Some Problems of the Security of Country's Information Space

Giorgi IASHVILI
Msc., Department of Information Technology, Faculty of Exact and Natural Sciences at Ivane Javakhishvili Tbilisi State University, GEORGIA

Abstract

Cyber-security is the concern of every country. Recent events have demonstrated once again that this is a particular challenge to Georgia. Georgia appeared not ready for cyber-attacks on its information space performed in August 2008.There are a lot of threats to the information space. In general, the information threat may be defined as such an event occurring in the information communication network at a certain moment and a certain stage that resulted in an adverse effect on the information. The information threats are diverse. They are distinguished by their origin, location, character, form and other criteria.

Introduction

You cannot imagine the functioning and development of modern society without information and information flows. Economics, education, social spheres, industry, agriculture, science – all types of human activities depend on the quality of information used, its completeness and reliability, and its operativeness and forms. Hence, the issues of formation, application and protection of information resources by using novel information and communication technologies deserve special attention.

Moreover, the viability of each country is determined by the quality of collection, processing, saving, use and transmission of information, proper technological schemes and – information - communication policy. All these factors can be represented as a complex organizational – engineering information system, in which information - communication technologies are realized. This involves hardware, software, mathematical, methodical, legal and other support.

Cyber security is a challenge for all countries. Recent events have demonstrated that this problem is still pressing for Georgia. Georgia appeared not ready for cyber attacks on its information space performed in August 2008.

Those events revealed that the information - communication networks existing in the country were unprotected and unstable against cyber attacks and other threats. The quality of cyber security in both governmental and other organizations was inadequate and did not correspond to the requirements of International Standards.

It should be noted that ensuring of the cyber security is a global problem and the country that does not pay due attention to it risks to face serious problems.

Basic Cyber Threats to the Country

Analyzing the period before the war occurred in 2008 and the post-war experience, we can say that the Georgian Government, defense and security services, state bodies and large commercial entities could face the following threats:

1. falsification of websites and IP addresses in the Internet;

2. hacking of SQL databases;

3. stealing of passwords, codes, IDs and other data;

4. destructive viruses;

5. destruction of networks and servers;

6. breaking-off of the international Internet communication;

7. unauthorized accessibility to important information for enemies or terrorists;

8. covert control over ICT and Web resources of state, defense, security, commercial and other bodies.

It is noteworthy that, when they discuss the problems of country's national security, many specialists consider defense, political, social, economical and ecological security, but they give less attention to informational security (or it is not taken into consideration at all), whereas just the security of country's informational space is one of basic elements of the national security, representing an important condition of normal functioning of the country.

For our country, as well as for many other countries, the creation of the network of informational support and its security is directly associated with national security. The existence and development of our country would be impossible without information security.

To emphasize the importance and topicality of the security of country's informational space, it is enough to mention that, in as far back as 1983, the document of the Department of Defense of the USA titled ``Trusted Computer System Evaluation Criteria`` was published. In it the definition of system security was introduced. This document is de facto standard for computer security today. This standard is known for the specialists in the field of information, communication and computer network security as The Orange Book (owing to the color of its cover). It is interesting that network security classifications were established according to The Orange Book.

Historical Aspects of Information Security

Let us touch on the history of origination and development of the information security. The need for information security occurred immediately after origination of information communication means. People guessed that there may be some people who would wish to distort or destroy information sources or information transmission facilities. In 1816, when radio and electro communication facilities became available, a new stage in the development of information security began. There emerged the possibilities for protection of information by its encoding and subsequent decoding. The invention of radar and hydro-acoustic aids allowed them to affect engineering systems by using radio-electronic interfering devices. At the beginning of the computer era it became possible to solve the problems of information security without physical access to and contact with the equipment. When first information computer networks were built up, the problem of management of network resources arose.

The work on the problems of information security especially developed after building up of global information-communication systems and application of space facilities for this purpose. Actually, in the 80-ies of the 20th century a number of countries began working on the doctrine of state security which compromises the informational space security as one of its basic components.

In the period when primitive information carriers were used, the protection of information was performed by various organizational ways, which involved limitations on the access to information carriers and severe punishment for disclose of secrets. According to Herodotus, in as early as the 5th century B.C. encryption of information was used for its security. Codes appeared in ancient times in the form of

cryptograms. The Spartans had a special mechanical tool that allowed them to write secret letters and messages in a special way. Julius Caesar used a special alphabet for similar purposes. In the Middle Ages and the Renaissance times many famous people worked on ciphers.

The change-over to engineering facilities of information transmission brought about accidental influence on the information: equipment faults, operator's errors etc., which could cause the detetion or distortion of information or create the conditions that would allow unauthorized access to information. With further development of communication facilities and their wide application, there appeared more opportunities for unauthorized access to information.

About Hackers and Crackers

The development of complex automated control systems and computer networks, which involve automated entering, saving, processing and display of information, made the information security even more topical.

Today, information processing industry has reached a high level of development, the access to the global communication networks from a personal computer is a routine event, and there appeared ``electronic`` money (credit cards), which set the stage for misappropriation not only of information, but also of large amounts of money. Hence we can say whith reasonable confidence that just the scientific and technological progress engendered computer malefactors so called hackers and crackers.

The hackers is a computer hooligan who is well aware of computer engineering and who breaks in the computers of other users without authorized access. By using telephone lines and personal computers, the hackers connect to data transmission networks which are connected to large economical, scientific and technological, financial and other computer centers.

You can find information about cyber crimes in special literature. For instance, on October 5, 2002, the Italian police revealed a group of hackers who had performed computer attacks on thousands of computer centers and networks, including the ones belonging to the Pentagon and NASA, were violated. The cites in Great Britain, China, Sweden, Australia and Latin America were attacked. The group began its attacks during the Big Eight Summit held in Italy in 2001, which was accompanied by demonstrations of antiglobalists which this group belonged to.

