КРАТКИЕ СООБЩЕНИЯ

А.М. ФАЛЬ

УДК 681.3

СТАНДАРТИЗАЦИЯ В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. Рассмотрены европейское и национальное законодательства, касающиеся защиты персональных данных, а также предложения по разработке стандартов в сфере защиты персональных данных. Приведен список опубликованных стандартов и проектов, включенных в программу работ по стандартизации.

Ключевые слова: персональные данные, принципы прайвеси, лучшие практики, менеджмент идентификационных данных, гармонизация стандартов.

Стандарты играют важную роль в повседневной жизни. Основное их преимущество — использование общих для заинтересованных сторон методов, механизмов, процедур и т.д. Обычно стандарты направлены на конкретные области знаний и секторы экономики. Не являются исключением и вопросы, касающиеся защиты персональных данных.

В Украине существует законодательная база для контролирования надлежащего использования персональных данных. В настоящей статье сделана попытка анализа существующих международных стандартов в области защиты персональных данных (в статье употребляется термин прайвеси) и рассмотрена возможность их гармонизации в Украине. Первым среди стандартов, который гармонизируется в нашей стране, является выпущенный в декабре 2011 года стандарт ISO/IEC IS 29100 «A privacy framework».

Термин «privacy» не имеет аналогов в русском языке. В одних случаях он может обозначать частную жизнь, в других — право на частную жизнь, в третьих — право на защиту неприкосновенности частной жизни.

Прайвеси подразумевает право контролировать собственную персональную информацию и возможность определять ее способ получения и использования.

Прайвеси — намного более широкий концепт, нежели конфиденциальность, так как он имеет в виду ограничения на широкий диапазон действий, касающихся персональной информации: это сбор, хранение, использование и разглашение.

Первые принципы относительно прайвеси определены в документах «Bill of rights of Virginia» 1776 г. и «Declaration of Human and Citizen Rights», принятой во время Французской революции 1789 г.

После Второй мировой войны Генеральная Ассамблея ООН 10.12.1948 года приняла «The universal declaration of human rights», в первой статье которой утверждается, что «Каждый человек рождается, чтобы быть свободным и равным в своих правах».

Следующими актами в Европе были «European Convention of human rights» от 4 ноября 1950 года и для Европейского Союза «Charter of Fundamental Rights» от 18.12.2000 года.

Извлечение выводов относительно прайвеси из центральных прав на достоинство и свободы понятно, потому что неправильное использование информации, которая может идентифицировать личность, т.е. Privacy identifiable information (PII), может нанести вред субъекту данных и быть причиной нанесенного ему урона. То, что вред и урон влияют на чувство собственного достоинства и свободы, также понятно. Следовательно, право на прайвеси — логическая производная от прав на достоинство и свободы.

Развитие информационных технологий за прошедшие 50 лет продемонстрировало, что достоинство и свобода личности могут быть нарушены неправильным использованием PII или игнорированием ее. Эти нарушения стали причиной отделения права на прайвеси от прав на достоинство и свободу, и они требуют адекватных юридических средств, которые не могут быть реализованы в рамках обычных санкций.

Реакцией на нарушение прайвеси стало введение принципов прайвеси, которые впервые были сформулированы в отчете Комитета по системам автоматизированной обработки персональных данных Министерства здравоохранения США. Этот отчет послужил основой для формулирования документа «Privacy Act» 1974 г., которым регулируется обработка персональных данных в правительственных базах данных США.

В последующие годы в ряде стран в актах, касающихся прайвеси, были сформулированы схожие принципы. Эти юридические акты привели позже к международным рекомендациям, принятым в OECD, Совете Европы, Международной организации труда, ООН, Европейском Союзе и APEC.

Все эти правовые акты и рекомендации определяют правила обрабатывания персональных данных и ответственность за нарушение правил или неправильное использование PII, что наносит вред и влечет убытки. К сожалению, эти правовые акты и рекомендации лишь частично отражены в процессах стандартизации в соответствующих стандартах по обеспечению безопасности информационных технологий (ИТ). За последние десять лет ISO и IEC совместно приняли стандарты, касающиеся безопасности ИТ. Эти стандарты помогают защищать персональные данные.

