International Journal of Engineering & Technology, 7 (4.38) (2018) 1227-1230

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Topical Issues of Information Security in Modern Economic Conditions

T. L. Shugunov [1], T. Yu. Khashirova [2], A. S. Ksenofontov [3], M. A. Georgieva [4], S. M. Arvanova [5],

[1]Candidate of Physical and Mathematical Sciences, Associate Professor
[2]Doctor of Technical Sciences, Professor
[3]Candidate of Physical and Mathematical Sciences, Associate Professor
[4,5]Senior Teacher
«Kabardino-Balkarian State University named after H.M. Berbekov»

Abstract

This article discusses the burning issues of ensuring information security in modern economic conditions. The purpose of this study is to analyze the current state of the effectiveness of information security in the conditions of the emerging digital economy in the Russian Federation. According to the research conducted, the number of cybercrimes in the economic sphere increases every year. The largest percentage of cybercrime is committed in the banking sector of the economy. Banks of the Russian Federation have developed information security systems and services that deal with issues of ensuring the security of economic operations. One of the key security tools is the use of cryptography. The Russian Federation is actively developing software products in the field of encryption, but these programs do not have recognition in the global information security market. The obtained results allow us to make a conclusion about the development of the market of information products in the field of protection of economic security, but it is necessary to develop software products that will meet international standards in the field of information security. The results obtained are of theoretical and practical importance for specialists in the field of security and economics. The results obtained can serve as a foundation for conducting more extensive research on the state of the information security system of the digital economy in the Russian Federation.

Keywords: *Information Security, Digital Economy, Cybercrime, Cryptography, Encryption, Information Protection, Ddos Attacks, Banking Systems.*

1. Introduction

The active development of the digital economy leads to the emergence of new directions in the field of information security. The pace of digitalization of economic processes is very high and the issues of ensuring the information security of economic information are becoming increasingly important. The formation of the digital economy takes place in extremely difficult economic conditions, the number of cybercrimes in the economic sphere is increasing and it is necessary to form an effective information security system in the field of economic relations. The processes of becoming a digital economy are very difficult to implement in the world, since the level of economic and information development of the countries is different. In the Russian Federation, these processes are difficult, as there is an unstable development of the economy and information technology.
Ensuring the information security of economic operations is of strategic importance for the state. In the Russian Federation, the largest bank in terms of the number of economic transactions is Sberbank of Russia and the most interesting is the analysis of information security in this bank.

1.1. The purpose

of the article is to study current issues of information security in the modern conditions of digitalization of the economy.

1.2. Materials and methods.

The following theoretical methods were widely used in this study: an analytical review of theoretical information, analysis of information of statistical bodies, generalization and presentation of the research results in graphical form.
There is no doubt that the processes of digitalization of the economy have a positive impact on the information and economic development of society. The use of modern information technologies greatly simplifies the processes of economic operations, expands the capabilities of all categories of users of economic services.
It should be emphasized that the informatization of the economy also has specific risks that can lead to high economic losses of individual individuals, legal entities, and the entire state.
This is due to the fact that some of the information that belongs to consumers (individuals and legal entities) of these information services is confidential, and is subject to such threats as its loss or access to it by other individuals and legal entities. [1]
The issue of protection of personal data in modern conditions is becoming increasingly important. Personal data is one of the most valuable assets of the modern information society.
Every year there is an increase in the leakage of various information [4].
In the first half of 2018, the InfoWatch Analytical Center registered 1039 cases of confidential information leaks, which is 12% more than in the same period of 2017 (Figure 1) [11].
In the first half of 2018, for the first time in the entire history of

observations, the amount of data compromised as a result of the actions of an internal violator was more than three times higher than the amount of data compromised as a result of external influence.

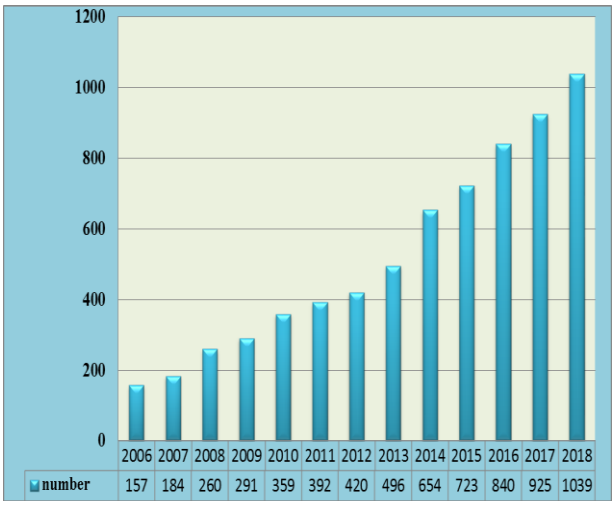

Figure 1: The number of information leaks in the first half of 2006–2018

If the amount of data compromised as a result of "internal" leaks decreased by 32% to the previous period and amounted to 1.6 billion records, then the amount of data compromised due to an external attacker decreased 10 times to 0.56 billion records.