According to the report of the Information Technology and Risk Company Ernst & Young, in Russia and the countries of the former Soviet Union they do not conceive weak points of the information systems operating on their territories and real risks creating danger to them. The damage caused by the hackers to only separate developed countries makes up millions dollars.

Viruses – a Kind of Informational Threats

In recent years a new kind of computer crime has become common. This is the creation of so-called computer viruses, which are special programs launched by a special signal. The virus could spread immediately after contacting with other program. Such ``infection`` of programs with viruses may pose different consequences: from a mere joke to deletion of complex programs that could not be restored, which would cause irreparable damage.

In 1980 computer virus Turman occurred. Harmful programs have the features characteristic of biological viruses: a small size, the capabilities of spreading rapidly, propagating and introducing into an object (its infection), and, in general, having an adverse effect on the system. That is why we call such programs computer viruses.

The computer viruses are small-size executable or interpretable programs which are capable of spreading and self-propagating in automated systems. The viruses can change or destroy software or data

stored in an automated system (AS), a network or a computer. In the process of propagation, the viruses are capable of self-modifying.

The appeal of the operational system (OS) for the viruses is determined by the following factors:

· how widely OS is used;

· the absence of incorporated antiviral tools;

· comparative autonomy;

· service life.

A wide spread of viruses, serious adverse consequences caused by them generated a need for the development and application of special antiviral aids and methods of their use.

The antiviral aids are used for the following purposes:

· revealing of viruses in AS;

· blocking of programs – viruses;

· elimination of the consequences caused by viruses.

It is desirable to reveal viruses immediately after their introduction or at least before they begin their destructive action. It should be noted that there is no antiviral tool capable of revealing of all possible types of viruses. The elimination of adverse effects of viruses is generally performed in two directions:

1. Elimination of the virus.

2. Restoration (if necessary) of file memory areas.

For the struggle with viruses, software and hardware aids are used. Their operation is performed in a certain sequence and combination.

The following methods of revealing the viruses are known:

· scanning;

· revealing of changes;

· heuristic analysis;

· use of resident guards;

· vaccination of programs;

· hardware and software protection against viruses.

Despite the fact that the experts note that the interest to the creation of viruses has mitigated, this problem is still topical.

It should be noted that, besides the criminals threatening different countries, there are quite respectable companies terrorizing everyone who uses e-mail. These are spammers sending useless information (commonly advertisements) to e-mail users without any requirements. This useless information, so-called spam, is a real calamity for the Internet.

The unauthorized use of information may have serious consequences, including political ones involving launching of wars.

One more aspect of the problem is noteworthy – this is users' irresponsibility. The experts point to many ways of the unauthorized access to the information in data processing systems: scanning, copying and alternation of the data; entering of false programs, commands and messages, connection to communication

lines and channels; the use of faulty programs and devices; memory scanning and receiving and recording of induced signals, the use of hardware failures, operator's and software errors etc.

Cryptography as a Way of Information Protection

We could not speak about the security of informational space if we do not touch on the subject of cryptography.

Cryptography, i.e. encryption (masking or hiding information), is one of the most natural manifestations of the man or, in general, of a living organism. Cryptography (in Greek "Kryptos" means secret, and "Grapho" - writing , drawing) is the practice and study of hiding information.

In general, the protection of information by its cryptographic conversion consists in the conversion of information components (words, letters, sentences, numbers etc.) by using special algorithms, engineering solutions and key codes. For reading the coded information, an inverse operation of decoding is used.

Cryptographic methods are among the most widely used ones which improve significantly the security of data transmission in computer networks and of the transmission of the data stored in memory.

As was mentioned above, for coding usually an algorithm or a device that operates by the given algorithm is used. The process of coding is controlled by the variable-key code, which provides the representation of original information when the same algorithm or device is used. Knowing the key, it is easy to decode reliably the transmitted text. However, if you do not know the key, it is actually impossible to perform this operation (even if the coding algorithm is known).

It should be noted that the ``cipher`` is an Arabic term emerged in the XV century.

The block diagram of coding/decoding is shown in Figure 1.

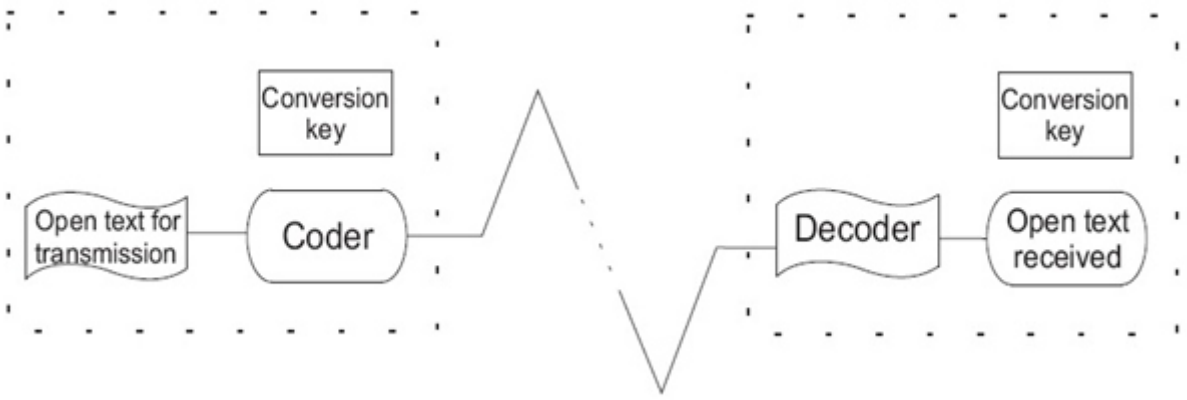


Figure 1. Block diagram of encoding/decoding

Codes and ciphers had been used long before the invention of computers. There is no noticeable difference between coding and encoding.

