

Хранение и защита персональных данных администраторов доменов

Александр Панов

Сентябрь 2010

Storage and protection of domains administrators personal data

Alexander Panov

September 2010

Персональные данные

персональными данными является любая информация, с помощью которой можно однозначно идентифицировать физическое лицо

**ЗАЧЕМ И ОТ КОГО
ИХ ЗАЩИЩАТЬ**



Personal data

personal data is information, which allows you to indentify a physical person unambiguously

**WHY AND FROM
WHOM MUST THEY BE
PROTECTED**

Персональные данные в жизни

Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар:

- информация в руках мошенника превращается в орудие преступления
- в руках уволенного сотрудника – средство мщения
- в руках инсайдера – товар для продажи конкуренту...

Именно поэтому персональные данные нуждаются в самой серьезной защите.



Personal data in real life

Personal information has always had great value, but today it has become the most expensive commodity:

- in the hands of a fraudster information becomes a crime instrument
- in the hands of a fired employee it becomes a tool of revenge
- in the hands of an insider it becomes a commodity that can be sold to a rival...

Therefore personal data should be seriously protected.

Зарубежный опыт: США

International experience: the United States of America

- ❖ В США до сих пор отсутствует общее (федеральное) законодательство о персональных данных.
- ❖ Основными действующими документами являются Privacy Act of 1974 и Privacy Protection Act of 1980, регулирующие деятельность органов государственной власти при обработке персональных данных граждан.
- ❖ В качестве рекомендаций по обеспечению защиты данных широко применяются документы «Дирекции управления и бюджета» (OMB — Office of Management and Budget) и «Национального института стандартов и технологий» (NIST - National Institute of Standards and Technology). Они регулируют деятельность по защите персональных данных в государственных структурах, для коммерческих же организаций они носят рекомендательный характер.
- ❖ Очередным шагом к централизованному регулированию отношений, связанных с обработкой персональных данных граждан, является документ NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

- ❖ USA still do not have a common (federal) legislation on personal data.
- ❖ The main operational documents regulating the governmental bodies activities during citizens' personal data processing are «Privacy Act» of 1974 and «Privacy Protection Act» of 1980.
- ❖ Documents of the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) are widely used as recommendations for ensuring data protection. They regulate personal data protection in governmental organizations and serve as recommendations for private organizations.
- ❖ The NIST's «Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)» is the next step towards centralized regulation of relations concerning citizens' personal data processing.

Зарубежный опыт: Евросоюз

- ❖ В ряде конституций европейских стран с начала 30-х гг. XX в. были закреплены нормы о защите информации личного и семейного характера (Конституция Ирландии (1937 г.), Исландии (1944 г.), Италии (1947 г.), Хартия испанцев (1945 г.) и др.)
- ❖ Первый в мире специальный закон о защите персональных данных был принят германской землёй Гессен в 1970 г. В 1977 г. принимается Федеральный закон ФРГ «О защите персональных данных»
- ❖ В 70 - 80-х гг. XX в. появились законодательные акты, содержащие специальные нормы о защите персональных данных работника (Швеция (1973 г.), Франция (1978 г.) и др.)
- ❖ С 28 января 1981 г. была открыта для подписания Конвенция Совета Европы "О защите физических лиц при автоматизированной обработке персональных данных", вступившая в силу с 1 октября 1985 г.

International experience: the European Union

- ❖ Constitutions of a number of European countries enshrined the norms on protection of personal and family information as early as the beginning of the 1930s (the Constitution of Ireland (1937), Iceland (1944), Italy (1947), the Charter of the Spaniards (1945), etc.)
- ❖ The first in the world special law on personal data protection was adopted in German land Hesse in 1970. In 1977 the federal law «On personal data protection» was passed in the Federal Republic of Germany.
- ❖ In the 1970s — 1980s legislation containing special norms on protection of employees' personal data was adopted (Sweden (1973), France (1978), etc.)
- ❖ On January 28, 1981 the Council of Europe Convention «On protection of physical persons during automated processing of personal data» was opened for signing, becoming operational on October 1, 1985.

