçün (Şəkil 3).

Arxiv daşıyıcıları da yol verilməyən müdaxilələrə məruz qala bilər. Oğurluq, başqa nüsxələrlə əvəzləmə və s. hallar yarandıqda məlumatları təcili silmək üçün istifadə edilir. Lakin bəzi fövqəladə hadisələr (yanğın, zəlzələ, daşqın və s.) ehtiyat nüsxələrdəki məlumatların itirilməsinə səbəb ola bilər. Ona görə də ehtiyatlı təşkilatlar saxlancları bir neçə nüsxədə yaradıb müxtəlif ərazilərdə (təşkilatın bölmələrində, xüsusi təşkilatlarda və s.) yerləşdirirlər.

Kompüterlərin icazəsiz başqa yerə daşınması, daşıyıcının oğurlanması məqsədilə gövdəsinin sökülməsi (açılması), daşıyıcılardakı kontentin dəyişdirilməsi və s. yol verilməyən hərəkətlərdən mühafizə məqsədilə digər texniki vasitələrdən də (troslar, qıfıllar, siqnalizasiya qurğuları və s.) istifadə edilir.

Şəkil 3. İinformasiya daşıyıcısının ehtiyat nüsxələrinin saxlanması üçün təhlükəsizlik şkaf-saxlancı

Köhnədən qalmış və istehsaldan çıxarılmış yumşaq diskləri – disketləri əvəz edən daha böyük həcmli ZIP-saxlancları da maqnit yazma prinsipinə əsaslandığı üçün konstruksiyaları fərqlənən eyni iş prinsipli qurğular vasitəsilə silinir. Əsasən, audio-video yazılışları, onların arxivləşdirilməsi və ehtiyat nüsxələrin yaradılması üçün istifadə edilən strimmerlərin – maqnit yazma prinsipli lent daşıyıcıların etibarlı təmizlənməsi üçün müxtəlif təyinatlı utilizatorlardan istifadə edilir.

Fləş-yaddaş ailəsindən olan qurğularda saxlanılan informasiyanın etibarlı şəkildə silinməsi də xarici qurğulardan istifadə etməklə aparılır. Lakin bu qurğuların yaddaş elementini elektrik cərəyanı ilə proqramlaşdırılan və təkrar yazıla (oxuna) bilən Böyük İnteqral Sxemlərin tranzistorları (*EPROM*) təşkil etdiyi üçün silinməsi maqnit-optik sahəsi ilə yox, elektrik cərəyanı ilə xüsusi formalı yüksək gərginlikli impuls siqnalları ilə aparılır. Silmə nəticəsində yaddaş qurğusu təkrar yazma-oxuma üçün yararsız hala düşür. Məxfi olmayan və dövlət sirri daşımayan fləş-yaddaş qurğusunu kompüterin əməliyyat sistemləri ilə sildikdə (yuxarıda qeyd olunan üç metoddan ilk ikisi vasitəsilə) təkrar istifadə edilə bilər. Bu qurğular da bir sıra əlavə mühafizə funksiyaları (məsafədən radiokanalla silmə, təhlükəsiz daşınma üçün keyslər və s.) olan müxtəlif variantlarda hazırlanır.

Maqnit-optik disk qurğularından informasiyanın etibarlı şəkildə silinməsi üçün həmçinin bir sıra elektrik-maqnit əsaslı olmayan metodlardan da istifadə edilir. Məsələn, bu metodlardan birinin mahiyyəti ondan ibarətdir ki, diskin səthinə pirotexnik tərkibli nazik qat çəkilir və elektrik impulsu vasitəsilə alışdırılır. Bu zaman diskin səthinin temperaturu qısa müddətə 2000 C°-dək qızır və informasiyanı məhv edir, diskovodun özü isə korlanmır [8].

ETTKİ-nin tullantıları (maket, qovşaq və s.), elektrik və elektron avadanlıqları istehsalının zay məhsulları elektron tullantı kimi, yəni tətbiq edilən ETİE sisteminin elementi kimi emal edilir.

