Fərdi məlumatların proqram vasitələri ilə qorunması üsullarının araşdırılması

Şəfəqət Mahmudova
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
shafagat_57@mail.ru

***Xülasə*— İşdə fərdi məlumatlar və onların qorunması mərhələləri haqqında məlumat verilmişdir. Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanununun bəzi müddəaları nəzərdən keçirilmişdir. Proqramlar vasitəsilə fərdi məlumatların qorunması məsələsinə baxılmışdır. Bu sahədə görülmüş işlər barədə məlumat verilmişdir. Proqramlar vasitəsilə məlumatların qorunması üsulları araşdırılmış və analiz edilmişdir. Gələcəkdə bu işlərin daha da inkişaf etdirilməsi üçün tövsiyə verilmişdir.**

Açar sözlər*— *fərdi məlumat; qorunma; proqram təminatı; texniki tapşırıq; SDN

I. GİRİŞ

Fərdi məlumatların qorunması müasir dövrün aktual məsələlərindən biridir. İnformasiya texnologiyalarının inkişafı bu sahəyə daha çox diqqətin ayrılmasını tələb edir və onun üçün xüsusi vasitələrin işlənməsini zəruri edir.

Fərdi məlumatların qorunması müəyyən edilmiş informasiyaya əsasən fiziki şəxsə (şəxsi məlumatların subyektinə) aid olan məlumatların müdafiəsinə yönəldilmiş təşkilatı-texniki xarakterli tədbirlərin kompleksidir [1]. Fərdi məlumatların qorunması müəssisədə əməyin qorunması bölməsinə daxil edilmişdir. Dövlət işçilərə onların fərdi məlumatlarından (şəxsiyyət vəsiqəsi) istifadəni nəzərə alaraq əmək hüquqlarının qorunmasına zəmanət verir.

Fərdi məlumatların qorunması üçün görülən işlərin mərhələləri aşağıda göstərilmişdir:

- Fərdi məlumatların emalını həyata keçirmək tələb olunduğu halda bütün vəziyyətləri müəyyən etmək;
- İstənilən fiziki şəxsə (şəxsi məlumatların subyektinə) aid olan fərdi məlumatların doğruluğunun yoxlanılması;
- Fərdi məlumatları emal edən biznes-proseslərin seçilməsi (Biznes-proses — bu istehlakçılar üçün müəyyən məhsulun və ya xidmətin yaradılmasına yönəldilmiş qarşılıqlı əlaqəli tədbirlərin və ya işlərin məcmusudur. Fəaliyyətin qrafik təsviri kimi biznes-proseslərin blok-sxemləri tətbiq edilir);
- Analitikanın keçirilməsi üçün biznes-proseslərin məhdudlaşdırılmış sayının seçilməsi. Bu mərhələdə öz xidməti fəaliyyəti çərçivəsində fərdi verilənlərin emalında iştirak edən şirkətin əməkdaşlarının siyahısı formalaşdırılır;
- Fərdi məlumatların emalı avtomatlaşdırılmış vasitələrin və ya fərdi məlumatlara aid olan əməliyyatların məcmusudur; yazı, sistemləşdirmə, yığım, saxlama, dəqiqləşdirmə, istifadə, ötürülmə, mühafizə etmə, silinmə, şəxsi məlumatların məhvi və s [1].

Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu (№ 998-IIIQ) 11 may 2010-cu ildə Azərbaycan Respublikasının Prezidenti tərəfindən verilmişdir [2].

Bu qanun fərdi məlumatların toplanılması, işlənilməsi və mühafizəsi ilə bağlı münasibətləri, milli informasiya məkanının fərdi məlumatlar bölümünün formalaşdırılması, habelə fərdi məlumatların transsərhəd ötürülməsi ilə əlaqədar məsələləri tənzimləyir, bu sahədə fəaliyyət göstərən dövlət və yerli özünüidarə orqanlarının, hüquqi və fiziki şəxslərin hüquq və vəzifələrini müəyyən edir.

Bu qanunun əsas məqsədi fərdi məlumatların toplanılmasının, işlənilməsinin və mühafizəsinin qanunvericilik əsaslarını və ümumi prinsiplərini, həmin sahədə dövlət tənzimləməsinin qayda və tələblərini, fərdi məlumatların informasiya ehtiyatlarında formalaşdırılması, informasiya sistemlərinin yaradılması, informasiyanın verilməsi və ötürülməsi qaydalarını, bu prosesdə iştirak edən şəxslərin hüquqlarını, vəzifələrini və məsuliyyətinin əsaslarını müəyyən etməkdən, əsas insan və vətəndaş hüquqlarını və azadlıqlarını, o cümlədən şəxsi və ailə həyatının sirrini saxlamaq hüququnu müdafiə etməkdən ibarətdir.

