Verilənlərin sanitarizasiyasının informasiya təhlükəsizliyinin təmin olunmasında rolu

Sabirə Ocaqverdiyeva
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
allahverdiyevasabira@gmail.com

Xülasə **– Məqalədə verilənlərin sanitarizasiyasının mahiyyəti və kateqoriyaları haqqında məlumat verilmişdir. Verilənlərin sanitarizasiyasının alqoritmləri analiz edilmişdir. Həssas verilənlərin konfidensionallığının təmin olunmasında və İnternetdə uşaqların təhlükəsizliyinin təmin edilməsində onun rolu göstərilmişdir.**

Açar sözlər– verilənlərin sanitarizasiyası, sanitarizasiya alqoritmləri, təhlükəsizlik, uşaqların təhlükəsizliyi.

I.GİRİŞ

İnformasiya texnologiyaları və vasitələrinin inkişafı məlumat əldə etmək imkanını asanlaşdırsa da, informasiya təhlükəsizliyi baxımından ciddi təhdidlərə yol açır. İnternet sürətlə inkişaf edərək cəmiyyətin bütün seqmentlərinə hərtərəfli və dərin nüfuz edir, ondan həm fərdlər, həm də təşkilatlar müxtəlif məqsədlərlə istifadə edirlər. İnformasiya cəmiyyətində insan fəaliyyətinin, demək olar ki, bütün sahələri üzrə məlumatlar (dövlət idarəçiliyi, biznes, şəxsi məlumatlar, elm-təhsil, səhiyyə sistemi və s.) ənənəvi mühitdən elekton mühitə inteqrasiya olunur. İnformasiya mübadiləsi artır və məlumatlar istifadəçi üçün əlçatan olur. Məlumat şəxsin kimliyini aşkar edikdə və ya məxfi hesab olunan məsələləri açıqladıqda, konfidensionallıq üçün ciddi bir təhlükə yaradır. Araşdırmalar göstərir ki, fərdlərə və ya təşkilatlara məxsus olan məlumatların məxfiliyinin pozulması riski getdikcə artır [1]. Hazırda mütəxəssisləri ən çox narahat edən məsələlərdən biri verilənlərin onlayn mühitdə təhlükəsizliyinin təmin edilməsidir.

Virtual mühitdə istifadəçilərin, xüsusilə, uşaqların müəyyən informasiya ilə qarşılaşması bir çox neqativ hallara səbəb olur. İstər İnternet, istərsə də televiziya məkanında ziyanlı kontentlə qarşılaşmanın nəticəsində onların təhlükəsizliyi pozulur və zəif uşaq psixologiyası ciddi mənfi təsirlərə məruz qalır.

İnformasiya təhlükəsizliyi ilə əlaqədar məsələlərin həllində və zərərli informasiyanın qarşısının alınmasında müxtəlif proqram təminatlarından istifadə olunmasına baxmayaraq, çox vaxt uşaqlar təhlükələrin qurbanı olur. Bu problemlərin qarşısının alınmasını və təhlükəsizliklə bağlı məsələlərin həllini tələb edən avtomatlaşdırılmış texniki vasitələrdən istifadəni və yeni elmi yanaşmaları tələb edir.

Məqalədə verilənlərin sanitarizasiyası ((təmizlənməsi –VS) (*ing. Data Sanitization*)) texnologiyalarından istifadə etməklə ziyanlı kontentin qarşısının alınmasında, məlumatların konfidensionallığının təmin olunmasında və yaddaş qurğularının sanitarizasiyasında istifadə olunan təmizlənmə alqoritmləri və sanitarizasiyanın kateqoriyaları haqqında məlumat verilir.

