Advances in Economics, Business and Management Research, volume 171
Proceedings of the 1st International Scientific Conference "Legal Regulation of the Digital Economy and Digital Relations: Problems and Prospects of Development" (LARDER 2020)

Features of Ensuring Information Security of Institutions in the Context of the Formation of the Digital Economy

Galia Aralbayeva[1,*] Azamat Aralbaev[1] Natalia Kharitonova[1]

[1] *Orenburg State University, Orenburg 460018, Russian Federation*
[*] *Corresponding author. Email: galia5@mail.ru*

ABSTRACT
The article deals with the issues of ensuring information security of institutions in the modern conditions of the formation of the digital economy. It is stated that activation of operation of institutions in the field of informatization make it necessary to protect information from unauthorized leakage and various influences, in particular: electronic interdepartmental interaction; development of electronic document management systems; provision of services to state and municipal organizations on an electronic basis; formation of databases on the socio-economic development of the country, regions, municipalities; the data of the research centers and other organizations. The stress is made on the fact that non-compliance with information security measures and violations of security regimes can lead to unpredictable economic and social consequences. The article gives valuable information about information security measures and systems. Methods and means of organizational protection of information in institutions are defined as well as risks and threats of information loss and methods of their prevention.
Keywords*: Digital economy, information, security, information security of institutions, electronic services, threat model, probabilistic approach.*

1. INTRODUCTION

Digital technologies play a major role in the development of society. The digital economy is an economic production based on the application of digital technologies. The level of threats in computer systems increases with the constant growth of users who have access to information resources, various databases and other information stored in digital form.

There is a huge number of possible ways to protect information - legal, software and hardware, physical and other methods. The use of the methods mentioned above allows increasing the level of protection of confidential information, reducing the risk and possible losses from the actions of an attacker or other unforeseen circumstances.

The relevance of the problem is related to the emergence of new technologies, the creation of new tools and methods of automation and new programs. In such conditions there is a possibility of unauthorized use of information. That is why businesses are looking for new ways and means to protect their business and products from hackers.

Information security is designed to prevent losses resulting from violations of the integrity, availability and confidentiality of information in any form. The information security system must be implemented in full compliance with current laws and regulations on information security as well as the interests of information owners. To ensure a high degree of information security, it is necessary to constantly solve complex scientific and technical problems of creating and modernizing the means of its protection.

One should consider the list of possible threats in the process of designing a security system in an institution and therefore determine the means of protection that will be used to prevent illegal actions on information resources stored in the institution. In particular, the digital economy is associated with the sphere of providing of electronic services. The most important requirement for any institution is its own information security which has significantly worsened with the development of information technologies.

This article considers The State Autonomous Institution of the Orenburg region “Orenburg regional multifunctional center for providing state and municipal services” (MFC) to identify the features of ensuring information security. MFC provides a wide range of services based on the Decree of the Government of the Russian Federation dated 22.12.2012 No. 1376. These services include: issuance (reissuance) of a Russian passport, issuance of a certificate of federal subsidies for multiple-child families, state registration of rights of realty and property and many others.

2. RESEARCH BACKGROUND

Information security is ruled by a number of laws and regulations that should be taken into account when developing data protection tools [1-7]. Special attention in the literature is given to the problem of ensuring information security of institutions and enterprises. Thus, the authors Ignatiev, Koneev and Belyaev note that a multi-level information security system is being created in groups engaged in industry along with the security center which closely monitors organizations and individuals [8], [9]. This concept helps not only identify threats but also detect gaps in firms' security systems in a timely manner.

A number of studies indicate that most problems arise from underestimating threats which can lead to the company becoming bankrupt. Even an isolated situation of employee negligence can lead to multi-million dollar losses and loss of customer confidence. A list of current threats and methods of protection is provided [10- 12].

One of the most important modern problems is an effective protection of information since the information resource has become one of the main drivers of economic development in the modern world. Researchers note that the process of information protection is a process of interaction between threats that affect information and information security tools that prevent their impact [13- 15].