Bu qanunda istifadə olunan informasiya, informasiya texnologiyaları, informasiya sistemləri və ehtiyatı, korporativ informasiya sistemi və digər anlayışlardan informasiyanın toplanılması, işlənilməsi və mühafizəsi sahəsində münasibətləri tənzimləyən Azərbaycan Respublikasının qanunlarında müəyyən olunmuş mənalarda istifadə olunur.

Qanundan göründüyü kimi fərdi məlumatların dövlət səviyyəsində qorunmasına böyük əhəmiyyət verilir. Həmçinin proqramlar vasitəsilə fərdi məlumatların qorunması da vacib və aktual məsələlərdən biridir. Proqramlar vasitəsilə məlumatların qorunması – informasiyanın qorunmasını təmin edən və proqram təminatının tərkibinə daxil edilən xüsusi proqramların sistemidir.Məqalədə məhz bu məsələyə toxunulmuşdur.

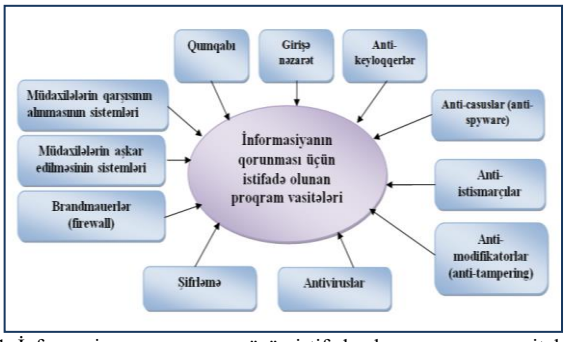
II. PROQRAMLAR VASİTƏSİLƏ FƏRDİ MƏLUMATLARIN QORUNMASI

Proqramlar vasitəsilə fərdi məlumatların qorunması – informasiyanın qorunmasını təmin edən və proqram təminatının tərkibinə daxil edilən xüsusi proqramlar sistemidir. Qoruyucu proqram kodu ayrıca və yaxud proqramların tərkibinə qoşula bilər. Çünki çoxfunksiyalı

DOI: 10.25045/NCInfoSec.2019.16

proqramların qoruyucu funksiyaları özünümüdafiənin əhəmiyyətli vasitələrinə malik deyil və təyininə görə ixtisaslaşdırılmış qoruyucu proqram təminatından zəifdir. İstənilən əhəmiyyətli kompüter sistemi fərdi məlumatın qorunmasının proqram vasitələrinin dəyərli inteqrasiyasını tələb edir [3].

İnformasiyanın qorunması üçün istifadə olunan proqram vasitələri şəkil 1-də göstərilmişdir.



Şəkil 1. İnformasiyanın qorunması üçün istifadə olunan proqram vasitələri

Keyloqqer - təcavüzkarların istifadəçilərə casusluq etmələrinə (həssas məlumatlara, bank kartları məlumatlarına, etimadnamələrinə və s.) imkan verən xüsusi zərərli proqram növüdür .

Məlumatların proqram təminatı ilə funksiyalarının bir çox cəhətdən üst-üstə düşməsinə baxmayaraq kompüterlərin icazəsiz istifadədən qorunması və ya kompüterlər şəbəkəsinin qorunması ilə qarışdırılmamalıdır. Məlumatlar əməliyyat sistemində rəqəmsal formada olmasına baxmayaraq yenədə qorunur. Bir serverlə işləyən kompüterdə məlumatların tam bir şəkildə qorunması eyni vaxtda bir neçə növ qorumanı birləşdirən müxtəlif növ təhlükəsizlik proqramlarının istifadəsini tələb edir.

İnformasiya sistemi (İS) fərdi məlumatların qorunmasında əsas rol oynayır. İS dedikdə saxlama, axtarış, informasiyanın işlənilməsi və uyğun təşkilati resursların (insanlar, texnikalar və s., ISO/IEC 2382:2015) informasiya ilə təmin edilməsi və yayılması başa düşülür [4].

