Секция 2. МЕТОДЫ ИССЛЕДОВАНИЙ И МЕТРОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИЗМЕРЕНИЙ

UDC 004.056:006

ABOUT INFORMATION SECURITY MANAGEMENT SYSTEM APPLICATION IN REPUBLIC OF BELARUS

Kupreeva Galina
Belarus National Technical University
Minsk, Republic of Belarus

Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address. The EU Charter of Fundamental Rights says that everyone has the right to personal data protection in all aspects of life: at home, at work, whilst shopping, when receiving medical treatment, at a police station or on the Internet.

In the digital age, the collection and storage of personal information are essential. Data is used by all businesses – from insurance firms and banks to social media sites and search engines. In a globalized world, the transfer of data to third countries has become an important factor in daily life. There are no borders online and cloud computing means data may be sent from Berlin to be processed in Belarus and stored in Bangalore.

Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organizations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law.

Every day within the EU, businesses, public authorities and individuals transfer vast amounts of personal data across borders. Conflicting data protection rules in different countries would disrupt international exchanges. Individuals might also be unwilling to transfer personal data abroad if they were uncertain about the level of protection in other countries.

Whenever you open a bank account, join a social networking website or book a flight online, you hand over vital personal information such as your name, address, and credit card number.

What happens to this data? Could it fall into the wrong hands? What rights do you have regarding your personal information?

Therefore, the European Commission plans to unify data protection within the European Union (EU) with a single law, the General Data Protection Regulation (GDPR). The current EU Data Protection Directive 95/46/EC does not consider important aspects like globalization and technological developments like social networks and cloud computing sufficiently and new guidelines for data protection and privacy were required. Therefore a proposal for the regulation has been released on 25 January 2012. The adoption is aimed for in 2014 and the regulation is planned to take effect in 2016 after a transition period of 2 years.

The EU's Data Protection Directive also foresees specific rules for the transfer of personal data outside the EU to ensure the best possible protection of your data when it is exported abroad

It is known that the IT sphere is rather popular in Belarus. According to official statistics there 125 IT companies in Belarus High Technology Park.

Therefore Belarus IT companies should be prepared for new requirements from their European customers. Information Security Management System (ISMS) implementation could be very supportive in this case.

Information security is the protection of information to ensure:

- Confidentiality: ensuring that the information is accessible only to those authorized to access it.
- Integrity: ensuring that the information is accurate and complete and that the information is not modified without authorization.
- Availability: ensuring that the information is accessible to authorized users when required.

Information security is achieved by applying a suitable set of controls (policies, processes, procedures, organizational structures, and software and hardware functions).

An Information Security Management System is way to protect and manage information based on a systematic business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. It is an organizational approach to information security. ISO/IEC publishes two standards that focus on an organization's ISMS:

- The code of practice standard: ISO/IEC 27002:2005. This standard can be used as a starting point for developing an ISMS. It provides guidance for planning and implementing a program to protect information assets. It also provides a list of controls (safeguards) that you can consider implementing as part of your ISMS.
- The management system standard: ISO/IEC 27001:2005. This standard is the specification for an

ISMS. It explains how to apply ISO/IEC 27002:2005. It provides the standard against which certification is performed, including a list of required documents. An organization that seeks certification of its ISMS is examined against this standard.

The standard contains 11 domains (apart from introductory sections):

1. Security policy - management direction;
2. Organization of information security - governance of information security;
3. Asset management - inventory and classification of information assets;
4. Human resources security - security aspects for employees joining, moving and leaving an organization;
5. Physical and environmental security - protection of the computer facilities;
6. Communications and operations management - management of technical security controls in systems and networks;
7. Access control - restriction of access rights to networks, systems, applications, functions and data;
8. Information systems acquisition, development and maintenance - building security into applications;
9. Information security incident management - anticipating and responding appropriately to information security breaches;
10. Business continuity management - protecting, maintaining and recovering business-critical processes and systems;
11. Compliance - ensuring conformance with information security policies, standards, laws and regulations.

ISO/IEC 27001 requires that management:

- systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable;
- adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

The key benefits of 27001 are:

- it can act as the extension of the current quality system to include security;
- it provides an opportunity to identify and manage risks to key information and systems assets;
- provides confidence and assurance to trading partners and clients; acts as a marketing tool;
- allows an independent review and assurance to you on information security practices.

A company may want to adopt ISO 27001 for the following reasons:

- it is suitable for protecting critical and sensitive information;
- it provides a holistic, risk-based approach to secure information and compliance;
- demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers;
- demonstrates security status according to internationally accepted criteria;
- creates a market differentiation due to prestige, image and external goodwill;
- if a company is certified once, it is accepted globally.

In conclusion I would like point out that for the organizations that want to be competitive in fast changing digital world it is essential to protect their information assets from different types of threats and vulnerabilities.

УДК 006.83.053:665.723.033.2(047.31)(476)

МЕТРОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИЗМЕРЕНИЙ КОМПОНЕНТНОГО СОСТАВА СЖИЖЕННЫХ УГЛЕВОДОРОДНЫХ ГАЗОВ

Ананьин В.Н., Ключиц А.С., Мохнач М.В.

Республиканское унитарное предприятие «Белорусский государственный институт метрологии» (БелГИМ), Минск, Республика Беларусь

Республика Беларусь производит и импортирует из России более 1 млн. тонн в год сжиженных углеводородных газов (СУГ). СУГ - смеси легких углеводородов (пропана, пропилена, бутанов, бутиленов и бутадиенов с незначительным содержанием метана, этана, этилена и/или пентанов и пентенов), которые используются в качестве топлива для коммунально-бытового и производственного потребления, а также в качестве моторного топлива для автомобильного транспорта [1, 2].

Основным физико-химическим показателем, определяющим качество различных марок СУГ, является компонентный состав. На основе компонентного состава рассчитываются октановое число по моторному методу, плотность жидкой фазы и избыточное давление насыщенных паров СУГ, низшая теплота сгорания [2]. Определение компонентного состава СУГ в молярных или массовых долях осуществляется методами газовой хроматографии с использованием для калибровки хроматографов стандартных образцов состава (СО) СУГ [3, 4].

Для метрологического обеспечения измерений компонентного состава СУГ в рамках подпрограммы «Эталоны Беларуси» создан эта-