There is an opinion that countering threats should be timely and comprehensive. Sometimes information leaks can cause damage to the business months or years after it has occurred falling into the hands of hackers. Thus the protection should be comprehensive. Everything that concerns the company's activities and is not intended for publication should stay inside the company and should be protected from various attacks [16].

It is stated [17], [18] that each enterprise has computer equipment and access to the World Wide Web. Hackers skillfully connect to almost every component of this system and use a large arsenal (viruses, malware, password matching and others) to steal valuable information. The information security system should be implemented in every organization. Managers need to collect, analyze and classify all types of information that should be protected and use an appropriate security system.

2.1 Methods of Assessment

The following methods of assessment were applied and described in the present article: building a model of information flows in an institution, threat models, intruder models, a probabilistic approach to assessing risks and losses as a result of threats to information security.

2.2 Building a Model of Information Flows in an Institution.

Information is one of the most important elements of any institution. Information flow is the movement of information from one employee to another or from one department to another. The scheme of MFC information flows is shown in Figure 1.

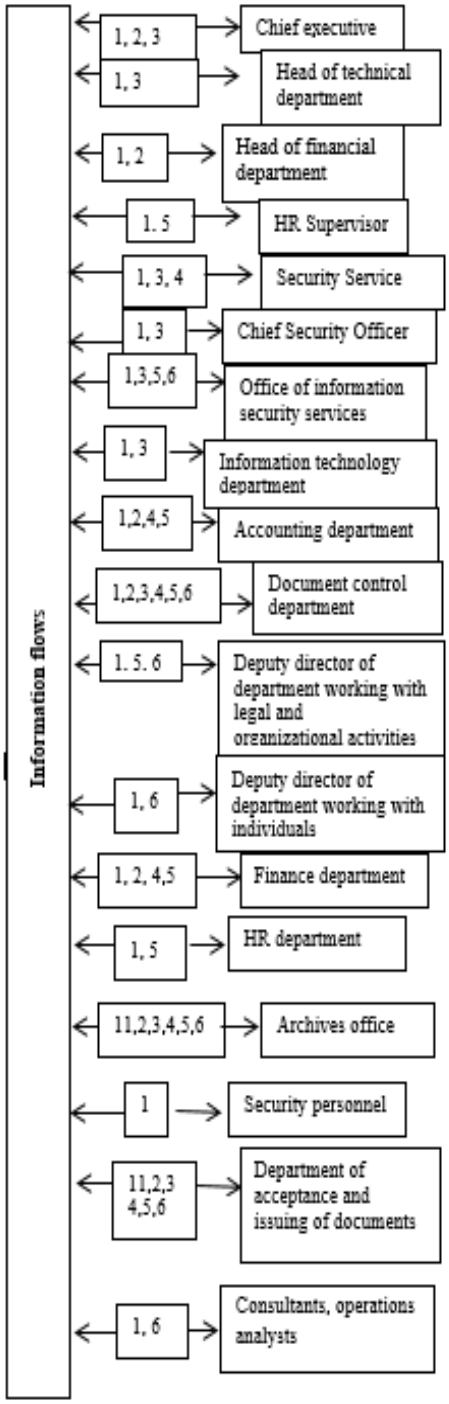

Figure 1 Diagram of information flows in an institution

The information flow diagram establishes the flow of information between departments and divisions of the institution. Information flows are integrated into the electronic circulation of information. Table 1shows the main information flows of the MFC. Table 2 represents the description of the controlled zones in the institution.