Зарубежный опыт: Великобритания

- ❖ В Великобритании в 1998 году был принят «Закон о защите персональных данных» – «Data Protection Act 1998». 2 июля 2009 года в Британии вышла первая версия стандарта BS10012:2009 "Защита данных – Спецификация системы управления персональными данными". Этот документ стал первым в мире стандартом на систему управления персональными данными.
- ❖ Выпуск стандарта BS10012, безусловно, является важным шагом на пути к международной стандартизации обработки персональных данных, но первая версия этого документа еще далека от совершенства и уж тем более не является панацеей.
- ❖ В отличие от документов российских регуляторов, английские стандарты дают более общие рекомендации по обеспечению безопасности ПДн и не предписывают, как конкретно должны защищаться персональные данные.

International experience: the United Kingdom

- ❖ In 1998 «Data Protection Act» was passed in the UK. On July 2, 2009 version 1 of standard BS10012:2009 «Data protection — Specification of personal data management system» was released. This document became the first in the world standard for personal data management system.
- ❖ The release of BS10012 standard is certainly an important step on the way towards international standartization of personal data processing, but the first version of that document is still far from being perfect and definitely is not a cure-all.
- ❖ Unlike documents of Russian regulators, the UK standards give more generic recommendations on ensuring personal data security and do not specify how exactly personal data must be protected.

Закон «О персональных данных» в России

- Федеральный Закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных"
- Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»
- Постановление Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»



The law «On personal data» in Russia

- The federal Law from July, 27th, 2006 N 152-FZ "About the personal data"
- The federal Law from July, 27th, 2006 № 149-FZ «About information, information technology and about information protection»
- The decree of the President of the Russian Federation from 6 march 1997 year № 188 «About the statement of the list of data of confidential character»
- The governmental order of the Russian Federation from November, 17th, 2007 № 781 «About the position statement about safety of the personal data at their processing in information systems of the personal data»
- The order of Federal Agency of technical and export control, FSB of the Russian Federation and the Ministry of information technology and communication of the Russian Federation from February, 13th, 2008 № 55/86/20 «About the statement of the Order of carrying out of classification of information systems of the personal data»

Сущность и разновидность

Категория 1

- Персональные данные, касающиеся расовой, национальной принадлежности, политических, религиозных и философских убеждений, состояния здоровья, интимной жизни

Категория 2

- Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1

Категория 3

- Персональные данные, позволяющие идентифицировать субъекта персональных данных

Категория 4

- Обезличенные и/или общедоступные данные

Essence and types

Category 1

- Personal data concerning race, nationality, political, religious and philosophic beliefs, health and love life

Category 2

- Personal data that allow you to identify of personal data owner and receive additional information about them, except for personal data pertaining to category 1

Category 3

- Personal data that allow you to identify the personal data owner

Category 4

- Impersonal and/or public data

Законодательство о персональных данных и доменные реестры

Регистратура

- Автоматизированная ИС, осуществляющая хранение персональных данных

Регистратор

- Автоматизированная ИС, осуществляющая хранение и обработку персональных данных

Партнер/ресе
ллер

- Лицо, осуществляющее сбор персональных данных

Взаимо-
действие

- Защита информации при передачи через сети общего пользования

The legislation on the personal data and domain registers

Registry

- Automated IS, carrying out storage of the personal data

Registrar

- Automated IS, carrying out storage and processing of the personal data

Partner/Reseller

- The person who is carrying out gathering of the personal data

Interaction

- Information protection at transfer through public networks

Сложности приведения системы регистрации в соответствие требованиям закона

Complexities of reduction of system of registration in conformity to law requirements

Барьер

- Невозможность выполнения требований закона небольшими компаниями

Техника

- Необходимость существенной модификации и сертификации информационных систем

Трансграничная передача

- Взаимодействие с международными реестрами

Бизнес

- Различные бизнес модели регистраторов

Координация

- Отсутствие поддержки со стороны Регистратуры по причине "бизнес"

Barriers

- Impossibility of performance of requirements of the law the small companies

Technics

- Necessity of essential updating and certification of information systems

Transboundary transfer

- interaction with the international registers

Business

- Various business of model of registrars

Coordi-nation

- Absence of support from Registry for the reason "business"

Пути решения

Каждый сам за себя

- Ведение реестра ПД только на стороне регистратора
- Проблема смерти регистратора
- Проблема смены регистратора

Закон есть закон

- Все участники системы – операторы ПД
- Проблема маленьких
- Проблема Реселлеров/Партнеров

Собрал – зашифруй

- Хранение данных Регистратурой в зашифрованном виде
- Проблема смены регистратора
- Проблема периодической смены ключей