The number of recorded "mega-leaks" has not changed; there were 21 registered cases in the study period when the volume of compromised data exceeded 10 million records, against 20 cases for the same period a year earlier. The "mega-leaks" accounted for 2.3 billion compromised records (97% of the total).

Addition to the mega-leaks for the study period recorded another 15 cases of information leakage, during which the volume of compromised data exceeded one million records. [2]

Probably, a decrease in the volume of data compromised as a result of external influence, and a decrease in the aggregate amount of compromised data in the period under study is associated with administrative influence from the state (first of all, the USA, European countries) on companies that have leaked. Tangible penalties against such organizations have forced the management of companies processing large amounts of data to think about improving the level of information protection of limited access.

In the study period, in 56% of cases, the perpetrators of information leaks were current (54%) or former employees (2%).

Figures 2 and 3 provide information on the sources of information leakage following the results of the first half of 2017 and 2018. The percentage of leaks caused by external intruders has decreased, which indicates an increase in the effectiveness of information security tools against external intruders. [9]

Quality and information in modern society are important for all spheres of society. Replacement or unreliability of information can cause both material and moral damage. In these conditions, the issue of ensuring the information security of public authorities, personal data and data of legal entities is relevant. [10]

Information security in the Russian Federation was formed as a separate industry, which has its own goals and objectives, but has several disadvantages.

Most of the information in the Russian information space passes through foreign servers, which increases the ability of external users to access this information. [15] In the current situation, this negatively affects the effectiveness of information security in the Russian economic space.

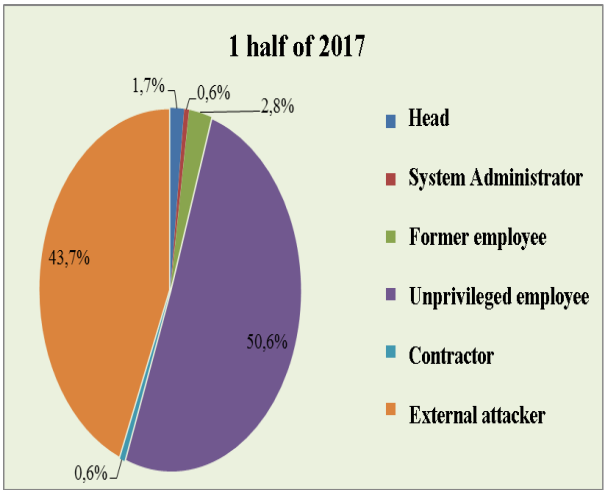

Figure 2: Perpetrators of information leaks in the first half of 2017

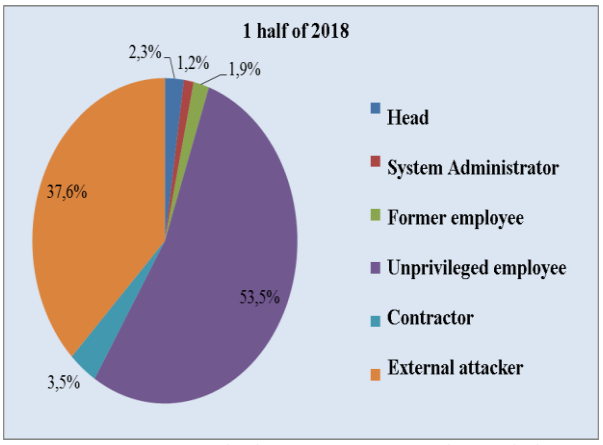

Figure 3: Perpetrators of information leaks in the first half of 2018

The entry into force of the law "On the Security of the Critical Information Infrastructure of the Russian Federation" became a significant event for the industry in 2017.

