Elektron tullantılarda məlumat daşıyıcılarının təhlükəsizliyinin təmin olunmasının bəzi məsələləri haqqında

Bikəs Ağayev[1], Şakir Mehdiyev[2], Tərlan Əliyev[3]

AMEA İnformasiya Texnologiyaları İnstitutu

[1,3]depart6@iit.ab.az, [2]depart11@iit.ab.az

***Xülasə*— 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 təhlükəsizliyinin idarə edilməsi sisteminin yaradılması məqsədəuyğunluğu məsələsi nəzərdən keçirilir.**

Açar sözlər*— *elektron tullantıları; elektron tullantıların utilizasiyası; elektron məlumat daşıyıcıları; kağız daşıyıcılar; maqnit/optik daşıyıcılar; strimmerlər; informasiya təhlükəsizliyi; informasiya mühafizəsi

I. GİRİŞ

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

Məqalədə əsasən elektron tullantıların məlumat daşıyıcılarının (MD) İT-nin proqram-aparat təminatı məsələlərinə baxılacaq.

II. MƏLUMAT DAŞIYICILARI İNFORMASİYA TƏHLÜKƏSİZLİYİ OBYEKTİ KİMİ

İT-nin təmin edilməsi məlumatların əks edildiyi 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 daşıyıcılarda yadda saxlanılır:

- bərk və yumşaq maqnit daşıyıcılar (disklər, disketlər);
- maqnit-optik daşıyıcılar (disklər);
- strimmerlər;
- ZIP-yaddaş diskləri;
- fleş-yaddaş (Flash memory) prinsipi əsasında yaradılmış fleş-disklər (Flash Drive), fleş-saxlanclar, fleş-kart (Flashcard);
- kağız və s.

Bütün bu maddi yaddaş vasitələrində mətn, fonoqram, audio-video materiallar, şəkillər, çertyojlar, 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 (atıla) 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. Ona görə də MD-də yadda saxlanılan məlumatların İT-nin təmin edilməsi dövlət, təşkilatlar və hər bir şəxs üçün əhəmiyyətli və aktual məsələdir. MD-dən informasiyanın arzu olunmayan 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, partnyorlar və s. tərəfindən İT-nin pozulması), eləcə də autsorsinq fəaliyyəti (təşkilatın işçi, iş yeri, iş funksiyalarını və s. resurslarını başqa təşkilatın xidmətinə verməsi) prosesində autsorser əməkdaşları tərəfindən İT-nin pozulması əsasən, məlumatların qeyri-qanuni əldə edilməsi və digər tərəfə ötürülməsi yolu ilə baş verir. ETTKİ, eləcə də istehsal prosesində yaranan kağız sənədlər (eskizlər, çertyojlar, 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 İT də mövcud qanunvericilik, təşkilatdaxili hüquqi-normativ sənədlər, təşkilati qaydalar və s. üsullarla təmin edilməlidir.

Texnika və texnologiyaların indiki inkişaf səviyyəsində istər emal olunan (toplanması, emalı, yadda saxlanması və ötürülməsi), istərsə də arxivləşdirilmiş informasiyanın əsas daşıyıcıları elektron daşıyıcılardır. Elektron daşıyıcılardakı məlumatların İT-nin pozulması hallarının böyük əksəriyyəti saxlanan informasiyanın lazımi hallarda silinməməsi və ya məhv edilməməsi nəticəsində baş verir. Burada "lazımi 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;
- ETİE sisteminin tələblərinə uyğun olaraq ilkin və təkrar emal məqsədilə tullantı mərkəzlərinə təhvil verilməsi;
- məişət və sənaye tullantıları kimi atılması;
- avadanlıqların təmir məqsədilə başqa təşkilata göndərilməsi və ya digər yerdəyişməsi;
- elektron tullantıların (məsələn, kompüterlərin) hədiyyə, yardım və ya başqa formada digər təşkilatın balansına keçirilməsi.

