Fərdi məlumatların qorunması üçün proqram təminatı alətləri haqqında

Bayramova Tamilla
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
tamilla@iit.science.az

***Xülasə*— Məqalədə rəqəmsal iqtisadiyyata keçidlə əlaqədar fərdi verilənlərin qorunmasında yeni problemlərin yaranması şərh edilmişdir. İnformasiya mühafizəsi sistemlərinin yaradılmasına müasir yanaşmalar araşdırılmışdır. Proqram sənayesinin inkişafı ilə əlaqədar olaraq informasiyaya olan təhdidlər artdığına görə müasir şifrələmə texnologiyaları, onların tətbiq sahələri tədqiq edilmişdir. İnformasiyanın qorunması üçün intellektual sistemlərin işlənilməsinin vacibliyi vurğulanmışdır.**

Açar sözlər— fərdi verilənlər, proqram təminatı, şifrləmə, informasiyanın qorunması

I. GİRİŞ

Müasir informasiya texnologiyaları şəxsi həyat anlayışı ilə bağlı təsəvvürlərdə əhəmiyyətli dəyişikliklərə səbəb olmuşdur. Gerçək dünyada baş verən hadisə və proseslər – əmtəə və xidmətlərin əldə edilməsi, yaxın adamlarla ünsiyyət, dövlət orqanları ilə qarşılıqlı əlaqə və s. virtual mühitə keçərək bir qədər fərqli mahiyyət daşımağa başlamışdır. Bunun nəticəsində insanların bilərəkdən, yaxud bilməyərəkdən açıqladığı və müxtəlif təşkilatların hədəfinə çevrilən fərdi məlumatlar misli görünməmiş miqyas almışdır. Xüsusilə, İnternet kütləvi sosial hadisəyə, cəmiyyət həyatının ayrılmaz hissəsinə çevrildikdən sonra insanlar bu texnologiyanın onların şəxsi həyatına təsirindən ehtiyat etməyə başlamışlar. Bu gün insanlar narahatdırlar ki, onların sağlamlığı, maliyyə vəziyyəti, şəxsi münasibətləri, siyasi baxışları və s. ilə bağlı kimlərdəsə məlumatlar toplanır [1]

İnformasiya texnologiyaları sahəsində sürətli inkişaf, Əşyaların İnternetinin, müxtəlif təyinatlı intellektual sistemlərin geniş yayılması, elektron dövlət strukturlarında elektron sənəd dövriyyəsinin formalaşması və sosial şəbəkələrdən istifadə edilməsi çox böyük sayda və həcmdə verilənlərin toplanmasına səbəb olmuşdur. Bu verilənlərin analizi və emalı problemi (toplanması, saxlanılması, analizi, ötürülməsi, dəyişdirilməsi, silinməsi və s.) Big Data texnologiyalarının yaranmasına gətirmişdir. Bu verilənlərin çox böyük hissəsi konfidensial xarakter daşıyır və qəbul edilmiş normativ-hüquqi aktlar vasitəsilə qorunur. Konfidensial informasiyaya vətəndaşların fərdi verilənləri, kommersiya sirlərinə aid verilənlər, xidməti verilənlər və s. daxildir.

Cəmiyyətin həyat fəaliyyətinin bütün sahələrində proseslərin rəqəmsallaşması konfidensial informasiyanın həcminin artmasına və onun qorunması üzrə xidmətlər bazarının inkişafına gətirmişdir. Fərdi məlumatların toplanılması və işlənilməsi, həmin məlumatların mühafizəsinin tam təmin olunmaması nəticəsində subyektə dəyən maddi və mənəvi ziyan və onun həcmi məhkəmə tərəfindən müəyyən edilir, qanunvericilikdə nəzərdə tutulmuş qaydada ödənilir [2].

II. FƏRDİ MƏLUMATLARIN QORUNMASININ NORMATİV-HÜQUQİ ƏSASLARI

Zaman keçdikcə informasiyanın qorunma metodları və üsulları əhəmiyyətli dəyişikliyə uğramışdır. Son illərdə bu sahədə xüsusi tələblər, tövsiyələr, normativ-hüquqi aktlar və araşdırma metodikaları işlənilmişdir.

Konfidensial informasiyanın və eyni zamanda fərdi məlumatların ələ keçirilmə hallarının artması nəticəsində informasiyanın qorunmasının hüquqi normativ bazası əhəmiyyətli dəyişikliyə uğramışdır.