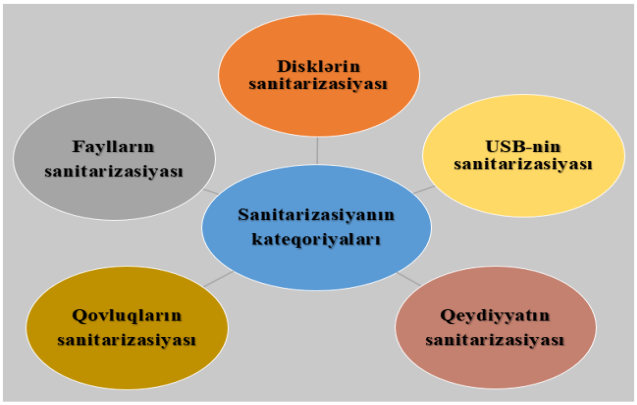
II. VERİLƏNLƏRİN SANİTARİZASİYASININ KATEQORİYALARI

VS-nin mahiyyəti həssas, fərdi, məxfi, konfidensional, tövsiyə olunmayan və s. məlumatların geniş ictimaiyyətə çatdırılmasının qarşısını almaqdan və ya müəyyən məhdudiyyətlərin tətbiq olunmasından ibarətdir [2]. Sanitarizasiya prosesi sənəd daxilində olan həssas məlumatları aradan qaldırmaqla sənədlərin təsnifat səviyyəsini formalaşdırır [3]. Sanitarizasiya (*ing. sanitization* (*classified information*)) həssas məlumatların (mətn, audio, video və s.) təmizlənməsi prosesidir [4]. Adətən, çap olunmuş materiallar üzərində redaktə kimi həyata keçirilən bu xüsusi emal prosesindən onlayn resurslarda da istifadə edilir.

Təhlükəsizlik məsələsi geniş sahəni əhatə edir. Sanitarizasiya prosesi verilənlərin əhəmiyyətli hesab olunduğu yerlərdə tətbiq edilir. Buraya hökümət təşkilatları, hərbi təşkilatlar, maliyyə müəssisələri və s. aid edilə bilər. İnformasiyanı icazəsiz girişlərdən məxfi saxlamaq üçün məlumatların konfidensionallığının təmin edilməsi vacibdir [5]. Fərdlərə məxsus olan şəxsi, həssas məlumatların gizlədilməsi (kommersiya sirrini təşkil edən məlumatlar, işçilərin şəxsi məlumatları, informasiyanın sahibinin nüfuzuna zərər verə bilən və digər məxfi məlumatlar) həmin məlumatların qorunmasında daha əhəmiyyətlidir [6].

Sanitarizasiya prosesi tətbiq sahələrinə görə aşağıdakı kateqoriyalara bölünür (Şəkil 1.) [7]:

DOI: 10.25045/NCInfoSec.2018.28



Şəkil 1. Sanitarizasiya prosesinin tətbiq sahələrinə görə kateqoriyaları

- Disklərin sanitarizasiyası – xarici yaddaş qurğularını və ya sabit disk sürücülərini təmizləmək üçün istifadə olunur;
- Qeydiyyatın sanitarizasiyası – qeydiyyat tarixi və ona aid olan məlumatların silinməsinə kömək edir;
- Faylların sanitarizasiyası – faylların tarixini və onlara olan bütün müvafiq istinadları silir;
- USB-nin sanitarizasiyası – USB-ləri, daşınabilən disk sürücülərini və fləş diskləri təmizləmək üçündür;
- Qovluqların sanitarizasiyası – qovluğun daxilində olan bütün qovluqları /alt qovluqları və orada saxlanılan faylları tamamilə silmək imkanına malikdir.

Ümumiyyətlə, sanitarizasiya prossesi özündə verilənlər bazasının hər hansı proqramla silinməsini, sanitarizasiya olunacaq qurğunun başqa qurğu ilə əlaqələndirilməsini, yaxud da fiziki olaraq qurğunun məhvini ehtiva edir. Bu yol ilə verilənlərin yaddaşdan silinməsi nəticəsində həmin verilənlərin geriyə qaytarılması mümkünsüz olur [6].

III. VERİLƏNLƏRİN SANİTARİZASİYASI ALQORİTMLƏRİ HAQQINDA

VS – termini verilənlərin silinmə üsulu (ing. data erasure methods), silmə alqoritmi *(ing.* wipe algorithms*)* və verilənlərin təmizlənmə üsulu *(ing. data wipe methods)* və ya verilənlərin silinməsi standartı *(ing. data wipe standards)* kimi də adlandırılır [8]. Aşağıda VS-nin icra alqoritmləri haqqında məlumat verilir. Qeyd edək ki, bu alqoritmlərin iş prinsipi demək olar ki, eynidir, yalnız keçidlərin təsvirində və sayında fərqlər vardır.

