Tahmasib Kh. Fataliyev

Institute of Information Technology of ANAS, Baku, Azerbaijan

depart3@iit.ab.az

SECURITY PROVISION ISSUES OF E-SCIENCE

The article is devoted to the information security issues of e-Science, which is under formation in Azerbaijan. The basic components of e-Science are investigated and importance of ensuring its security is highlighted as a complex technological and social problem. The paper analyzes works implemented in this area and priority directions of effective eScience security are shown.

Keywords: *eScience, information society, AzScienceNet, eScience information security, CERT, computational resources, e-services.*

Introduction

The application of information and communication technologies (ICT) in Azerbaijan has caused fundamental changes in all sectors of society. One of these areas is the science. The reforms carried out at Azerbaijan National Academy of Sciences (ANAS), as well as the special attention of the government to ICT has urged the realization and development of e-science as a part of emerging "Electronic Azerbaijan". Apparently, e-science aims at reconstructing the performance of all institutes and organizations of ANAS as well as other research institutions across the country with the use of advanced ICT, and at forming the national science infrastructure and online information medium. Accordingly, joint and efficient activity of the research organizations and scientists in the virtual medium is provided. The main tasks of e-science include the formation of science, communications, networking and computing infrastructure, the wide application of the ICT in scientific activity and management as well as generating information resources, improving the regulatory framework, and staff training [1].

E-science infrastructure is geographically distributed, and has to fully cover all research institutions of Azerbaijan. Obviously, most research institutions of ANAS, including other educational institutions and organizations are located in Baku, Nakhchivan and Ganja departments of ANAS. Shaki and Lankaran Regional Scientific Centers are geographically distributed in the areas. e-Science Emerging in Azerbaijan has a complex infrastructure, which is based on AzScienceNet computer network.

Hence, the protection of the emerging e-science as a unified system, is very important both economically and in terms of the security, and becomes one of the most complex technological and social problems [2]. This is also of great importance as an integral part of national security [3].

Along with the integration to the global network and potential threats to the system, growing demand of users increased the importance of knowledge, professional skills, and human resources in solving problems in the field of information security [4].

E-science components

E-science is a complex system, comprising integral parts as infrastructure, data acquisition, storage, processing, search, analysis, transmission, presentation and so on. Evidently, formation of each of these blocks is related to the solution of complex issues and information security problems.

Being imagined as a unified system, e-Science includes the subsystems shown in Figure 1.
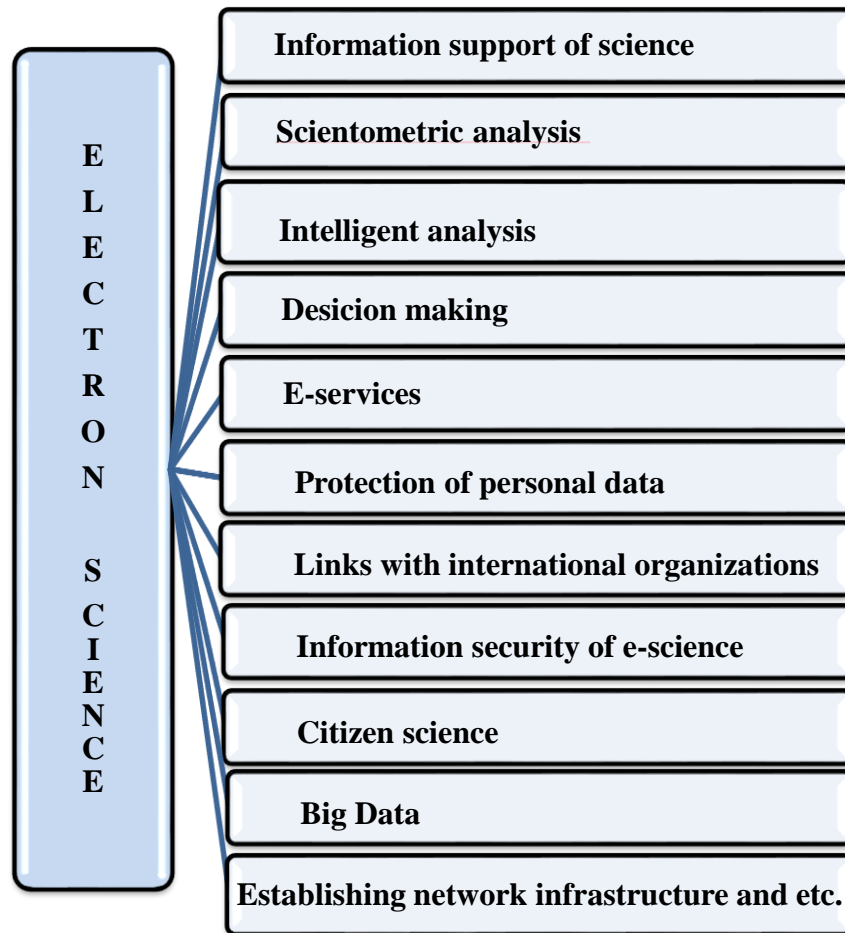
Figure 1. Subsystems of e-science

