International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:3, No:10, 2009

Institutional Aspects of Information Security in Russian Economy

Mingaleva Zhanna, Kapuskina Tatiana

***Abstract*—**The article touches upon questions of information security in Russian Economy. It covers theoretical bases of information security and causes of its development. The theory is proved by the analysis of business activities and the main tendencies of information security development. Perm region has been chosen as the bases for the analysis, being the fastest-developing region that uses methods of information security in managing it economy.

As a result of the study the authors of the given article have formulated their own vision of the problem of information security in various branches of economy and stated prospects of information security development and its growing role in Russian economy[1]

***Keywords*—**security of business, management of information security, institutional analyses.

I. Introduction

IT is necessary to pay close attention to the issue of information security for a number of reasons. Firstly, post-industrial society is characterized by a high level of information and telecommunication technologies that are intensively used by ordinary people, businesses and government authorities.

Secondly, as international experience shows, high technologies, including information and telecommunication ones, contribute a lot to social and economic development of many countries in the world; moreover, providing people with a guaranteed free access to information is a sign of democracy and one of the most important tasks that states should do to develop human rights and freedoms.

Thirdly, in information society both individuals and the main social institutions (government bodies, enterprises, etc.) are becoming increasingly dependent on information and telecommunication technologies as the technologies make them more efficient in doing their functions, running their business and providing goods and services. As a result of growing interconnection, information systems and networks, being the basis of information society infrastructure are exposed to various threats which cause new problems in providing security. Information has become a valuable asset for all social groups. Failures to protect important data effectively endanger security of individuals, states and businesses [1]. Information protection is becoming a top priority for individuals, businesses and nations and it concerns each member of society.

Zhanna Mingaleva is with the Faculty of Economics, Perm State University, 15, Bukireva street, Perm, Russia (corresponding author to provide fax: +7-342-239-66-85, e-mail: mingal1@psu.ru).

Tatiana Kapuskina is with the Faculty of Economics, Perm State University, 15, Bukireva street, Perm, Russia (corresponding author to provide fax: +7-342-239-66-85, e-mail: tkapuskina@yandex.ru).

People are beginning to realize that it is impossible to provide information security only with the help of technologies. An effective solution to the problems does not only depend on government and law-enforcement bodies; most of all it requires coordinated actions of the whole society. Government bodies, businesses, organizations, individual owners and users of IT industry products have to be aware of factors threatening information security and potential illegal actions; they all have to realize their responsibility and take measures to increase IT security. For this purpose modern society has to create a culture of information security, which is part of information culture of society [2].

However, tendencies in the development of high technologies and the level of information security in Russia show that the situation in this area is not quite good.

II. Data and statistics used in the study

Finding the main problems in the area of information security and making recommendations to raise it was based on data of foreign and Russian statistics as well as relevant analytical reviews.

The international study of information security in 2008 conducted by Ernst and Young company have revealed that more and more companies understand the importance of information security in protecting their image and trademark and enhancing their business reputation. According to the study in which 1.4 thousand executives were interviewed, most of them think that incidents concerning information security cause more damage to a company's reputation, image and trademark than to its revenues and financial condition. 85% of respondents pointed at severe damage caused to a company's reputation and trademark and 72% of respondents said a company can have financial losses. Only 68% of respondents think that regulating bodies can take appropriate sanctions.

That's why companies are increasing investment in information security. More than 2/3 (67%) of respondents said that their companies had already introduced measures to protect personal data. In spite of the economic decline in the biggest countries 50% of respondents said that their companies are ready to increase their outlay on information security and only 5% of them plan to cut it.

Russian studies of this topic show that the most serious problem concerning information security over the last years has been data leaks. Types of leaking information have been the same over the last few years (see Table 1).