Proqram vasitəsilə İS-də məlumatların qorunması üçün aşağıdakı imkanlardan istifadə etmək lazımdır:

- emal edilən PT kateqoriyalarının sayının azalması üçün ölçülər hazırlamaq;
- hər informasiya sistemi üçün şəxsi məlumatların emalında təhlükələrinin qarşısını almaq üçün aktual modellər formalaşdırmaq;
- tələb edilən sistemin mühafizəsini təmin etmək üçün texniki tapşırıq hazırlamaq.

PT-nin qorunması — analoqların icazəsiz təşkili, istifadəsi, bölüşdürülməsi, dəyişdirilməsi, öyrənilməsindən qorunmaq məqsədilə bir sıra tədbirlər deməkdir.

Proqram təminatının icazəsiz istifadədən qorunması — proqramın qeyri-qanuni istifadəsinə qarşı yönəlmiş tədbirlərdir. Təşkilati, hüquqi, proqram təminatı və avadanlığın qorunması üçün istifadə edilə bilər.

Proqram təminatının köçürülməsindən müdafiə nadir hallarda tətbiq edilir, bu da istifadəçilərin kompüterlərinə onun yayılması və quraşdırılması ehtiyacıyla əlaqədardır. Proqramların köçürülməməsi üçün onun ayrı-ayrı alqoritmləri lisenziya ilə qoruna bilər.

Avropa ölkələrinin ədliyyə nazirlərinin şəxsi məlumatların qorunması haqda ümumi qanunu bütün Avropa İttifaqı ərazisində işləməlidir. Hazırda birliyə daxil olan 28 ölkə fakt olaraq 28 cür müxtəlif şəxsi məlumatların qorunması haqda qanuna malikdir. Qanun vətəndaşlarla dövlətin fərdi məlumatları ilə iş modelinin yaradılmasına istiqamətlənib. Bu layihənin təşəbbüskarı Avropa Şurasının hüquq komissarı, lüksemburqlu Vivian Redinqdir. Qaydalara əsasən, fərdi məlumatlar bir neçə Avropa İttifaqı (Aİ) ölkəsində şirkətlər tərəfindən emal edilir, ancaq monitorinqi yalnız bir nəzarət orqanı həyata keçirməlidir. Burada məlumatları emal edən şirkətin əsas nümayəndəliyi yerləşən ölkənin nəzarət orqanı nəzərdə tutulur.Əvvəllər Fransa dövləti milli qurum səviyyəsində nəzarətə çağırırdı, lakin digər Aİ ölkələri bu modelə qarşı çıxıblar. Belə ki, bir pəncərəli Mini One-Stop Shop (MOSS) sisteminin “Facebook” və ya “Google” kimi Amerika şirkətlərinə əhəmiyyətli təsiri vardır. Bu gün bu şirkətlər məlumatların emalını və saxlanılmasını bir ölkədə həyata keçirirlər, halbuki, nümayəndəlikləri digər ölkələrdə fəaliyyət göstərir və maliyyə vəsaitləri orada toplanır. Avropada bu İrlandiyadır, belə ki, şirkətlər əsas nümayəndiliyə malikdir. "Bizim məqsədimiz Aİ üçün ümumi qaydalar yaratmaq və həmçinin milli tənzimləyicilər üçün inzibati maneələri azaltmaqdır", deyə Litvanın ədliyyə naziri Yuozas Bernatonis bildirib [5].

Şəxsi məlumatların məxfiliyi və qorunması ilə bağlı narahatlıqlar Avropa Birliyində (AB) mövcud qanunvericilikdə islahatlara səbəb oldu. Ümumi Məlumatların Qoruması Qaydaları, vətəndaşların məlumatlarına nəzarətin gücləndirilməsinə və fərdi məlumatların işlənməsi qaydalarının yaradılması ilə əlaqədar olaraq AB vətəndaşlarının fərdi məlumatlarının qorunması ilə bağlı mövcud direktivin islah edilməsinə yönəlmişdir [6].

