The Third International Conference "Problems of Cybernetics and Informatics"
September 6-8, 2010, Baku, Azerbaijan. Section #1 "Information and Communication Technologies"
www.pci2010.science.az/1/19.pdf

ARCHITECTURE OF E-GOVERNMENT INFORMATION SECURITY MANAGEMENT SYSTEM

Yadigar Imamverdiyev

Institute of Information Technology ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

1. Introduction

Current development level of civilization is characterized with rapid development of information technology and creation of global communication networks. In modern period, state organizations and other structures of civil society increasingly use potential of information and communication in order to perform their functions. Informatization process of the entire space of the government as a geopolitical unit and a sovereign state with its own juridical system prompts transmission intro a new development stage as a results of rapid development. This condition is characterized as "electronic government" (e-government) term.

The main object of the research is the information security of e-government; therefore exact definition of e-government term is important. The point is that "electronic state" definition is often identified with "electronic government" term. Besides, often "state" and "government administration institutions" definitions are used in the same meaning. Certainly, such approaches reflect the essence and coverage area of electronic government definition wrongly. Electronic government definition considers performance of functions of administrative power using information and communication technologies. In this paper, e-government definition is understood as a geopolitical unit and it is accepted that information society and e-government coincide geopolitically [1, 2].

It is often required for provide mutual connection – mutual requests to information resources, and close integration on data exchange between information systems. This requirement is met by unique information infrastructure. During the formation and development of e-government, national information infrastructure is created as results of integration of different information systems and resources. Currently, information infrastructure is as important as traditional infrastructures such as – transportation, electricity, gas, water supply, communication etc. Differentiating several critical segments included in national information infrastructure is quite important. Segments supporting critical infrastructure are especially important, because currently majority of critical infrastructures are highly dependent on used information-communication technologies.

Doubtless, malfunction of any important element of information infrastructure can result in significant damage and drastic consequences. In [2], new threats occurred in information infrastructure, quality changes occurred in threat actors are analyzed in detail, difficulties in application of traditional security models to a complex object such as e-government are presented. It is also noted that threats sourced from asymmetrical actors are especially dangerous for e-government. Asymmetrical actors – a group of petty criminals can conduct a chain of highly probable terror acts in minor infrastructure objects using relevant information weapons.

The level of information security of e-government significantly affects the condition social-political, economical, defense and other elements of national security, and become the leading component of national security. Development of e-government information security provision system is a vitally important issue for e-government. In connection with the increase of scale and complexity of threats, it is important to purposefully control the processes of e-government information security provision and widely apply information technologies.

In modern information-communication environment, in case of subjection of information infrastructure of e-government to threats and risks, complex and complete solution of security problems is impossible without formation of information security management system. New

models of information security management are required in order to solve security problems arising in a new environment such as e-government.

Strategic issues of this field include prevention of cyber attacks to the critical infrastuctures, reduce the sensitivity of e-government to such attacks, and reduce the damage and recovery period to minimum.

2. Approaches to information security management

In information security management field, necessity of theoretical researches is acknowledged in recent periods [3]. First researches in this field were started in late 1980s, and first national and international standards (ISO/IEC 17799) were developed by late 1990s. But development of standards doesn't signify solution of all problems in information security management field. In contrary, information security management issues increase on a daily basis, due to intensive use of information technologies in practically all activity fields of people. Generalization of information security management experience makes development of information security management theory necessary.

Main approach to information security management is the process model described in [4]. Process model consists of four main phases: planning, realizing, analysis and improvement. Realization of organization of information security management is presented with relevant methods supporting process model [5].

It must be noted that, information security management usually signifies the level of large companies. But in recent periods of time, information security management of regional and national infrastructures is discussed more often. It must be considered that, in each of these levels, information security management requires development of particular methodological base for their solution.

3. Architecture of information security management system

ISO/IEC 42010:2007 (former ANSI/IEEE 1471-2000) standards defines architecture as following [6]: «Architecture is the fundamental organization of the system and is realized in system components, interrelation of components and their relation with environment, structure of the system and principals determining the development".

Usually, three levels of architecture are separated: strategic (or conceptual), logical and system (or technological). System level is often called as realization level. Security Architecture for Enterprise, SAFE presented by Cisco Company can be identified as an example to security architecture, this architecture was designed for corporate level.

Architecture of information security management system of e-government consists of a complex collection of models describing the system and functions of the system. Important application fields of these models are – system planning and development of architecture, as well as strategic decision making.

In architecture, different models are logically regulated and allow a detailed description of e-government information security management system as well as these objectives and duties, processes and their organization, systems, used technologies.

.4. Information security management functions

We can review information security management on three different levels as one of the approaches to structurization of e-government information security management functions: strategic, tectical and operative. Let's group main functions of information security management in accordance with these levels.