Kağız daşıyıcıların informasiya təhlükəsizliyi haqqında

Kağız daşıyıcılar da özündə məxfi informasiya və dövlət sirri daşıya bilər. Təcrübə göstərir ki, istənilən kiçik ölçülərdə, əllə cırılıb atılmış kağız parçalardakı informasiyanı bərpa etmək mümkündür. Ona görə kağızdakı məlumatları məhv etmək üçün xüsusi kağız məhvedən qurğulardan (KMQ): şreder, qrinder, dezinteqratordan istifadə edilir (Şəkil 4).

Şəkil 4. Şreder, qrinder və dezinteqrator

Təyinatına görə KMQ, adətən, aşağıdakı qruplara bölünür:
- fərdi KMQ – kiçik ofislər və mənzil sektorunda istifadə edilir, kiçik ölçülü və ucuzdur;
- ofis üçün KMQ – orta və iri təşkilatlarda istifadə üçün nəzərdə tutulub;
- arxiv üçün KMQ – böyük həcmdə kağız daşıyıcıların məhv edilməsi üçün nəzərdə tutulub;
- universal KMQ – kağızdan başqa karton, qovluq, kitab, jurnal və s. kiçik hissələrə doğramaq üçün istifadə edilir.

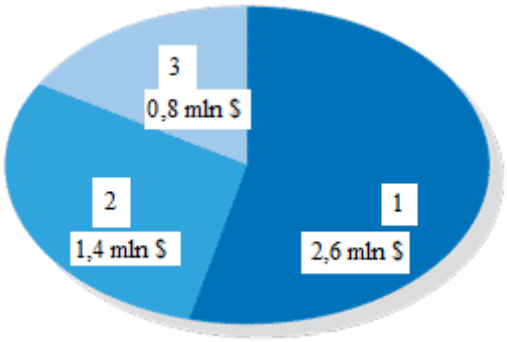
Məxfilik və sirlilik dərəcəsindən asılı olaraq kağızlar müəyyən en və uzunluğa malik zolaqlar şəklində doğranır. 4-cü və 5-ci sirlilik dərəcəli məlumat daşıyan vərəqlər şaquli və üfüqi xətt üzrə doğranır. Məsələn, ABŞ hökumətinin sənədləri üçün 0,8x4mm ölçüsü standart kimi qəbul edilib. 5-ci dərəcəli mənbələr kimyəvi həlletmə və ya xüsusi sobalarda yüksək temperaturda yandırma yolu ilə məhv edilir. Yüksək statuslu dövlət sirri saxlayan kağız daşıyıcılar üçün son metod daha etibarlı hesab edilir. Sirli məlumatları məhv etmək üçün vərəqi en və uzunluq ölçüləri və ya diametri bir millimetrdən kiçik hissələrə doğrayan qrinder və dezinteqratorlardan da istifadə edilir. Məlumatın sirlilik dərəcəsindən asılı olaraq kağız daşıyıcıların qeyd olunan qurğularda doğranma ölçüləri aşağıdakı cədvəldə göstərilir (R – dairəvi kəsilən hissələrin radiusudur).

Cədvəl 1.
Sirlilik dərəcəsi-doğranma qaydası asılılığı

Məlumatın sirr dərəcəsi	Şreder	Qrinder	Dezinteqrator
	Hissələrin ölçüləri (mm)		
I II II IV V	12 x qeyri-məhdud 6 x qeyri-məhdud 4 x 80 0,8 x 20 0,1 x 13	R = 1,0	0,8 x 0,8

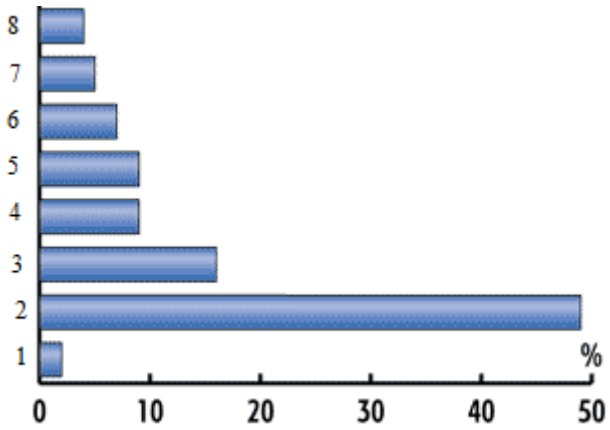
Göründüyü kimi, böyük həcmli daşıyıcıların kontentinin araşdırılması, təsnifatlaşdırılması, rezervləmə, saxlancların yaradılması və istismarı mürəkkəb və xeyli məsrəflər tələb edən iş olsa da, mühüm informasiyanın itirilməsi və ya yenidən bərpasına çəkilən xərclər daha böyük olur.