III. PROQRAMLAR VASİTƏSİLƏ MƏLUMATLARIN QORUNMASI ÜSULLARININ ANALİZİ

Zərərli proqramlar, kompüter virusları, fişinq və şəxsi məlumatların oğurluğu kimi İnternet təhlükəsizliyi problemləri son illərdə daha da kəskinləşdi və İnternet istifadəçilərinin düzgün olmayan davranışları ilə daha da ağırlaşdı. Bu sahə üzrə mütəxəssislər insanlara İnterneti öyrədilər. Bununla birlikdə, mütəxəssislər İnternetdə yeniyetmələrin təhlükəsizlik davranışlarının formalaşmasında mühüm rol oynayır və gündəlik həyatda qarşılıqlı münasibətlər vasitəsilə İnternet təhlükəsizliyi anlayışını onlara çatdıra bilirlər. Nəticə etibarilə mütəxəssislər yeniyetmələrin İnternetdəki riskli davranışlarının motivlərinin daha da öyrənilməsini tələb edir. Qrup analizindən istifadə edərək moderatorların rolu və sosial normaları öyrənilmişdir. Statistik təhlilin nəticələrini təsdiqləmək üçün keyfiyyətli müsahibələr də aparılmışdır. Nəticələr göstərir ki, yeniyetmələrin İnternetdə riskli davranışının qarşısını almaq üçün müəllimlərin İnternet təhlükəsizliyi problemlərini həll etmək bacarıqlarını artırmaq və ya onları qoruyucu tədbirlər görməyə təşviq edən atmosfer yaratmaq lazımdır. [7] işində onlayn təhlükəsizlik təlimi üçün

nəzəri anlayış və praktiki təkliflərin nəticələri müzakirə olunur.

İcazəsiz giriş və ya məxfi fərdi informasiyanın oğurluğu tez tez baş verir. Gizli məlumatların mediada qeyri-qanuni yayılması hər il sənayedə milyonlarla bərpa və itki xərcləri ilə başa gəlir Target Inc. sorğu sisteminin 2013-cü ildəki məlumatına görə 70 milyon müştəriyə dəyən ziyan bir milyarddan çox dollar dəyərində idi. Oğurlanan məlumatlar siyasətçilərə zərər vermək üçün istifadə olunur və xarici və daxili siyasətə mənfi təsir göstərir. [8] işində şəbəkələrin sağlamlığını və təhlükəsizliyini daha yaxşı qorumaq üçün bəzi üsullar təqdim edilir. Bu üsullar mütəxəssislərə şəbəkə davranışları, anomaliyaları və gizli, sistematik problemləri müəyyən etməyə kömək edəcəkdir.

Şəxsi məlumat hissələrinə icazəsiz daxil olmaq çətin bir iş kimi görünür. Şəbəkələrin sağlamlığını yaxşılaşdırmaq üçün zərərli fəaliyyət və digər gizli sistem problemlərini göstərən şəbəkə anomaliyalarını təyin etmək lazımdır. [9] işində gizli sistemlərin problemlərini müəyyənləşdirmək, daha etibarlı şəbəkə yaratmaq və kiber cinayətkarlar tərəfindən məlumat oğurlanmasının qarşısını almaq üçün istifadə edilə bilən şəbəkənin yolunun təhlili xidməti metodlarını təklif edir.

Dövlət qurumlarından yüksək keyfiyyətli elektron hökumət xidmətləri göstərmək üçün onların bir-biri ilə əməkdaşlıq etməyi tələb olunur. Bu əməkdaşlıq ümumiyyətlə xidmət yönümlü yanaşmaya əsaslanır və əməkdaşlıq platformaları tərəfindən dəstəklənir. Bu cür platformalar, uyğun proqram xidmətlərini təqdim etməyə imkan verən ixtisaslaşdırılmış orta proqram əsaslı infrastrukturlardır. Öz növbəsində, hökumətlər tərəfindən işlənən fərdi məlumatların çox həssas olduğu nəzərə alınsa, əksər hökumətlər fərdi məlumatların qorunması haqqında qanun hazırlamışlar. Bu sənəd, elektron hökumətin əməkdaşlıq platformasının bir hissəsi olaraq məlumatların qorunması qanunlarına nəzarət və tətbiq etmək üçün həll yollarını təklif edir [10].