Yeni texnologiyaların inkişafı və interenetə qoşulan intellektual qurğuların yayılması konfidesiallığın qorunmasına dair yeni qanunların qəbul edilməsini labüd etmişdir. 2018-ci ildə belə qanunlardan biri ***Fərdi məlumatların mühafizəsi üzrə Ümumi Qanun*** (*General Data Protection Regulation – GDPR*) qüvvəyə minmişdir. Bu Avropa Birliyi (AB) və Avropa İqtisadi fəzası vətəndaşlarının fərdi verilənlərinin konfidensiallığı və qorunması haqda qanundur. GDPR-in əsas ideyası aşağıdakılardan ibarətdir [3]:

- ✓ fərdi verilənlərin qorunması;
- ✓ insanlarının məlumatlarının qorunma hüququnun və azadlıqlarının qorunması;
- ✓ Avropa Birliyi çərçəvəsində fərdi verilənlərin yayılmasına məhdudiyyət qoyulmasından ibarətdir.

GDPR-in məqsədləri:

- ✓ Fiziki şəxslərə onların fərdi verilənlərinə nəzarət etmək üçün instrumental vasitələrin verilməsi;
- ✓ Fərdi verilənlərin qorunması üzrə müasir standartların tətbiq edilməsi;
- ✓ AB-nin fərdi verilənlərin qorunması üzrə rəqəmsal fəzasının inkişaf etdirilməsi;

DOI: 10.25045/NCInfoSec.2019.46

- ✓ AB-yə üzv dövlətlərin səlahiyyətli orqanları daxil olmaqla bütün iştirakçılar tərəfindən qaydalara ciddi şəkildə əməl edilməsinin təmin edilməsi;
- ✓ Fərdi məlumatların beynəlxalq səviyyədə ötürülməsinə hüquqi dəstək verilməsi.

GDPR qanunu AB ərazisində və ondan kənarda fiziki və ya hüquqi şəxslər, dövlət orqanları və digər müəssisə və təşkilatlar tərəfindən AB vətəndaşlarının fərdi məlumatlarının tam və ya qismən avtomatlaşdırılmış emalını əhatə edir. Şəxsi məlumatların emalı ilə əlaqəli hər hansı bir fəaliyyət (hətta qeyri-kommersiya fəaliyyəti də) GDPR-ə tabedir. AB vətəndaşlarına təmənnasız xidmət göstərilərsə, həmin xidmət də bu qanunun fəaliyyət sahəsinə düşür. Məsələn, əgər onlar İnternetdə qeydiyyatdan keçərək hər hansı bir saytın təmənnasız xidmətindən istifadə edərsə və fərdi məlumatlarını daxil etmiş olarsa, GDPR qanunları onlara da aid edilir.

GDPR-in tələblərinə uyğun gəlmək üçün şirkətlər aşağıda göstərilənləri nəzərə almalıdır:

- ✓ Layihəyə hansı fərdi verilənlərin toplanacağı, onların harada və necə qorunacağı və istifadə ediləcəyi əvvəlcədən müəyyən edilməlidir. Əgər bu verilənlər əsasında konkret insanı identfikasiya etmək olmursa şirkət bu qanunun fəaliyyət dairəsindən kənarda qalır.
- ✓ Fərdi verilənlərin istifadəsinə nəzarət edilməlidir və müəyyən edilməlidir ki, onları kim, necə, harada və niyə emal edir.
- ✓ Fərdi verilənlərin mühafizə mexanizmləri işlənilməlidir.
- ✓ GDPR qanunlarına uyğun olaraq hesabatlar hazırlanmalıdır.

GDPR şərtlərinə əhəmiyyət verməyən şirkətlər 20 milyon avro və ya müəssisənin illik gəlirinin 4%-ə qədəri məbləğində cərimə edilə bilər. Cərimənin məbləği müxtəlif amillərdən (qanun pozuntusunun dərəcəsi, səhlənkarlıq və ya qəsdən törədilməsi, zərər çəkənlərin sayı, onlara dəyən ziyan və s.) asılıdır.

Azərbaycanda bu sahədə əsas qanun 2010-cu ildə qəbul edilən "Fərdi məlumatlar haqqında qanun"dur [4].

