Разпределено информационно обслужване и защита на личните данни

Проф. д.т.н. Ради Романски
Технически университет - София

1. Въведение

Инициативите за усъвършенстване на информационното общество (ИО) поставят нови изисквания към съвременните информационни технологии (ИТ) за решаване на проблеми с глобализацията [1] и разпределеното информационно обслужване. Това се потвърждава от доклада на Европейската комисия (ЕК) за резултатите от прилагане на инициатива i2010 през периода 2005-2009 г. [2], както и от обобщаващия доклад за 2009 г. [3] в сектор „предприятия и промишленост". В тази посока е и един от трите основни приоритети на представената през март 2010 г. стратегия Europe 2020 [4], свързан с „изграждане на икономика, основаваща се на знания и иновации". Задачата е не само да се разработват и внедряват нови технологични решения за съхраняване, обработка и пренасяне на информацията (GRID [5], Cloud Computing [6, 7], Mobile Cloud Computing [8]), но и да се осигури висока ефективност на тяхното приложение в различни области на науката, образованието, икономиката, индустрията и социално-битовата сфера [9]. Създаването на разпределени информационни ресурси и предоставянето на услуги за разпределено обслужване налагат изграждане на знания в обществото за принципите, методите и технологичните средства за целесъобразното им използване.

От друга страна, съвременните ИТ позволяват все по-силно навлизане на разпределената компютърна обработка в социалните взаимоотношения и утвърждаване на направлението "social computing", свързано с изграждане на социални мрежи от сайтове (MySpace, Facebook, Twitter, etc.) [10]. Социалните мрежи провокират всеки участник да открива профил с лични данни (ЛД) и да публикува персонална информация, която да бъде достъпна през глобалната мрежа от множество други потребители. Това разширява

възможностите за социални контакти, но открива и опасности за спекулации, в някои случаи нежелателни, както и поставя доста въпроси относно персонализацията на социалните контакти и правото на личен живот [11, 12]. В този смисъл защитата на персоналната информация на потребителите е един сериозен проблем при разпределените услуги и комуникациите в глобалната мрежа [13, 14]. Това с пълна сила важи и за облачните услуги (cloud services), при които се налага да бъдат приложени технологични мерки за защита на личните данни [15, 16].

Статията е насочена към основните проблеми, свързани с осигуряване на адекватна защита на персоналните данни при разпределената обработка на информацията, достъпа до разпределени информационни ресурси (включително профили в социални мрежи) и ползване на разпределени услуги в глобалната мрежа. В този смисъл в следващите части са обсъдени някои проблеми на разпределения достъп в съвременното ИО, предоставянето на облачни услуги и технологичните възможности за организация на защита на ЛД на потребителите.

2. Аспекти на разпределения достъп и облачните услуги

Развитието на съвременното ИО (в частност и у нас) е насочено главно в три направления – към подобряване на услугите в обществената сфера (e-servicing), за комплексна информатизация в стопанската сфера (e-business, e-commerce, e-banking) и за осигуряване на непрекъснато развитие на науката и подобряване на иновациите (e-learning). За решаване на проблемите в тези направления се изисква усилено внедряване на специфичните ИТ, които да позволят:

ü ефективно използване на информационните ресурси на обществото;

ü оптимизиране и автоматизация на информационните процеси;