3.1. Təhlükəsiz silmə metodu (ing. Secure Erase Wipe Method) – bu metodun komandaları vasitəsilə sərt diskdə mövcud olan bütün məlumatların tamamilə yenidən yazılması mümkündür [9, 10]. Bu silmə metodunun alqoritmi VS-ni aşağıdakı şəkildə icra edir:

- Keçid 1: ikilik ədəd yazır (sıfır və ya bir).

3.2. CSEC ITSG-06 verilənlərin silinmə metodu (ing. CSEC ITSG-06 Data Wipe Method) – bu metodun iş alqoritmi başqa metodlardan bir qədər fərqlənir. Alqoritmin icrası zamanı sıfır və təsadüfi verilənlər hər ikisi birlikdə istifadə edilir. Bu proses aşağıdakı şəkildə icra edilir [9, 10]:

- Keçid 1: bir və ya sıfır yazır;
- Keçid 2: əvvəlki keçiddə yazılmış simvolu tamamlayır (məs. bir əgər Keçid 1 sıfır olarsa);
- Keçid 3: təsadüfi verilən yazır və yazını yoxlayır.

3.3. NCSC-TG-025 verilənlərin silinmə metodu (ing. NCSC-TG-025 Data Wipe Method) – sərt disk və ya digər yaddaş qurğularının üzərinə mövcud informasiyanı yenidən yazmaq üçün bəzi fayl və verilənləri parçalama proqramlarında istifadə edilən VS metoduna əsaslanmış proqram təminatıdır [9, 10]. Bu metodun iş alqoritmi *sıfır, bir* və *təsadüfi ədədlərin* kombinasiyası ilə aşağıdakı kimi göstərilir:

- Keçid 1: sıfır yazır və yazını yoxlayır;
- Keçid 2: bir yazır və yazını yoxlayır;
- Keçid 3: təsadüfi verilən yazır və yoxlayır.

3.4. Gutmann verilənlərin silinmə metodu (ing. Gutmann Data Wipe Method) – Gutmann metodu kimi tanınan təkrar-təkrar üzərinə məlumat yazmanı həyata keçirən Peter Gutmann və Colin Plumb tərəfindən 90-cı illərdə inkişaf etdirilən silmə metodu sənaye standartı olaraq qəbul edilmişdir. Bu metod 1996-cı ildə Peter Gutmann tərəfindən inkişaf etdirilmişdir [11]. Bu metodun icrası zamanı Peter Gutmann alqoritmindən istifadə etməklə sərt disk üzərində 35 dəfə üst-üstə məlumat yazmaqla əvvəlki veriləni silir. Bu etibarlı sanitarizasiya metodlarından biri hesab olunur [9, 10]. Alqoritm aşağıdakı kimi icra olunur:

- Keçid 1 - 35: təsadüfi verilən yazır.

3.5. Schneier verilənlərin silinmə metodu (ing. Schneier Method Data Wipe Method) – bu metod dünyada kriptoqrafiya üzrə tanınmış mütəxəssis Bryus Şnayer (Bruce Schneier) tərəfindən təklif olunmuşdur və təhlükəsizlik baxımından çox etibarlı metoddur. Həssas və konfidensional sayılan fayllarda istifadə olunur. Schneier metodu yeddi keçiddən ibarətdir [9, 10]:

- Keçid 1: bir yazır;
- Keçid 2: sıfır yazır;
- Keçid 3: bir qrup təsadüfi verilən yazır;
- Keçid 4: bir qrup təsadüfi verilən yazır;
- Keçid 5: bir qrup təsadüfi verilən yazır;
- Keçid 6: bir qrup təsadüfi verilən yazır;
- Keçid 7: bir qrup təsadüfi verilən yazır.

3.6. Pfitzner verilənlərin silinmə metodu (ing.Pfitzner Data

Wipe Method) – sərt disk və ya digər saxlama cihazlarından məlumatların silinməsi üçün Roy Pfitzner tərəfindən yaradılan proqram əsasında işləyən VS metodudur [8]. Bu metod sadə bir proseslə icra olunur. Hər hansı verilənin üzərinə 33-dəfə təsadüfi bir verilən yazmaqla sanitarizasiyanı yerinə yetirir [9, 10].

