Information Security as the Basis of Digital Economy

Skrypnikov A.V.*
Voronezh State University of Engineering Technologies
Voronezh, Russia
skrypnikovvsafe@mail.ru

Kozlov V.G.
VSAU
Voronezh, Russia

Denisenko V.V.
Voronezh State University of Engineering Technologies
Voronezh, Russia
v.denisenko1@yandex.ru

Kuznecova E. D.
VSAU
Voronezh, Russia

Saranov I. A.
Voronezh State University of Engineering Technologies
Voronezh, Russia

Savchenko I. I.
Voronezh State University of Engineering Technologies
Voronezh, Russia

***Abstract* — This scientific article is devoted to the analysis of ensuring the information security of an enterprise, as a basis for the functioning of a business in digital economy, as well as the improvement of its directions with the use of individual technologies and methods. The relevance of this scientific research is explained by the fact that the old methods and mechanisms for creating the information security system at enterprises has become economically ineffective and reduce the level of protection of commercial and other important information. In this regard, the application of new technologies, both individually and as part of an integrated information security system, is becoming increasingly relevant. The main ways of improving the information security system to counter the economic intelligence of competitors have been considered. Methods and ways of improving the information security system using biometrics technologies have been proposed. The role of ensuring information security in enterprise cloud technologies as the most vulnerable element in the digital economy has been analyzed.**

Keywords — information security; digital economy; biometrics; cloud technologies; economic intelligence; industrial espionage; digital technology.

I. INTRODUCTION

The current period of transformation of the global and domestic economies contributes to strengthening the integration processes between commercial activities and digital technologies, the latter of which is the main factor in the rapid development of business entities. In the context of this trend we can observe such processes as the development of information technologies, the development of intelligent technologies, and the practical application of highly intelligent innovations in the framework of improving the business processes of enterprises.

II. DISCUSSION

One of the latest processes is the development of digital technologies as part of an integrated system of information security organizations; these technologies improve the activities of organizations for the collection, processing, analysis and storage of information data. Their task is the formation of the basis and foundation of information security of an enterprise, which is extremely important in view of the development of the digital economy of the Russian Federation.

The relevance of this scientific research consists in the fact that the old methods and mechanisms for creating the information security system of enterprises have become economically ineffective and weaken the level of protection of commercial and other important information. In this regard, the application of new technologies, both individually and as part of an integrated information security system, is becoming increasingly relevant.

The goal of the scientific article is to analyze the information security of an enterprise, as a basis for the functioning of a business in digital economy, as well as to improve it using separate technologies and techniques.

For this end, in the framework of this scientific research we have to solve the following tasks:

- to study the main directions of improving the information security system to combat the economic intelligence of competitors;
- to suggest techniques and ways to improve the information security system using biometrics technologies;
- to analyze the role of information security in enterprise cloud technologies as the most vulnerable element in the contest of the digital economy.

Copyright © 2020 The Authors. Published by Atlantis Press SARL.
This is an open access article distributed under the CC BY-NC 4.0 license -http://creativecommons.org/licenses/by-nc/4.0/.

A key reason explaining the importance of information security as the basis of the digital economy is economic competitive intelligence, leading to industrial espionage and theft of company confidential information and intellectual property.

Due to the active development of economic intelligence in modern business, enterprises are exposed to various risks and threats associated with the loss of information and intellectual resources. Since such a resource as intellectual capital is one of the main criteria for the competitiveness of an enterprise, counteraction to economic intelligence is becoming the primary task of the information security system.

To ensure the information security of the enterprise as part of protection from economic intelligence, the following methods can be used:

- introducing a restriction of access to commercial information for employees who are not related to the performance of these operations and business processes;
- ensuring total security of computer systems and networks by using new information technologies.

However, despite the active use of such enterprise methods, economic intelligence often leads to theft and loss of commercial information and intellectual capital. For this reason, the actions aiming to protect information resources should include the implementation of a system increasing the confidentiality of information within the company. The following recommendations [1] are able to perform this task:

- to create proper documentation in the realm of security;
- to increase the delimitation of access to information for certain groups of company employees;
- to introduce "the trade secret" labels and documentation identification codes;
- to introduce special modes of using the Internet;
- to use DLP system software and SIEM system.

Thus, the key recommendation for improving the security system and protection against economic intelligence is the creation of a new computer security information system.

Also, the functioning of biometric systems is an important aspect of improving the information security system of enterprises in the context of the development of the digital economy in Russia.

Biometrics is defined as a system for recognizing people according to one or more physical or behavioral traits.

Today, the tools of biometric methods for protecting information data can be classified into two key groups: dynamic and statistical (Figure 1).