III. ET DAŞIYICILARININ UTİLİZASİYASI HAQQINDA

Qeyd olunan halların İT ilə əlaqəsini kompüterlərin misalında, ümumiləşdirilmiş halda araşdıraq. Ölkə qanunvericiliyinə görə işlək vəziyyətindən, mənəvi köhnəlmə və ya fiziki aşınma dərəcəsindən asılı olmayaraq, 7 il istismar müddəti bitdikdən sonra kompüterlər balansdan silinə bilər. Balansdan silinmiş kompüterlər müvəqqəti saxlanma yerinə, məsələn, anbara göndərilir. "İstehsalat və məişət tullantıları haqqında" AR Qanununa (son redaktəsi 2007-ci il) [1] və "Qiymətli metallar və qiymətli daşlar haqqında" AR Qanununa (2005) [2] 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 respublika qanunvericiliyində "elektron tullantıları" (ET), "elektron tullantıların idarə edilməsi" (ETİE) məhfumları olmadığı kimi, bu sinif tullantıların ilkin və təkrar emalı müəssisələri, uyğun infrastruktur da yoxdur. Ona görə də reallıqda bu qanunlar işləmir [3]. 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 bağçalarının, məktəblərin və s. təşkilatların balansına keçirir [4]. Bir çox hallarda kompüterlər məişət və istehsalat tullantıları kimi atılır. Eyni sözləri ev təsərrüfatlarına (əhaliyə) da aid etmək olar.

Aparılmış müşahidələr göstərir ki, bir çox hallarda istər ev təsərrüfatları, istərsə də təsərrüfat subyektləri "atılmaq üçün nəzərdə tutulmuş" kompüterlərin MD-dəki informasiyanı ümumiyyətlə silmirlər və ya etibarlı (keyfiyyətli) məhv etmirlər. Burada "etibarlı 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 etməsi üçün çox "sevdiyi" mənbələrdən biri tullantı yerləridir (zibilxanalar, poliqonlar). Qeyd edək ki, mətndə istifadə edilən ET, ETİE, "atılmaq üçün nəzərdə tutulmuş" terminləri Avropa İttifaqının 2012/19 EC/EP Direktivindən [5] ("Elektrik və elektron avadanlıqlarının tullantıları haqqında") götürülmüşdür.

MD-dəki informasiyanın silinməsi onlardakı məlumatların məxfilik və sirlilik dərəcəsindən asılı olaraq iki texnologiya üzrə aparılır:

- informasiyanı daşıyıcıya yazma prinsiplərinə əsaslanan silmə texnologiyaları.

Bu texnologiyada əsasən iki qrup metodlardan istifadə edilir: a) kompüterin əməliyyat sisteminin (ƏS) funksional imkanları ilə silmə; b) xüsusi silmə qurğularından istifadə etməklə məhvetmə.

- digər mexanizmlərə əsaslanan metodlarla silmə/məhvetmə.

Kompüterin ƏS-nin proqram vasitələrinin imkanları ilə daşıyıcılardakı informasiyanı etibarlı silmək mümkün deyil. Prinsip etibarilə ilə ƏS 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 disklər, maqnit-optik disk və disketlərə, eləcə də maqnit lentlərə (strimmerlərə) yazma/oxuma prinsiplərinə toxunmadan kompüterlərdən informasiyanın ƏS vasitəsilə silinməsi texnikasını nəzərdən keçirək. Silmə əməliyyatı əsasən üç metodla həyata keçirilir:

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

Deyildiyi kimi 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 dönməz 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 (xüsusilə mobil kompüterlərdə) ziddir. Yəni, xüsusi texniki vasitələrlə daşıyıcıların qalıq

maqnitizminə/optik selinə əsasən ilkin informasiyanı bərpa etmək mümkündür. Ona görə 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 silir.