Indicators of significance criteria for them will be established by a government decree. [6]

It is supposed that the daily average number of the operations which are carried out by the subject of domestic information infrastructure will form the basis of criteria. According to this indicator the information and automated systems of the Bank of Russia, Sberbank, the National Payment Card System, other significant credit and financial institutions can be carried to significant objects of critical information infrastructure of the third category in the credit and financial sphere. Assistance in providing data in the state detection system, prevention and mitigation of consequences of the computer attacks on information resources of Russia becomes important function of the regulator. [8]

In 2018, Sberbank defended 32 billion rubles of depositors' funds from cyber frauds thanks to its fraud monitoring system.

Social engineering has become the most common type of fraud. The number of high power DDoS attacks increased by 1.5 times compared with 2017. On the International Information Protection Day, November 30, Sberbank summed up the preliminary results of 2018 in the field of cyber security. More than 80% of cases recorded by Sberbank in 2018 were attributed to social engineering, a method of obtaining unauthorized access to information based on the use of human weaknesses. At the same time, 86% of all cases of social engineering were transfers of funds under the influence of fraudsters. The most typical translation case is fraud on free ad sites. Sberbank has analyzed cybersecurity work since the beginning of 2018. The client places an ad on the site, a potential "buyer" calls the client, the client informs the "buyer" of his bank card details during the conversation, often providing SMS passwords so that the attacker

can perform all operations on behalf of the client. Since the beginning of the year, Sberbank has saved 32 billion rubles from clients' cyber frauds with customer funds using a fraud monitoring system based on artificial intelligence. The fraud monitoring system analyzes more than 150 million transactions per day and blocks suspicious transactions. Its effectiveness exceeds the best global indicators. [5]

The Sberbank cyber defense center processes more than 3 billion events every day, several thousand of which are associated with malicious software. On average, in 2018, Sberbank recorded 1-2 DDoS attacks on its systems every week. Since the beginning of this year, the bank has repelled 62 DDoS attacks, 25 of them are high power attacks. The number of high power attacks exceeds this indicator in 2017 by 1.5 times. The work of the Cyber Defense Center resulted in uninterrupted operation of banking systems and services from DDoS attacks and uninterrupted customer service. In a week, on average, Sberbank unties about 5 phishing sites from the server, and for a quarter, the bank's security systems record about 190,000 attempts to send emails containing malicious attachments and phishing to bank employees.

Cyber criminals often crack not an IT system, but a person, so people need to know the rules of cybersecurity and always follow them. Sberbank constantly teaches clients, helps them acquire and develop skills to protect against cyber fraudsters. One of the most important tasks of Sberbank is to form a cybersecurity culture in Russia and promote its development. There is a test on the knowledge of the rules of cyber-safe behavior on the Sberbank website. These rules are set out in detail in the section of the Sberbank website "Your Security"

In order to ensure maximum information security, it is necessary to use modern software and hardware, as the main threat to computer systems is associated with them: these are software errors, incorrect actions of users and system administrators.

Cryptography is one of the tools for protecting economic information.

Cryptography technologies allow implementing the following information protection processes:

identification of the object or subject of the network or information system;

authentication of the object or subject of the network;

control / delimitation of access to local network resources or off-network services;

ensuring and monitoring data integrity.

The transition to the Russian encryption software is one of the key tools for protecting information in the modern economic space of Russia. [3]

The Interdepartmental Commission of the Ministry of Digital Development, Communications and Mass Communications of the Russian Federation has developed a draft state program "Digital Economy", within which transition to the domestic cryptographic software is provided.

The program developers are planning to complete the transition of the participants in the digital information exchange process to the Russian data encryption systems by 2021. Within the framework of this project, it is necessary to integrate Russian encryption programs into the software.

There are currently two schools of encryption in the world: Russia and the United States. China has also begun to actively pursue this. [13]

Russian algorithms are very reliable. A special committee of the International Organization approves Russian algorithms for Standardization (ISO). The world's largest IT corporations are wary and refuse to use Russian algorithms, despite their recognition by the International Organization for Standardization. At the moment, data is encrypted using US security certificates; in this situation, Russian users are at risk of declassifying their data, which is stored on various websites in case of withdrawal of these certificates by their owners [10,19].

The security of information systems has a strategic importance for the country. At the same time, the situation is obviously aggravated by the growth of the level of threats in the information space; methods, ways and means of such crimes are naturally becoming more sophisticated, which requires adequate measures to improve the cyber resistance of financial market entities [14,16].

The system of information protection passes a formation stage in the sphere of digital economy of the Russian Federation. The existing systems of encryption of economic information, which are developed by Russian specialists, are not recognized in the world market. It is necessary to identify the factors that negatively affect the level of efficiency of the developed information protection algorithms, and to carry out further work on their further development. Creating world-class software products will reduce dependence on foreign information protection systems, which will increase the level of information protection of the Russian economy.