TABLE I
CRIME STRUCTURE IN THE SPHERE OF INFORMATION IN RUSSIA IN 2007-2008

Type of crime	2007	2008
Theft of personal data	93	95
Theft of know-how	-	2
Commercial secret leak	6	2
State secret leak	1	1

Table 1 shows that wrongdoers in Russia are most interested in personal data which are also in great demand in European countries. Moreover, the number of this type of crime is growing year by year. In 2008 95% of crimes in the sphere of information were personal data thefts with 93% in 2007. The rest three types of crimes (commercial and state secret leaks and thefts of know-how) account for less than 10%; in 2008 commercial secret leaks accounted for 2% and state secret leaks accounted for 1%.

Study of channels of technical leaks of confidential information has revealed the following. Technically data may leak through the following main channels: through a corporate mail server, through an Internet channel when using public mail systems or Web-services for installing files, through wireless connections (WiFi, Bluetooth), a printer and mobile carriers. The list can also include cameras, smart-phones, DVDs, IM systems (Skype), iPod devices. Most planned leaks of valuable information happen through the Net (48%) and mobile computers (37%) [3].

A more detailed structure of channels of technical leaks of confidential information is given in Fig.1 [4].

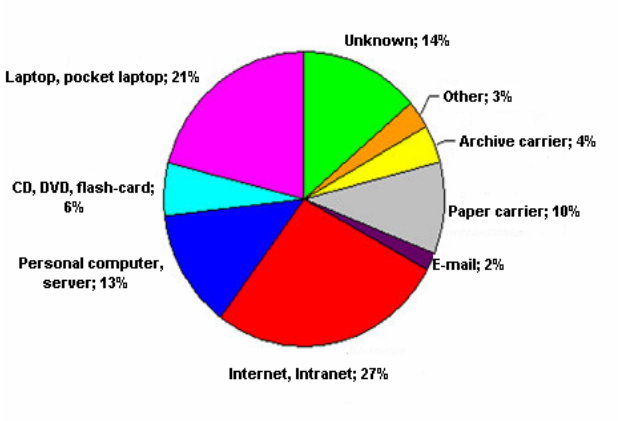

Fig. 1 Channels of confidential information leaks in 2008

The evolution of different channels through which information leaks happen is shown in Table 2.

TABLE II
MAIN CHANNELS OF CONFIDENTIAL INFORMATION LEAKS IN RUSSIA

Channels	2007	2008
Theft or loss of laptops	39	31
Accidental publication of confidential files in the Net	-	-
Hacker attacks	-	-
Internet (including local networks)	25	27
Leaks through desk computers	13	13
Leaks through paper documents	7	10

To see what types of organisations are most exposed to attacks and where most information leaks happen, use Table 3.

TABLE III
STRUCTURE OF ORGANISATIONS EXPOSED TO INFORMATION SECURITY THREATS IN RUSSIA

Type of organisation	2007	2008
Businesses	58	50
Educational establishments and non-profit organisations	20	31
Government bodies	22	18

As we see in table 3 businesses as well as government bodies are beginning to protect themselves from confidential information thefts more effectively. At the same time the level of information protection in educational establishments and non-profit organisations is getting lower.

Taking the data into account it is possible to outline the main ways to fight confidential information leaks and improve information security in the country in general.

There are the following types of damage caused by valuable information leaks: damage to national security; damage to a company; damage to individuals.

As for sectors of Russian economy, studies show that the most vulnerable of them, are:

- the system of government statistics;
- financial system;
- Information and registration automated subdivision systems of federal bodies of executive power making it possible for the society and the state to function in the economy.
- Book-keeping systems in companies regardless of their form of ownership;
- Systems which collect, process, store and transfer financial, exchange, tax and customs information as well as information about external economic activity of a state and different organisations regardless of their form of ownership.

III. Improving the Information Security System in Russia

Today practically everyone admits that the only way to provide information security is to take a complex approach combining measures at four levels: legislative, administrative, procedural, programme-technical and economic [9].

A. Legislative regulation of information security in Russia

Nowadays in Russia the main normative documents concerning information security are as follows.

Firstly, the Doctrine of information security in the Russian Federation released dated 09.09.2000, № Пр-1895, where information security is defined as the condition in which national interests combining individual interests with state and social ones in the area of information are protected [5].