In addition to statistical and dynamic methods, there are also modern tools of biometric information security systems [3]:

- the LBP method is a description of the neighborhood of an image pixel in binary form;
- the method of k-nearest neighbors relating objects to the class to which the majority of its k-nearest neighbors belongs.

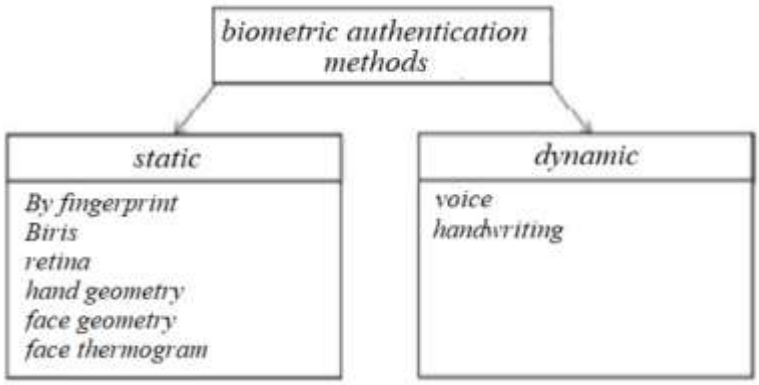

Fig. 1. Types of biometric authentication methods [3].

These methods are extremely new and difficult to use, as a result they are often used by such foreign corporations as Amazon, Oracle, IBM and others.

Speaking about the domestic space it is to note that the use of biometric systems as part of an integrated information security system is quite active, which is associated with the country's large-scale banking sector. It is credit organizations that most actively use biometrics when managing financial systems and the funds of their clients.

So, in 2018, banks began to actively use and introduce a biometric identification system. For example, in "VTB" biometric identification opens up remote access options, simplifies access to personal account and increases the level of information security for users of remote bank channels [2].

Also, since July 1, 2018, the Unified Biometric System has been launched. It is a database in which biometric data of citizens is stored. At the same time, several large banks began to accept biometrics, including Sberbank, Alfa Bank, Pochta Bank, Raiffeisen bank and others. The developer and operator

of the system is Rostelecom, the company which processes data and ensures their safe storage [4].

The active process of implementation and application of biometric systems in the formation of information security at enterprises is associated with the following advantages:

- convenient use because there's no need of contact;
- no risk of data loss because you can't forget your "Personal biometric data";
- high degree of difficulty in falsifying or stealing biometric data for fraudulent identification.

In addition, in order to improve the process of ensuring the company's information security, it is necessary to use methods responsible for the reliability of cloud technologies that are actively used in the Russian economy:

- encryption is the most efficient and easiest way in which the cloud storage provider is obliged to encrypt customer information and permanently delete it in case of termination of the provision of services;
- data protection during information transfer; the method involves prohibiting access to information data in the cloud storage until one is authenticated after the transfer;
- authentication is the method that involves the establishment of one-time passwords, the key generation of which occurs using technologies such as SAML and LDAP;
- isolation of users is the most difficult way to ensure information security in cloud technology storages, because the provider isolates the data of clients from each other by modifying the code inside the system. In this regard, there's a possibility of mistakes due to which customers may randomly access other customers' data.

In addition to standard methods of protecting information and data in cloud technology storages separate tools can be used, the difference of which depends on the cloud technology system itself (Figure 2).

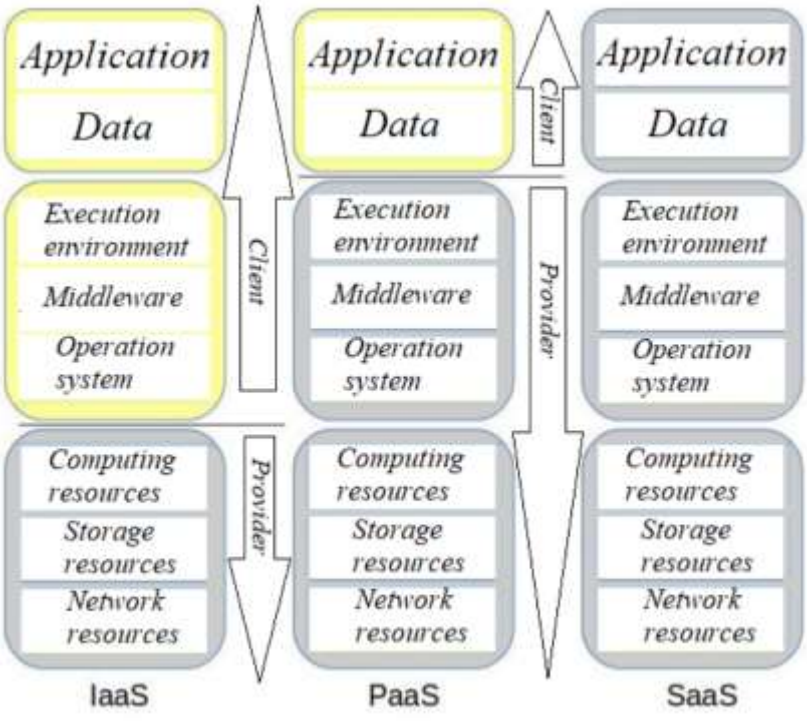

Fig. 2. Multilevel information security system of the three main cloud technology models [4].