ЭЦП

- Замена ПД на ЭЦП
- Проблема применимости
- Проблема образованности
- Проблема безопасности

Possible solutions

Everyone for itself

- Conducting register PD only on the party of the registrar
- Problem of death of the registrar
- Problem of change of the registrar

The law is the law

- All participants of system – personal data operators
- Problem of the small
- Problem of Resellers/partners

Has collected – cipher

- Data storage Registry in the ciphered kind
- Problem of change of the registrar
- Problem of periodic change of keys

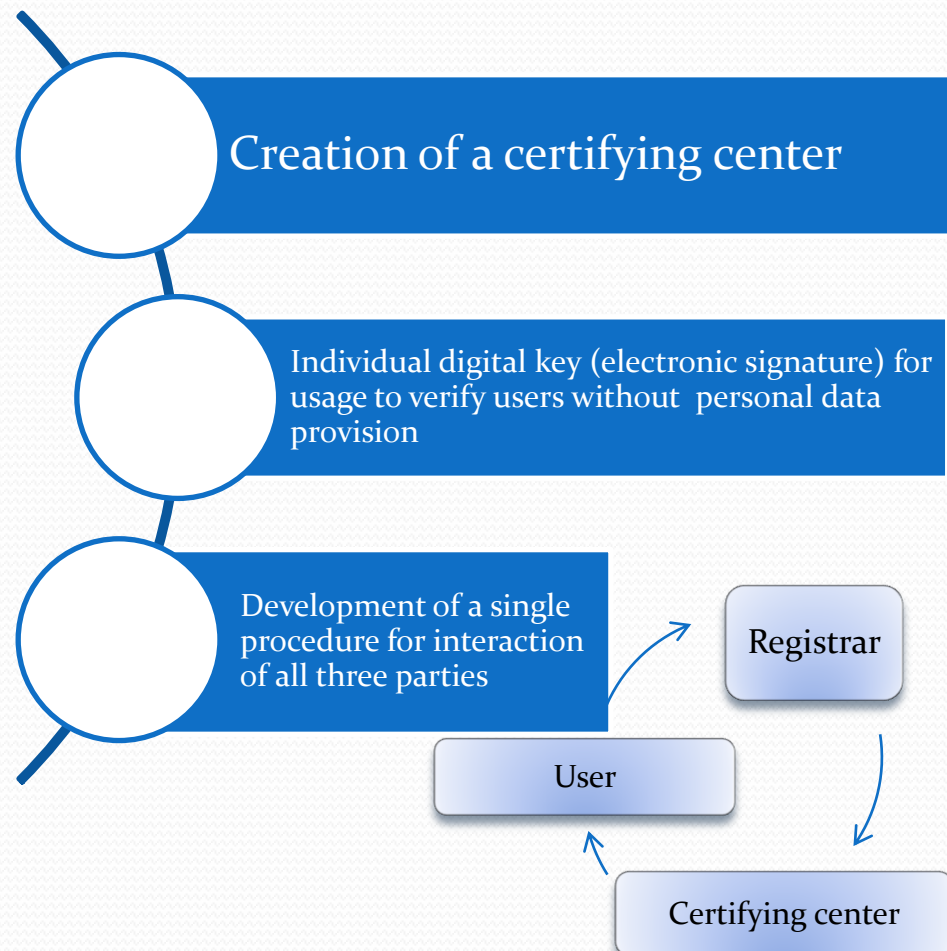
Electronic Signature

- Replacement PD to ES
- Applicability problem
- Erudition problem
- Carelessness problem

Использование закона «О цифровой электронной подписи»



Use of the law «On digital electronic signature»



Hosting Community



**ПЕРВЫЙ РЕГИСТРАТОР
СО СТАТУСОМ**

**«ОПЕРАТОР
ПЕРСОНАЛЬНЫХ
ДАННЫХ»**

**THE FIRST REGISTRAR
IN RUSSIA THAT HAS**

**« PERSONAL DATA
OPERATOR
STATUS»**

Спасибо!

Вопросы?

Сюда их!

a.panov@hostcomm.ru

Александр Панов

www.hostcomm.ru

Thank you!

Questions?

**Do not hesitate to contact
me**

a.panov@hostcomm.ru

Alexander Panov

www.hostcomm.ru