Currently the term ``coding`` is used when we speak about digital representation of information during its processing by hardware, whereas ``encryption`` means the conversion of information with the aim of its protection against the unauthorized access. Today some methods of encryption are well developed and recognized as classical.

It is well known that in ancient Schumer, Egypt, China, Greece and Rome secret writing and other encryption means were widely used.

Julius Caesar (the I century B.C.) used his own secret cipher. That is why today in scientific literature one of cryptographic algorithms is called by his name (Caesar algorithm).

It is also well known that in the Middle Ages and the time of the Renaissance many prominent people (philosopher Francis Bacon, mathematicians Francois Viet, Giordano Cardano, John Wallis and others) worked on secret algorithms. Comparatively complex methods of encryption were invented.

In as early as the end of the XV century, in the Arabic encyclopedia much attention was given to cryptography.

Among other issues, the statistical method of cryptographic analysis of algorithms (i.e. crypto analysis) was described for the first time. The statistical method implies that separate symbols, in particular separate letters-signs of a natural language, have different probabilities. Even today the consideration of frequency values of letters-signs represents one of the ways of algorithm decoding.

General classification of the methods of cryptographic conversion is shown in Figure 2.

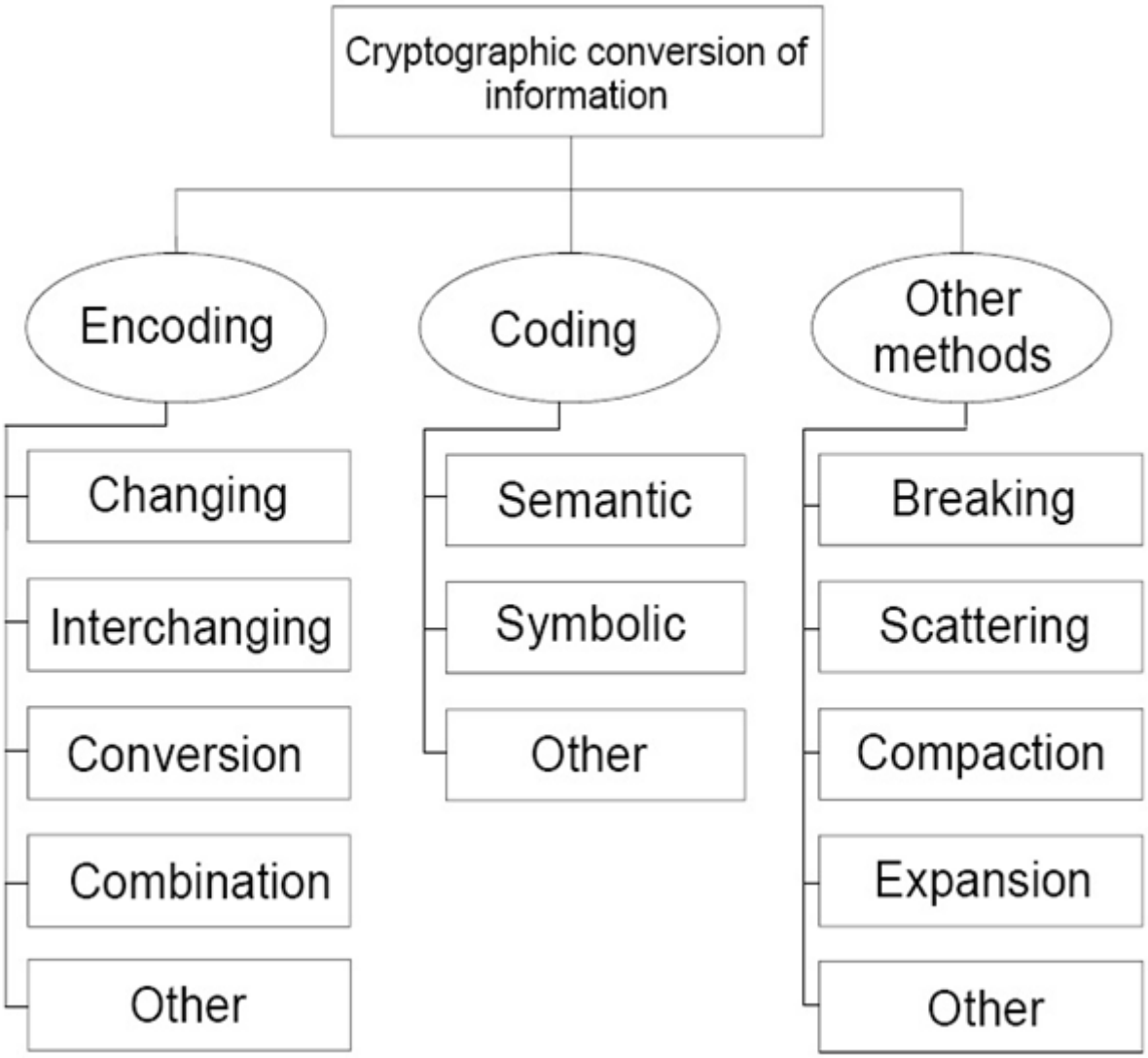


Figure 2. Classification of the methods of cryptographic conversion of information.