ABŞ-ın Larri Ponemon institutu informasiya təhlükəsizliyi insidentlərinin xarakteri və vurduğu ziyanın qiymətləndirilməsi məsələləri üzrə tədqiqat işləri aparır və nəticələri illik hesabat şəklində dərc edir. 31 iri kommersiya təşkilatı üzrə aparılmış araşdırmaların nəticələri Şəkil 5 və Şəkil 6-da göstərilmişdir [9].



Şəkil 5. Bir təşkilat üzrə illik orta maliyyə itkiləri (ABŞ üzrə)

Bir təşkilat üzrə illik orta maliyyə itkilərinə aiddir: 1) itirilmiş mənfəətin orta qiyməti: imicin aşağı düşməsindən, müştərilərin itirilməsindən yaranan itkilər, yeni müştərilərin cəlb edilməsinə çəkilən və s. xərclər; 2) birbaşa itkilər: müştərilərə ödənilən kompensasiya, məhsul və xidmətlərin aşağı düşməsi və s.; 3) dolayı itkilər: məhkəmə çəkişmələrinə, müştərilərin məlumat sızması haqqında məlumatlandırılmasına çəkilən xərclər, poçt, telefon ödənişləri və s.



Şəkil 6. Məlumat sızmalarının xarakteri

Məlumat sızmalarının səbəblərinə aiddir: 1) ziyanlı proqramlar; 2) verilənlərə əlyetərliliyin əngəllənməsi; 3) informasiya daşıyıcılarının ehtiyat nüsxələrinin itməsi; 4) insayder fəaliyyəti; 5) kağız daşıyıcılarının itməsi; 6) autsorsinq fəaliyyəti; 7) mobil kompüterlərin itməsi; 8) məlum olmayan səbəblər.

İnformasiya təhlükəsizliyinin pozulması nəticələrinin ciddiliyini göstərmək üçün aşağıdakı bir neçə faktı qeyd etmək olar:

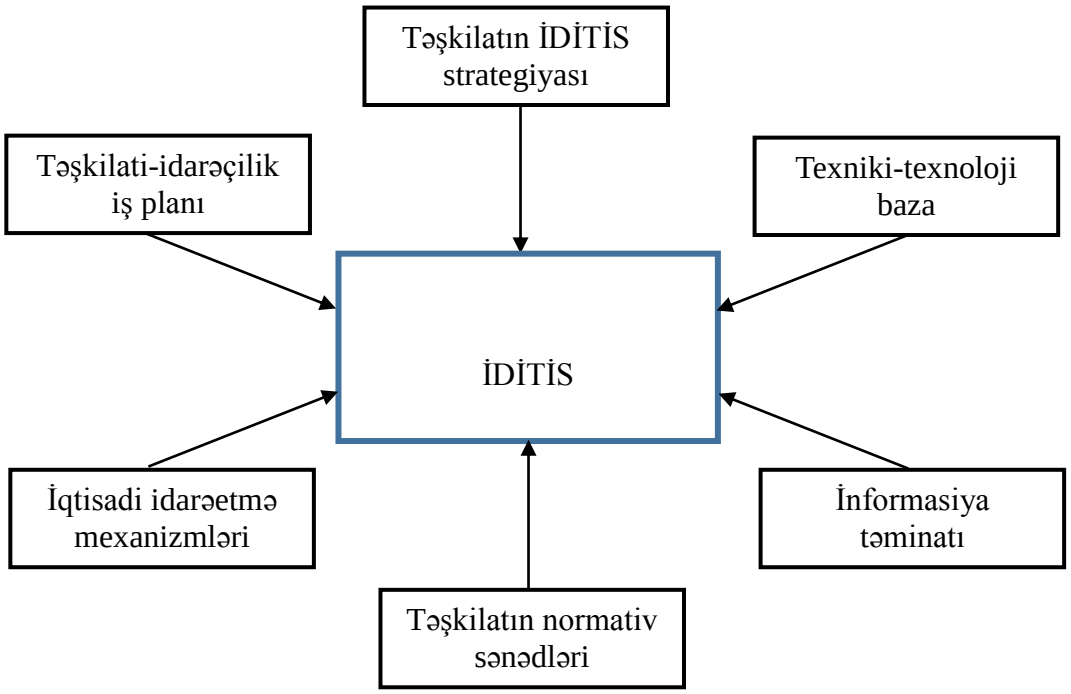
1. ABŞ-da ixtisaslaşdırılmış şirkətlərin bir vərəq həcmində itirilmiş mühüm məlumatın bərpaetmə haqqı orta hesabla 1000,0 dollardır [9].