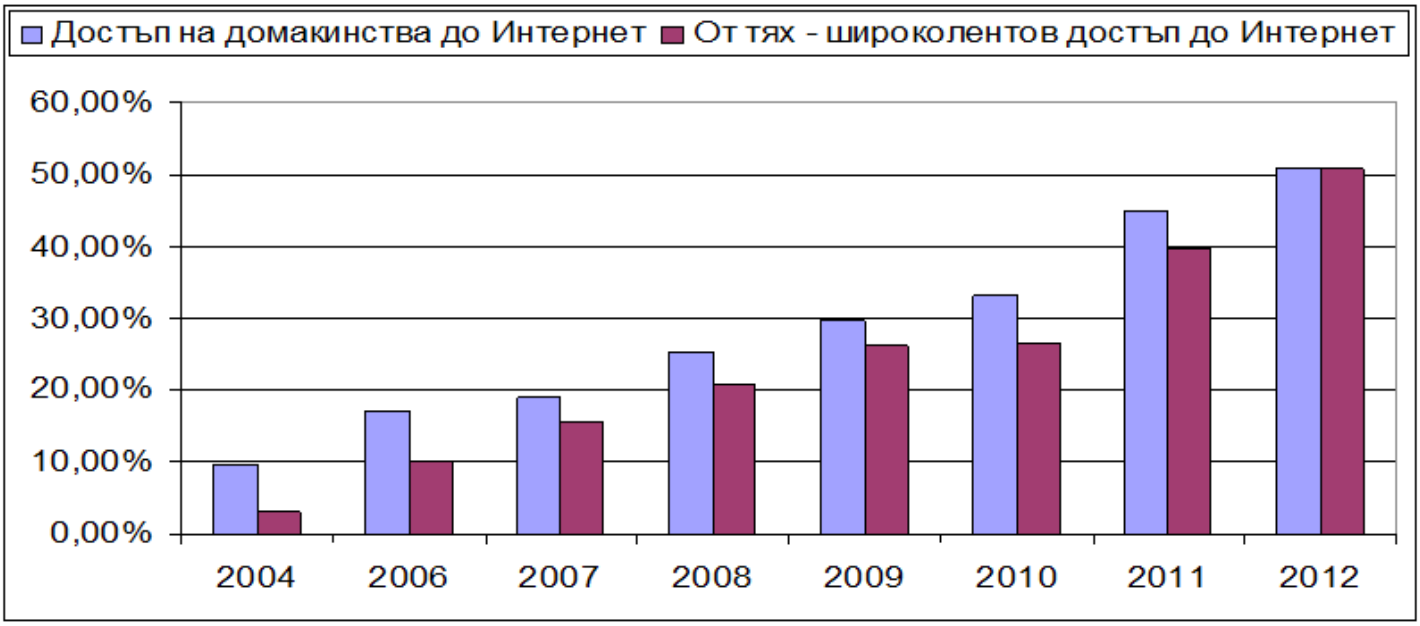
ü прякото им участие като активен компонент в бизнеса или в социалната дейност ;

ü информационно взаимодействие между граждани, бизнес и администрация;

ü информатизацията на обществото и натрупване на знания.

Европейският съюз (ЕС) поддържа последователна политика за ефективното изграждане на глобално ИО като съвкупност от отделните национални ИО чрез инициативи и програми за стимулиране творчеството, научните изследвания и иновациите в областта на ИТ, както и за развитието на информационни услуги в европейски мащаб. Освен с ефикасно и модерно управление в стопанската сфера, това се постига и чрез създаване на информационни среди, системи и платформи за отдалечен достъп до информационните ресурси и тяхното разпределено използване. Това се свързва с компонентите *„е-достъп”* и *„е-общество”* на ИО, отразяващи развитието на технологичните възможности за свързване и взаимодействие в електронна (мрежова) среда и нарастване на използването на компютърните и мрежови технологии от гражданите

и бизнеса. Показателно в тази насока е статистиката за достъп на домакинствата в България до Интернет (фиг. 1), като относителният дял на широколентовия достъп значително нараства през годините. Посочените 50,9% за проникване на Интернет в домакинствата, обаче, поставя България в дъното на класацията за ЕС (според Евростат). Подобна е позицията и относно широколентовия достъп (50,8%) при средно 72% за ЕС. В същото време у нас достъпът до глобалната мрежа се използва главно за онлайн четене на вестници и новини, дейност в социалните мрежи, а само 7% от потребителите се занимават с онлайн банкиране или работа по сайт или блог.



Фиг. 1. Достъп до Интернет в България (по данни на НСИ) http://www.nsi.bg/otrasal.php?otr=17&a1=2405&a2=2406&a3=2407#cont

Глобалната информатизация на обществото води до включването на все по-голям брой потребители с различни интереси, възможности и поведение, както и поддържане и предаване на разнородна мултимедийна информация в разпределените компютърни системи. Повишената активност в Интернет-пространството, обаче, налага решаване и на един друг проблем, свързан с основните Европейски разбирания за неприкосновеност на личния живот и защита на персоналните данни при е-достъп до разпределени информационни ресурси [13, 14, 17], включително и в "облака" [18]. Това изисква при създаване на среди за отдалечен мултипотребителски достъп да се предвидят технически и организационни мерки за защита на предоставените от регистрираните потребители ЛД срещу тяхното неправомерно разпространение и използване за други цели, различни от обявените, както и строги правила за авторизация и автентификация [19, 20].