Secondly, a number of Federal laws of the Russian Federation concerning information security such as Federal law № 85-ФЗ dated 04.07.1996 “About participating in the international information exchange”; Federal law №149-ФЗ

dated 27.07.2006 "About information, information technologies and information protection"; Federal law of the Russian Federation №152 "About personal data" dated 15.03.2008. A special feature of the third law is that it states the requirements which organizations dealing with personal data have to follow. Organizations have to make all the arrangements by January 1st 2010. By the end of this year they need to revise all the data they have and select personal ones. Then the organizations need to classify the personal data (PD) and provide places for their storing, processing and moving; they also need to take organizational and technical measures to protect them. Staff have to be instructed on how to deal with such information and the organizations have to enter into an kind of agreement with personal data owners who will allow them to use the data. In addition, PD owners need to register in Russian Communication Monitoring. Many experts on information technology admit that the law requirements are not quite precise. First of all, the law lacks a unified standard of PD protection, which would establish concise benchmarks of how to execute the law items. That's why certain organizations use their own branch standards, for example, СТО БР ИББС 1,0 or Payment Card Industry Data Standard (PCI DSS) for banking [6].

Thirdly, the Strategy of creating information society in the Russian Federation №Пр-212, dated 07.02.2008.

Fourthly, a number of Standards concerning information security such as ГОСТ ИСО/МЭК 27001:2005 "Information security management system" where information security is defined as an act of keeping information confidential, full and available, the definition can also describe such information as authentic, copyright and reliable [7]. Other standards are ГОСТ ИСО/МЭК 17799:2005; 15408; COBIT; SOX; ITIL; BASEL II; SANS SCORE; ISACA, etc.

Fifthly, regional laws concerning information security such as the target programme in Perm region "Electronic Prikamie 2008-2010 (see the appendix).

Finally, some firms follow international standards concerning information security, for example, BS 17799:2005 – British standard BS 7799 Part 1; BS 7799 Part 1 – Code Practice for Information Security Management; ISO/IEC 27001:2005 – "Information Technologies – Methods of Providing Security – Information Security Management Systems – Requirements" and others.

However, such a multitude of laws and standards together with the absence of unified legal measures of regulating information security in Russia created a situation when IT do not contribute to the development of Russian economy; moreover, they sometimes make the development difficult. There are several reasons for that but the main one is that the very nature of the information sphere of social life is misunderstood. As a result, instead of improving this promising but poorly developed sphere, the government is mainly aimed at regulating it [8].

B. Administrative Aspects of Providing Information Security in Russia

A key factor of upgrading the information security system in Russia is its organisational structure. Today the basic elements of the information security system in Russia are as follows:

1) government and management bodies of the Russian Federation and its regions that are in charge of providing information security within their competences (for example, the Committee headed by the president of the Russian Federation that controls information policy, the Federal agency of government communications and information headed by the president of the Russian Federation);

2) government and interdepartmental committees and councils specialising in problems of information security (for example, the State Technical Committee of Russia);

3) structural and intersectoral divisions responsible for protecting information of government and management bodies as well as structural divisions of companies using in their job data classified as state secrets or specialising in information protection;

4) research, project and design organisations which provide information security (for example, the Centre of complex security headed by the Special Scientific-Productive Organisation "Eleron", Russian Science and Research Institute of intersectoral information);

5) educational establishments training and retraining employees to provide information security (for example, specialised centres for information protection)[9].

The main aims of the information security system in Russia are as follows:

1) observing constitutional human rights and freedoms to receive and use information, providing conditions for Russia to improve spiritually, keeping and strengthening moral values, patriotism and humanism in the society, the country's cultural and scientific potential;

2) providing reliable information about the government policy of the Russian Federation for the Russian and foreign public, stating its official attitude to socially important events in Russia and abroad, as well as giving people a free access to open government information resources;

3) developing modern information technologies and the domestic information industry, supplying the domestic and world markets with products of the industry; saving, securing and using domestic information resources effectively;

4) protecting information resources, Russian information and telecommunication systems (both complete and incomplete) from an illegal use;

Regarding these components the government creates long-term and short-term tasks for their internal and external policies concerning information security.

