

## Problems in Ensuring the Information Security of Society\*

*Vassil Sgurev\*\* , Rafael Jussupov\*\*\**

*\*\* Institute of Information Technologies, 1113 Sofia*

*\*\*\* SPIIRAN, Saint Petersburg*

One of the most complex problems, retarding the society informatization speed, is the necessity for priority ensuring of the national security – social, economic, ecological and military-strategic – in the receiving and processing of valuable, confidential and secret information in state and private enterprises, in state authorities, in bank and stock-exchange infrastructure [1].

Information security will denote the status of protection of society information environment, providing its formation and development with respect to the interests of the citizens, the organizations and the state [2].

The social-economic consequences from the wide application of computers in material production and the society practice have caused a number of problems concerning the information security, such as:

- Protection of the property rights of the citizens, the state and the economic subjects possessing their own information in conformance with the requirements of the civil, administrative and commercial right. These property rights include the protection of the corresponding secret data as well as of the intellectual property.

- Maintenance of complex offices for automation and informatization, that will provide the necessary physical safety of the people, of the ecological environment and of the most valuable material and property achievements by their continuous and correct functioning.

- Defence of the citizens rights and freedom, guaranteed by the respective legislation.

The problems of protecting the property rights on certain information occur due to the necessity of ensuring the proper functioning of the administrative-managing, social and economic mechanisms during the wide informatization of the material production and the society practice, which leads to the information conversion into a property object, i.e., into an object of stock-monetary relations.

The aims of protecting the information in computer networks and systems can be defined most generally in the following way:

---

\* The research presented has been done in conformance with the international cooperation between Institute of Information Technologies at BAS (Sofia) and SPIIRAN (St. Petersburg), contract No 360012.

- Constraining the embezzling, the losses, the illegitimate destruction, distortion, the illegitimate modification, the illegal copying, blocking, outflow and other interventions on information and information systems;

- Preserving the completeness, the validity and the integrity of the information in the corresponding files and programs for its processing, created by the owner or a person, authorized by him;

- Preserving the possibility to direct the procedures of information processing and use depending on the conditions, established by the possessor of the information or a person, authorized by him;

- Ensuring the constitutional rights of the citizens to preserve their personal and confidential information stored in data bases;

- Protecting the rights of the authors of software information products, used in information systems.

The problems and purposes above mentioned lead to a large amount of different problems and requirements towards modern information technologies, which implies the necessity for development of methods and means for information protection, as well as the design of efficient systems for information security (SIS).

When evaluating the current status of SIS in society, analyzing the efficiency of the realized activities and predicting the efficiency of some future actions, it is necessary to account the following most important facts and circumstances:

In all the components of national security – political, economic, military, juridical, ecological, etc. – the weight of the corresponding information factors continually increases. The quality of the information, its validity, actuality and completeness depend not only on the quality of the decisions accepted by the authorities. The information-psychological influences, invoked by the mass media activity can cause an atmosphere of tension and instability, can provoke social, national or religious conflicts and disorders, leading in this way to destructive sequences for the democratic development of society. The illegal embezzling, use or distortion of business (bank, commercial, statistical) information leads inevitably to great economic losses. The level of the information technologies determines the status of modern secret services, of the radio-electronic battle, the control of the armies and the precise aiming of the weapons, which on its turn resolves the settlement of military conflicts. Some purposeful information activities can lead to hardly overcome obstacles for the equal in rights cooperation of the democratic world countries. The information interactions influence to a significant degree the educational processes and personality formation and can provoke inadequate social or criminal behaviour of a group of people or of separate persons, causing physical, material or moral damages to the citizens. All this implies the necessity of paying particular attention to the dangers against national security, resulting from uncontrollable processes in the information sphere.

As a rule SIS are developed on the basis of the following main notions:

a) The objects of information security include the information resources, despite of the information content, representing a state secret or being with restricted access, a commercial secret or any other confidential information, and also open, accessible information, as well as the ways for its storing.

b) The systems that are generating, distributing and using the information resources consist of different classes of information systems with different purposes – libraries, archives, data bases, means for telecommunication, information technologies, scientific-technical and service staff.

c) The information infrastructure, involving different centers for information processing and analysis, channels for information exchange and telecommunications, mechanisms providing the efficient functioning of the telecommunication systems and networks,

including systems and means for information protection.

d) The information spread by the mass media, which influences the view of life, the political concepts, the moral values, the social and individual behaviour of people, etc.

e) The rights of the citizens, the state and the organizations to receive, distribute and use information, protection of the confidential information and of the intellectual property.