Разбира се, *облачните изчисления (cloud computing)* имат доста предимства, свързани с инфраструктурата, програмното осигуряване и предлаганите платформи, достъпни при наемане във вид на услуга (*облачни*

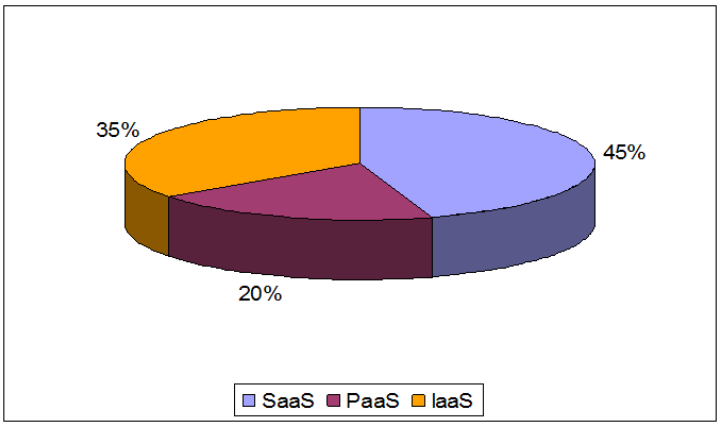
услуги – cloud services) от отдалечени потребители в глобалната мрежа. Това позволява значително намаляване на разходите за създаване и поддържане на собствена инфраструктура и нейното поддържане. „Облакът", от гледна точка на потребителя, е виртуална среда за компютърна обработка и съхраняване на данни, включваща и решаване на проблемите по осигуряване на информационната сигурност. Съществениият проблем е, че доста от правилата по информационната защита не са приложими във вида, в който са възприети (особено за законовите норми, приети на ниво ЕС). Последното налага актуализиране на нормативните разпоредби в ЕС и разработване на адекватни и ефективни процедури, адаптирани към виртуализацията на разпределеното информационно обслужване. В това отношение ЕК не трябва да разчита само на прилагане от потребителите на технологичните средства за информационна защита, известни като PET (Privacy Enhancing Technologies). Основните предизвикателства на облака към защитата на ЛД са дискутирани в [16].

В различни литературни източници, включително и на Националния институт по стандарти и технологии (NIST) [20], се дават дефиниции на облака, на базата на които може да се направи заключението, че всеки компютър, свързан с глобалната мрежа, може да се разглежда като терминал за достъп до отдалечени компютърни мощности, софтуерни технологични средства и хранилища на данни (център за данни) при осигурена информационна защита. Управлението и предоставянето на тези възможности се осъществява от доставчик (Cloud Service Provider – CSP), като са дефинирани три основни модела на облачни услуги (едно разпределение по наемане е дадено на фиг. 2):

ü Инфраструктура като услуга (Infrastructure as a Service – IaaS) – използване на наета компютърна мощност и/или памет (долно ниво на облачната обработка.

ü Платформа като услуга (Platform as a Service – PaaS) – разработване на клиентски приложения чрез виртуални средства в облака, осъществявайки връзката между останалите два типа услуги.

ü Софтуер като услуга (Software as a Service – SaaS) – високото ниво на облачните услуги за предоставяне на софтуер за разработване на собствени потребителски приложения.



Фиг. 2. Относителен дял на наети облачни услуги

Основно твърдение на доставчиците на облачни услуги е, че това е бъдещето на разпределената информационна обработка, основаващо се на намалените разходи по нейната организация и поддръжка. Изследвания от последните години, обаче, показват, че над 70% от фирмите изтъкват

като довод за отказ от облачни услуги нивото на информационна сигурност и защита на персоналните данни [20]. Това се потвърждава и от направения в [21] анализ на риска, налагащ извода, че доставчиците на облачни услуги трябва да убедят своите клиенти относно прилаганата адекватна политика за информационна сигурност. Тази несигурност за предоставените данни се определя от основна характеристика на облака – множественото наемане, както и от редица особености на облачния модел, влизащи в противоречие с основни директиви на ЕС за защита на личните данни [16].

3. Основни принципи на защита на личните данни

Неприкосновеността на личния живот е основно човешко право, получило своето международно признание в редица международни договори и документи, като „Всеобщата декларация на човешките права и основни свободи", „Международен пакт за граждански и политически права", „Европейска конвенция за защита на правата на човека и основните свободи" и др. Защитата на ЛД е неизменна компонента на правото на личен живот и неговата неприкосновеност ("privacy"), като идеята се развива в обществените отношения още от средата на XIX век. Развитието на автоматизираната обработка на информацията, разширяване на мрежовите комуникации и нарастващите възможности за отдалечен достъп до разпределени информационни ресурси налага все по-строги изисквания към прилаганите политики за информационна сигурност. В рамките на ЕС са приети редица документи за регулиране на обработката на ЛД, поставящи конкретни изисквания за тяхната защита. В съвременното ИО, обаче, нарастващото споделяне на информационни ресурси и възможности за отдалечен достъп до тях, както и навлизането на социалните мрежи и „облачните" услуги, създават бариери при прилагане на основни диирективи по защита на ЛД.