As it is noted above, one of the main goals of e-science is forming the communication-network and computing infrastructure. The work carried out in this direction resulted the establishment of data processing center based on the AzScienceNet, which has a large computing and memory resources:

- AzScienceNet covers all academic institutions of ANAS [5]. It needs to be noted that the development of e-science is possible through covering all other academic institutions of Azerbaijan. Therefore, the work carried out in this direction have to be intensified.
- Technical features of the Data Center, which has large memory and computational resources (memory - 200 terabytes, computational efficiency - 14 Tflops) are constantly updated.
- The functioning network and computing infrastructure connects scientific institutions, and offer many services (hosting, AzCloud, *AzStorage*, e-mail, e-library, distance learning, *AzScienceCERT*, *eduroam* etc.) to the users, and at the same time, provide integration opportunities to the international systems.
- On the initiative of ANAS, the Ministry of Communications and High Technologies of the Republic of Azerbaijan, and the Ministry of Education of the Republic of Azerbaijan, AzScienceNet has been registered at GEANT Association to represent Azerbaijan. As the national operator, AzScienceNet cooperates to inform scientific and educational community of the country about the projects services of the Association.

The status of the implementations within the framework of e-Science confirms the importance and urgency of researching and solving scientific, theoretical and practical problems of information security.

The implementations in the field of information security

The rapid development of ICT, its spread and intensification of competition coordinate the provision of information security based on the scientific and methodological principles, as well as the legal, organizational, technical and physical security measures. Consequently, it is necessary to create a unified information security system in AzScienceNet network. Provision of information security means ensuring data confidentiality, integrity and availability. Information confidentiality is provided when it is available only to the authorized people; and information integrity is provided when authorized persons are allowed to access the data, when necessary.

The most important issues of developing information security system are as follows:

- identification and analysis of the list of potential threats to information security;
- classification of information resources;
- determination of the unified information security requirements to the new applicable information technologies;
- specifying requirements for the establishment of information security system.

To this end, a common information security policy of the AzScienceNet is developed. The policy aims at minimizing the possible material and moral damages of threats to the network and information resources of ANAS; raising the business prestige of ANAS; forming common principles for the establishment of information security system; creating information security systems; and finally forming proper organizational and methodological framework for the development and actions of the system.

To benefit from the capacity of the AzScienceNet, registry of the user computers was developed. Information about all computers connected to the AzScienceNet is accumulated in a unified database of the register. This system assists in the resolution of the following issues:

- Preventing the access of unauthorized users to the network;
- Implementing more detailed analysis of the monitoring results;
- Fighting against threats;
- Minimizing possible damages caused by the threats within the network;
- Preventing users' requests to banned sites;
- Preventing network traffic overload with unnecessary information;
- Preventing requests to the Web resources, inappropriate to the profile of network.

To ensure efficient management of *AzScienceNet* and its safety network security monitoring (NSM) system has been established and operated. Core functions of NSM are acquisition and analysis of data about the network. Moreover, the system directs these results to respective people or systems, meets modern requirements, and consists of software and hardware [6]. The monitoring system provides many functions, which also increases the efficiency of the network. Main duties of the NSM can be described as below:

- Internet traffic monitoring and recording;
- security controlling of Internet-related real-time systems;
- security, confidentiality and protection of the Internet users;
- identification of the system vulnerabilities;
- uninterrupted operation;
- risk assessment.

AzScienceCERT (CERT-Computer Emergency Response / Readiness Team) service has been established In order to ensure information security risk management [7]. The main objective of the service is to ensure high-level management of information security risks [8]. To this end,

AzScienceCERT assists the users to detect and prevent the incidents aimed at disturbing security, and informs the users. AzScienceCERT service realizes collection, storage and analysis of statistical data related to the spread of malicious programs and network attacks on AzScienceNet e-science network platform. For the fulfillment of the objectives, AzScienceCERT cooperates with other similar groups and national authorities operating in Azerbaijan as well as with the foreign groups and organizations dealing with the processing of information security incidents. Obviously, CERT centers, including national and international networks linking these centers, are functioning in advanced countries in ICT. They hold exchange of experience and form knowledge databases. Taking into account that the spread of cyber attacks, threats, information warfare manifestations turn into a real danger, Azerbaijan has to be represented in international organizations to establish its adequate system of counter-measures. Therefore, on May 31, 2011, *AzScienceCERT* team was registered and accredited in TI (*Trustel Introducer*), affiliated with TERENA (Trans-European Research and Education Networking Association). Its main duty is to create the trust infrastructure between European CERT centers. TI service deals with CERTs' registration, accreditation and certification. TI provides a range of services to accredited CERT, such as access to specific information materials and warning systems; the usage of the particular database and the registration of incident objects in these databases; the participation in the events intended for members only; encryption and e-signature infrastructure for the information exchange of during the processing of incidents, and so forth. Accordingly, international cooperation is of particular importance for the prevention of information security incidents and responding to them in the global information infrastructure. For this reason, integrating into *TI* and similar international infrastructures, *AzScienceCERT* team gains opportunities to effectively cooperate with the partners from around the world.