Table 1 Description of the main information flows of the MFC

Flow designation	Information flow (IF)
IF 1	Orders and instructions, reports, claims and statements
IF 2	Information about financial flows, material and labor resources of the MFC
IF 3	Information on vulnerabilities, information on access to physical and hardware-software protection tools, reports on security risks
IF 4	Personal information and reports on the client's financial flows
IF 5	Personal data of employees, salary information
IF 6	Processing of clients ' personal data

Table 2 Description of the controlled zones in the MFC

Category	Name of the zone	Functional purpose of the object's zone	Access conditions for employees	Access conditions for clients	Availability of security
2	Under observation	Temporary presence of clients and employees	Free	Free	Available
3	Registrarial	Reception of clients and employees	Free	Free with registration using ID cards	Available
4	Restricted	Contact area of employees	Using work permit pass or ID cards	Using one occasion pass	Increased security

Security zones are defined to protect the object. The institution has a system of access and control that allows minimizing the threat of violations of physical protection. Multi-zoning provides differentiated authorized access for different categories of employees and clients of the MFC.

2.3 Determining the Cost of Information Resources of the Institution

Table 3 is drawn up according to the laws of the Russian Federation [1-5] which specifies the stored information, the sensitivity label, the cost of this information, the data carrier, and the location of the information.

Table 3 Types of information that should be protected in the MFC

Information element	Sensitivity label	Cost	Data carrier	Location of the information
Accounting Department	Commercial sensitivity	3 000 000	PC, contracts, reports	Accounting Department
Staff salaries	Personal data	150000	PC, paper data carrier, reports	Accounting Department
Security policy	Confidential information	100000	PC, security services documents	Security service
Information on security	Commercial sensitivity	121 000	PC, contracts, reports	Information security

system				department / Chief Executive / Information technology department
Business plan	Commercial sensitivity	100000	PC, contracts, reports	Chief Executive, Deputy director of department working with legal and organizational activities,
Clients databases	Personal data	100000-300000	PC	Department of acceptance and issuance of documents / Archive / Chief Executive
Clients agreements	Personal data	500000	PC, contracts, reports	Accounting Department / Archive / Documents examination department
Partners databases	Commercial sensitivity	100000-300000	Web server, PC	Chief Executive / Archive / Accounting Department / Department of acceptance and issuance of documents
Partners agreements	Commercial sensitivity	500000	PC, contracts, reports	Chief Executive, / Deputy head of department working with legal and organizational activities

The price of information is set according to its value for the organization. The present paper calculates the cost information in accordance with the Criminal Code of the Russian Federation in the amount of 200 000 (two hundred thousand), Federal Law No. 152 «On personal data», article 183 of the Criminal Code of the Russian Federation, the fine for illegal collection and dissemination of information constituting commercial, tax secrecy. Article No. 155 of the Criminal Code of the Russian Federation, dissemination of official secrets of Federal law No. 125 FZ «On archival business in the Russian Federation». Taking into account the total cost of information the stored information on the MFC is 5,071,000 rubles.

2.4 Identification of the Intruder's Penetration Routes

The MFC has 2 floors at its disposal. The floor plans of the building indicate the premises allocated for clients and employees, computer network, surveillance zones, etc. The locations and areas of operation of technical security equipment, video surveillance systems and outdoor lighting, the places of cable output through which information flows can be transmitted are marked on the territory of the institution. Unauthorized entry into the institution can be carried out through windows and doors.

Possible ways of penetration of intruder are shown in Figures 2 and 3.