C. Procedures

An important element of an information security system is designing and approving standards.

The main aim of information security standards is to provide the grounds for producers, customers and experts on IT products to interact with each other. Each of these groups has its own interests and its own understanding of the information security problem. That's why information security standards are designed to help all these parties interact with each other. Here are the most common characteristics of information security standards which are important for each of the three parties: the standards have to be universal, flexible, guaranteed, achievable and topical.

In addition, any standard makes a company's activities more transparent for its counterparts as it says that certain parameters of the company meet the standard. By

standardising the company makes its structure quite transparent for its partners and clients; this in its turn assures them that the information they give to the company (personal data, business information, etc.) is properly protected [10].

Any information security system has to cover the following aspects [11]:

1) awareness. Participants need to understand the importance of securing information systems and networks and know what they can do to increase the security;

2) accountability. Participants are responsible for securing information systems and networks as their role requires it. They need to review and evaluate their policy, measures and procedures on a regular basis and they need to check if these are properly used;

3) response. Participants have to collaborate in preventing, finding and responding to incidents concerning information security. They need to share information about threats and factors making information vulnerable. In some cases it requires international information exchange and cooperation;

4) ethics. As information systems and networks are widely spread in modern society, participants need to take into account each other's interests and admit that their actions may harm other participants.

5) democracy. Security has to be provided in accordance with values of a democratic society which include the freedom to exchange thoughts and ideas, free information flow, confidentiality of information and communication, proper protection of personal information;

6) risk assessment. All participants have to assess risks regularly as it allows them to discover threats; risk assessment has a good base to cover key internal and external areas such as technologies, human factors, methods that are used and a third party's services influencing security; risk assessment gives an opportunity to determine the highest possible level of risk; it also helps to select appropriate means of control which allow to regulate risks of potential damage to information systems and networks regarding the type and importance of protected information;

7) designing and introducing security measures. Participants have to regard security as the most important thing when planning, designing and using information systems and networks;

8) security management. Participants have to take a complex approach to manage security based on regular risk assessment which covers all activities of participants and all aspects of their operations;

9) reassessment. Participants have to review and reassess the security level of information systems and networks and change their policy and security measures taking into account new threats and changes of the old ones.

It is necessary to go through the following stages when creating a system of information security (see Fig.2).

Stage I (in Fig.2) includes developing, adapting and unifying standards concerning information security at all levels of the economic system – from the corporate level to the national one.

Stage II includes structuring information and determining the level of its confidentiality (i.e. classifying information resources according to their functions and choosing their owner, determining a confidentiality level for each resource and for each owner.

