PROTECTION OF INFORMATION IN SMALL AND MEDIUM SIZE ENTERPRISES

Hristo Ivanov

***Abstract**: Protection of information could help to create theoretical and practical mechanism for defining security level and to formulate specific measures to be taken to counteract the existing threats.*

Keywords: *Information, protection of information, middle and small sized enterprises.*

ITHEA Keywords: *K.6 Management of Computing And Information Systems; K.6.5 Security and Protection.*

Introduction

The protection of information is secured by means for protection of information. They shall foresee control for their own efficiency and shall provide evaluation of this efficiency. The protection means shall not limit the functional characteristics of the information system.

Protection of information

Protection of information is the safety of the information as well as the means and facilities where it is accumulated and stored. The protection of information is responsibility of the information owners or managers authorized by them who:

- Secure their rights of owning, managing and exerting other rights;
- Preventing the disclosure of information;
- Store and secure the integrity, availability of the information, its data base and the program application;
- Protect confidentiality or secrecy of the protected information in compliance with the legislation.

Therefore it is of extreme importance to analyze the legal base for protection of information. The legal base is following the business activities and the relationships between the parties. Measures for state and administrative control sometimes suitable, sometimes not are introduced, as well as sanctions for natural persons and legal entities which affect the rights of the business entities. The purpose is to permanently improve the legal aspect for protection of information. The legal base as a whole is defined by security regime and is in compliance with means which define and support this regime. It creates the legal fundament for the impact of protection of information.

Means for protection of information

2.1. The most important mean for protection of information is the legislation.

During the latest years in Republic of Bulgaria a complex of means for protection of information was introduced. Good base was formed, which can be seen by the following acts:

- ✓ Data Protection Act (State Gazette, issue 1/ 2002)
- ✓ Classified Data Protection Act (State Gazette, issue 45/ 2002)
- ✓ Access to Public Information Act (State Gazette, issue 55/ 2000)
- ✓ Local Self-Governance and Local Administration Act (State Gazette, issue 77/ 1991)
- ✓ Administrative Infringements and Penalties Act (State Gazette, issue 92/ 1969)
- ✓ Ratification Act for Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (State Gazette, issue 56/ 2002)

In addition, ordinances were enforced:

- ❖ Council of Ministers Decree 73 for creation of Coordination council for information society (State Gazette, issue 38/ 2000)
- ❖ Council of Minsters Decision 213 for approval of Updated National Program for Development of Information Society in Republic of Bulgaria (State Gazette, issue 36/ 2001)
- ❖ Decision XXXIX of the National Assembly for assigning a Data Protection Commission (State Gazette, issue 54/ 2002)
- ❖ When drafting the legal base there was an attempt to list the means for protection of information and as an addition the term systematization was used, which is not implemented in another important ordinance: Ordinance for the obligatory conditions for security of the automated information systems and nets, in which classified information is processed, stored and transferred
- ❖ Another ordinance of importance is the Ordinance for system of measures, ways and measures for physical security of the classified information and the conditions and procedure for their use.

The list of legislation document is not exhaustive but rather selective due to the purpose for which this article is drafted.

2.2. Standards

The European and international standards which are implemented and applied in Republic of Bulgaria have the status of Bulgarian standards. In the National Standardization Act the process of national standardization and the process of creation, structure and activities of the Bulgarian Standardization Institute are regulated [Ivanov, 2011, Temelkova, 2017].

The standard is a bunch of norms, rules, requirements towards goods and services or in other words this is a sample, model of a product or process agreed as a reference. Standards are developed and exist not only for the production processes and the products, but also for all other areas of social and economic life. It is important for us to define what standard is, its purposes, system, types, requirements, their application and the business security.

The standard is a document which is drafted based on a mutual consent and defined for general and repeated application of the rules, basic guidance or characteristics for activities or their results, in order to reach an optimum process under the specific circumstances. It could be accepted as a statement that the standard is a combination of strictly defined parameters and requirements towards them in order to reach uniformity and high quality for specific structures, products, processes, services and activities. This is a template, sameness, uniformity [Temelkova, 2018].

Historically, the first evaluation standard which had been widely used and had a great impact over the standardization base in the protection of information area in a lot of countries is the MO standard in US “Trusted Computer Systems Evaluation Criteria”. The document which accepted the title the Orange Book is published in August 1983 for the first time. In the title it is defined that the standard is not about safety system, but a systems that can be trusted to some extent.

The technical specification X800 is published little after the Orange Book. This specification defines in detail the protection of information issues in defines systems. This is rather extensive document.