В световен мащаб се дефинират няколко основни модели за защита на ЛД:

Ø *Модел на централизирано законодателство*. Предвижда съществуване на специален закон, уреждащ изцяло принципите на защита на ЛД в съответната държава. Възприет е в страните от ЕС, включително и в България.

Ø *Модел на съвместна регулация*. Моделът е модификация на горния, като правилата за защита на ЛД се развиват и налагат от бизнеса, а специален орган следи за тяхното изпълнение. Предимство на модела е по-голяма гъвкавост, но е възможно занижаване на изискванията относно нивото на защита. Моделът е възприет в Канада и в Австралия.

Ø *Модел на секторното законодателство*. Насочване на законодателната дейност за защита на ЛД към определен икономически сектор или компании в дадена област и се прилага при липса на национален закон. Примери са закон за електронната търговия (приети в Мексико и Южна Корея), закони за свобода на инфор-

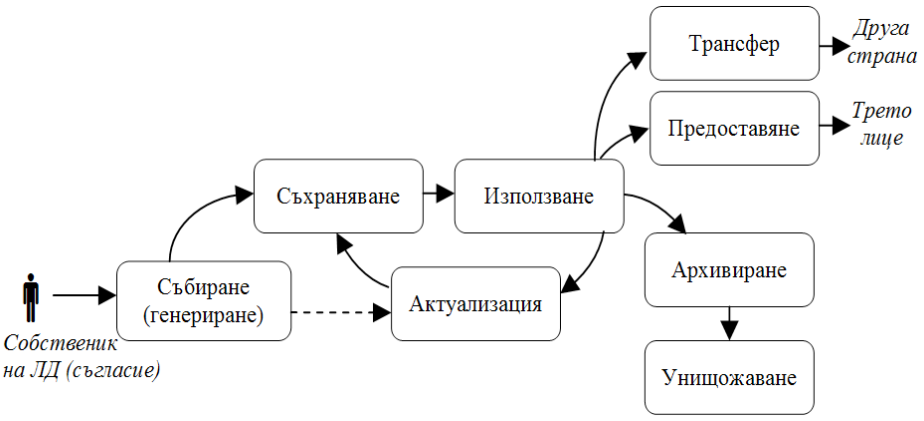
мацията (приети в над 50 страни). Основен недостатък на секторните закони е, че с развитие на ИТ конкретни разпоредби могат да станат неприложими, както и проблемът с осъществяването на контрол.

Ø Модел на саморегулирането. Компаниите и фирмите сами определят правилата и ограниченията при обработка на ЛД (например, чрез етични или браншови кодекси). Основният недостатък е свързан с осъществяване на надзора, който обикновено е в ръцете на самите компании. Подходът е ефективен при поддържане на общи (разпределени) бази данни и отдалечен достъп до информационните ресурси на отделни компании.

Ø Модел на индивидуална защита. Прилага се от индивидуални потребители на глобалната мрежа, които разчитат на собствени технологични средства (кодиране, шифроване, криптиране, прокси-сървъри, електронни пари, смарт карти и пр.), чрез които се осигурява необходимата конфиденциалност и ограничаване на достъпа до данните. Индивидуалната защита на личното информационно пространство възниква преди всичко поради опасенията на потребителите на Интернет-комуникациите, че средата не предоставя достатъчно ефективни средства за сигурност.

Моделите показват различните схващания за защита на ЛД в различните страни, определяно и от приетата дефиниция за ЛД. Например, в Европа е възприето определение за ЛД като *“всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци”* (чл.2 от Закон за защита на ЛД на Р. България). В САЩ популярна дефиниция се свързва с *„правата и задълженията на лицата и организациите относно събиране, използване, съхраняване и разкриване на персонална информация”*. В тази връзка моделът на индивидуална защита е показателен за недоверието на доста потребители към прилаганата политика за информационна сигурност при разпределеното информационно обслужване. Това налага актуализиране на законовата база за по-прецизно следене на действията в глобалната мрежа и повишаване на отговорностите на предоставящите услуги в нея.

На фиг. 3 е представен модел на жизнен цикъл на традиционна обработка на ЛД, описващ последователните фази от началното събиране на ЛД (основно със съгласие на физическото лице) до приключване на тяхната обработка чрез унищожаването им.