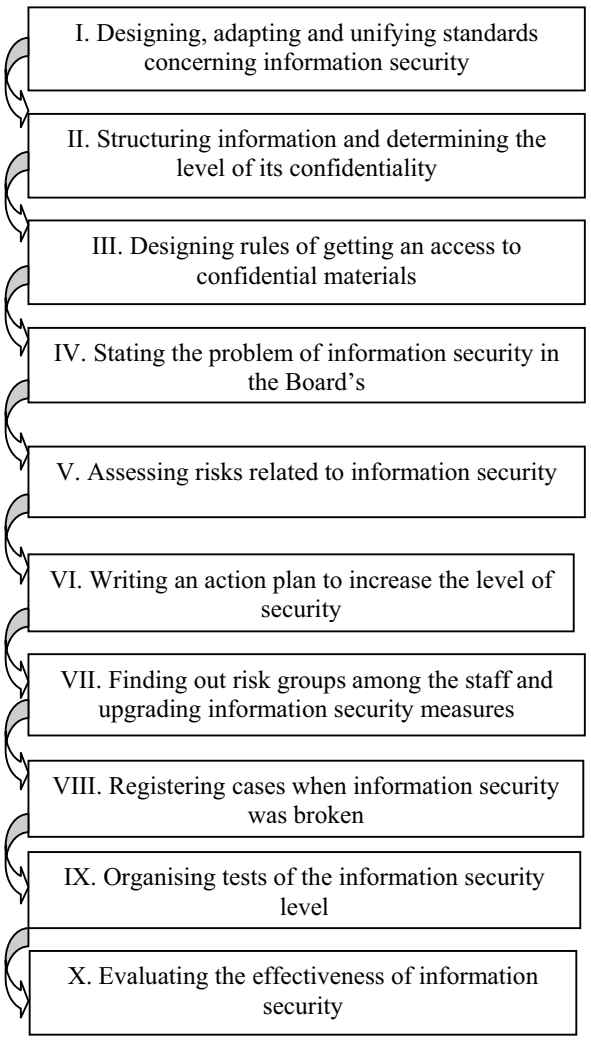

Fig. 2 The main steps of building an information security system

At stage III measures are taken to regulate an access to the materials: an access to the materials is fixed in the order of business. It is necessary to fix it as quickly as possible as it influences the company's competitiveness.

Stage IV covers discussions of information security issues at various meetings: at the Board's meetings, at meetings of shareholders, the Security Council meetings, etc. All company managers have to take part in managing information security; regular discussions of that kind will help to make the management process continuous.

At stage V experts evaluate information security risks (most often they use risk-oriented approach which is about discovering and evaluating information security risks typical of the company; today this is the most effective methods);

Stage VI includes writing an action plan to raise the level of information protection which states who, when and where will take certain measures to prevent or minimise a certain kind of threats and what resources will be used for that.

At stage VII risk groups from a company's staff are formed and a suitable system of motivating managers and staff is introduced.

At stage VIII cases when information security is broken are registered and that provides statistics that is important in managing information security.

At stage IX the information security level is tested, for example, all measures related to preventing and registering

risks as well as providing an access to the information are checked to be correct.

Stage X includes assessing effectiveness of the information security management system.

The process of building an information security system is continuous and cyclical.

Taking a complex approach to building security systems will help do the following: to prevent confidential information leaks; to protect applied information servers and to ensure they function

properly; to provide a safe access to the Net protected from virus attacks and spam; to protect systems of an electronic document exchange; to build a system of centralised information security monitoring and management of a corporate network; to arrange safe information interaction with distant offices and mobile users; to get a safe access to all information systems of an organisation; to ensure the information is full and available [12].

The main component of complex information security is a security policy, i.e. a number of rules and regulations determining ways of processing information in a given system.

Designing a security policy includes the following stages: determining information categories, processed by separate subsystems; determining the structure of the system, its vulnerable elements, risk factors, a type of wrongdoer, choosing a security policy. Means of protection are the most powerful mechanism of protecting the system from risk factors [13].

As information security risks are essential only for a few organisations, there are three approaches to manage them. For non-critical systems where information assets are supplementary and the information level is not high (which is characteristic of most modern Russian companies), the necessity to evaluate risks is minimal. Such organisations need only a basic level of information security, determined by existing norms and standards, the best in-house practices and experience, as well as other companies' experience. However, the existing standards presenting basic security requirements and mechanisms always make it prominent that it is necessary to assess risks and economic benefits from using certain control mechanisms to choose the most appropriate ones for a given organisation.

For critical systems where information assets are not the main ones but the information level of business processes is very high and information risks can have a significant influence on basic business processes, risk evaluation is necessary but it is enough to use only informal qualitative approaches paying special attention to the most critical systems.

When an organisation's activity is based on information assets and information security risks are the main ones, they need to be assessed with the help of a formal approach and quantitative methods.

For some companies several kinds of assets can be vital at the same time, when, for example, a business is diversified or when a company makes information products and then both human and information resources can be equally important for it. In this case it is best to have a thorough risk assessment to decide which systems are the most vulnerable and which ones are the most useful to run business operations and then to give the systems a detailed evaluation. As for the rest of non-critical systems, it is enough to apply a basic approach and make decisions concerning risk management based on experience, experts' reports and best practices.

