Conceptual Architecture of National Information Space Security System of Azerbaijan

Rasim Alguliyev[1], Yadigar Imamverdiyev[2], Elchin Aliyev[3]
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]*director@iit.az*, [2]*yadigar@lan.ab.az*, [3]*elchinaa@gmail.com*

Abstract— **The provision of security in the national electronic information space (national e-space) is a complicated and complex problem. It requires an application of a unified state policy, the balance of the interests, formation of hierarchical registry of information resources, specification and distribution of executors' authority working for information security, the unification of security procedures, structured approach, "divide et impera" and other vital principles. The architecture of the security system (SS) of nature e-space shall be determined for the development of complex action program, and security objects (what?), security procedures (how?), the subjects ensuring the execution of these procedures (who?) shall be identified. The study offers the constituent classification of 3 stability sides ("What, How, Who") of SS architectural components, and3D matrix form (4D matrix – by adding time and cause and result dependencies - "when?") which is the synthesis of tables indicating mutual relations between them – "objects &procedures", "objects & subjects", "subjects & procedures".**

Keywords— security systems; security architecture; unified state policy; balancing the interests; security objects; security subjects; hierarchal registry of information resources; security services; security culture; 3D matrix of security

I. Security Problems in the National Information Space

Information Society development considers the formation of national electronic information space (national e-space) and its security system (NES SS). Plans and targets are established in this area, an adequate legal basis, organizational procedures, technological security tools and standards are developed and applied, and professionals are trained. Development of the technologies and increasing demand of the users creates new perspectives and risks, as well as the improvement of these juridical and organizational tools. As the result, NES SS starts to be formed in spiral cyclic manner in a new level.

The main problems in the field of national information security:

1) Collegial identification, monitoring and audit of the real situation and problems;
2) Collegial development of strategy and action plans, including the identification of targets, security objects;
3) Improvement of the legal tools by the professionals;
4) Identification and classification of the executive subjects and procedures (duties), distribution of the competencies, organization of the coordination;
5) Selection and transfer of technological innovations, real application of standards, systematic organization of certification and expertise;
6) Training the new specialists and users beforehand in a planned form and their safety;
7) Monitoring of technological development and increasing demand;
8) Prognosis and assessment of new perspectives and risks;
9) Preparation for the critical level of the real situation change state.

Certain measures in the field of information security have been taken, for example, the main objectives, normative-legal acts setting out principles and national interest, and national strategy on ICT has been approved, adoption procedures of the international standards has been organized.

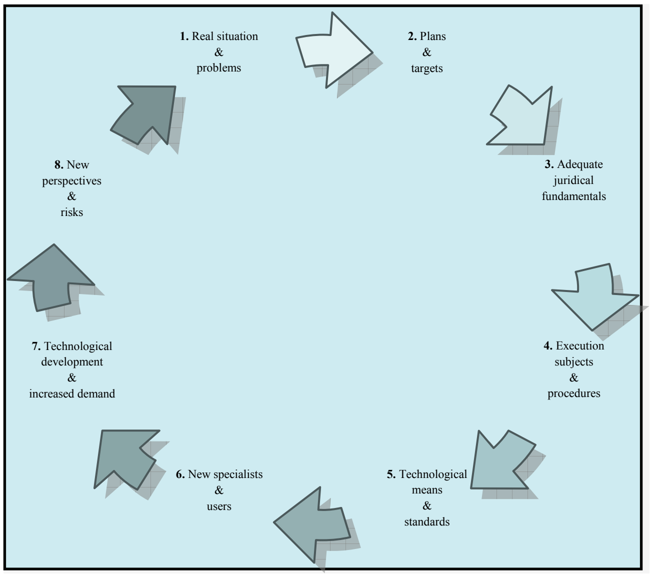
1. Real situation & problems
2. Plans & targets
3. Adequate juridical fundamentals
4. Execution subjects & procedures
5. Technological means & standards
6. New specialists & users
7. Technological development & increased demand
8. New perspectives & risks

Figure 1. Cause and effect "wheel" of continuous formation processes of NES SS.

II. Problem Statement: Identification of Goals and Objectives

2.1. National interests and main objectives in the field of information security [3]*:*

a) prevention of all the actions related to the attacks against the information freedom and directed to the information systems, destruction, theft, and falsification of information, as well as unauthorized actions related to the modification, copying, and blocking of information, information loss and information aggression;
b) protection of the state secrets on legal basis or confidential information with limited access;
c) ensuring the rights of legal entities and individuals at the time of information processes and the development, production and application of information systems, technologies and their provision means;
d) elimination of the underdevelopment in the field of information technology and the barriers in access to the world information space.