References

[1] Averyanov M.A., Evtushenko S.N., Kochetkova E.Yu. Digital Society: New Challenges. Economic Strategies. 2016, No 7 (141), pp. 90-91

[2] Andreeva G.N., Badalyants S.V., Bogatyreva T.G., Boroday V.A., Dudkina O.V., Zubarev A.E., Kazmina L.N., Minasyan L.A., Mironov L.V., Strizhov S.A., Sher M.L. The development of the digital economy in Russia as a key factor in economic growth and improving the quality of life of the population. Nizhny Novgorod: Professional Science publishing house, 2018. 131 p.

[3] Doshina A. D., Mikhailov A. E., Karlova V. V. Cryptography. Basic methods and problems. Modern trends in cryptography. Modern trends in technical sciences. Proc. of the IV Intern. scientific conf. (Kazan, October 2015). Kazan: Beech, 2015, pp. 10-13. Available at: https://moluch.ru/conf/tech/archive/163/8782/ (accessed 25.11.2018).

[4] Keshelava A.V. Budanov V.G., Rumyantsev V.Yu. Introduction to the "Digital" economy. 2017. 28 p.

[5] Kuznetsov, I. N. Business Security. Publishing and Trading Corporation 2016. 416 p.

[6] On approval of the program "Digital economy of the Russian Federation: Order of the Government of the Russian Federation of July 28, 2017 N 1632-p. Available at: http://www.consultant.ru/document/cons_doc_LAW_221756/ (accessed 11.30.2018).

[7] The program of development of the digital economy in the Russian Federation until 2035. Available at: http://spkurdyumov.ru/uploads/2017/05/strategy.pdf (accessed 01.11.2018)

[8] Tarchokov B. A. Analysis of criminal acts committed in the banking sector using Internet technologies. Gaps in Russian legislation, 2017, No 5, pp. 211-212

[9] Udalov D.V. Threats and Challenges of the Digital Economy. Economic Security and Quality, 2018, No 1, pp. 12-18

[10] Khochueva F.A., Shugunov T.L., Zhukov A.Z., Ingushev Ch.Kh. Information security through the prism of the digital economy. Modern high technologies, 2018, No 11, pp. 65-71.

[11] Economy. Available at: https://data-economy.ru/security (accessed 01.12.2018)

[12] Aja A., Bustillo D., Darity Jr. W., Hamilton D. Jobs Instead of Austerity: A Bold Policy Proposal for Economic Justice. Social Research: An International Quartlery, 2013, No 80 (3), pp.781–794.

[13] Boutin K.J.D. China's Industrial Development and Regional Economic Security. Alfred Deakin Research Institute. Available at: www.deakin.edu.au/research-services/forms /v/7808/wps-44w.pdf (accessed 12 November 2014).

[14] Cavelty M.D., Mauer V. The Role of the State in Cyberspace. 2016, Routledge.182 p.

[15] Frolova E. E. Information Security of Russia in the Digital Economy: The Economic and Legal Aspects.Journal of Advanced Research in Law and Economics, 2018, Vol. 9, No 1, pp. 89-95.

[16] Miles I. Services in the New Industrial Economy. Futures, 1993, No 25 (6), pp. 653-672.

[17] Peltier T.R. 2013. Information Security Fundamentals (2nd ed.). CRC Press. 438 p.
[18] Roshidi Din, Osman Ghazali, Alaa Jabbar, Qasim Analytical Review on Forms of Comparative Physics and Computer Science Vol. 5, No. 3, March 2017, pp. 401-408. DOI: 10.11591 / ijeecs.v5.i3.pp401-408
[19] Securing Information in the New Digital Economy, McKinsey & World Economic Forum, 2014.
[20] Sobranie Zakonodatelstva Rossiiskoi Federatsii [SZ RF], 2017, No. 42. Available at: http://www.szrf.ru/szrf/oglavlenie.phtml?nb=100&issid=1002017042000 (accessed November 3, 2017).
[21] Solms R. von, Niekerk J. From Information Security to Cyber Security. Computers & Security, 2013, No 38, pp. 97-102.
[22] Teoh, C.S., Mahmood, A.K. 2017. National Cyber Security Strategies for Digital Economy. Proc. of the 5th International Conference on Research and Innovation in Information Systems (ICRIIS), Langkawi, 16-17 July 2017, pp. 1-6.