On the Security of Information Computer Networks

The control and protection of the security of information communication and computer networks is of great importance for every country. That is why international cooperation in this field has become a common practice, as it is almost impossible for a country to cope with cyber threats by itself. One of the ways of

international cooperation are Computer Emergency Response Teams (CERT) operating in different countries. These teams are intended for observation of the events happening in computer networks and response to any incident (failure, disruption etc.) with the aim of elimination of its cause. In general, in computer networks different incidents such as DDOS Attack, Virus, Malware, Spam, Worm, scanning of IP-ports etc. could occur. It is noteworthy that, like the Interpol, CERTs exchange information and help different countries to eliminate the threats coming out from these countries. In Georgia such CERT has been established at Scientific Educational Association ``Grena``.

Besides, a new project on coordination and management of Computer Emergency Response Teams has been launched. This project is financed by the NATO, and its objective is to establish CERTs in the Caucasian Region, and their training and support. In this project, along with CERTs from Georgia, Armenia and Azerbaijan, CERTs from Ukraine and Poland are involved. It is envisaged to include Kazakhstan, Turkmenistan and other countries into this project in the future.

It was mentioned above that, in general, governmental bodies, defense, law and other institutions, large commercial companies of all countries, including Georgia, may face such cyber threats as viruses, stealing of codes and passwords, destroying of servers, etc.

There are many other technological and electronic types of threats, but the above-listed ones completely correspond to the conditions of our country, which appeared unprepared for recent cyber attacks. It became evident that country's information communication networks were unprotected and unstable. Moreover, it appeared that the problem of information security was not solved adequately, and our information security fell behind International Standards.

Types of Informational Threats and their Sources

Generally, the informational threat can be defined as such an event occurred at a certain time and stage that influenced the information transmitted via the information communication system. The threats are distinguished by their origin, location, type and many other criteria.

There is an interesting approach to the classification of informational threats, according to which they exert an adverse effect on information. According to this approach, the threats are divided into four groups:

1. Informational
2. Software-mathematical
3. Physical
4. Organizational

It should be emphasized that the identification and classification of the informational threats and the investigation of their causes is not only topical, but also essential when developing the measures, devices and systems for protection of information security.

The classification of informational threats represents the grounds for the basic direction of information protection. In our opinion, for development of the means and systems of information space security, it is necessary to study thoroughly the informational threats and to take into consideration their properties. For this purpose, it is essential to formalize and classify the threats of all types and origin. Hence, we paid much attention to characterization of the threats and to the requirements to be posed.

There are different approaches to the classification of threats. Different authors use different criteria for such classifications. Among them are such criteria as a type, a degree of malicious intent, a location, an origin, a cause of threat occurrence, etc.

By their origin the threats can be random and intentional, whereas the conditions of threat occurrence

may be divided into two groups: objective and subjective.

The sources of threats may be:

1. People

2. Engineering facilities

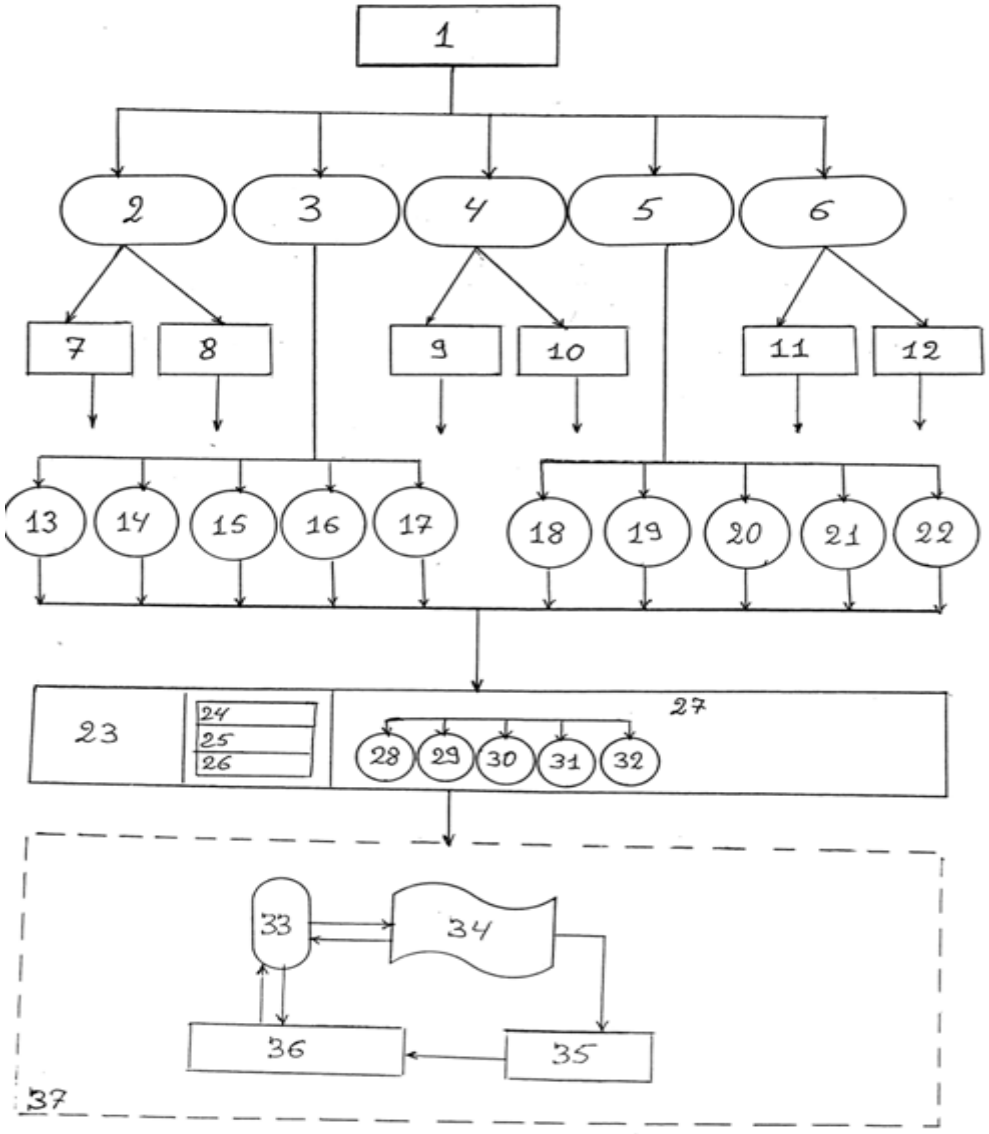
3. Software, algorithms, models

4. Information processing technologies

5. The environment.

By the type of damage, there are distinguished violations of the integrity, of the logical structure, of the sense, of the confidentiality and of the copyright.

All the above-listed threats should be characterized separately. According to the proposed classification, we elaborated the block diagram of the threats to information, communication and computer networks and their protection (Fig. 3). It can be used for working out the program of the security of country's information space.



-

Figure 3. Block Diagram of information space threats and security:

1. Threats;
2. Threat origin;
3. Threat type;
4. Origin environment;
5. Sources;
6. Threat occurrence conditions;
7. Random threats;
8. Intentional threats;
9. Internal threats;
10. External threats;
11. Objective threats;
12. Subjective threats;
13. Violation of the physical integrity;
14. Violation of the logical structure;
15. Violation of the sense;
16. Violation of confidentiality;
17. Copyright violations;
18. People;
19. Engineering facilities;
20. Models, algorithms, software;
21. Technology;
22. The environment;
23. Security measures, facilities, systems;
24. Protective systems;
25. Assaulting systems;
26. Preventive systems;
27. Security level;
28. Weak;
29. Medium;
30. Strong;
31. Very strong;
32. Extremely strong;
33. People;
34. Information;
35. Information technologies;
36. Engineering facilities.
37. Information environment.

Means and Systems of Information Security Protection

The information security is the information space state, and the information protection is the action aimed at preventing unauthorized access, disclosure, use, disruption, modification or destruction of information and providing its integrity, confidentiality and reliability.

Using the system approach, the issues of the security of country's information space can be grouped in the following way:

1. Scientific, normative and legislative bases.

2. The structure and objectives of services (departments, authorities, etc.) providing the information security.

3. Organizational and technological methods and measures.

4. Software and hardware aids.

The objective of realization of the information security of some entity (a country, a region, an industry, a department, etc.) by the system approach is the establishment of the information security system for building up and efficient operation of which it is necessary:

· to elucidate specific requirements essential for protection of the given entity;

· to take into consideration the national and international legislation;

· to use the experience accumulated in the practice of building up such systems.

Basic technical and organizational requirements making part of information security policy must be specified.

· From the outset there must be appointed the subdivision(s) responsible for the realization of the information security system, and the limits of its (their) responsibilities must be defined.

· Suitable algorithmic, software and hardware methods and means of information security must be implemented and introduced.

· The management system must be used in the operation of the information security system.

· Monitoring of the operation of the designed and introduced system must be performed, and, if necessary, appropriate modifications and corrections should be made regularly.

From the above it follows that the process of realization of the information security system is continuous and that it cyclically returns to the first measure at each alternation or correction.

At this point it is worth noting that there should exist the national doctrine of country's security which, in concert with national and international standards, and methodical instructions, will comprise the unity of normative-methodological documentation for the security system.

By their purpose, the information security systems may be protective, assaulting and preventive (Fig. 4). By the security level, five categories of security systems are distinguished: weak, medium, strong, very strong and extremely strong (Fig. 4).