İstifadəçilərin konfidensiallığını qorumaq və GDPR qaydalarına uyğunluğa nail olmaq üçün bir sıra müasir proqram vasitələri işlənilmişdir. Müəssisədə belə proqram vasitələrinin tətbiqi baha başa gəlir. Lazım olan proqram təminatını seçərkən təşkilatın ölçüsünü, verilənlərin konfidensiallığının nə qədər vacib olduğunu və konfidensiallığın pozulmasının müəssisəyə vuracağı zərərin potensial dəyərini nəzərə almaq lazımdır [5].

Verilənlərin sızmasının qarşısını almaq üçün avtomatlaşdırılmış korporativ siyasətin həyata keçirilməsi mühafizə olunan verilənlərin təşkilatdan kənara çıxmadan aşkar etmək lazımdır. Belə vasitələr verilənlərin itirilməsinin qarşısının alınması (*Data Loss Prevention – DLP*) vasitələri adlanır.

III. İNFORMASİYANIN MÜHAFİZƏSİ VASİTƏLƏRİ

2009-cu ildə Avropa İstehlakçı Hüquqlarını Müdafiə Komissarı Meglena Kuneva fərdi şəxslərə aid məlumatların rəqəmsal iqtisadiyyatda necə vacib bir hala gəldiyini göstərmək üçün şəxsi məlumatları neftlə müqayisə etmişdir. Hər gün dünyada insanlar 196 milyard elektron poçt göndərir və ya qəbul edir, Twitter-də 500 milyondan çox tvit göndərir və Facebook-da 4,75 milyard müxtəlif məzmunda məlumat paylaşır [6].

Konfidensial informasiyanın emal edilmə prosesində əlyetərliyi olmayan kənar şəxslər tərəfindən informasiyanın əldə edilməsi və qanundan kənar məqsədlər üçün istifadə edilməsi neqativ hallara gətirir, bəzən isə fəlakətlə nəticələnə bilər. Ona görə də informasiya mübadiləsi və emalı üçün elə şərait yaratmaq lazımdır ki onun qeyri-qanuni istifadəsinin qarşısını almaq mümkün olsun. Bu yeni problem deyil informasiyanın toplanması və saxlanılmasına başlanılan vaxtdan onun qorunması əsas məsələlərdən biri olmuşdur. İnformasiyanın qorunması aktual problemə çevrilmişdir və əsasən aşağıda göstərilənləri nəzərdə tutur:

- İnformasiyaya icazəsiz girişin (və ya icazəsi olmayan digər şəxslərə ötürülməsinin) qarşısının alınması;
- İnformasiyaya icazəsiz giriş faktlarının vaxtında aşkar edilməsi;
- İnformasiyaya giriş qaydasının pozulmasının neqativ nəticələri haqda xəbərdarlıq edilməsi;
- İnformasiyanın emal eilməsinin texniki vasitələrinin fəaliyyətini pozan təsirlərə imkan verilməməsi;
- İcazəsiz giriş nəticəsində dəyişdirilmiş və ya silinmiş informasiyanın dərhal bərpa edilməsi;
- İnformasiyanın etibarlı şəkildə qorunmasına daimi nəzarətin olması.

Fərdi məlumatların təhlükəsizliyinə cavabdeh təşkilatlar adətən aşağıda verilmiş de-identifikasya üsullarından istifadə edirlər [7]:

- ✓ Anonimləşdirmə (anonymization) – verilənlərin anonimləşdirilməsi zamanı fərdi məlumatlara aid atributlar (ad, ünvan və sosial təhlükəsizlik nömrələri və s.) elə silinir və ya dəyişdirilir ki, bu verilənlər əsasında hər hansı bir şəxsi müəyyən etmək mümkün olmur. Ona görə də belə məlumatların yenilənməsi, bir neçə mənbədən alınmış verilənləri birləşdirmək mümkün deyil.
- ✓ Psevdonimləşdirmə (pseudonymization) – təxəllüsün verilməsi zamanı da fərdi məlumatlara aid atributlar silinir və ya dəyişdirilir. Lakin bu üsulda dəyişdirilmiş verilənlər şəxsin gizli təxəllüsü altında yadda saxlanılır. Anonimləşmədən fərqli olaraq bu verilənlər dəyişdirilə bilər, müxtəlif vaxtlarda alınmış məlumatlar birləşdirilə bilər.

- ✓ Açar-kodlaşdırma (key-coding) – açarla kodlaşdırma fərdi məlumatları kodlaşdırır və onların dekodlaşdırılması üçün açar yaradır.
- ✓ Şifrləmə (encryption) və s.