The information security of the objects in all the main notions above mentioned creates conditions for reliable functioning of the state and public institutions, as well as the formation of a properly functioning democratic society.

The complete classification of the dangers for the information security and their sources is impossible to be done. Some of them may be outside the country. The inner sources of danger involve the illegal activity of improperly registered organizations or economic structures in the area of the information sphere, as well as the irregular activity of some state organs, leading to the violation of the legal rights of the citizens and organizations. There are some involuntary faults of the regulations defined for information acquisition, processing and transmission; unintentional errors of the information systems personnel; failures of the technical means and random errors in the realization of the software in information and telecommunication systems – all this influences also negatively the information security.

In order to provide the information security at all the levels of material production, services and public practice as a whole, it is appropriate to realize efficient activity connected with the formulation of a concept about information security, which must esteem the following aspects:

1. Organizational-juridical insurance of the information protection:
  - Legal regulating and organization of the activities providing information security;
  - Methodological, organizational and standard technical documents and manuals in information technologies area;
  - Organizational activities and procedures assuring the information protection in computer systems.
2. Protection of the information against illegitimate access:
  - Main presumptions in the protection against illegitimate access;
  - Formalized models of such a protection;
  - Systems for access distinction.
3. Information protection in telecommunication channels:
  - Architecture of the information protection at the level of sample models of the open systems interaction;
  - Algorithms and protocols for encoding in the computer systems, cryptosystems with secret and open keys;
  - Algorithms and protocols realizing the functions of a digital sign in computer networks and systems.
4. Protection against information outflow through the channels due to side electromagnetic emissions:
  - Methodology for protection against information outflow due to side electromagnetic emissions;
  - Protection against information outflow achieved with the help of computer tools improvement;
  - Objective means for information protection.
5. Information protection against computer viruses and other dangerous influences along the channels of software distribution:

- Types and ways of distribution of the destroying programs (viruses);
- Juridical and organizational procedures for protection;
- Software-hardware methods and means for protection.

6. Protection of programs and valuable data bases against illegal copying and distribution.

7. Coordinating of the activities for information security in conformance with the requirements of the International Standard Organization.

8. Evaluation of the efficiency of the information security systems (SIS):

- Stating of the general system aspects in the design of SIS;
- Generating an appropriate class of SIS functional structures;
- Development of the problem for estimating the efficiency of SIS and the information, entering it;
- Development of methods for the evaluation of SIS.

The above mentioned does not cover all the aspects of information security in society.

These problems possess to a large extent some national specifics also and that is why their development requires the study of various experts and specialists in the country. They have to be integrated in working teams, where the information security problems must be complexly discussed and developed.

## References

1. Raikov, A. N., S. V. Ulyanov. Fuzzy modeling of support decision as intelligence technology in the control of computing social-political object. - In: Proc. of the Intern. Conf. on Application of Fuzzy Systems, ICAFS'94. Tebriz, Iran, 17-19 Oct., 1994, 281-284.
2. Smolian, G. L., D. S. Chereskhin. Democratization of Russia and the Information Security. "Informatization Problems", No 2-3, Moscow, 1995, 15-18 (in Russian).

## Проблемы обеспечения информационной безопасности общества

*Васил Стурев\*, Рафаел Юсупов\*\**

*\*Институт информационных технологий, 1113 София*

*\*\* СПИИРАН, Санкт Петербург*

(Резюме)

В статье информационная безопасность рассматривается как "состояние защиты информационной среды общества", обеспечивающей его формирование и развитие в интересах граждан, организации и государства.

В общем виде сформулированы цели защиты информации в компьютерных сетях и системах. Даны ряд особенностей, возникающих при обеспечении информационной безопасности на разных уровнях – в неправительственных организациях, в обществе и в государственных структурах.

Приведены ряд требований к системам, обеспечивающим информационную безопасность на разных уровнях общества и государства.