2. Bir neçə il əvvəl ABŞ ordusunun kompüter təchizatının yaxşılaşdırılması proqramı çərçivəsində on minlərlə işlək fərdi kompüter məktəblərə paylanmışdı. Şagirdlər heç bir qərəzli məqsəd güdmədən, maraq xatirinə İnternetdən götürdükləri adi proqramlarla informasiya daşıyıcılarının məxfi və dövlət sirri daşıyan məlumatlarını bərpa edərək mətbuata ötürmüşdülər. Yaranmış qalmaqaldan sonra proqramın icrası dayandırıldı. Araşdırmalar göstərdi ki, fərdi kompüterlərin daşıyıcıları əməliyyat sistemlərinin proqram imkanlarından istifadə etməklə silinibmiş, yəni etibarlı silmə aparılmayıbmış [9].

3. 1979-cu ildə İran inqilabı zamanı ABŞ səfirliyini ələ keçirmiş üsyançılar ofis şrederlərində məhv edilmiş kağızlardakı informasiyanı bərpa edib kitab halında yaydmışırlar və bu, beynəlxalq səviyyədə siyasi qalmaqala səbəb olmuşdur [10].

Hər bir fəaliyyət sahəsi, hər bir təşkilat öz iş xüsusiyyətlərini və imkanlarını nəzərə almaqla informasiya daşıyıcılarının informasiya təhlükəsizliyinin idarəetmə sistemini (İDİTİS) yaratmalıdır. Bu məqsədlə bir sıra qabaqcıl təşkilatların, hökumətlərin iş təcrübəsindən istifadə etmək olar. İdarəetmə sistemi bu sahədə təşkilatın dayanıqlı inkişaf konsepsiyasının və idarəetmə siyasətinin, cari və perspektiv proqramlarının, konkret fəaliyyət planlarının işlənməsini və həyata keçirilməsini nəzərdə tutmalıdır (Şəkil 7).

Təcrübə göstərir ki, idarəetmə sisteminin yaradılmasına və istismarına çəkilən xərclər, məxfi və sirr daşıyan, o cümlədən kommersiya sirli məlumatların bədniyyətli tərəfindən əldə edilməsi və ya itirilməsi, itirilmiş məlumatların bərpa edilməsi və s. nəticələrinin aradan qaldırılmasına çəkilən xərclərdən dəfələrlə azdır.



Şəkil 7. İDİTİS-in arxitektur sxemi

Nəticə

Məqalədə informasiya daşıyıcılarının informasiya təhlükəsizliyi və mühafizəsi problemlərininin bəzi elmi və praktiki aspektləri araşdırılmışdır. İnformasiya daşıyıcılarında saxlanılan məlumatların "etibarlı silinməsi" anlayışı qəbul edilmiş və elektron tullantıların maqnit (maqnit-optik), strimmer, ZİP-saxlanclar, fləş və s. yaddaş qurğularındakı məlumatların məxfilik və sirlilik dərəcəsindən asılı olaraq saxlanması, ötürülməsi və etibarlı silinməsi (məhv edilməsi) məqsədilə optimal metodların və müvafiq avadanlıqların seçilməsi üçün təkliflər verilmişdir. Eynilə kağız daşıyıcılardakı məxfi və dövlət sirri daşıyan məlumatların etibarlı məhv edilməsi metodları və qurğuları, onların seçilməsi məsələləri şərh edilmişdir. Araşdırmalar nəticəsində məlum olmuşdur ki, bir sıra ölkələrin qabaqcıl təşkilatları elektron tullantıların məlumat daşıyıcılarının informasiya təhlükəsizliyini təmin etmək məqsədilə effektiv idarəetmə sistemi yaratmışlar. Göstərilir ki, idarəetmə sistemi elektrik və elektron avadanlıqların balansdan silinməsi, saxlanması, yerdəyişməsi (nəqli), ehtiyat nüsxələrin yaradılması, arxivləşdirilməsi, tullantı kimi emalı təşkilatdaxili normativ sənədlərin, iqtisadi həvəsləndirmə mexanizmlərinin,