IV. FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİNİ TƏMİN EDƏN MÜASİR TEXNOLOGİYALAR

Diferensial gizlilik metodu fərdi məlumatlara müraciətləri alqoritm və interfeys (etibarlı kurator kimi çıxış edir) vasitəsilə idarə edir [8]. Tədqiqatçı verilənləri analiz etmək üçün kuratora sorğu göndərir və kurator da təsadüfi küy əlavə etməklə verilənlərin konfidensiallığını qorumağa və eyni zamanda sorğulara düzgün cavab verməyə çalışır [7].

Homomorf şifrlmə şifrlənmiş məlumatlarla şifrini bilmədən və onları deşifrləmədən işləməyə imkan verir. Homomorf şifrləmədə istifadəçi verilənlərini şifrləyir və sonra buludda yadda saxlayır. Bulud xidmətləri göstərənlər isə əslində hansı informasiyanın saxlanıldığını bilmir. Əgər istifadəçi yeni verilənlər əlavə etmək istəyərsə o, homomorf şifrləmənin additiv və multiplikativ xüsusiyyətlərindən istifadə edə bilər. Adi şifrləmədə verilənlərlə işləmək üçün onu de-şifrləmək lazımdır, bu zaman informasiyanın bədniyyətli insanların əlinə keçmə ehtimalı artmış olur. Homomorf şifrləmə vasitəsilə şifrlənmiş mətn üzərində əməliyyatlar (toplama, çıxma birləşmə, kəsişmə) aparmaqla adekvat nəticələr almaq olar. Məsələn, elektron seçkilərdə (seçicilərin anonimliyini qorumaqla səsləri hesablamaq), bulud hesablamalarında, mühafizə olunan bazalarda axtarış (məzmunu analiz etmədən nəticənin alınması) və s. sahələrdə tətbiq edilə bilər [9].

Homomorf şfrələmə ideyasının 40 il əvvəl yaranmasına baxmayaraq ancaq 2009-cu ildə tam homomorf sistem IBM şirkətində işlənilmişdir [10]. Lakin belə sistemlərin məhsuldarlığının aşağı olması onların real həyatda aktiv tətbiqini məhdudlaşdırır.

Funksional şifrləmə – şifrlənmiş məlumat əsasında müəyyən *f* funksiyasının qiyməti hesablanır: *m* açıq məlumatının şifrlənmiş mətninə əsasən *f*(*m*) hesablanır, bu zaman *m* haqqında (o cümlədən, *f*-in hesablanması zamanı aralıq nəticələr haqqında) hər hansı əlavə məlumat əldə etmək mümkün olmamalıdır [4]. Funksional şifrləmə 2005-ci ildə təklif edilmişdir və açıq açarlı şifrləmə ideyasına əsaslanır. Funksional şifrləmədə şifrlənmiş verilənlər deyil, şifrlənmiş funksiya ötürülür. Burada da homomorf şifrləmədə olduğu kimi verilənlər tam deşifrlənmir. Bu sxemi proqram təminatının bədniyyətlilər tərəfindən analiz olunmasının qarşısını almaq üçün tətbiq etmək olar. Proqram kodunun funksional şifrlənməsindən sonra funksionallığına görə eyni, lakin analiz üçün əlyetərli olmayan ilkin kodu alırıq. İntellektual mülkiyyəti qorumaqla yanaşı funksional şifrləmədən bulud hesablamalarında da istifadə etmək olar [8].

Funksional şifrləmənin öyrənilməsi kriptoqrafiya sahəsində texnologiyaların inkişafına və daha güclü alətlərin və metodların yaranmasına səbəb olmuşdur [11, 12]

Bal şifrləməsi (*Honey Encryption*). Əlavə aldadıcı resurs yaratmaqla bədniyyətliləri məqsəddən yayındırır. Honeypots serverləri yaradılır, burada doğruya oxşar sadə şifrlənmiş resurslar yerləşdirilir. Ona görə “bal” şifrləməsi deyilir ki, kriptoanalitik mətni deşifrləmək istədikdə o, əhəmiyyətsiz, aldadıcı bir məlumat alır və başa düşmür ki, aldığı real informasiya deyil. Bal şifrləməsində əsil şifrlənmiş mətni ancaq açarı bildikdə deşifrləmək olur. Şifrləmənin bu növü daim təkmilləşdirilir və geniş yayılmaqdadır [13].