The measures taken to ensure the safety of the services offered by *AzScienceNet* has significantly increased the quality of these services, and the efficiency and reliability of their usage [9].

Priorities to ensure the safety of e-science

E-science safety embraces ensuring its sustainable performance within the allowable deviations and deliberate impacts aimed at undermining the normal operation. E-science protection is characterized by its broad boundaries. Hence, its security can be exposed to both internal and external threats. On the other hand, formation and development of e-science poses new threats and dangers to its security. This is primarily due to the introduction of new technologies. Therefore, the above-mentioned reasons, requires a complex approach to ensuring the security of e-science. Solution of the complex issues shown in Figure 2 should be considered for the effective protection of e-science.
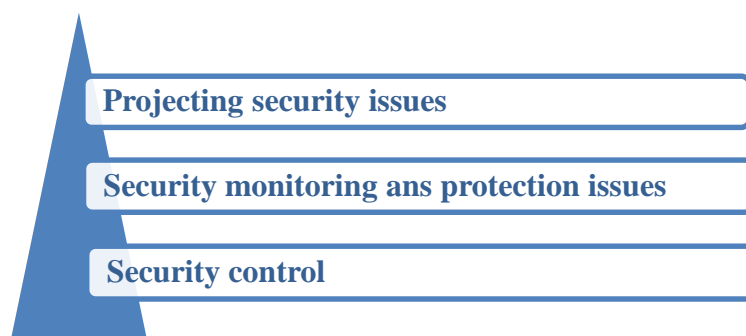

Figure 2. Complex issues of e-science protection

Review of these issues is separately provided below:

Security issues of e-science projecting:
- projecting the network and computing infrastructure in accordance with safety requirements;
- safe configurations options for hardware and software of mobile devices, computers, work stations and servers;
- safe configurations options for network devices (firewalls, routers, switches, etc.);
- application of security software;
- inventorying authorized and unauthorized devices and software;
- restrictions and supervision of network ports, protocols and services;
- defining protection border.

E-science safety control and protection issues:
- authority access control;
- wireless access control;
- monitoring the usage of administrative privileges;
- malicious software protection;
- data protection;
- consideration of backup opportunities.

E-science safety management issues:
- maintenance, monitoring, audit, and analysis of relevant journals;
- preparation of the report on monitoring and control;
- response to the incidents and their control;
- continuous assessment and removal of threats;
- application of the tests and training teams;
- holding trainings in information security assessment skills and studying vulnerabilities.

Solution of all abovementioned issues that ensure effective organization and implementation of e-science security protection take into account the followings:
- establishing practical protection based on the knowledge obtained as a result of examination and prevention of security threats;
- giving priority to the measures to ensure protection of the most dangerous threats;
- common indicators for the assessment of the effectiveness of security measures to specify and prompt adoption of the necessary adjustments;
- performing continuous diagnostics and maximum automation of protection for the assessment of the effectiveness of available security measures.

Conclusion

Security of e-science, which is emerging as a segment of E-Azerbaijan, is an important component of the national security system. This is multidisciplinary, complicated and urgent issue. Explored e-science components and presented security mechanisms prove it once again. As an example of the AzScienceNet, the work done in this area is of great importance and should constantly be developed within the framework of the issues solved in the e-science.

References

1. Alguliyev R.M., Fataliyev T.Kh. E-science as a part of e-government building // proceedings of the 1st Republican scientific-practical conference on "Problems of E-government building", Baku, Dec. 4, 2014, pp. 5-7.
2. Fataliyev T.Kh., Imamverdiyev Y.N. Information security problems in e-science // 1st Republican scientific-practical conference on "Problems of information security", Baku, May 17-18, 2013, pp. 113-115.
3. Law of the Republic of Azerbaijan on "National security", June 29, 2004, http://www.e-qanun.az
4. Critical Security Controls for Effective Cyber Defense, http://www.sans.org/critical-security-controls
5. http://www.azsciencenet.az
6. Alguliyev R.M., Imamverdiyev Y.N., Nabiyev B.R. Analysis of network security monitoring methods // Information Technologies Problems, Baku, 2014, No 1, pp. 60-68.
7. http://www.sciencecert.az
8. Alguliyev R.M., Imamverdiyev Y.N. Information security incidents, Baku, "Information Technologies" Publishing House, 2012, p. 219.
9. Alakbarov R.G. et.al. Security issues of AzScienceNet Internet services // proceeding of the 2nd republican scientific-practical conference "Multidisciplinary problems of information security" dedicated to the 150th anniversary of the International Telecommunication Union, Baku, May 14, 2015, pp.119-122.