The target of strategic level is to present information security management as an important component of general strategic plans of the country. Following functions can be included in the level:

- Evaluation of information security condition; detection of internal and external threats to information security, strategic analysis and forecasting;
- Strategic planning of scientific researches, technological strategies;

- Organization of development of government programs for provision of information security and coordination of activities for their implementation;
- organization of scientific researches, coordination of development of scientific, scientific-technical programs and their implementation in information security field;
- strategy of cooperation of government and private sector for protection of critical infrastructures;
- Planning of international cooperation strategy

The objective of the tactical level is to cover aspects important for development of information security management system:

- Development of a complex system of juridical, economical, technical and other measures and methods directed at provision of information security;
- Staff training in information security field;
- Coordination of activity of government institutions and other organization in information security field;
- Analysis of information security risks;
- Standards of information security management;
- Humanitarian issues of information security (for example education);
- Licensing of actives in information security field;
- Certification of information systems and program hardware;
- Management of information security provision;
- Implementation of international cooperation in information security field.

The objective of operative management of information security is the introduction of information security services necessary for creation of a secured environment. Following are included in this level:

- Identification and authentification;
- Authorization (logical control of entrance);
- Protection of confidential information;
- Prevention of technical intelligence;
- Prevention, detection and investigation of infringements in information security field;
- Monitoring of information security;
- Processing of information security incidents;

As seen from listed functions, politics (strategic level), administrative directions (tactical level) and information security management (operative level) are main motivators for information security management. Other distinguishing factors among different organizational levels are as following: strategic level affects the government strategy; tactical level concerns processes and methodologies used for information security management, operative level covers application and exploitation of security measures and devices. It must be noted that, traditional approach to information security management concentrates the attention mainly on operative level.

5. Structure of information security management system

In this abstract, organization structure of administration is understood and a summary of government institutions, juridical and physical persons are considered under information security management system. Information security management system is constructed based on correct determination of authorities of legislative, administrative and court institutions. Authorities of organizational elements of information security management system are determined by the legislation of the country.

Structure of information security management system is depicted in Picture 1. Main elements of this system are Information Security Council, National Information Security Center, government institutions engaged in issues of information security, organizations providing informational security of critical infrastructure, and organizations providing information security in government institutions.

Subsystems (systems) directed to solutions of different directions of information security management issues can be created in Information Security Management System.

Information Security Council performs control of provision of information security as

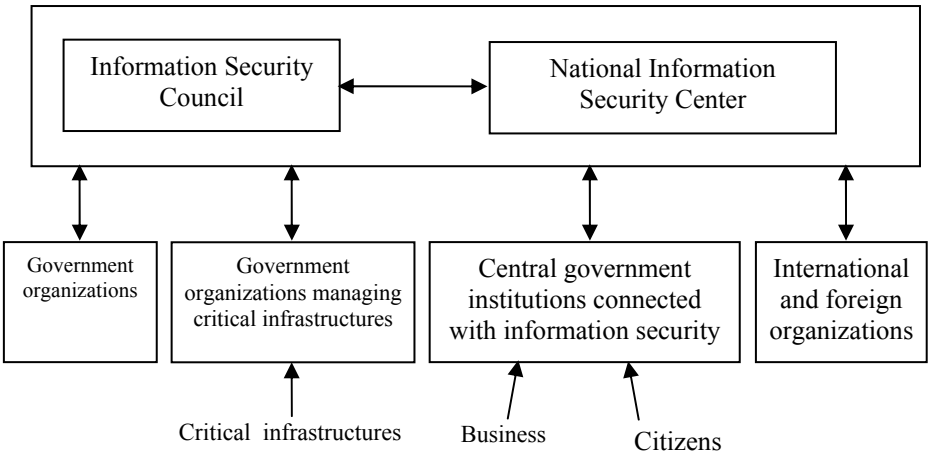

Fig. 1. Structure of e-government information security management system

well as functions concerning strategic level of administration.

The main objective of National Information Security Center is creation of government infrastructure for information security, development of potential meetings information security risks, as well as early warning infrastructure, conduction of evaluation, certification, licensing in information security field, collection and analysis of information on incidents related to information security, coordination of activities, performance of inter-sector cooperation, staff training in information security field, conduction of international cooperation and development of international relations.

Conclusion

As a result of global informatization processes, society gradually becomes fully dependent on security condition of information infrastructure. This problem makes development of information security management system based on a single methodological approach necessary. Development of such security infrastructure creates broad capabilities for development of e-government – information society.

In this abstract, methodological and theoretical bases of development of information security system of e-government are explained, system analysis of problems was presented, and proposals on functional structure of the system and its separate components were formed.

References

1. И.Л. Бачило. Правовая платформа построения электронного государства / Информационное право. - М.:Юрист, 2008, № 4, с. 3-8.
2. R.M. Əliquliyev, Y.N. İmamverdiyev. E-dövlətin informasiya təhlükəsizliyi: aktual tədqiqat istiqamətləri / İnformasiya Cəmiyyəti Problemləri, 2010, № 1, s. 3-13.
3. Д.С. Черешкин (ред.). Проблемы управления информационной безопасностью: Сборник трудов. -М.: Изд-во « Эдиториал УРСС» - 2002, 192 с.
4. ISO/IEC 27001:2005. Information Technology - Security Techniques - Information Security Management Systems -- Requirements. 2005.
5. А.М. Астахов. Искусство управления информационными рисками – М.: ДМК Пресс, 2010. – 312 с.
6. ISO/IEC 42010:2007. Systems and Software Engineering - Recommended Practice for Architectural Description of Software-Intensive Systems. 2007.