DNT şifrləmə. Hesablamalar, verilənlərin yadda saxlanılması və kriptoqrafiyada tətbiq etmək üçün DNT molekullarına məxsus olan enerji səmərəliliyi, paralellik, informasiyanın qeyri-adi dərəcədə sıxlığı araşdırılmışdır və onun əsasında yeni texnologiyalar işlənilmişdir. 1994-cü ildə Leonard Adleman (RSA alqoritminin müəlliflərindən biri) DNT molekullarının xüsusiyyətlərindən kriptoqrafiyada istifadə edilməsini təklif etmişdir. DNT-şifrləmə kriptoqrafiyanın yeni sahəsidir. Mürəkkəb bioloji proseslərə əsaslanması və mürəkkəb kriptoqrafik hesablamalar verilənlərin ikiqat mühafizəsini təmin edir. Təhlükəsizlik analizi göstərmişdir ki, bu şifrləmə sxemi çox yüksək konfidensiallığı təmin edə bilər [14, 15].

İnformasiyanın musiqi vasitəsilə kodlaşdırılması. MusicXML formatında yazılan musiqi akkordlar adlanan 2-4 saniyəlik kiçik fraqmentlərdən ibarətdir. Şifrləmənin mahiyyəti simfoniya vasitəsilə ondan ibarətdir ki, bu akkordlar bir simvolla əlaqələndirilir və cədvəldə yazılır. Belə şifrlənmiş məlumat açıq kanalla ötürülə bilər [16].

V. DİFERENSİAL GİZLİLİK METODUNUN TƏTBİQ SAHƏLƏRİ

Verilənlərin intellektual analizi sistemlərində (veb-axtarış, tövsiyə sistemləri, kraudsorsinq platformaları, analitik proqramlar və s.) istifadəçilərin konfidensiallığının qorunması əsas tələbdir. Aşağıda diferensial konfidensiallığın tətbiq etməklə istifadəçilərin konfidensiallığını qoruyan bir neçə aparıcı sistemlər göstərilmişdir:

- ✓ Google şirkətinin tətbiqi – RAPPOR sənayedə diferensial konfidensiallığın geniş yayılmış ilk tətbiqidir. RAPPOR (Randomized Aggregatable Privacy-Preserving Ordinal Response – konfidensiallığı qoruyan, təsadüfi yığıla bilən nizamlı cavab) istifadəçinin verilənlərinə ümumilikdə baxmağa imkan verir, lakin onun ayrı-ayrı detallarını analiz etməyə imkan vermir. RAPPOR kliyent proqram təminatıdır, istifadəçinin statistikasını toplayan yeni mexanizmdir və təsadüfi cavablandırma metodlarından istifadə edərək konfidensiallığı etibarlı şəkildə təmin edir [17].
- ✓ Apple iOS 11/macOS əməliyyat sistemində öz proqramlarında məxfiliyi qorumaq üçün diferensial konfidensiallıq metodundan istifadə etmişdir [18]. Verilənlərə əlavə edilmiş statik küy istifadəçilərin fərdi verilənlərini maskalayır və konfidensiallığı qoruyur. Aşağıda göstərilən funksiyalarda tətbiq

edilmişdir: QuickType; Emoji; Safari; Sağlamlıq haqda məlumat (*Health Type Usage*).

- ✓ LinkedIn sosial şəbəkəsində də konfidensiallığın qorunması üçün diferensial konfidensiallıqdan istifadə edilir. LinkedIn Salary tədqiqatçılar, iş axtaranlar və gənc kadrlar üçün informasiyanın toplanması və təqdim edilməsi üçün kraudsorsinq sistemidir [19].
- ✓ Microsoft Windows telemetriyasının toplanması üçün lokal diferensial konfidensiallıq təminatını tətbiq edir. Windows olan milyonlarla qurğularda statistik məqsədlərlə toplanan informasiyanın konfidensial-lığını qorumaq üçün diferensial konfidensiallıqdan istifadə edilir [20].

NƏTİCƏ

Verilənlərin konfidensiallığını qorumaq üçün adları çəkilən proqram vasitələrinin heç biri informasiyanı tam olaraq qoruya bilmir. Son illərdə informasiyanın qorunması üçün intellektual sistemlərin işlənilməsinə başlanılmışdır. Əsas diqqət şəxsiyyətin identfikasiyası üçün biometrik sistemlərin qurulmasına, icazəsiz girişin avtomatik müəyyən edilməsi və qarşısının alınması, informasiya risklərinin analizi və idarə edilməsinə yönəlmişdir. Bu sinif informasiya sistemlərinin yaradılması zamanı neyron şəbəkələr, süni immun sistemləri, qeyri-səlis məntiq və s. kimi soft-kompütinq texnologiyalarından istifadə edilməsi fərdi məlumatların daha etibarlı qorunmasını təmin edə bilər.