Многие стандарты накладывают требования относительно обеспечения безопасности ИТ, но до недавнего времени ни в одном из них не было сформулировано общего правила, которое с самого начала составляло бы принцип предотвращения использования персональных данных. Этот принцип важен потому, что недоступная PII не может неправильно использоваться и неправильно интерпретироваться.

ЕВРОПЕЙСКИЙ ОПЫТ

В феврале 2002 года выпущен окончательный отчет «Initiative on Privacy Standardization in Europe» (IPSE). Цель IPSE — анализ текущего состояния усилий, направленных на защиту прайвеси и определения, способствует ли деятельность по стандартизации процессам имплементации Директивы 95/46/ЕС Европейского парламента и Совета «О защите физических лиц при обработке персональных данных и о свободном перемещении таких данных» от 24 октября 1995 года [1].

В отчете делается вывод, что существует достаточная база для конкретных инициатив, касающихся стандартизации. В этом документе сформулированы следующие рекомендации.

Рекомендация 1. Voluntary Best Practices (Добровольные лучшие практики). Определить общее европейское множество добровольных лучших практик для защиты данных и сделать их доступными (бесплатно или по низкой цене), чтобы помочь менеджерам удостовериться в том, что они действуют в соответствии с Директивой и, где есть возможность, с различными национальными законами и дополнительными требованиями. Эта рекомендация должна быть применима во всех секторах, но может быть дополнена рекомендациями, специфичными для каждого сектора.

Рекомендация 2. Management Standards (Стандарты по менеджменту). Позже не была принята.

Рекомендация 3. Generic Contract Clauses and Terms (Общие разделы и условия контрактов). Разработать множество общих разделов контрактов. Существует требование, чтобы все владельцы данных, которые пользуются сторонними распорядителями, применяли соответствующие контракты. Разработка контрактов стандартной формы общепринята в сфере предоставления профессиональных и других услуг. Контракты должны работать в национальном законодательном поле, поэтому стандартные европейские формы должны позволять национальные вариации в таких делах, как правовые формальности, но они должны иметь возможность достижения высокого уровня общности. Контракты считают полезными инструментами для обеспечения соответствующей защиты данных.

Рекомендация 4. Inventory of Data Protection Auditing Practice (Реестр практик аудита защиты данных). Подготовить реестр практик аудита защиты данных для того, чтобы вести записи лучших практик в этой сфере и чтобы оценить пределы возможности получения пользы от стандартизации для практики проведения аудита защиты данных. Исследование должно рассмотреть существующие практики проведения аудита и получить информацию от всех заинтересованных сторон, которые предлагают услуги по аудиту защиты данных, а именно представителей аудиторских компаний, специалистов по безопасности и организаций, которые заказывают аудит.

Рекомендация 5. Conduct a survey of web seals as a basis for considering further standardization work in this area (Осуществить обзор веб-печатей как основу для рассмотрения дальнейшей работы по стандартизации в этой сфере). Обзор должен выяснить, как работают различные программы веб-печатей и как печати осуществляют вклад в развитие доверия потребителей. Обзор будет использован как основа для решения, могут ли быть разработаны общие стандарты для печатей с тем, чтобы, возможно, гарантировать поставки минимальных стандартов для программ печатей.

Рекомендация 6. Analysis of the impact of technologies on data protection, coordination and the initiation of longer-term processes (Анализ влияния технологий на защиту данных, координация и инициирование долгосрочных процессов). Разработать надлежащий подход к оценке влияния развития технологий на реализацию Директивы с тем, чтобы обеспечить диалог между разработчиками стандартов и техническим сообществом, а также между надзорными инстанциями и потребителями.