- Keçid 1 - 33: təsadüfi bir verilən yazır.

3.7. Sıfır yazmaqla verilənlərin silinmə metodu (ing. Write Zero Data Wipe Method) – sərt diskin və ya digər yaddaş qurğularının üzərinə sıfır yazmaqla proqram təminatı əsasında işləyən VS metodudur. Metod bəzən Sıfır doldurma və ya sıfır silmə olaraq da adlandırılır. Bu VS metodunun iş prinsipi aşağıdakı kimidir [9, 10].

- Keçid 1: sıfır yazır.

3.8. Təsadüfi verilənlərin silinmə metodu (ing. Random Data Wipe Method) – çox vaxt Random Number metodu kimi də tanınır. Sərt disk və ya digər saxlama cihazlarında VS-ni tətbiq etdikdə yalnız təsadüfi verilənlərdən istifadə olunur. Məlumdur ki, təsadüfi verilənlər gizlilik və təhlükəsizlik baxımından daha əhəmiyyətlidir [9,10]:

- Keçid 1-? Təsadüfi bir verilən yazır.

3.9. DoD 5220.22-M verilənlərin silinmə metodu (ing. DoD 5220.22-M Data Wipe Method) – metod Amerika Birləşmiş Ştatlarının Müdafiə Departamenti tərəfindən silinmə standartı olaraq qəbul edilmişdir. DOD 5220.22-M silmə metodu VS-ni aşağıdakı şəkildə verilmiş alqoritmik ardıcıllıqla yerinə yetirir [9,10].

- Keçid 1: sıfır yazır və yazını yoxlayır;
- Keçid 2: bir yazır və yazını yoxlayır;
- Keçid 3: təsadüfi verilən yazır və yazını yoxlayır.

3.10. AFSSI-5020 verilənlərin silinmə metodu (ing. AFSSI-5020 Data Wipe Method) – Amerika Birləşmiş Ştatları Hava Qüvvələri (USAF) tərəfindən təsis edilmişdir. Amerika Birləşmiş Ştatları Hava Qüvvələri (USAF) indi də VS-nın bu metodundan təhlükəsizlik standartı kimi istifadə edir. AFSSI-5020 verilənlərin silinmə metodu aşağıdakı şəkildə həyata keçirilir. Əvvəlcə bir, sonra sıfır yazıldığı hallar mümkündür və hər bir keçid yoxlanılır [9,10].

- Keçid 1: sıfır yazır;
- Keçid 2: bir yazır;
- Keçid 3: təsadüfi verilən yazır və yazını yoxlayır.

3.11. AR 380-19 verilənlərin silinmə metodu (ing. AR 380-19 Data Wipe Method) – İlk dəfə ABŞ ordusu tərəfindən yayımlanan Army Regulation 380-19 (Ordu Tənzimlənməsi 380-19) nəşri tərəfindən istifadə edilmişdur. Hazırda həmin təşkilat bu metodu təhlükəsizlik standartı kimi istifadə edir [9,10]. Alqoritmin icrası aşağıdakı kimidir:

- Keçid 1: təsadüfi verilən yazır;
- Keçid 2: xüsusi simvol yazır (məs., sıfır);
- Keçid 3: xüsusi simvolu tam olaraq yazır və yazını yoxlayır.

3.12. NAVSO P-5239-26 verilənlərin silinmə metodu (ing. NAVSO P-5239-26 Data Wipe Method) – hazırda ABŞ Hərbi Dəniz qüvvələri NAVSO P-5239-26 metodundan sanitarizasiya standartı kimi istifadə edir. Bu metod sərt disk və ya digər yaddaş qurğularına mövcud informasiyanı yenidən yazmaq üçün müxtəlif fayl və verilənləri parçalama proqramlarından istifadə edilən VS metoduna əsaslanmış proqram təminatıdır. NAVSO P-5239-26 metodu silmə işini aşağıdakı kimi həyata keçirir [7]:

- Keçid 1: xüsusi simvol yazır (məs., “bir”);
- Keçid 2: xüsusi simvolun ardını yazır (məs., “sıfır”);
- Keçid 3: təsadüfi veriləni tam olaraq yazır və yazını yoxlayır.