D. Economic aspects

An important aspect of building an information security system is its economic effectiveness. It is important to take into account the fact that total costs of creating and making a security system work, total costs of maintaining security and the level of information environment security are interconnected. All the costs of increasing a company's security level amount for total security costs and are calculated with the help of the following formula:

$$Tsc = Cpm + Cc + Ccl,$$

where

Tsc – Total security costs;

Cpm – costs of preventive measures;

Cc – control costs;

Ccl – costs of compensating losses (internal and external ones).

Changes of the level of information environment protection cause changes of components of total costs and therefore, their sum – total security costs.

The interconnection between all security costs, total security costs and the level of information environment protection in a company has a form of the function (see Fig.3).

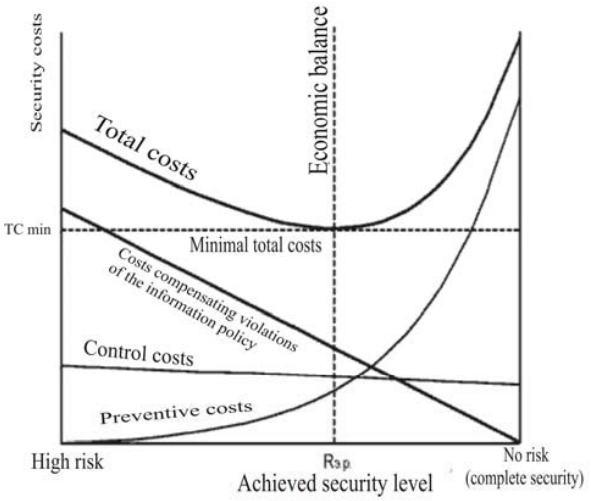

Fig. 3 Interconnection between security costs and an achieved security level

Fig. 3 shows that the achieved security level is measured in the categories "High risk" and "No risk" (complete security). On the left side of the graph we can see that total security costs are high mainly because losses compensating breaks of a security policy are high. Costs of security system service are very low.

If we move to the right of the graph the achieved security level will increase (information risks will decrease). It happens due to the increase in the number of preventive measures serving the protection system. Thanks to preventive measures, costs compensating violations of the information policy fall. As the graph shows, expenditures on losses fall quicker than expenditures on preventive measures

grow. As a result total security costs decrease. Control expenditures change slightly [14].

As for risk assessment methods, today there is a sufficient number of widely used methods which proved to be good for information security risk assessment and management. One of such methods is OCTAVE, designed in Carnegie Mellon University to be used inside a company. To assess risks it is necessary to use a consequence of internal workshops appropriately organised. There are three stages of risk assessment preceded by a number of preparatory measures which include coordinating the timetable of the workshops, assigning roles, planning, coordinating actions of the project group members.

IV. Conclusion and Recommendations

1. As the analysis of the information security level in Russia has shown, in the nearest future significant changes of information-technological and human basis for the country development are unlikely to happen. For the changes to happen it is necessary to combine efforts of the government, businesses and society. The main special feature of information security is that the government has to play a special role when defining priorities in the sphere of information.

2. It is impossible to increase information security of an object without a system providing information security (SPIS). To build and use the SPIS effectively, the following needs to be done:

* determinig information protection requirements specific for the given object of protection;
* taking into account requirements of national and international legislation;
* using practices (standards, methodologies) of building similar systems providing information security;
* choosing divisions responsible for putting the system into practice and maintaining it;
* distributing responsibilities for following the requirements among the divisions;
* stating general regulations, technical and organisational requirement making up information security policy for a protected object;
* observing requirements of the information security policy by introducing appropriate programme-technical means of protecting information;
* implementing the information security management system (ISMS);
* organising regular checks of the effectiveness of the system providing information security and, if necessary, reviewing and upgrading the information security system and the information security management system [15].

That's why it is necessary to upgrade the information security system to protect information effectively and to meet new requirements of constant updating information systems.

3. Information security management has to meet information security standards, including international ones.

4. Information security risk management is a business task, set by an organisation's leadership as they realise information security problems. The task is to protect the business from real threats to information security. The level of realising the problems indicates several levels of maturity of an organisation which correlate to some extent with maturity levels determined by COBIT and other standards.