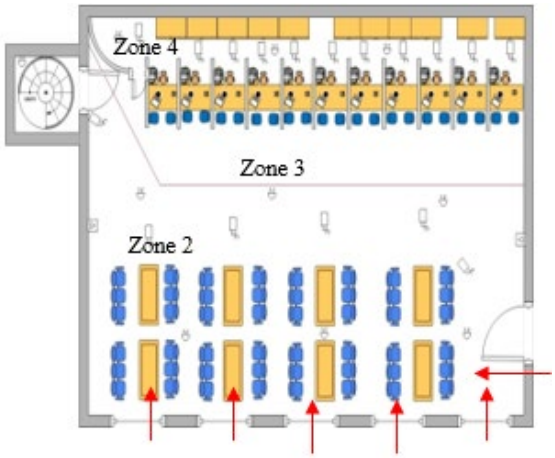

Figure 2 The ways of entry of the intruder on the first floor of the institution

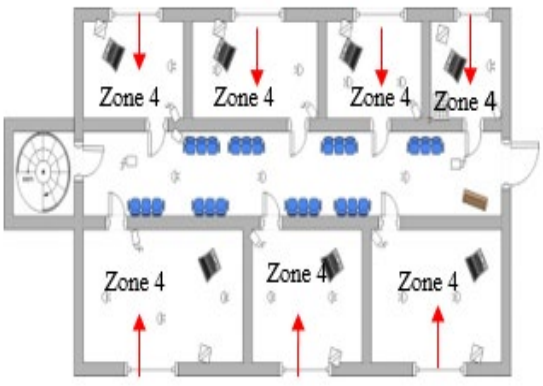

Figure 3 The ways of entry of the intruder on the second floor of the institution

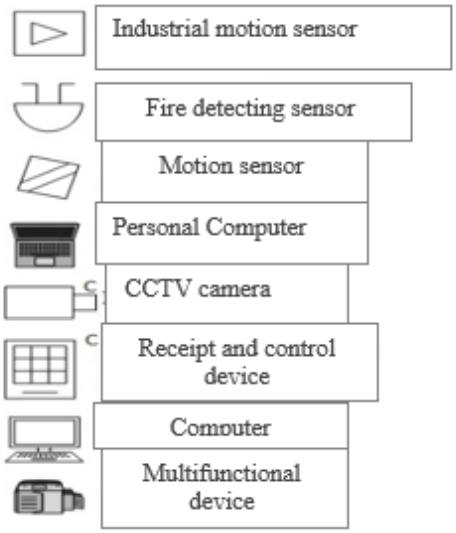

Figure 4 Designations used in Figures 2 and 3

Ways of penetration of intruder are highlighted on the object under analysis (21 way). Six of them are the following: client area, staff room, offices of the head of document circulation department, archive, human resources department, information technology department, security department.

2.5 Building a Model of the Intruder

To identify ways of protection information the intruder model is built. It is a set of characteristics of the attacker essential for the evaluation of the level of security at the research object. The main tasks of information protection are to determine the characteristics of the intruder and determine the purpose of the intruder (Table 4).

Table 4 Characteristics of the intruder

Feature of the intruder's characteristic	Characteristics
1	2
Goals and objectives	entering a protected object without causing visible damage to the object
	causing damage to the object
	deliberate penetration in the absence of hostile intent
	accidental entry
The extent to which the potential intruder belongs to the object	security officer
	employee of the institution
	client
	unauthorized person
The degree of awareness of the potential intruder about the object	detailed awareness of the object
	awareness of the object's designation, its external traits and features
	uninformed potential intruder
The degree of awareness of the intruder about the object's security system	full information about the object's security system
	information about the security system
	uninformed potential intruder
The level of professional training of the potential intruder	no special training
	special training
The degree of physical training of the potential intruder	low physical training
	average physical training
	special physical training
The level of equipment capability of the potential intruder	high
	average
	low
Method of penetration of the potential intruder into the object	breaking the lock
	destruction of walls and windows
	leaving the intruder on the object's territory until it is closed
	free access of the intruder to the object due to a temporary violation of the integrity of the building due to the influence of natural and man-induced factors or during the repair period;
	preliminary collusion of the intruder with the staff
	«bypass» of technical means of protection

Thus, four categories of intruders can be identified based on these criteria:

- Intruder of the first category – specially trained in a broad program intruder who has a sufficient experience – a professional with

hostile intentions, with special knowledge and means of overcoming various systems of protection of objects;

- Intruder of the second category – an unprofessional intruder with hostile intentions acting under the direction of another subject who has a certain training of entering a specific object;
- Intruder of the third category – an intruder without hostile intent who enters a secure facility out of curiosity or some other personal intent;
- Intruder of the fourth category – an intruder without hostile intent who accidentally violates the security of an object.