2.2. Key principles of providing national information security [4]*:*

a) **substantiating on the rights** - respect for human rights and fundamental liberty, complying with existing legislation;
b) **unified policy** - substantiating the national information security on the unified state policy and balancing its provision directions;
c) **coordination** - defining accurately the competencies between the authorities ensuring the national information security, coordinating their performances and informing these agencies operatively and mutually;
d) **control** – controlling implementations to ensure the national information security;
e) **integration** - integrating into the international security systems [2];
f) **balancing the interests**–maintaining the balance among the interests of the state, society and person and their mutual responsibility [3];
g) **structured approach** - complex systems management problem, decomposition, "divide et impera" ("divide and rule") [7].

2.3. The main objectives of NES SS:

a) effectiveness of the struggle with the facts set out against the cases indicated in the principles and objectives of information security and avoiding the risks;
b) provision of security confidence for e-services and security services for e-government;
c) complex organization of the protection process of national interests, rights and interests of person, society and state in the field of information security.

III. Problem solution model - conceptual architecture of NES SS

3 stability sides (facets) of the architectural components of NES SS:

1) NES SS objects **(**what?)
2) NES SS methods and procedures (how?)
3) NES SS subjects (who?)

3.1. NES SS objects and their unified hierarchical registry (What?)

Centralized information about the NES SS objects are collected and used in the "Unified hierarchical registry of information resources". The main objectives of this registry are:

a) Registration, classification and monitoring of existing and new information resources;
b) Coordination of new resources projecting, and minimizing the excess;
c) Information support for e-services and ensuring the conformance of information resources;
d) hierarchical coordination between this registry and corporate registries, multi-parameter queries formation and its routing.

Classification of NES SS objects in "Unified hierarchical registry of information resources" [5]:

1) state, public and private electronic information resources;
2) provision means related to these resources;
3) security means related to these resources;
4) the staff related to these resources.

3.1.1. Information Resources (*IR*)*:*

a) IR name, databases (tables, fields), primary sources;
b) information with security status (1 - open, including Internet information; 2 - confidential (private data, commercial, banking, investigation, medical treatment and etc. secrets); 3-state secret data);
c) the scope of users;
d) other related IR, exchange methods with them and their coordination properties;
e) reserve (backup) copy.

3.1.2. Security means:

a) mission and components (parts) of the related information systems (IS), including e-services;
b) information media and technical support means;
c) storage facilities of information media and tools and engineering facilities (buildings);

d) information processes software, standard copies and open source codes;
e) computer networks and its telecommunication lines;
f) project and technical documents, license, expert opinion, documentation, certificates.

3.1.3 . Protection means:

a) software and technical;
b) cryptographic;
c) administrative (including the security policy);
d) engineering.

3.1.4. Related persons:

a) information developer;
b) information maintainer;
c) information user;
d) security personnel.

3.2. Classification of the methods and procedures applied in NES SS (*How?*)

NES SS is an integral part of the national security system. SS performance directions:

1) regulatory;
2) protection;
3) management;
4) education and training.

It is considered beforehand, that envisaged methods, procedures and services applied for reducing, preventing and avoiding the threats in NES SS, shall be regularly improved in coordination with the development information technologies.

3.2.1. NES SS regulatory performance:

a) **juridical framework** - the development of regulatory juridical framework for information security, the study of international tools;
b) **licensing** – improvement of licensing, control over the observance of the license terms;
c) **standardization** - development of national standards and selection of international standards for usage, improvement of standards fund and state scientific and technical information system, establishment of information exchange with the relevant international systems on the basis of modern technologies [4];
d) **certification** - organization and improvement of certification and relevant testing centers, determination of foreign centers the certificates of which are recognized [4];
e) **expertise** – expertise of information systems and projects with one or more purposes (for juridical compliance, standardization, coordination, prospects, adequacy, safety, technical and economical substantiation, assessment of the originality and initial rates), standardization of juridical and technical documentation in this area, organization of the usage of the software with proven open source codes [5];
f) **ICT-monitoring** (state registry) – definition of the registry rules of information security objects, i.e. information systems, including their owners, manufacturers and operators [5];

3.2.2. NES SS management performance:

a) **coordination** - taking into account the infrastructure of mutual dependence at NES, the development of the system for competency distribution, security monitoring and management;
b) **national situation center** –improvement of cyber-security performances and of the infrastructure for confidential information protection, organization of "security and warning" (CERT/CIRT) networks, systematization and analysis of data on critical situations detected in the information systems, and on their elimination, recommendations, conducting trainings and tests, the development of knowledge bank [1];
c) **scientific maintenance** - support for research and development on information security, determination of leading research institution in this field, improvement of the intellectual property protection system;
d) **risk assessment** - regular assessment of the threats to NES SS objects and protection level [6];
e) **modernization** - provision of the high level of ICT facilities and its continuous improvement;
f) **national production** - organization of provision and production of technical, cryptographic, software and etc. tools of information security, support for the development of these tools and national ICT producers, improvement of state procurement processes in terms of information security [2];
g) **operator maintenance** - organization of the operators' (centers) activity for the management and services of corporate, particularly inter-organization information systems;