Фиг. 3. Жизнен цикъл на обработката на ЛД

Реализацията на жизнения цикъл се осъществява от администратор на ЛД (АЛД), на когото са вменени и конкретни задължения по осигуряване на организационна и технологична защита на поддържаните регистри с ЛД. Особености на отделните фази са следните:

ü *събирането* на ЛД трябва да става със съгласие на физическото лице-собственик, освен за специфични случай, предвидени в закон;

ü *съхраняването* се извършва в регистри за ЛД (автоматизирани или не) при предварително дефинирани категории от данни, съобразени с целта на обработката;

ü *използването* трябва да става правомерно съгласно определената цел и от упълномощени (легитимни) служители, спазвайки инструкция за защита на ЛД, като в зависимост от характера и типа на категориите данни трябва да са предвидени адекватни технически и организационни мерки за защита;

ü *актуализацията* се налага от принципите на коректност на ЛД и изискването за поддържане на прецизна, пълна и актуална информация;

ü *предоставянето* на ЛД може да става само при строго регламентирани правила, спазвайки принципа, че собственик на данните е физическото лице;

ü *трансфер* на ЛД е прехвърляне през граница, като основно изискване е приемащата страна да осигурява защита не по-слаба от тази в изпращащата страна;

ü *архивиране* на конкретни ЛД за определен срок се налага главно при законови изисквания;

ü *унищожаване* на ЛД се извършва след изпълнение на поставената цел, освен ако не предвидено предаване на друг администратор на ЛД (например, за архивиране).

В смисъла на представеното погоре и насочено към организацията на разпределеното информационно обслужване, субектът, предлагащ и администриращ съответната виртуална (разпределена) среда, ще трябва да се разглежда като АЛД, защото обработва лични профили на регистрираните потребители и носи законови отговорности. Трябва да се има предвид, че процесите по предоставяне и обработване на лични данни се осъществяват в web-пространството, което поставя допълнителни изисквания относно средствата и мерките за информационна защита. Не на последно място трябва да се отбележи, че възникващите в Интернет-пространството проблеми тангират до тези на облачните услуги, разгледани в [16] и отнасящи се главно за фазите „*съхраняване*" (известно ли е къде точно се съхраняват ЛД?), „*използване*" (при множествено наемане в облака има възможност за неправомерен достъп), „*трансфер*" (периодичното прехвърляне на данни в хранилища в различни страни е типично за облака) „*унищожаване*" (как се гарантира унищожаването при многократното презаписване в различни точки на облака?). В този смисъл дискусионен е и въпросът относно предприеманите организационни и технологични мерки за защита на данните в облака или разпределената виртуална среда, още повече че при

тази обработка смисълът на „Администратор на ЛД" се размива. Последното позволява на собственика или доставчика на облачни услуги да не се ангажира пряко с изпълнението на законови разпоредби по защита на ЛД, като например:

ü да информира лицата, от които се събират ЛД, за основанието, целта, формата на събиране, правото на достъп, възможното предоставяне на трети лица и пр., както и да обработва ЛД само за обявената цел(и);

ü да предприеме необходимите технически и организационни мерки за осигуряване на адекватна защита на ЛД в поддържаните от него регистри;

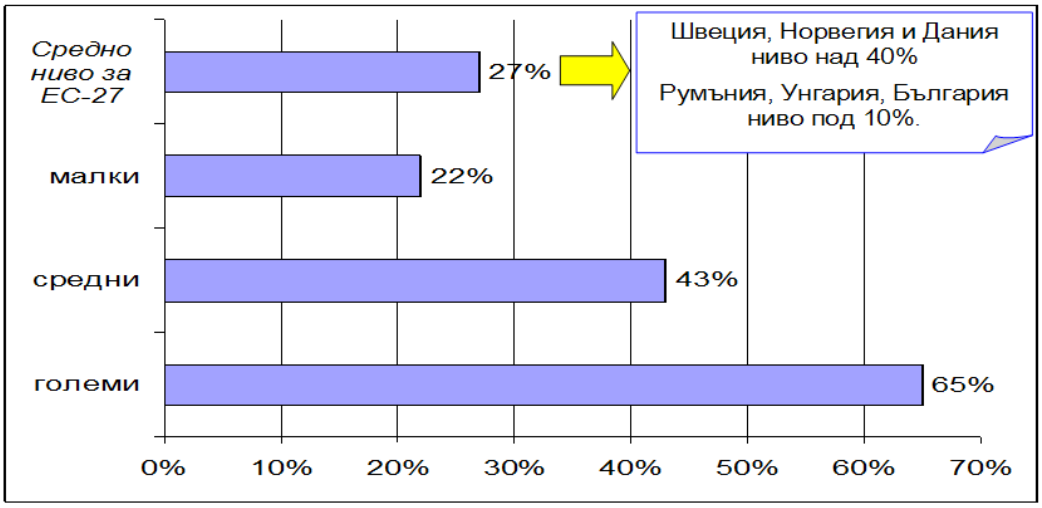
ü да осигури достатъчно гаранции и да носи отговорност за коректната обработка на ЛД, както от своите служители, така и от обработващ ЛД, на когото е възложил тези функции.