3.13. HMG IS5 (Infosec Standard 5) verilənlərin silinmə metodu (ing. HMG IS5 (Infosec Standard 5) Data Wipe Method) – bu metoddan istifadə etməklə sərt diskin silinməsi, proqram təminatına əsaslanan bütün faylbərpa metodlarının diskdə olan informasiyanı tapmasının qarşısını alır. Bir çox aparat təminatına əsaslanan faylbərpa metodları vasitəsilə isə informasiyanı aşkarlamasına mane olur. HMG IS5 metodunun eyni zamanda HMG IS5 Baseline və həm HMG IS5 Enhanced kimi iki oxşar versiyalarına da rast gəlmək olur. HMG IS5 Baseline VS metodu aşağıdakı şəkildə işləyir [9,10]:

- Keçid 1: sıfır yazır;
- Keçid 2: təsadüfi verilən yazır və yazını yoxlayır.

HMG IS5 Enhanced metodu isə aşağıdakı kimi işləyir:

- Keçid 1: sıfır yazır;
- Keçid 2: bir yazır;
- Keçid 3: təsadüfi verilən yazır və yazını yoxlayır.

3.14. ISM 6.2.92 verilənlərin silinmə metodu (ing. ISM 6.2.92 Data Wipe Method) – sərt disk və ya digər yaddaş qurğularına mövcud informasiyanı yenidən yazmaq üçün müxtəlif fayl və verilənləri parçalama proqramlarında istifadə edilən VS metoduna əsaslanmış proqram təminatıdır. ISM 6.2.92 metodu aşağıdakı alqoritmlə təmizləmə işini həyata keçirir [7].

- Keçid 1: təsadüfi simvol yazır və yazını yoxlayır.

3.15. NZSIT 402 (401) verilənlərin silinmə metodu (ing. NZSIT 402 (401) Data Wipe Method) – Yeni Zellandiya hökuməti və hökumətə xidmət edən istənilən təchizatçı yaxud məsləhətçilər tərəfindən standart silmə metodu kimi istifadə edilir. NZSIT 402 metodu aşağıdakı alqoritmlə işləyir [9, 10]:

- Keçid 1: təsadüfi bir verilən yazır və yazını verifikasiya edir.

3.16. VSITR verilənlərin silinmə metodu (ing. VSITR Data Wipe Method) – bu metod Almaniya Federativ Respublikasının təhlükəsizlik standartı kimi qəbul edilmişdir. Alqoritmin icrası aşağıdakı kimidir [12,13]:

- Keçid 1: sıfır yazır;
- Keçid 2: bir yazır;
- Keçid 3: sıfır yazır;
- Keçid 4: bir yazır;
- Keçid 5: sıfır yazır;
- Keçid 6: bir yazır;
- Keçid 7: təsadüfi bir verilən yazır.

3.17. GOST R 50739-95 verilənlərin silinmə metodu (ing. GOST R 50739-95 Data Wipe Method) – Rusiya Federasiyasının təhlükəsizlik üzrə dövlət standartı kimi 01.01.1996- cı ildə təsis edilmişdir [9, 10]. GOST R 50739-95 metodu çox vaxt səhvən GOST p50739-95 adı ilə adlandırılır. Bu metodun alqoritmi aşağıdakı kimidir:

- Keçid 1: sıfır yazır;
- Keçid 2: təsadüfi verilən yazır;
- Keçid 1: təsadüfi verilən yazır.