Эти рекомендации реализованы и изложены в следующих документах:

CWA 15262:2005 Inventory of Data Protection Auditing Practices (Реестр практик проведения аудита защиты данных);

CWA 15263:2005 Analysis of Privacy Protection Technologies, Privacy-Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management Systems (IMS), the Drivers thereof and need for standardization (Анализ технологий защиты прайвеси,

Технологии, усиливающие прайвеси (PET), Системы менеджмента прайвеси (PMS) и Системы менеджмента идентификационных данных (IMS), Стимулы и необходимость стандартизации);

CWA 15499-1:2006 Personal Data Protection Audit Framework — Part 1: Baseline Framework (Схема проведения аудита защиты персональных данных — Часть 1: Базовая схема);

CWA 16111:2010 Voluntary Technology Dialogue Framework (VTDF) (Схема добровольного диалога по технологиям);

CWA 16112:2010 Self-assessment framework for managers (Схема самооценки для менеджеров);

CWA 16113:2010 Personal Data Protection Good Practices (Лучшие практики защиты персональных данных).

МЕЖДУНАРОДНЫЙ ОПЫТ

В октябре 2003 года на пленарном заседании совместного технического комитета ISO / IEC JTC1 «Information technology» (Информационные технологии) была создана группа по изучению технологий прайвеси (SGPT), которая в течение одного года (до октября 2004 года) должна была определить потребности в стандартизации прайвеси.

В октябре 2004 года на пленарном заседании JTC1 было решено:

- распустить SGPT;
- поручить подкомитету ISO / IEC JTC1 / SC27 дальнейшую деятельность в сфере Privacy Technologies (Технологий прайвеси).

Деятельность SC27 выразилась в следующем.

- **Октябрь 2004 года**

установлен период изучения по управлению идентификационными данными;

- **Май 2005 года**

установлен период изучения по прайвеси;

предложение относительно нового проекта: «A framework for identity management» (Основные положения менеджмента идентификационных данных).

- **Май 2006 года**

создана новая рабочая группа WG5 по вопросам технологий прайвеси и менеджмента идентификационных данных;

- предложена разработка двух стандартов:

a privacy framework (ISO / IEC 29100) (Основные положения обеспечения прайвеси);

a privacy reference architecture (ISO / IEC 29101) (Эталонная архитектура обеспечения прайвеси).

На данный момент в программе работы SC27 указаны следующие проекты:

- A Framework for Identity Management (ISO / IEC 24760) (Основные положения менеджмента идентификационных данных);
- Privacy Framework (ISO / IEC 29100) (Основные положения обеспечения прайвеси);
- Privacy Architecture Framework (ISO / IEC 29101) (Эталонная архитектура обеспечения прайвеси);
- Entity Authentication Assurance Framework (ISO / IEC 29115/ITU-TX.eaa) (Основные положения обеспечения аутентификации субъектов);
- A Framework for Access Management (ISO / IEC 29146) (Основные положения управления доступом);
- Biometric information protection (ISO / IEC 24745) (Защита биометрической информации);
- Requirements on partially anonymous, partially unlinkable authentication (ISO / IEC 29191) (Требования к частично анонимной и частично не связываемой аутентификации);
- Authentication Context for Biometrics (ISO / IEC 24761) (Контекст аутентификации для биометрики);
- Privacy Capability Assessment Model (ISO / IEC 29190) (Модель оценивания возможности обеспечения прайвеси).

Начато голосование по таким новым проектам (NWI):

- Privacy impact assessment (Оценивание воздействия на прайвеси);
- Identity proofing (Проверка идентификационных данных);
- Blind digital signatures (Слепые цифровые подписи);
- Code of practice for data protection controls for public cloud computing services (Практические правила для мероприятий по защите данных в услугах облачных вычислений);
- Cloud computing security and privacy (Безопасность и прайвеси облачных вычислений).

СПИСОК ЛИТЕРАТУРЫ

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Offic. J. L. — 1995. — **281**. — P. 0031–0050.

Поступила 29.01.2013