ü да осигури достъп на лицата, собственици на ЛД, до водените от него регистри и да не пречи на контрола върху процеса на обработка на ЛД;

ü да съхранява ЛД само за времето, което е необходимо за изпълнение на поставената цел.

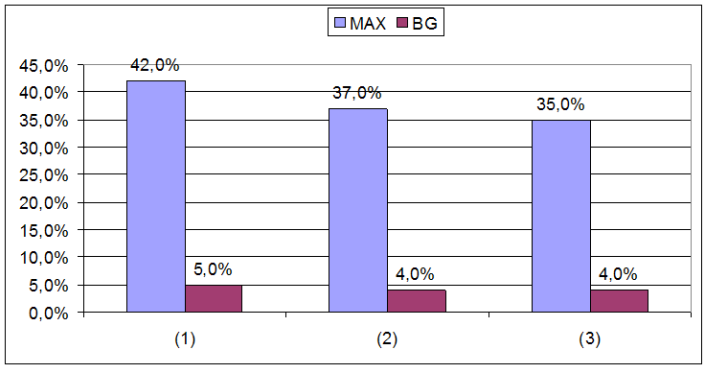
4. Организация на защитата на лични данни при информационното обслужване

Прието е под *информационна сигурност (Information Security)* да се разбира състоянието на защитеност на информационните ресурси в съсредоточени и разпределени компютърни среди, включително и тяхното пренасяне по комуникационни линии, от незаконен достъп, разрушаване и други въздействия, нарушаващи тяхната функционалност и цялост. Това налага прилагане на строга политика за информационна сигурност, базирана на ясно дефинирана концепция (резултати от изследване на Eurostat са дадени на фиг. 4) [22].

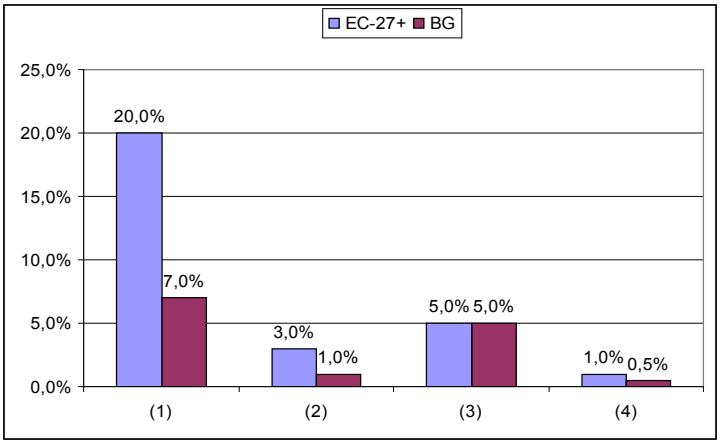


Фиг. 4. Оценка за нивото на ясно дефинирана концепция за информационна сигурност в предприятията (малки, средни, големи) на ЕС-27 при средно ниво от 27%

Глобализацията и виртуализацията на информационното общуване в съвременния интернет-свят изисква прецизно анализиране на основните типове нарушения и причините за компрометиране на информационна сигурност. Едно обобщение на резултати от изследването на Eurostat за ЕС-27+ и за България са дадени на фиг. 5 и фиг.6.



Фиг. 5. Основни типове нарушения на информационната сигурност
(1) Разрушаване на данни поради атака или друг неочакван инцидент; (2) Разкриване на конфиденциални данни чрез проникване или прихващане; (3) Невъзможност на ИТ-инфраструктурата да противодейства на външни атаки;
***MAX** (максимална стойност за страна от ЕС-27+); **BG** (оценка за България)*



Фиг. 6. Базови причини (типове инциденти) при нарушаване на информационната сигурност
(1) Апаратни и програмни неизправности; (2) Външни атаки; (3) Вируси и несанкциониран достъп; (4) Проникване в БД и прихващане на съобщения;
***ЕС-27+** (средна стойност за страните от ЕС+); **BG** (оценка за България)*

Подобни изследвания, както и представени в различни източници анализи на риска при информационно обслужване във виртуални и облачни среди налагат решаване на проблеми като:

· осигуряване на надеждна информационна сигурност на ресурсите;

· защита на ЛД на потребители и участници в информационните процеси;

· дефиниране на права за достъп до определени информационни ресурси в зависимост от правомощията.