The unformalized model of the intruder is presented in Table 5.

Table 5 Unformalized model of intruder

Type of intruder	**Category**	**Training of intruder**								
		Psychophysical			Technical			Awareness		
		H	A	L	H	A	L	H	A	L
1	2	3	4	5	6	7	8	9	10	11
Internal	Employees who have authorized access to material assets	+			+			+		
	Employees who have access to financial assets	+				+		+		
	Employees who have access to confidential information		+			+			+	
	Employees who have access to the elements of protection system	+				+		+		
	Service personnel (security, engineering and technical services)		+		+			+		
External	Dismissed employee		+			+		+		
	Saboteur	+				+			+	
	Emergency services representatives			+			+			+
	Clients			+			+			+

Table 5 shows that the most dangerous potential intruders for the organization are employees who have access to information resources.

A threat is a combination of various factors that may have an adverse effect on the information resources of an institution. A threat model is a description of potential threats in an institution as well as their relevance, probability of occurrence and consequences.

The model of threats to the security of information in an institution is presented in Table 6.

Table 6 The model of threats to the security of information

Threat	**Probability of threat realization**	**The possibility of realization of threats**	**The indicator of threat danger**	**Relevance of threat**
Unauthorized access to computers	Probable	0,11 (low)	Average risk	Relevant
Theft of technical means with information stored in them	Low probability	0,1 (low)	Low risk	Irrelevant

Threat	Probability of threat realization	The possibility of realization of threats	The indicator of threat danger	Relevance of threat
Theft of data carriers	Low probability	0,1 (low)	Low risk	Irrelevant
Theft of material and financial assets	Average probability	0,17 (average)	Average risk	Relevant
Viewing information from display screens and other means of displaying it, paper and other data carriers	High probability	0,23 (high)	High risk	Relevant
Wiretapping of the phone and radio conversations	Average probability	0,09 (low)	Low risk	Irrelevant
The implementation of instrument «bugs»	High probability (0)	0,20 (high)	High risk	Relevant

2.6 Determination of Possible Losses of the Institution from the Implementation of Threats to Information Security

Probabilistic losses – losses that take into account the probability of occurrence of this threat. It is evaluated using the losses from each of the threats and the probability of these threats occurring.

We calculate the probable losses using the formula (table 7):

$R = P \times U$ (1)

R – risk, potential damage, RUB;

P – probability of threat realization;

U – losses, RUB.

Table 7 Calculation of economic losses for each threat

Threat	P	U	R
Threat of unauthorized access to the system via wireless channels	0,23	3721000	855830
Impact on information system software	0,37	871 000	322270
Information leakage via the acoustic information channel	0,14	4000000	560000
Implementing of the instrument «bugs» into the hardware system	0,09	950 000	85500
Threat of interception of data transmitted over the computer network	0,1	5071000	507100
Infection of computers with malicious codes	0,07	3821000	267470
Total:			2598170

Calculations have shown that the minimum loss experience to the institution as a result of loss of information will be 2,598,170 rubles. Therefore, it is advisable to install the necessary equipment and software or apply the necessary measures to eliminate or minimize the identified threats to information security.

4. CONCLUSIONS

As a result of the analysis of information security of institutions that provide services in digital form the following features were identified that should be taken into account when establishing security measures:

1) A significant amount of information resources, including confidential information resources that are to be protected. There is a regular database provisioning, data modification and withdrawal, data ingestion about the new clients;

2) The components of the information system including the clients of the institution and its employees are distributed at the level of the municipality, region, country, other countries, i.e. interdepartmental, inter-client and other interaction is carried out;

3) Clients and employees of the institution have joint access to information resources;

4) Information security is affected by the location of the institution, the number of floors, and the location of neighboring buildings.

Confidential information is of great interest to competing firms. It becomes the cause of attacks by intruders. Nowadays there is a need to protect information from unauthorized access, therefore the correct analysis of information flows and

identification of places where they are lost plays an important role.