fəaliyyət planlarının işlənməsi və həyata keçirilməsi aspektlərini əhatə edir. Sonda təşkilatların uyğun idarəetmə sistemini yaratması məqsədəuyğunluğu əsaslandırılmışdır.

Ədəbiyyat

1. Directive 2012/19/EU of the European Parliament and the Council of 4 July 2012. On waste electrical and electronic equipment, http://www.ec.europa.eu
2. http://www.idtheftcenter.org/artman2/uploads/1/ITRC Breach 2011 20120207.pdf
3. "İstehsalat və məişət tullantıları haqqında" AR Qanunu, http://www.qanun.az
4. "Qiymətli metallar və qiymətli daşlar haqqında" AR Qanunu, http://www.qanun.az
5. Ağayev B.S., Əliyev T.S. Azərbaycanda və Avropa İttifaqında elektron tullantıların idarə edilməsi sistemlərinin müqayisəli analizi / "Elektron dövlət quruculuğu problemləri" I Respublika elmi-praktiki konfransının əsərləri. Bakı: İnformasiya Texnologiyaları, 2014, s. 196-199.
6. Əliquliyev R.M., Ələkbərov R.Q. İstifadədə olmuş kompüterlərin utilizasiyasının sosial-ekoloji problemləri.// İnformasiya cəmiyyəti problemləri. Bakı, 2010, №2, s.3-8.
7. Прокофьев Н. Тяжелая артиллерия информационной безопасности // КомпьютерПресс, 2002, №3, с. 115-118.
8. Ağayev B.S., Əliyeva K.T. Elektron tullantılar problemi və informasiya təhlükəsizliyi / Azərbaycan xalqının ümummilli lideri Heydər Əliyevin 90 illik yubileyinə həsr olunmuş "İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı". Konfrans materialları. Bakı: İnformasiya Texnologiyaları, 2013, s.145-148.
9. http://www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime
10. http://ru.wikipedia.org/wiki/Шредер_(устройство)

УДК 504.064.47

Агаев Бикес С.[1], Мехтиев Шакир А.[2], Алиев Тарлан С.[3]
[1,2,3]Институт Информационных Технологий НАНА, Баку, Азербайджан
[1,3]depart6@iit.ab.az, [2]depart11@iit.ab.az

Электронные носители информации как объекты информационной безопасности

В статье рассматриваются проблемы информационной безопасности и методы защиты некоторых носителей информации. Анализируются методы и устройства для защиты, утилизации, восстановления, резервного копирования информации, хранящейся в носителях электронных отходов, и бумаги, которые содержат конфиденциальные сообщения и государственные тайны. Также рассмотрен вопрос целесообразности создания системы управления безопасностью носителей информации.

Ключевые слова: *электронные отходы, утилизация электронных отходов, электронные носители информации, бумажные носители, магнитные/оптические носители, стримеры, информационная безопасность, защита информации.*

Bikes S. Agayev[1], Shakir A. Mehdiyev[2], Tarlan S.Aliyev[3]
[1,2,3]Institute of Information Technology of ANAS, Baku, Azerbaijan
[1,3]depart6@iit.ab.az, [2]depart11@iit.ab.az

Electronic media as objects of information security

The article addresses the problem of information security and protection methods some media. Analysis of methods and devices for protection, recycling, recovery, backup information stored in electronic media and paper waste, which store confidential communications and state secrets. Also consider the feasibility of establishing a safety management system media.

Keywords: *electronic waste, recycling electronic waste, electronic media, paper storage, magnetic/optical media, tape drives, information security, information security.*