Kvant kompüterlərinin yaranması mövcud kriptoqrafiya texnologiyalarının sonu ola bilər. Ona görə də kvant mexanikasının imkanlarından istifadə etməklə kvant kriptoqrafiya metodlarının işlənilməsi gələcəyin ən aktual problemlərindən biri ola bilər.

İSTİNADLAR

[1] R.Ş. Mahmudov “Big Data erasında fərdi məlumatların hüquqi rejimininin müəyyənləşdirilməsi problemləri,” İnformasiya cəmiyyəti problemləri, 2018, №2, 28–33

[2] В. Кияев, О. Граничин. Безопасность информационных систем. Открытый Университет «ИНТУИТ». 2016. с. 192.

[3] “General Data Protection Regulation”https://gdpr-info.eu/

[4] “Fərdi məlumatlar haqqında Qanun” http://www.e-qanun.az/framework/19675

[5] M..Hansen, A.Lehmann, D.Whitehouse, S.Fischer-Hübner, L.Fritsch, C.Raab. Data Protection by Design and by Default à la European General Data Protection Regulation. Privacy and Identity Management. Facing up to Next Steps. Privacy and Identity 2016. IFIP Advances in Information and Communication Technology, vol 498. Springer, Cham.

[6] S. Spiekermann, A. Acquisti, R. Bohme, Kai-Lung Hui. The challenges of personal data markets and privacy, Electron Markets, 2015, Vol. 25, Issue 2, pp 161–167.

[7] Y. İmamverdiyev. “Big Data və fərdi məlumatların təhlükəsizliyi,” “Big data: imkanları, multidissiplinar problemləri və perspektivləri” I respublika elmi-praktiki konfransı, 2016, s.

[8] M. U. Hassan, M. H. Rehmani, & J. Chen “Differential privacy techniques for cyber physical systems: A survey,” IEEE Communica-tions Surveys & Tutorials, 2019, pp. 1–46. doi:10.1109/comst.2019.2944748

[9] Jigar M. Shah, H. Kothadiya. “A survey on homomorphic encryption techniques in cloud computing,” International Journal of Advance Engineering and Research Development, Vol. 2, No 2, 2015.

[10] N. Mohammed, R. Chen, B. C. M. Fung, and P. S. Yu. Differentially private data release for data mining, Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (SIGKDD), pp. 493-501, 2011

[11] C. Gentry, C. Peikert and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In STOC, 2008, pp. 197–206

[12] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In EUROCRYPT, 2010, pp. 523–552

[13] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In EUROCRYPT, 2013, pp. 1–17

[14] N.S. Noorunnisa, K. R. Afreen. Review on Honey Encryption Technique, International Journal of Science and Research (IJSR), Vol. 5, Issue 2, 2016, pp.1683-1686.

[15] G. Cui, L. Qin, Y. Wang and X. Zhang. An encryption scheme using DNA technology, 3rd International Conference on Bio-Inspired Computing: Theories and Applications, 2008, pp. 37-42.

[16] М. Гриффин. Хранение мировой информации в обувной коробке, Fanatical Futurist, 2016.

[17] Богданов М.Р., Габитов И.А. Кодирование текста с помощью музыки, IT & Transport / ИТ & Транспорт: сб. науч. статей, Самара: Интелтранс, 2018, Т.10, стр. 89-96

[18] H. Haddadi, Privacy-Preserving Analytics: The Browser nightmares, https://haddadi.github.io/

[19] Differential Privacy, https://www.apple.com/ru/privacy/docs/Differential_Privacy_Overview.pdf

[20] K. Kenthapadi, I. Mironov, A. Guha Thakurta. Privacy-preserving Data Mining in Industry, Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining, 2019, pp. 840-841.

ABOUT SOFTWARE TOOLS FOR PERSONAL DATA PROTECTION

Tamilla Bayramova

Institute of Information Technology of ANAS, Baku, Azerbaijan

tamilla@iit.science.az

Abstract— The article describes new challenges in protecting personal data related to the transition to the digital economy. Modern technologies for information protection have been investigated. Due to the increasing threats to information as software industry evolves, modern encryption technologies and their application areas have been explored. The importance of the use of intellectual systems for the protection of information was emphasized.

Keywords— *personal data, software, encryption, data protection*