We consider an example of a security system for open banking resources, its security level is determined by the reliability of its least protected node. However, a properly configured system can often mitigate the risks of an existing vulnerability.

If we assess the safety of official websites and remote banking services (RBS) in accordance with modern practice, we can see that one of the major vulnerabilities is checking SSL / TLS settings, since these cryptographic protocols are the most popular method of providing secure data exchange via the Internet today. In order to perform SSL/TLS connection, the server must have an authenticated digital certificate confirming the domain authenticity and indicating the site owner. This is necessary so that users could visit the resources they need, but not fake intruder pages. SSL / TLS have a wide

range of settings and features that affect the security of sensitive data to varying degrees. Connection encryption is an important feature necessary to prevent theft of transmitted confidential data. We suppose that a user pays for purchases through mobile banking or a browser by connecting to an open Wi-Fi network. An SSL / TLS connection is established between the client and the remote banking system, and the data is transmitted in encrypted form. Even if an attacker intercepts them, it will take him years to decrypt. SSL / TLS testing. Suppose that the RBS system does not use SSL / TLS, therefore all information is transmitted in clear text. This could permit a malicious user being online to gain access to traffic, this could make it possible to intercept or replace data using the Man-in-the-middle attack, to gain access to user accounts, or completely take over their accounts. In case there is a vulnerability of Heartbleed or Ticketbleed type on the server, the hacker will be able to access the users' data stored in the server's operating memory. Basic tests of settings and vulnerabilities are given in table 1.

TABLE I. TESTS

Test's name	Description
Rating	Overall rating of SSL configuration according to SSL Labs resource. It depends on many factors: certificate correctness, server settings supported by the server algorithms, etc. Graduation from A to F.
Support of weak parameters of the Diffie-Hellman algorithm	Weak parameters can be used for Diffie-Hellman protocol key exchange; they reduce the security of the resource.
POODLE Vulnerability	This allows you to decrypt user's data. For more information, see the publication of researchers.
FREAK Vulnerability	An attacker can force the user and server to use "export" keys, the length of which is very limited, when establishing a connection and exchanging data.
Logjam attack Vulnerability	Like FREAK, Logjam is based on lowering the level of encryption to the export level, where the key length is 512 bits. The difference is that Logjam attacks the Diffie-Hellman algorithm.
Vulnerability DROWN	This allows you to decrypt the client's TLS traffic if the server side does not disable support for SSL 2.0 in all servers operating on the same private key.
ROBOT Vulnerability	Completely violates TLS privacy when using RSA to obtain a session key.
Beast Vulnerability	The intruder can decode data exchanged between two parties using TLS 1.0, SSL 3.0 and lower versions.
CVE-2016-2107 Oracle Vulnerability	A remote attacker can use this vulnerability to extract text from encrypted packages using Padding technique
Heartbleed Vulnerability	Obtaining access to data stored in the client or server memory.
Ticketbleed Vulnerability	A remote attacker could extract fragments of server memory content using the TLS protocol Session ID field.
SSL Renegotiation	Secure SSL renegotiation reduces the risk of DoS or MITM attacks.
RC4 support	Researchers have discovered that it is possible in a short time to decrypt data that was hidden using the RC4 cipher.
Forward Secrecy Support	Property of certain key reconciliation protocols, which guarantees that session keys will not be compromised even if the private server key is compromised.
TLS Version support	TLS protocol encrypts Internet traffic of all types, making Internet data exchange safe.
SSL 2.0 and SSL 3.0	Both protocols are considered obsolete and have much vulnerability, so they are recommended for disconnection on the server side.
NPN and ALPN support	Allows you to specify which protocol to use after establishing a secure SSL / TLS connection between the client and server.