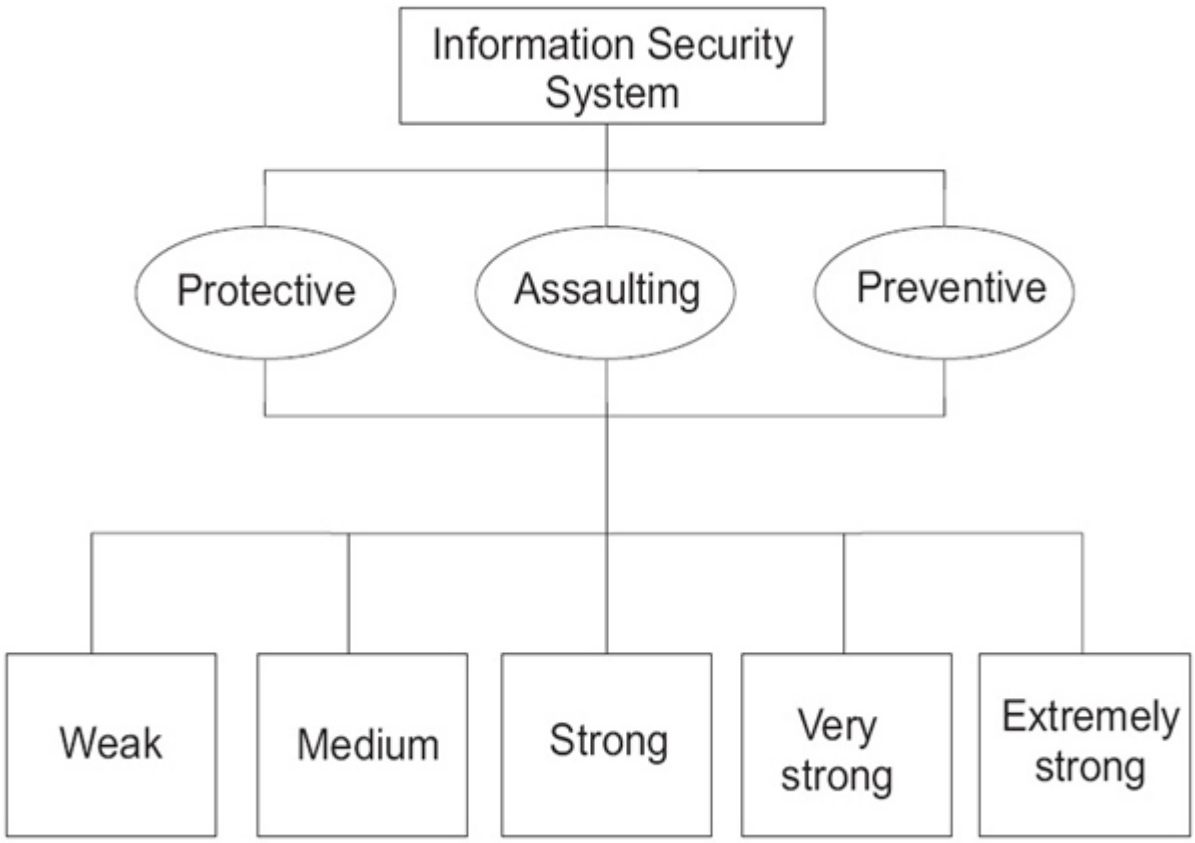


Figure 4. Types of information security systems.

The following directions of creating the information security system are also worth noting:

· protection of the objects of the information security system;

· protection of information processing and programs;

· protection of communication channels;

· protection of hardware;

· neutralization of side electromagnetic radiation;

· security system management.

Let us separate out a few types of software and hardware methods and means providing the information security from a variety of these:

1. Means protecting the system against unauthorized access.

2. Network monitoring systems.

3. Information Flow Simulation and Analysis Systems (CASE).

4. Protocol analyzers.

5. Antiviral aids.

6. Internetwork screens.

7. Cryptographic means.

8. Continuous feed systems.

This list can be continued. It is evident that all these means demand detailed characterization and definition of the requirements to be posed on them. Only after doing so, we can use them in the information security system.

From the standpoint of information security, the information that is used and disseminated in the society can be divided into two large groups:

· the information open for general use;

· the information of limited access.

The information open for general use is, for instance, the information spread by mass media and the Internet. Governmental acts, Parliament's public decisions, statistical data, etc. belong in this category.

The information of limited access may be:

· state secrets;

· commercial secrets;

· private information and other.

It is necessary to distinguish not only information, but also the sources of informational threats. Three groups of such sources are distinguished:

a) The sources of threats which are conditioned by subject's action (such sources are called anthropogenic). Here are meant those subjects whose actions may damage the information security. These actions could be random or intentional (planned beforehand).

b) The sources of threats conditioned by engineering facilities (so-called technogenic threats). The sources of this type are dependent on the characteristics of engineering facilities and thus require special

attention. Such sources of informational threats may be internal and external.

c) Natural sources of threats. This group of sources comprises the force majeure states (natural calamities, earthquakes, floods, etc.). Such sources could not be predicted, and thus the measures against such sources must be always in action. The objects must always be protected against external sources of threats.

The general classification of the sources of threats is shown in Figure 5.