3.18. RCMP TSSIT OPS-II verilənlərin silinmə metodu (ing. RCMP TSSIT OPS-II Data Wipe Method) – bütün məzmunu silmək üçün Kanada təhlükəsizlik üzrə təmizləmə üsuludur. Alqoritm aşağıdakı kimi icra olunur [9,10]:

- Keçid 1: sıfır yazır;
- Keçid 2: bir yazır;
- Keçid 3: sıfır yazır;
- Keçid 4: bir yazır;
- Keçid 5: sıfır yazır;
- Keçid 6: bir yazır;
- Keçid 7: təsadüfi verilən yazır və təsdiqləyir;

NƏTİCƏ

Məlumatların sanitarizasiyası inkişaf etməkdə olan tədqiqat sahəsi olduğundan burada bir sıra problemlər vardır. Əsas problemlərdən biri də gizlilik, təhlükəsizlik tədbirlərinin daha geniş və səmərəli yerinə yetirilməsində müəyyən xətaların olmasıdır. Məlumatın strukturunda dəyişikliklər etdikdə, yeni informasiya sisteminə keçdikdə və ya məlumatın birdən çox məlumat mənbəyinə inteqrasiya edilməsi zamanı informasiya auditoriyaya fərqli formada təqdim oluna bilər. Yaranmış problemlərin həlli məlumatların strukturunda, təqdimatında və ya məzmununda hər hansı dəyişikliklərin edilməsi ilə yanaşı, onların təhlükəsizliyi məsələsini də təmin etməlidir.

VS metodlarının tətbiqi ilə uşaqları İnternetdə mövcud olan qanunazidd və təhlükəli kontentdən qorumaq üçün müxtəlif mexanizmlər işlənilməlidir.

ƏDƏBİYYAT

[1] Vasudevan V., John A., A review on text sanitization, International journal of computer applications (0975 – 8887), 2014, vol. 95, no.25, pp. 14-17.

[2] Əliquliyev R.M. Ocaqverdiyeva S.S. Uşaqların İnternetdə informasiya təhlükəsizliyini təmin edən sistemin konseptual modeli / İnformasiya təhlükəsizliyinin aktual problemləri III respublika elmi-praktiki seminarı, Bakı, 2017, səh. 84-87.

[3] Nettleton D.F., Abril D., An information retrieval approach to document sanitization, Advanced Research in Data Privacy, 2015, pp. 151-166.

[4] Crawford R., Bishop M., Bhumiratana B., Clark L., Levitt K. Sanitization Models and their Limitations / Proceedings of the 2006 Workshop on New Security Paradigms, Germany, 2006, pp. 41-56.

[5] Chakaravarthy V.T., Gupta H., Roy P., Mohania M. Efficient techniques for document sanitization / In Proceeding of the 17th ACM Conference on Information and Knowledge Mining (CIKM), 2008, pp. 843-852.

[6] Ivascu M. Data erasure on magnetic storage metra / International conference of scientific paper afases, Brasov, 2011, pp. 614-617.

[7] Deepika C., Bansal Dr. P. Study on need of data sanitization and sanitization techniques for memory devices/Open Access Journals Search Engine (OAJSE), vol.2, 2017, pp. 2456-3293

[8] Fisher T. Data Sanitization Methods, A List of Software Based Data Sanitization Methods, https://www.lifewire.com/data-sanitization-methods

[9] Kara Nance and Daniel J. Ryan. Proceedings of the 44th Hawaii International Conference on System Sciences - 2011 “Legal aspect of digital forensics” available at www.computer.org/csdl/proceedings/hicss/2011/ 4282/00/10-04-03.pdf access on 24/12/2015.

[10] “Degaussing” available at www.techtarget.com access on /24/6/2016. “Sanitization methods” available at http://googleweblight.com access on 15/7/2016.

[11] Gutmann metodu (35 kez silme) nedir?, www.dijitaldeliller.com

[12] Fisher T. VSITR Data Wipe Method [German Wipe Standard; 7 Passes], www.computercardinal.com, 26.04.2017

[13] Standard vom bundesamt für sicherheit in der informationstechnik (bsi-vsitr), https://dg-datenschutz.de

DATA SANITIZATION – AS PROVIDING INFORMATION SECURITY

Sabira Ojagverdieva

Institute of Information Technologies of ANAS, Baku, Azerbaijan

allahverdiyevasabira@gmail.com

Abstract – The article provides information about the essence and categories of data sanitization. Algorithms for the sanitization of data were analyzed. The role of ensuring the confidentiality of sensitive data and providing children security on the Internet is shown.

Keywords – Data sanitization, sanitization algorithms, safety, children safety