At the very first stage an organisation is not conscious of information security problems; its IT specialists take fragmentary measures on their own responsibility to provide information security.

At the second stage an organisation distributes responsibility for information security among its staff members, it attempts to take actions managed by the Board and to introduce some processes of information security (IS) management.

The third level is characterised by a process approach to information security management described in standards. IS management system becomes so important for the organisation that it is regarded as a necessary element of the organisation management system. Still the IS management system is not perfect because the system lacks its basic element – risk management processes.

Organisations which understand IS problems to full extent are characterised by their formalised approach to information security risk management; the approach covers documented processes of planning, implementing, monitoring and upgrading.

Thus, the effectiveness of information security risk management depends on a full risk analysis and evaluation as well as on the effectiveness of management decisions and control over their implementation [16]. Risk management helps to answer the question – where it is beneficial for a company to take risks and where it is dangerous.

Appendix

"Electronic Prikamie 2008-2010" is the region target programme which has been worked out to the order of the Perm region government. The main tasks of providing information security stated in the programme are [17]:

1) to create a model of threats in the sphere of information security;
2) to make a list of information objects (information systems, databases, etc.) containing or processing information vital for Perm region;
3) to make a list of potential users of the registered information objects;
4) to create a model of threats to the information objects mentioned above. This has to be done by finding out:

a) potential sources of ill-intentioned actions concerning the given information objects;
b) possible ways of implementing attacks on the part of threat sources;
c) vulnerable sides of the given information objects;
d) types of information objects being attacked;
e) a possible way of attacking information objects;
f) what regulation concerning security of information objects is violated.

Perm region authorities expect to find out which threats to information security are put into practice. The model of potential threats to security objects coming from internal and external sources influences activities concerning internal and external security.

References

[1] Kizza J.M. Computer Network Security. Springer US, 2005.
[2] Malyuk A.A. Forming Information Security Culture of the Society//Pedagogy. 2009. № 3.
[3] The Main Channels of Data Leaks [Electronic resource]. – http://www.webplanetnews.ru/security/id_20021/

[4] Ibid
[5] Doctrine of Information Security in the Russian Federation 09.09.2000. №ПР-1895; The Strategy of Creating Information Society in the Russian Federation (approved by the president of the Russian Federation V. Putin 07.02.2008.,№ Пр-212).
[6] See: Federal Law dated 04.07.1996. №85-ФЗ "About Participating in the international Information Exchange"; An Internal Enemy [Electronic resource]. http://www.osp.ru/ nets/2009/ 04/8386859/.
[7] The National Standard of the Russian Federation "The system of Information Security Management" (ГОСТ ИСО/МЭК 27001: 2005).
[8] Grinyaev S, Lokotsov I, Kazakevich O. Information Security of Russian Banks//Computer week. 2004. № 9 (423).
[9] Information Gurarantee of Information Security [Electronic resource].http://www.library.ru/1/kb/books/ businesslibs/is_system.php.
[10] International Standards of Information Security [Electronic resource]. http://nvisionsecurity.ru/analytics/17/
[11] Resolution of UN General Assembly A/RES/57/239 "Creating Global Culture of Cyber Security" [Electronic resource]. – http://www.ifap.ru/ofdocs/un/57239.pdf
[12] Information Security Management [Electronic resource]. – http://masu-inform.ru:8888/index.php
[13] Ryabtsev A.S. The concept of providing Information Security for Objects.
[14] Petrenko S, Symonov S, Kyslov R. Information Security: Economic Aspects//Jet Info Online. 2003. № 10.
[15] National Standard of the Russian Federation "Information Technology. Regulations of Information Security Management" (ГОСТ ИСО/МЭК 17799-2005).
[16] How to Run Information Security Risks. [Electronic resource]. – http://shop.globaltrust.ru/osnov.php?idstat= 61&idcatstat=12.
[17] The Programme of Perm Region for a Specified Purpose "Electronic Prikamie 2008-2010".