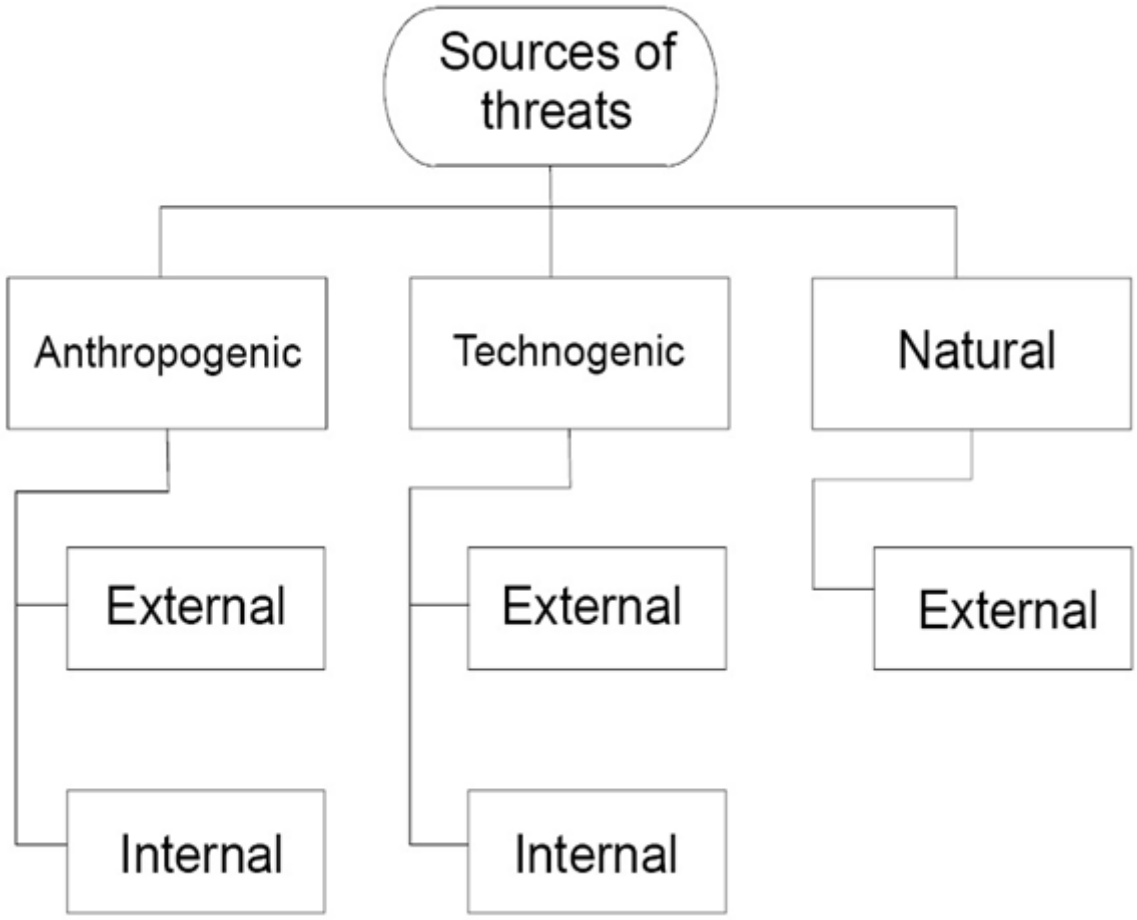


Figure 5. Sources of threats.

During our work on the subject, we found out that different authors gave different versions of classification of informational threats, and yet some points have not been taken into consideration. For instance, in our opinion the threats should be distinguished by their periodicity and action duration as well. By this criterion, the threats may be single-action and long-term; they also can be of periodic (cyclic) action.

Let us mention one more point that is not considered for in available classifications. There may be such consequences of the action of informational threats that it will be impossible or almost impossible to repair completely the damage caused (or it will be possible to restore partly the damaged information).

There are also the threats which cause the damage which is relatively easy to repair. All the above-mentioned is taken into consideration in our version of classification of threats shown in Figure 6, whereas Figure 7 represents the specific classification of anthropologic sources of threats.