Xətti proqramlar və onların arasındakı əlaqələrin əldə edilməsi proqram təminatının tədqiqatında geniş istifadə olunur. [11] işində tədqiqatın məqsədi təhlil olunan proqramların quruluşu barədə vahid məlumat təminatçısı yaratmaqla proqram təminatının təhlilini asanlaşdırmaqdır. İşdə təklif olunan yanaşma, bir-birinə bağlı xətti bloklar və onların əlaqələri şəkildə proqram kodunun parçalanmasına və təqdim edilməsinə yönəldilmişdir. Bu formada təqdim olunan kod, təhlükəsiz proqram təminatının hazırlanması prosesini asanlaşdırmaq və spesifik xüsusiyyətləri olan nümunələri müəyyən etmək üçün təhlil edilə bilər. Təklif olunan metod mövcud vasitələrdən məlumatları birləşdirən bir plaginin inkişafına əsaslanır. "MAR" sökücü cihazdan məlumatların çıxarılması və sonrakı iş üçün zəruri formada təqdim edilməsi üçün metod hazırlanmışdır. Metodun yoxlama testlərinə aid nümunə verilmişdir. Metodologiyaya uyğun olaraq əldə edilən məlumatlar hədəf olan proqram alətlərində istifadə üçün nəzərdə tutulub.

[12] işinin məqsədi İT sistemlərinin təhlükəsizliyini müzakirə etmək və icazəsiz girişdən qorunmalı olan elementləri müəyyənləşdirməkdir. Proqram təminatı, kiber sahənin xüsusiyyətlərinə əsaslanaraq yaradılmışdır. Proqram sistemlərinin mürəkkəbliyi informasiya təhlükəsizliyini daha mürəkkəb və etibarsız edir. Texnologiyanın inkişafı təhdidlərin inkişafı ilə ayrılmaz dərəcədə bağlıdır, yəni proqram həllərinin təkmilləşdirilməsi bütün istifadələr üçün son dərəcə vacib bir məqama çevrilmişdir. İşdə həm proqram təminatının təhlükəsizlik istifadəçisi olaraq, həm də təhlükəsizlik sistemini yaradarkən hansı təhlükəsizlik elementlərinin nəzərə alınmasının lazım olduğu göstərilmişdir.

Proqram Təminatı Şəbəkələri (Software-Defined Networking, SDN) ənənəvi şəbəkələrdən şəbəkə konfiqurasiyalarını toplamağa imkan verir. SDN, həmçinin proqram görüntülərini daha yaxşı edən proqram protokolları və vasitələrinin inkişafına imkan verir.

Hal-hazırda, SDN idarəetmə şəbəkə cihazlarının məlumat yayımını ayıran yeni quruluş sayəsində sürətlə inkişaf edir. Bir çox tədqiqatçı özlərini belə bir xüsusi şəbəkənin öyrənilməsinə həsr etmişlər. Bununla birlikdə bəzi məhdudiyyətlər SDN-nin inkişafını məhdudlaşdırır. Bir tərəfdən normal bir modeldə bir nəzarətçi bütün təhdidləri daşıyır və ziyanları şəbəkə iflicinə səbəb olur. Digər tərəfdən, məlumat yayımında SDN açarlarında daha çox artım olacaq, bu açarların saxlanmasının yeri məhduddur. Bu problemləri həll etmək üçün [13] işində iki müvafiq protokollar təklif edilir. Xüsusilə, biri təyyarə idarəediməsinin anonim protokolu, digəri isə təyyarədəki məlumatları təsdiqləyən xarici qaynaq protokoludur. Aparılan qiymətləndirmə təklif edilən protokolun düzgün, təhlükəsiz və effektiv olduğunu göstərir.

Məlumat sistemlərinin əldə edilməsi, tətbiqi və inkişafı rəqabət üstünlüyü əldə etmək üçün əsasdır. Texnologiyanın sürətli inkişafı eyni zamanda son istifadəçi məlumatlarının qorunması və məxfiliyinin pozulması ilə əlaqəli etik problemlərə səbəb olur. [14] işində təşkilatın strateji ehtiyaclarını dəstəkləyərkən keyfiyyətli proqram məhsuluna zəmanət verən standart keyfiyyət təminatı metodları müzakirə olunur. Keyfiyyətli proqram təminatının inkişafı prosesinin təkmilləşdirilməsini təşkilatın strateji ehtiyacları ilə əlaqələndirən bir çərçivə təqdim edilir. Nəzərdə tutulan standart təcrübələrə, təşkilatın strateji hədəflərini müəyyənləşdirmək və məlumat sisteminin inkişafı ilə əlaqəli effektivliyi izləmək üçün Balans Score Card metodologiyasından istifadə edilir və həmçinin əlaqələndirmək üçün Audit Assosiasiyası tərəfindən verilmiş “İnformasiya və əlaqəli texnologiyalar üçün idarəetmə nəzarəti ” (Control Objectives for Information and Related Technologies, COBIT) - 5 informasiyanın idarəetmə sistemini özündə birləşdirir [14].