Bəzi məlumatlara görə əkskəşfiyyat və digər xüsusi orqanlar üçün hazırlanmış müasir qurğular ən mükəmməl silmə vasitələri ilə təmizlənmiş daşıyıcılarda qalan izə görə ilkin məlumatları bərpa edir [6]. Ona görə də yüksək dərəcəli dövlət sirri yazılmış daşıyıcıları etibarlı 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;

Silinməsi nəzərdə tutulan daşıyıcılar kompüterdən çıxarılır, 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, qarət təhlükəsi və s. hallar yarandıqda cəld silmək məqsədilə istifadə edilir. Qurğunu işə salan düymə adətən gizli yerdə quraşdırılır. Qurğu avtonom qida mənbəyinə, radiokanalla (radiopult, mobil telefon və s. vasitəsilə) işə düşmə 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;

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

– daşıyıcıların ehtiyat nüsxələrinin saxlancları üçün:

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 ciddi 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.

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

Fleş-yaddaş ailəsindən olan qurğularda saxlanılan informasiyanın etibarlı 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 və dövlət sirri daşımayan Fleş-yaddaş qurğusunu kompüterin ƏS ilə sildikdə (yuxarıda qeyd olunan 3 metoddan birinci 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 disklərdən informasiyanı etibarlı silmək üçün, bir sıra qeyri-elektrik/maqnit əsaslı metodlardan da istifadə edilir. 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 [7].

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

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 məhvedici qurğulardan (KMQ) – şrederlərdən, qrinderlərdən, dezinteqratordan istifadə edilir.

Təyinatına görə KMQ adətən aşağıdakı qruplara bölünür:

– fərdi KMQ – kiçik ofislər və mənzil sektorunda istifadə edilir, kiçik ölçülü və ucuzdur.

– ofis KMQ – orta və iri təşkilatlarda istifadə üçün nəzərdə tutulub.

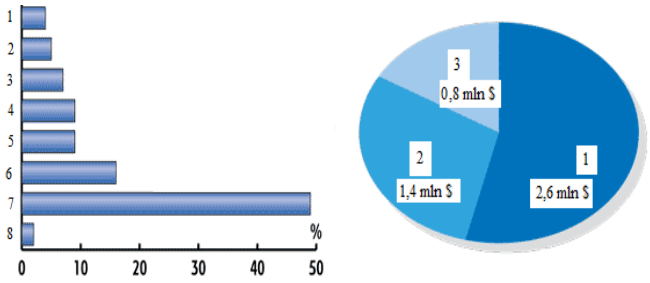
– arxiv KMQ – böyük həcmdə kağız daşıyıcıların məhv edilməsi üçün nəzərdə tutulur.

– universal məhvedicilər – 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 0,8 x 4 mm ölçüsü standart kimi qəbul edilib. 5-ci dərəcəli mənbələr kimyəvi həlletmə və ya xüsusi sobalarda yüksək temperaturda yandırma yolu ilə məhv edilir. Ən yüksək statuslu dövlət sirri saxlayan kağız daşıyıcılar üçün son metod

əvəzolunmaz ola bilər. Yüksək sirli məlumatları məhv etmək üçün vərəqi en və uzunluq ölçüləri və ya diametri bir millimetrdən kiçik hissələrə doğrayan qrinder və dezinteqratorlardan da istifadə edilir. 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 (Ponemon İnstitute) İT pozuntularının 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 şəkildə göstərilmişdir.



a) b)

Məlumat sızmalarının xarakteri və bir təşkilat üzrə orta itkilər

a) 1 – ziyanlı proqramlar; 2 – verilənlərə əlçatarlığın sındırılması; 3 – MD-nin ehtiyat nüsxələrinin itməsi; 4 – insayder fəaliyyəti; 5 – kağız daşıyıcıların itməsi; 6 – autsorsinq fəaliyyəti; 7 – mobil kompüterlərin itməsi; 8 – məlum olmayan səbəblər

b) 1 – itirilmiş mənfəətin orta qiyməti: imicin aşağı düşməsindən, müştərilərin itirilməsindən yaranan, 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 sızma haqqında məlumatlandırılmasına çəkilən xərclər, poçt, telefon ödənişləri və s.