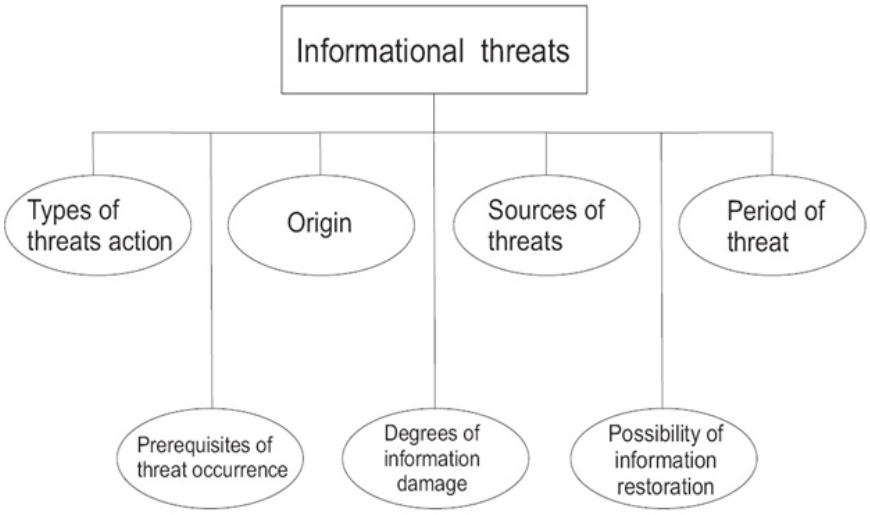


Figure 6. New classification of informational threats

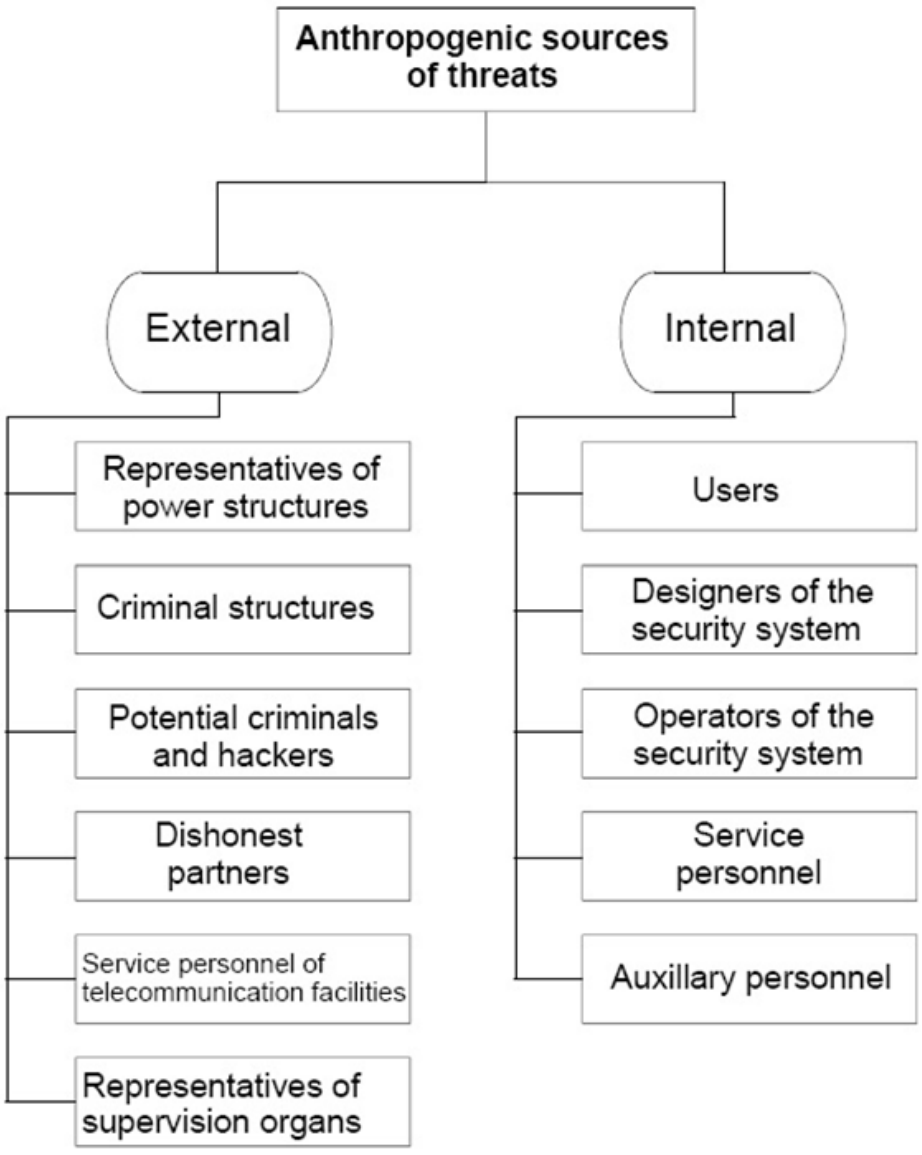


Figure 7. Anthropologic sources of threats.

The essence of the information security consisted in the protection of information by using software, hardware and firmware.

It should be noted that by engineering facilities were meant electric, electromechanical and electronic devices. These devices were divided into electronic and physical security aids. By security firmware were meant the aids incorporated into the automated system or the aids that were connected to the automated system via interface. Physical aids are the devices which are realized as self-contained units or systems (security signaling and observation systems, special door locks, guard nets, etc.)

Security software aids are computer programs intended for protection of information.

They used to assume that computer programs were primary security means. It was thought that these aids would operate more efficiently if they were incorporated into inter-system software. Hence, at first the software security mechanisms were realized being incorporated into operational systems or databases (for instance, IBM OS/360). The practice showed that the reliability of such mechanisms was insufficient.

The next stage of expansion of the framework of software security and improvement of its efficiency consisted in the differentiation of users' access to databases. For this purpose, identification of all users and databases to be protected was performed. The correlation between users' identifiers and data identifiers was established, and an algorithmic procedure was developed for determination of the loyalty to user's demands. One of the systems with such a security mechanism was system MULTIC. Three-year testing and a comprehensive study of this system revealed the mechanisms allowing circumventing the differentiation of access.

Conclusions

The analysis of the literature and other information sources in the scope of the Project convinced us once more of the topicality of the problems of the security of country's information space. Every day we feel that we are dependent on cyber space, and that the protection of this space, its security has become one of main and important functions of the state.

President Barack Obama devoted one of his speeches to the security of national infrastructure of the American Internet (May 29, 2009). In particular, he mentioned that the year before (i.e. in 2008) we had an opportunity to watch the war of the future; when the Russian tanks invaded Georgia, cyber attacks petrified governmental sites.

The study of the relevant materials showed that the information-communication sphere and the definition of basic requirements and directions call for long-term work (2-3 years) and involvement of a group of high-skilled scientists and specialists.

Nearly one-year work on the Project allowed us to define those basic directions the development of which is essential for working out the concept (strategy) of the security of country's information space.

It should be emphasized once again that the study of informational threats, the determination of the area of their action and their specific features is an essential condition for selection of the aids providing the security of country's information space and creation of security systems.

Just bearing in mind the above-mentioned, in our report we focused our attention on the sources of threats, the conditions of their occurrence and types of threats. When studying these topics, we did not find such a classification of threats that would completely represent all probable threats. We introduced new classifications of threats, which we had not found in the materials studied:

1. Duration of threat action

2. Possibility of information restoration

3. Degree of damage caused.

(These classifications are shown in Fig. 6)

Besides, one of the merits of our work is that we presented a block diagram of informational threats and information security (Fig. 3).

Our work on the Project of the World Federation of Scientists appeared to be very interesting. It laid the foundation for the work on the problems of the security of country's information space. A lot of information was collected from the literature and electronic resources. This topic calls for further investigation, which would allow us to analyze and compare investigations carried out in this field in different countries, and to reveal their advantages and drawbacks. We believe that further work on this topic will be useful and will yield interesting results.

References

http://www.hmso.gov.uk
http://www.nist.gov
http://java.sun.com/security
Щербаков А.Ю. "Современная компьютерная безопасность. Теоретические основи. Практические аспекты" – М. Книжный мир, 2009;
Петренко С.А., Курбатов В.А. "Политики информационной безопасности" – М. Компания АйТи, 2006;
Галатенко В.А. "Стандарты информационной безопасности" – М. Интернет-университет информационных технологий, 2006;
Петренко С.А. "Управление информационными рисками" - М. Компания АйТи, ДМК Пресс, 2004;
Шаньгин В.Ф. "Зашита компьютерной информации. Эффективные методы и средства" – М. ДМК Пресс, 2008;
Лепехин А.Н. "Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты" М. Тесей, 2008;
Лопатин В.Н. "Информационная безопасность России: Человек, общество, государство; Серия: Безопасность человека и общества" М. 2000;
Родичев Ю. "Информационная безопасность: Нормативно-правовые аспекты" – СПБ, Питер, 2008;
Бармен Скотт. "Разработка правил информационной безопасности" - М. Вильямс, 2002;
Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. "Информационная безопасность открытых систем";
Безопасность информационных технологий (Випускается МИФИ. Является рецензируемым научным журналом включенным в список ВАК);
Вопрпсы защиты информации;
Проблемы информационной безопасности. Компьютерные системы. (Является рецензируемым научным журналом включенным в список ВАК);
Jet Info - Информационный бюллетень;
Журнал "Защита информации. Инсайд"