Əşyaların İnterneti (İnternet of Things, IoT) texnologiyasının sürətli inkişafı və kompüterə quraşdırılmış cihazların hesablama gücünün artması təhlükəsizlik təhdidləri və hücumlarına açıq olma ehtimalını yaradır. Son zamanlarda daxil edilmiş fərdi məlumatların təhlükəsizliyi barədə Etibarlı İcra Mühiti (Trusted Execution Environment, TEE), ictimaiyyətin diqqətini çəkmiş və ixtiyari kodun sistemin müəyyən hissəsindən tamamilə təcrid olunmuş mühitlərində icra olunmasına imkan yaratmışdır. TEE- əsas prosessorun qorunan sahəsidir. Bununla birlikdə TEE-də mövcud yaddaş qorunması üçün mövcud olan metodlar yetərli deyildir. Ümumiyyətlə, proqram təminatına dair rəsmi metodlar praktik deyil və həyata keçirməyə aparıcı yanaşmalar nəzəri cəhətdən

təsdiqlənmir. TEE-də təcrid və yaddaşın qorunması problemlərini həll etmək üçün Qabaqcıl Risk Maşını (Advanced RISC Machine, ARM) platformasında yaddaşın bütövlüyünün təhlükəsizlik təhdidlərindən qorumaq üçün praktik metod təklif edilmişdir. ARM-dan həssas kodu və məlumatları hücumlardan qoruya biləcək təcrid olunmuş iş mühiti yaratmaq üçün istifadə edilir. Xilinx Zynq ZC702 qiymətləndirmə şurasında ARM tətbiq edilir. Maşınların avtomatik yoxlama nisbəti təxminən 78.32% təşkil edir və təklif olunan metod həm yükləmə vaxtı, həm də xərc baxımından səmərəli və məqsədəuyğundur [15].

Fərdi məlumatları idarə edən dövrdə Avropa Məlumatların Qorumasının Ümumi Qaydalarının (General Data Protection Regulation, GDPR) tətbiqi son zamanlarda populyarlıq qazanmışdır. [16, 17] işində proqram təminatçılarının diqqətinə çatdırmalı olan GDPR məqalələri təqdim olunur, həmçinin kompüter üzrə alimlər tərəfindən təqdim olunmuş tələblərin mənşəyini izləmək, istifadəyə nəzarət və uzaq protokolların yayılması kimi ən müasir texnologiyalara əsaslanaraq tətbiq oluna biləcəyi izah edilir.

NƏTİCƏ

Şəbəkə rabitəsi, qloballaşma və məlumat mübadiləsinə əsaslanan müasir rəqəmsal dünya, məxfilik və fərdi məlumatların qorunması sahəsində təklif olunan məlumat strukturlarına etibarlı giriş prinsiplərini əks etdirən yeni vacib vəzifələri müəyyənləşdirir. Bu səbəbdən elektron mühitin bütün mənbələrinə etibarlı daxil olmaq çox vacibdir və fərdi məlumatların identifikasiyası, avtorizasiyası və qorunması üçün adekvat texnoloji və təşkilati tədbirlər tətbiq edilməlidir. Uğurlu qeydiyyata alındıqdan sonra hazırlanmış istifadəçi profillərini və təlim zamanı toplanmış bütün şəxsi məlumatları qorumaq üçün ciddi təhlükəsizlik prosedurları təklif edilməlidir [18, 19].

Göründüyü kimi məqalədə proqram vasitəsilə fərdi məlumatların qorunması üsulları araşdırılmışdır. Fərdi məlumatları qoruyan proqramlar daha effektiv işləyir və səmərəlilik göstəriciləri yüksək olur. Dünya və respublika miqyasında bu sahə üzrə yeni qanunların qəbul edilməsi bu işlərin aktual olduğunu bir daha sübut edir. Avropa şurasının bu sahəyə böyük diqqət ayırması təqdirə layiqdir. Gələcəkdə bu sahəyə aid olan yeni proqramların təşkili və inkişaf etdirilməsi fərdi məlumatların daha sıx qorunmasına imkan verəcəkdir. Tövsiyə olunur ki, bu sahədə elmi tədqiqat işləri gücləndirilsin və fərdi məlumatları qoruyan yeni keyfiyyətli proqramlar yaradılsın.