3.2.3. NES SS security performance:

a) **identification of the resources** – on personnel, physical infrastructure, information infrastructure, including computers, software and data, information services of external organizations, documents [6];
b) **software and technical services of security**-identification/authentication and biometric technologies, distribution of roles and competencies, protocol and auditing, cryptography, integrity control and e-signature technology, tunneling, firewall [7];
c) **physical security** - maintenance, including telecommunication infrastructure security, fire and mobile system security [6];
d) **maintenance of work ability**– support for users and software, configuration management, permanent improvement, reserve (insurance) copying, media management, documentation, regulations [6];

e) **restoration planning** - determining the functions and priorities of critical importance, drawing up a list of possible incidents, development of recovery strategy, preparing for the implementation of the selected strategy, testing of the strategy [6].

f) **response to the violation of safety regulations** - localization of the incident and damage reduction, identification of the violator, prevent repeated violations [6];

3.2.4. NES SS education and training performance:

a) **personnel management** - identification of the personnel responsibilities, minimization of privileges [6];

b) **training and education** - expansion of adequate training and education programs ensuring the requirements of the national information security, in accordance with the development directions of technologies and improvement of its efficiency [2];

c) **providing with the personnel**– organization of international certified specialist preparation and providing the structural departments specialized on information security with appropriate personnel, attestation of the responsible persons;

d) **private information security** – providing information security for each person, improvement of Internet services [2];

e) **talents safety** - juridical and technical contribution for children and young people specializing in information technology, their protection from dangerous effects and the measures taken for their proper development;

f) **security culture** - effective use of coordination mechanisms of the state agencies and technical capabilities of the private institutions in the field of strengthening the fight against cybercrime, the development of the cooperation between government agencies and private institutions, and the development of partnership with international organizations, information infrastructure security, and dissemination of the global “security culture”;

3.3. Classification divisions of NES SS subjects by the functional directions (Who?):

1) state regulatory authorities specialized on information security
2) specialized agencies carrying out the state policy on ICT
3) scientific research institutions specialized in information security
4) education and training institutions specialized in information security;
5) law enforcement and court bodies;
6) financial and customs state bodies
7) state bodies for technical control upon engineering units
8) licensed private organizations and individuals participating in the provision of information security;
9) non-profit organizations and individual experts participating in the information security

IV. Conclusion –NES SS architectural matrix

NES SS subjects execute the responsibilities of providing interests and needs of the state, society and person in the field of information security in accordance with legislation and within the framework of its authority and in time mutually, and are responsible for the consequences individually.

(OX) **what**? - NES SS objects
(OY) **how**? - NES SS methods and procedures
(OZ) **who**? - NES SS subjects

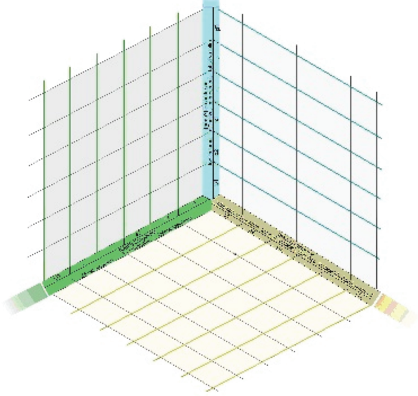

Figure 2. 3 stability facets of NES SS architectural components - 3D Matrix of the mutual relations among the objects, subjects and procedures.

The term (**when**?) and cause and effect dependencies are not visually described in this matrix.

REFERENCES

[1] Council of Europe, Convention on “Cybercrime”, November 23, 2001, № 185
[2] “National Strategy on information and communication technologies for the development of the Republic of Azerbaijan (2003, 2012)” // “Azerbaijan” newspaper, Baku, February 18, 2003, № 38, www.e-qanun.az.
[3] Law of the Republic of Azerbaijan on “National security”, June 29, 2004
[4] Law of the Republic of Azerbaijan on “Information, Informatization and Information Protection”, 1998. April 3, № 460-IQ, “Azerbaijan” newspaper, Baku, June 23, 1998, № 141, www.e-qanun.az.
[5] Decision of the Cabinet of Ministers of the Republic of Azerbaijan on the approval of “Regulation on the rules for conducting the State registry of information resources”, Baku, May 17, 2010, № 89, www.e-qanun.az
[6] Information technology. Security techniques. Information security management systems. Requirements of ISO / IEC 27001-2005) AZS 494-2010
[7] V.A.Galatenko. “Fundamentals of Information Security”, Moscow, 2006 / / www.intuit.ru