For example, consider the Diffie-Hellman key exchange. This is a popular cryptographic algorithm that underlies many protocols, including HTTPS, SSH, IPsec, SMTP, and allows parties to negotiate a common key using an insecure connection. Using prime numbers to exchange Diffie-Hellman keys does not endanger the system. Researchers have found that only a large enterprise possessing the necessary resources and time is able to hack a 1024-bit prime. The authors suggest that since most of the Internet uses only 1 or 2 specific 1024-bit prime numbers, it is quite feasible to make the necessary preliminary calculations at the right opportunity. For example, large 2048-bit primes can be used to improve the security of key exchange. A more reliable option is to switch to the Diffie-Hellman protocol using elliptic curves. Elliptic curves do not suffer from common problems with preliminary calculations, which means that attacks on parameters that are barely within computational reach threaten only one connection, but not all connections using this group. Weak keys have been detected in single cases and, for the most part, on the official websites of banks in Brazil, Belarus, Hungary, Liechtenstein, Malta, Norway, Switzerland, Great Britain and Japan. Among the RBS for individuals: Belarus, Bulgaria, Ireland and Liechtenstein. Among the RBS for legal entities: Belarus, Bulgaria, Italy, Sweden. As for Russian banks, statistics on the use of weak SSL certificates are as follows: Official website – 11 %; RBS for individuals – 6 %; RBS for legal entities – 14 %.

III. CONCLUSION

Thus, summing up the results of this scientific research, we can draw the following conclusions:

- information security is the basis and foundation of the activities of enterprises in the digital economy of Russia;
- the key reason for improving the process of information security of an enterprise is economic intelligence and industrial espionage of competitors;
- in order to ensure information security, it is necessary to use the latest programs and techniques such as biometrics and cloud technology protection.

The importance of ensuring the information security of enterprises is primarily associated with the development of the digital economy. Indeed, it is at this stage of development that information technologies, computer networks and digital models are actively used, allowing not only to increase the efficiency of economic activity, but also to increase the risk of losing or stealing valuable information that market competitors can use. In this regard, the conclusion of a scientific study is to confirm the hypothesis that information security is the basis for the functioning of a commercial organization in the context of the establishment and development of a digital economy model.

References

[1] D.R. Khlestova, K.G. Popov, “Features of the protection of confidential information at enterprises”, Simvol Nauki, vol. 5-2, 2016.

[2] V.A. Grebennikova, K.G. Pomogaeva, “Overview of biometric technologies and their application at VTB Bank”, Int. J. of Appl. Sci. and Technol. “Integral”, vol. 3, 2019.

[3] “Digital technology”, Retrieved from: https://digital.gov.ru/ru /activity/ directions/ 878/ (access date: the 20.01.2020). “

[4] “Information infrastructure”, Retrieved from: https://digital.gov.ru/ru/activity/ directions/870/ (access date: the 20.01.2020).

[5] David von Oheimb, IT Security Architecture Approaches for Smart Metering and Smart Grid. Springer-Verlag Berlin Heidelberg, 2013.

[6] L. Jin, Z. Yinghui, C. Xiaofeng, X. Yang, “Secure attribute-based data sharing for resource-limited users in cloud computing”, Computers & Security, vol. 72, pp. 1–12, 2018.

[7] S. Xu, “Cybersecurity dynamics: a foundation for the science of cybersecurity”, Advan. in Inform. Security, vol. 74, pp. 1–31, 2019.

[8] V. Kashyap, B. Hardekopf, “Security signature inference for Javascript-based browser addons”, p. 219, 2014 [Proc. of Annual IEEE/ACM Int. Symp. on Code Generation and Optimization].

[9] Y.A. Salikov, V.S. Mikhailiuk, “Methodological approach to the terminological analysis of the key concepts of economic security”, Proc. of Voronezh State Univer. of Engineer. Technol., vol. 81, no. 2, pp. 387–392, 2019, Retrieved from: https://doi.org/10.20914/2310-1202-2019-2-387-392

[10] C. Canongia, R. Mandarino, Cybersecurity: The New Challenge of the Information Society. Crisis Management: Concepts, Methodologies, Tools and Applications. Hershey PA: IGI Global, 2014, pp. 60–80, Retrieved from: http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

[11] M.Y. Afanasiev, M.A. Lysenkova, “Approach to the analysis and comparison of national innovation systems by the example of Russia and other countries”, Proc. of Voronezh State Univer. of Engineer. Technol., vol. 81, no. 1, pp. 434–442, 2019. Retrieved from: https://doi.org/10.20914/2310-1202-2019-1-434-442

[12] D. Rodrik, “Premature Deindustrialization”, J. of Econ. Growth, vol. 21, no. 1, pp. 1–33. Retrieved from: http://www.nber.org/papers/w20935 (access date: the 20.01.2020).

[13] World Bank, Digital Dividends: World Development Report 2016, Washington, DC. Retrieved from: http://www.worldbank.org/en/ publication/wdr2016 (access date: the 20.01.2020).

[14] Biometrics in Russian banks: what is needed for it, how to pass it, whether it is safe. Retrieved from: https://vsezaimyonline.ru/reviews /biometrija.html (the access date: the 27.01.2020.