Standard ISO/IEC 15408 “The Common Criteria for Information Technology Security Evaluation” is issued on 1 December 1999. Due to historical reasons this standard is often referred as “Common Criteria”. Actually the Common criteria are used as a meta-standard which defines the instruments for security evaluation of information systems and how they are used [Ivanov, 2011].

Net Configurations

In 1987 in the National Computer Security Center in US the Orange Book interpretation for net configurations is published. This document is in two parts: first contains its own interpretation, in the second security services, specific or pretty important for net configurations [Ivanov, 2011].

Standard ISO/ IES 17799-2000

The standard (emerged from the British Standard BS 7799-1) is a reply to the requirement for creation of common legal framework which allows the organizational structures to develop, apply and evaluate the effective procedures for management and protection of information. The goal is to build trust in the created relations between the organizations and without conflict in business processes by the limitation and minimization of the incident impact in relation to information protection. UK government had stated that each governmental structure, which functions as part of e-government shall have developed and effective management structure of information security in compliance with BS 7799-2 Standard [Ivanov, 2011].

Standard COBIT

Having in mind the great impact on information protection a special regard is given to the control over the risks for information emerging from the use of information technology. In this area the important aspects are COBIT standard, which manages the information technology from one side and the information technologies which develop dynamically and meet the rising need for functionality from the other.

Standard ISO 27001

Security of Information Management Systems

This international standard is valid for all types of organizations. It defines the requirements for creation, implementation, functioning, monitoring, review and support and improvement of documented system for security information management in regard to the common risk, connected to the organization’s activities [Ivanov, 2011].

ISO 27002

Code of a good practice for security information management

This international standard gives guidance and general principles for implementation, support and improvement of security information management in an organization. The purpose of this international standard is to provide direction for the general guidance of security information management.

The international standard ISO 27001 states the requirements for information security management systems (ISMS) in all organizations, no matter of the size, scope, type of products and processes or other specifics [Ivanov, 2011].

When an organization creates and supports ISMS, it does not only follow the aspects of its own business, but also the requirements of the law and its security obligations. So, a ISMS system of ISO/IEC 27001 model generates relative security and calmness not only in favor of the business, but also in favor of its clients, suppliers, partners and the society as a whole.

2.3. Activities

The information activities are classified in the following four types:

- *Collection of information*

The collection of information is used mainly to form the state policy in the information environment for improving its legal, methodological, technical and organizational guarantees for development of programs in this area. It is the base of the strategic management.

- *Information storage*

The information storage is enlarging and developing fast during the last years and it is difficult to make classifications of its categories.

- *Data processing*

Data processing is an informatics term meaning “collection and manipulation of records aiming at producing of readable information”.

Data processing involves a number of different operations with the data:

- Validation – assuring that the data is correct and of quality
- Sorting – organization of records of data
- Classification – dividing of data in different categories depending on different criteria
- Resuming of data – reduction of details of data to the most essential part of them
- Aggregation – combination of data from several different sources
- Analysis – collection, organization, statistical analysis, interpretation and providing of data
- Reporting – providing in detailed and resumed form the data or the information extracted from the data as well as its visualization

A lot of products offer protection in several of the above categories, as especially famous lately are UTM type (United Threat Management).

- *Dissemination of information*

Dissemination of information is a process in which the information available in one moment, in the following moment another information (or the same one) is received. Every information process is reviewed as combination of the basic information activities.

In general, none of the four types of activities is performed on its own.

Conclusion

Computer systems and nets are one of the highest technological products nowadays. Despite all advantages they can offer, they have a number of disadvantages. Problems with security such as disinformation, infringement of information rights, sending of undesired online advertising or spam affect almost every user of technology.

Bibliography

[Ivanov, 2011] Hristo Ivanov. Processes of standardization of extracurricular education in the European Higher Education Area. Sociosphere of 2011. Rusia

[Temelkova, 2017] Miglena Temelkova, Development of Controlling in the Organizations from the Service Sector under the Conditions of the Forth Industrial Revolution. International Journal of Advanced Research in Management and Social Sciences, Volume 6, Issue 3, ISSN 2278-6236, March 2017.

[Temelkova, 2018] Miglena Temelkova, Studying the leadership style of business organizations' management under the conditions of the Fourth Industrial Revolution. Asia Pacific Journal of Research in Business Management, Volume 9,Issue 2, ISSN: 2229-4104, February-2018.

Authors' Information

Hristo Ivanov *– Professor at the Information Technologies Department, University of Telecommunications and Post, 1st. Acad. Stefan Mladenov Str. Sofia-1700, Bulgaria; e-mail: xiza@abv.bg*

Major Fields of Scientific Research: Security, Control and administration