Всеки администратор на ЛД трябва да изгради подходяща Система за сигурност на ЛД (ССЛД) като следствие от политиката за сигурност и да създаде технологични структури за защита на ЛД [16].

Очевидна е пряката връзка на технологиите и мерките по защита на ЛД с процедурите за осигуряване на надеждна информационна сигурност. Същественият проблем е, че персоналната информация (включително и тази за персонална идентификация) в web-пространството нараства значително. Това се отнася както за разпределени приложения и среди (информационни системи с разпределени бази от данни, разпределени среди за обучение, виртуални лаборатории и пр.), така също и за използваните ресурси и услуги в облака за изчисления или за съхраняване на данни (включително масиви от лични данни) отдалечени хранилища и центрове за данни.

Управлението на достъпа до информационните ресурси е друга страна на дискутирания проблем, която се

свързва с две основни процедури на информационната сигурност:

ü авторизация (authorization) – процес на упълномощаване (предоставяне на определени права) за достъп до конкретни информационни ресурси или компоненти на дадена система и извършване на дадена дейност (модификация, въвеждане, изтриване, допълване и пр.);

ü автентификация (authentication) – удостоверяване самоличността на даден потребител за проверка на неговата легитимност.

Връзката между ССЛД и изграждането на среда за информационно обслужване е представена на фиг.7, като за защита на персоналните данни (включително и тези за автентификация) трябва да бъдат включени подходящи средства от всяко едно от представените йерархични нива за информационна сигурност.

Фиг. 7. Изграждане на ССЛД като част от среда за информационно обслужване

¨ Вградени средства за информационна сигурност – съвкупност от апаратни, програмни и криптографски средства, които осигуряват най-висока степен на защита и се явяват последна преграда пред данните срещу опитите на външни потребители за неправомерен достъп до тях. Апаратните средства се използват за разпознаване на легитимния потребител, за защита на процесора и външната памет, за шифроване на предаваните съобщения и т.н. Програмните средства се прилагат при разпознаване на правилно въведена от потребителя парола или ПИН, за ограничаване на достъпа до

части от диска, за проверка на наличие на вирусни програми и активиране на антивирусни програми и др. Криптографските средства се реализират апаратно или програмно, като осигуряват шифроване на данните със симетрични или асиметрични алгоритми. Използват се системи с различно предназначение – за засекретяване на необходимите данни и съобщения, за автентификация (проверка на достоверност), електронен подпис и пр.

¨ Физически средства за защита – технически средства за предотвратяване на достъпа на външни лица до помещения с работни станции и сървъри на бази данни, заключване на информационни носители и архивни данни, въвеждане на отличителни знаци, охрана и осигуряване на защитна сигнализация, сегментиране на локалната мрежа и изолиране на сървъра от Интернет, осигуряване на резервно захранване и др.

¨ Организационни мерки за административен контрол – допълват и разширяват функциите на физическите средства за защита, като особено внимание се обръща на правилното използване на предвидените апаратни и програмни средства. Включват: периодични проверки на потребителския достъп до информационните ресурси и спазване на изискванията относно периодична смяна на паролите; съхраняване на копия на данните; дефиниране на нивото на секретност на данните и определяне на права на достъп на служителите; определяне на пълномощията на администратора на БД за контрол на достъпа до съответните данни; допълнителна квалификация на персонала и др.

¨ Законови и нормативни средства за защита – най-външно ниво на ССЛД, основаващо се на въведени специални закони, гарантиращи сигурността на компютърните системи и предвиждащи санкции за нарушителите.

5. Заключение

Разработени са много приложения, стандарти и протоколи, които използват криптографски алгоритми за осигуряване на защита на данните в различни аспекти. Към тях могат да се добавят различни биометрични системи за идентификация и ограничаване на достъпа. Тези групи технологични средства могат да се прилагат на долните две нива от ССЛД. В същото време изграждането на система за защита на регистрите с ЛД решава част от проблемите при информационното обслужване в глобалната мрежа, но не може да преодолее известни заплахи, пораждани от взаимодействието с облака и използването на облачни услуги. Какво е решението? Преди всичко трябва да се актуализира законовата рамка на ниво ЕС и в национален мащаб, за да се регламентират правата и задълженията на собственици, доставчици и потребители на облачни услуги. Това може да стане чрез ясно дефиниране на субекта, изпълняващ ролята на администратор на ЛД в облака. На второ място трябва да се повиши отговорността на предлагащите облачни услуги относно внедряването на съвременни средства за защита на данните при всякакъв вид дейности с предоставените от потребителите дан-

ни и идентификационни профили. И на трето място да се прилагат стриктно изискванията и технологичните средства за защитеност (засекретяване) на изпращани в облака данни още при източника.

