Основное преимущество такого подхода определяется тем, что аппарат теории нечетких множеств требует от лица, принимающего решения, задания не точных вероятностных оценок, а интервальных, образующих расчетный коридор значений прогнозируемых параметров. Отсюда вытекает удобство этих методов, проявляющееся в повышенной степени обоснованности, поскольку здесь учитываются все возможные сценарии развития, образующие непрерывный спектр, в отличие, например, от метода Гурвица, рассчитанного на дискретное множество сценариев.

При этом оценки рисков могут быть получены в двух вариантах.

Первый - это величина финансовых, информационных и других потерь, которые возможны в случае нежелательного развития ситуации. Второй - это некоторый числовой или нечисловой показатель, характеризующий уровень риска, присущий анализируемой информационной системе, как степень неопределенности относительно будущего развития позитивных и негативных сторон ее функционирования и окружающей среды. Соответствующие методы оценки и программирования рисков нами в настоящее время развиваются с использованием программного обеспечения Matlab Fuzzy Toolbox, Fuzzytech и Fuzicalc и будут представлены в дальнейших публикациях.

POLICY OF PERSONAL DATA SECURITY

Łukasz Kister,
European Association for Security (Poland)

This article focuses on procedures of drawing up and bringing into effect a document which describes essential rules for personal data security. Possession of such a document is legal obligation to any organization that processes personal data on territory of the Republic of Poland.

1. Introduction

Once Poland run for joining the European Union structures it had to conform its national legal system to meet the international standards within the area of civil rights and obligations. At level of personal data se-curity, all EU countries are obliged to implement *Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (WE L 281)*. Poland im-

plemented the directive on 29 August 1997 by authority of the Act on the Protection of Personal Data (Journal of Laws No. 133 item 883).

Currently binding legal system in this area was established upon amendments passed to earlier legal acts in 2004 (Journal of Laws No. 25 item 219 with amendments) which in particular applied to mandatory organizational and technical means ensuring security of processed personal data.

2. Basic expressions in personal data security

In order to keep argument in the article correct, it is necessary to introduce some major expressions related to personal data security.

Personal data is any information concerning an identified or identifiable person. Modifier *any information* indicates wide range of the expression "personal data", that includes not only language signs but also images, sounds and, getting more important, biometrics as well. It is important that biometric data is finger prints or retina pattern as well as structure of face, voice projection, geometry of a hand, pattern of veins and even habits or acquired skills (e.g. walk style, handwriting, etc.).

Personal data processing is any operation made over personal data, especially in IT systems, such as collecting, saving, storing, editing, modifying, sharing and erasing data. Determining particular operations which are part of personal data processing, does not make the catalog of such operations closed. It specifies time frames of data processing, from collecting to erasing data, what gives frames for obligation of personal data security.

3. Documentation of personal data security

3.1 Definition

The legislature did not define expression "Policy of Personal Data Security" [further called: the Policy] therefore help of scientists and experts was necessary to make clear and precise definition of it.

Policy of Personal Data Security is a set of laws, regulations and practical experience that determine a way of management, protection and distribution of personal data inside and outside of an institution. The set is directly related to security of personal data processed traditionally as well as in IT systems.

3.2 Contents

Contents of the Policy document is described in the executive decree to the mentioned earlier Act, nevertheless almost all independent experts and researchers claim that it is not extensive enough to cover all legal obligation for personal data security. Therefore, according to the international standards ISO 27001 and ISO 17799, the Policy is supposed to include below listed elements:

- Declaration of an institution management;
- General statements (definitions, goals, extent);

- ◆ Structure of management;
- ◆ Strategy of organizational and technical security measures, including:
  - personnel security;
  - access control;
  - hardware protection;
  - access to IT systems;
  - notebooks and on-line work (remote access);
  - electronic information storage devices;
  - access to the Internet;
  - e-mail;
  - antivirus protection;
  - cryptographic protection;
  - emergency data back-up;
  - withdrawal from use and utilization of hardware and storage devices;
  - security audits;
  - trainings;
  - access to personal data for personnel from the outside.
- ◆ Registering of personal data sets;
- ◆ Audit and updating of documentation
- ◆ Final statements.

and also elements described in the executive decree:

- ◆ List of buildings, rooms and parts of room that make area in which personal data is processed;
- ◆ List of personal data sets with software used to processed the data;

- ◆ Description of structure of the data sets which shows contents of data records and relations between records;
- ◆ Algorithm of data flow between particular systems.

It is also important to indicate necessity of implementation into the Policy procedures for crisis management in personal data security system.

3.3 Preparation of the Policy

Documentation that specifies rules of security for processing personal data, apart from other detailed requirements, **must be adequate to reality** when treats actual state of its conformity with the law. Preparation of the Policy should be preceded by audit in a company that allows to collect all information needed to create the Policy.

Formally, the Policy may consist of one or few documents describing process of personal data security. According to the legal requirements, the Policy has to be prepared in a traditional way (hard copy).

4. In conclusion

Properly prepared and implemented in a company Policy of Personal Data Security makes procedures that allow to manage data of specific value professionally. Beside meeting legal requirements, the Policy creates long-term image of safe partner in business, client, employer, organization etc.

References:

1. Buller L.J.: *Influencja*, Stalowa Wola: KUL, 2008. ss. 165. ISBN 978-83-61307-08-2

2. Drozd A.: *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa: Lexis-Nexis, 2007. ss. 499. ISBN 978-83-7334-784-7

3. Dworzecki J.: *Podstawy prawne wykonywania zadań ochrony osób i mienia. Wybrane zagadnienia*, Gliwice: GWSP, 2009. ss. 138. ISBN 978-83-61401-20-9

4. Kister Ł.: *Polityka bezpieczeństwa danych osobowych*, Ochrona mienia i informacji, nr 6, 2009, s. 14-16. ISSN 1732-5951

5. Kister Ł., MACH V.: *Bezpieczeństwo przedsiębiorstwa informacyjnego*, Securitologia, nr 9, 2009, s. 19-28. ISSN 1898-4509

6. Korzeniowski L.F.: *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, Kraków: EAS, 2008. ss. 311. ISBN 978-83-925072-1-5

ЭЛЕКТРОРАЗРЯДНАЯ ЗАЩИТА ОТ ПОДДЕЛКИ БУМАЖНЫХ ДОКУМЕНТОВ

Шкилёв Владимир, Недиогло Виктор, Адамчук Аркадий
Министерство информационных технологий
и телекоммуникаций (Республика Молдова)

Is presented new information technologies at manufacturing paper documents with high level of protection. The way of formation a database of documents on the basis of association of the wave and digital information is offered.

Идея использования процессов, даже теоретически не поддающихся полному расчету и управлению, для высокоуровневой защиты документов не нова. Ещё в конце 60-годов С.Виснер предложил использовать фотоны с заданными поляризованными состояниями [1]. И хотя технологически идея не реализуема и по сей день, тем не менее, идея С.Виснера действительно была блестящей, хотя бы потому, что из нее со временем развились новые подходы в криптографии, которые дают надежду разработать, рано или поздно, простые и дешевые технологии изготовления бумажных документов с высочайшим уровнем защиты.