İT-nin pozulması nəticələrinin ciddiliyini göstərmək üçün bir neçə faktı qeyd edək.

1. ABŞ-ın bir neçə şirkəti bir vərəq itirilmiş mühüm məlumatı 100.000 $-a bərpa edir [8].

2. Bir neçə il əvvəl ABŞ ordusunun kompüter təchizatının yaxşılaşdırılması proqramı çərçivəsində on minlərlə işlək fərdi kompüter (PC) məktəblərə paylanmışdı. Şagirdlər heç bir qərəzli məqsəd güdmədən, maraq xatirinə İnternetdən götürdükləri adi proqramlarla MD-lərin məxfi və dövlət sirri daşıyan məlumatlarını bərpa edərək mətbuata ötürmüşdülər. Yaranmış qalmaqaldan sonra proqramın icrası dayandırıldı. Araşdırmalar göstərdi ki, PC-lərin daşıyıcıları ƏS-nin proqram imkanlarından istifadə etməklə silinibmiş, yəni etibarlı silmə aparılmayıb [8].

3. Son İran inqilabı zamanı ABŞ səfirliyini ələ keçirmiş üsyançılar ofis şrederlərində məhv edilmiş kağızlardakı informasiyanı bərpa edib kitab halında yaydılar və bu beynəlxalq səviyyədə siyasi qalmaqala səbəb oldu [9].

Hər bir fəaliyyət sahəsi, hər bir təşkilat öz iş xüsusiyyətlərini və imkanlarını nəzərə almaqla MD-nin İT-nin idarə edilməsi sistemini 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. Təcrübə göstərir ki, idarəetmə sisteminin yaradılmasına və istismarına çəkilən xərclər, məxfi və sirli, o cümlədən kommersiya sirli məlumatların bədniyyətli tərəfdən əldə edilməsi və ya itirilməsi, itirilmiş məlumatların bərpa edilməsi və s. nəticələrinin aradan qaldırılmasına çəkilən xərclərdən dəfələrlə azdır.

NƏTİCƏ

Məqalədə elektron tullantıların məlumat daşıyıcılarının informasiya təhlükəsizliyi və mühafizəsi problemlərinin bəzi elmi və praktiki aspektləri araşdırılmışdır. İnformasiya daşıyıcılarında saxlanılan məlumatların "etibarlı silinməsi" anlayışı qəbul edilmiş və elektron tullantıların maqnit/maqnit-optik, strimmer, ZİP-saxlanclar, fleş 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 edilir. 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 təşkilatımızın AMEA üçün uyğun idarəetmə sistemini yaratması məqsədəuyğunluğu əsaslandırılmışdır.

ƏDƏBİYYAT

[1] "İstehsalat və məişət tullantıları haqqında" AR Qanunu, 2007.

[2] "Qiymətli metallar və qiymətli daşlar haqqında" AR Qanunu, 2005.

[3] B. S. Ağayev, T. S. Əliyev, Azərbaycanda və Avropa İttifaqında elektron tullantıların idarə edilməsi sistemlərinin müqayisəli analizi," "Elektron dövlət quruculuğu problemləri" I Respublika elmi-praktiki konfransının əsərləri, 2014, s. 196-199.

[4] R. M. Əliquliyev, R. Q. Ələkbərov, "İstifadədə olmuş kompüterlərin utilizasiyasının sosial-ekoloji problemləri," İnformasiya çəmiyyəti problemləri, №2, s.3-8, 2010.

[5] Directive 2012/19/EU of the European Parliament and the Council of 4 July 2012 on waste electrical and electronic equipment.

[6] Н. Прокофьев, "Тяжелая артиллерия информационной безопасности," КомпьютерПресс, №3, 2002.

[7] B. S. Ağayev, K. T. Əliyeva, "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"nın materialları, 2013, s. 145-148.

[8] http://www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime

[9] https://ru.wikipedia.org/wiki/ШредерЪ_(устройство)