Литература

[1] Subramanian, A., M. Kessler (**2013**). The Hyperglobalization of trade and its future. *Global Citizen Foundation*, June (76 p.) http://www.gcf.ch/wp-content/uploads/2013/06/GCF_Subramanian-working-paper-3_-6.17.13.pdf

[2] EC (**2009**). *Main achievements of the i2010 strategy 2005-2009*. Europe's Digital Competitiveness Report, ISBN 978-92-79-12823-3.

[3] EC (**2010**). *ICT and e-business for an innovative and sustainable economy*. 7th Synthesis report of the sectoral e-business watch, ISBN 978-92-79-14682-4 (*available at*: http://www.ebusiness-watch.org/key_reports/documents/EBR09-10.pdf)

[4] EC (**2010**). *Europe 2020: a new economic strategy* (*available at*: http://ec.europa.eu/eu2020/)

[5] Bart Jacob, B., M. Brown, K. Fukui, N. Trivedi (**2005**). *Introduction to Grid computing*, IBM Redbooks, December, 268 p. (http://www.redbooks.ibm.com/redbooks/pdfs/sg246778.pdf)

[6] Khalidi, Y. (**2011**). Building a cloud computing platform for new possibilities. *Computer*, March, pp.29-34.

[7] Narasimhan, B., R. Nichlos (**2011**). State of cloud applications and platforms: the cloud adopters' view. *Computer*, March, pp.24-28.

[8] Simoens, P., F. De Turck, B. Dhoedt, P. Demeester (**2011**). Remote display solution for mobile cloud computing. *Computer*, August, pp.46-53.

[9] Banerjee, P., C. Bash, R. Frierich et al. (**2011**). Everything as a service: powering the new information economy. *Computer*, March, pp.36-43.

[10] Lampe, C., N. Ellison (**2012**). Understanding Facebook: Social computing isn't 'just' social. *Computer*, September, pp.98-100.

[11] Lam, S. K., J. Riedl (**2012**). Are our online „friend" really friends? *Computer*, January, pp.91-93.

[12] Garber, L. (**2012**). The challenges of securing the virtualized environment, *Computer*, January, pp.17-23.

[13] Bennett, C.J. (**2011**). Privacy advocacy from the inside and the outside: implications for the politics of personal data protection in networked societies. *Journal of Comparative Policy Analysis: Research and Practice*, vol. 13, No. 2, pp.125-141.

[14] Friedewald, M., D. Wright, S. Gutwirth, E. Mordini (**2010**). Privacy, data protection and emerging sciences and technologies: towards a common framework. *Innovation: The European Journal of Social Science Research*. vol. 23, No. 1, pp.61-67.

[15] Song, D., E. Shi, I. Fisher, V. Shankar (**2012**). Cloud data protection for the masses. *Computer*, January, pp.39-45.

[16] Романки, Р. **(2012).** Предизвикателствата на „облака" към защитата на личните данни. *Българска наука*, ISSN 2074-9007 (Online), № 50 (vol. 4), pp.192-203 (www.nauka.bg).

[17] Kagal, L., H. Abelson (**2010**). Access control is an inadequate framework for privacy protection. 6p. (*available at*: http://dig.csail.mit.edu/2010/Papers/w3cprivacy/paper.pdf).

[18] Balboni, P. (**2010**). Data protection and data security issues related to cloud computing in the EU. *ISSE 2010 Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe Conference*; Tilburg Law School Research Paper No. 022/2010 (available at: http://ssrn.com/abstract=1661437).

[19] Olden, E. (**2011**). Architecting a cloud-scale identity fabric. *Computer*, March, pp.52-59.

[20] Chen, D., H. Zhao (**2012**). Data security and privacy protection issues in cloud computing. *International Conference on Computer Science and Electronics Engineering (ICCSEE)*. 23-25 March 2012, vol. 1, pp.647-651.

[21] Rana, S., Pr. Kumar Joshi (**2012**). Risk analysis in web applications by using cloud computing. *International Journal of Multidisciplinary Research*, vol. 2, No.1, pp. 386-394.

[22] European Commission – Eurostat (**2011**). ICT security in enterprises. International Journal on IT and Security, 2 (vol. 3), pp.45-54 (ijits-bg.com).