Thus, in the context of the functioning of the digital economy the risk of unauthorized malicious actions to seize information is real and with the further development of digital technologies the threat of information loss is constantly growing despite all efforts to protect it. All this stipulates the necessity of thorough analysis of the experience with information security and a comprehensive organization of methods and mechanisms for protection.

It is possible to minimize or eliminate the identified security threats by taking into account the identified features of ensuring information security of an institution providing electronic services in the context of the formation of the digital economy.

REFERENCES

[1] Federal law (2004) «On commercially sensitive information» dated 29.07.2004 No. 98-FZ http://www.consultant.ru/document/cons_doc_LAW_48699/. Accessed 25 Mar 020

[2] Federal law (2004) «On archival business in the Russian Federation» dated 22.10.2004 No. 125-FZ https://base.garant.ru/12137300/. Accessed 25 Mar 2020

[3] Federal law (2004) «On information, information technologies and information protection» dated 27.07.2006 No. 149-FZ http://www.consultant.ru/document/cons_doc_LAW_61798/. Accessed 25 Mar 2020

[4] Federal law (2004) «On personal data» dated 27.07.2006 No. 152-FZ http://www.consultant.ru/document/cons_doc_LAW_61801/. Accessed 25 Mar 2020

[5] Decree of the President of the Russian Federation (1997) «On approval of the list of confidential information» dated 06. 03. 1997. http://www.consultant.ru/document/cons_doc_LAW_13532/. Accessed 25 Mar 2020

[6] SAUS ISO/IEC 15408-1–2001 (2014) Information technology. Methods and means of ensuring security. Criteria for evaluating information technology security. Part 2. Functional security requirements. http://docs.cntd.ru/document/1200101777 Accessed 25 Mar 2020

[7] The governing document of State Technical Commission of Russia dated 19.06.2002 No. 187 (2002) Information technology security. Criteria for evaluating the security of information technologies. https://fstec.ru/component/attachments/download/293. Accessed 25 Mar 2020

[8] V.A. Ignatiev, Information security of a modern commercial enterprise, OOOTNT, 2005, 448 p.

[9] I.R. Koneev, A.V. Belyaev, Information security of the enterprise, BCHV Peterburg, 2003, 752 p.

[10] M. Vergelis, T. Shcherbakova, T. Sidorina (2019) Spam and phishing in 2018, Reports on spam and phishing. https://securelist.ru/spam-and-phishing-in-2018/93453/. Accessed 25 Mar 2020

[11] Protection of information in the enterprise: sources of threats and the creation of a security system (2020) https://camafon.ru/informatsionnaya-bezopasnost/zashhita-na-predpriyatii. Accessed 25 Mar 2020

[12] M. Korolev (2010) Information security of the enterprise. Global security. http://www.globez.ru/press/148-.html. Accessed 25 Mar 2020

[13] N.V. Avilova, Methods for detecting unauthorized access to the information system and protecting the company's email address, Young researcher of Rostov- on -Don 2(11) (2018) 5-8.

[14] G.P. Zhigulin, M. Budko, The problem of comprehensive provision of information security and improvement of educational technologies for training specialists of law enforcement agencies, in: Intercollegiate collection of proceedings of the II all-Russian scientific and technical conference of ITMO University, ITMO, 2011, 222 p.

[15] V.F. Shangin, Information security of computer systems and networks, INFRA-M, 2008, 416 p.

[16] Information security of the enterprise: an internal threat http://rus.safensoft.com/security.phtml?c=775 Accessed 25 Mar 2020

[17] Yu. Namestnikov, D. Bestuzhev (2018) Threats for financial institutions: a review and forecast to 2019. https://securelist.ru/ksb-cyberthreats-to-financial-institutions-2019-overview-and-predictions/92852/. Accessed 25 Mar 2020

[18] A.G. Shavaev, S.A. Diev, Organization and modern methods of information protection, Bankovskiy delovoy centr, 1998, 472 p.