İSTİNADLAR

[1] «Защита_персональных_данных», https://ru.wikipedia.org/wiki/Защита_персональных_данных

[2] “Fərdi məlumatlar haqqında Azərbaycan Respublikasının qanunu”, 11.05.2010, http://www.e-qanun.az/framework/19675

[3] «Программная защита информации», 2000-2019, http://rus.safensoft.com/security.phtml?c=882

[4] Ю.А.Маглинец, «Анализ требований к автоматизированным информационным системам». Бином, 2008, 200 с.

[5] “Şəxsi məlumatların qorunması haqda yeni qanun”, 08.10.2013, http://www.lawreform.az/index.php?module=news&name=view&id=1098&lang=az

[6] G. Ferreira, M. Sousa, B. Silva, S. Frade, L Antunes, T. Beale, C.Correia, “Open EHR and General Data Protection Regulation: Evaluation of Principles and Requirements”, JMIR medical informatics, 2019, vol. 7, no. 1, https://www.ncbi.nlm.nih.gov/pubmed/30907730

[7] C. Hui-Lien, S. Jerry, “The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers”, Computers & education, 2017, vol. 112, pp. 83-96.

[8] A. Joshua, M. Scott, C. Edward, “SDN Data Path Confidence Analysis”, IEEE Conference on dependable and secure computing, 2017, pp. 209-216.

[9] A. Joshua, M. Scott, C. Edward, “A Framework for SDN Network Evaluation”, 2017 47th annual ieee/ifip international conference on dependable systems and networks workshops, pp. 111-112, 2017.

[10] E. Andres, M. Dahiana, G. Laura, “Monitoring and Enforcing Data Protection Laws within an E-government Interoperability Platform”, 2015 XLI Latin american computing conference, pp. 548-559, 2015.

[11] I.O. Bazhenov, “Lubkin Methodology of software code decomposition analysis”, 12th international IEEE Scientific and technical conference on dynamics of systems, mechanisms and machines (dynamics), 2018.

[12] K. Anna, O. Lidia, “Data Securityin Cognitive Information Systems”, Proceedings 2018 IEEE 32nd international conference on advanced information networking and applications (AINA), pp. 631-635, 2018.

[13] K. Pawel, “Digital image integrity a survey of protection and verification techniques”, Digital signal processing, 2017, vol. 71, pp. 1-26.

[14] H. Syeda Umema, A. Abu Turab, “Software Development for Information System Achieving Optimum Quality with Security”, International journal of information system modeling and design, vol: 8, no. 4, pp. 1-20.

[15] C. Rui, J. Liehui, C. Wenzhi, X. Yang, C. Yuxia, A. Alelaiwi “MIPE: a practical memory integrity protection method in a trusted execution environment”, Cluster computing-the journal of networks software tools and applications, 2017, vol. 20, no. 2, pp. 1075-1087.

[16] B. Pascal, K. Erik, W. Paul Georg, B. Juergen, “Identity Management and Protection Motivated by the General Data Protection Regulation of the European Union-A Conceptual Framework Based on State-of-the-Art Software Technologies”, Technologies, 2017, vol. 6, no. 4, pp. 1-14.

[17] C. Hui-Lien, S. Jerry Chih-Yuan, “The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers”, Computers & education, 2017, vol. 112, pp. 83-96.

[18] R. Radi, N. Irina, “Architecture of Combined e-Learning Environment and Investigation of Secure Access and Privacy Protection”, International journal of human capital and information technology professionals, 2017, vol. 7, no. 3, pp. 89-106.

[19] K. Peter, D. Glenn, “Practical uses of virtual machines for protection of sensitive user data”, Information security practice and experience, proceedings, 2007, vol. 4464, 145 p.

EXPLORING PERSONAL DATA PROTECTION METHODS WITH PROGRAM TOOLS

Shafagat Mahmudova

Institute of Information Technology of ANAS, Baku, Azerbaijan

shafagat_57@mail.ru

Abstract— The paper highlights the personal data and the stages of its protection. Some provisions of the Law of the Republic of Azerbaijan on the personal data are reviewed. The protection of personal data through programs is explored. The studies in this area are reviewed. Data protection methods through programs are studied and analyzed. Some recommendations for the further developments in this field are provided.

Keywords— *personal data; protection; software; technical task; SDN*