European Research Studies Journal
Volume XXI, Issue 4, 2018

pp. 744-753

Reliability of Cryptographic Information on Fiscal Data

D.V. Volkov[1], A.N. Maloletko [2]

Abstract:

The relevance of the study is due to the fact that modern data exchange systems transport information that stores elements of personal information. The operator of fiscal data is interested in secure transport of information.

The degree of security in modern realities is very important and is designed to ensure confidentiality on the one hand, and on the other hand, full transparency of information for state monitoring bodies.

In this regard, this article aims to identify the weaknesses of the adopted system of transport of cryptographic information by the operator of fiscal data and to systematize the theoretical data in relation to the theory on the question of part of the FTS data.

The leading approach to the study of the problem is the analysis of the existing system in conjunction with the synthesis of data through the compilation of information, which allows a comprehensive review and systematization of data on the economic phenomenon.

The article substantiates the need to reduce the state regulation of restrictions on the formation of information security barriers. The materials of the article are of practical value for the organization of big data stream transportation protection.

Keywords: *Cryptographic Information, Fiscal Data Operator, Big Data, Transport Information, Government Regulation.*

JEL code: *D83, L86.*

[1] *Russian State Social University, Moscow, Russia, VolkovDV@rgsu.net*
[2] *Russian State Social University, Moscow, Russia, MaloletkoAN@rgsu.net*

1. Introduction

Every day technologies play an increasing role in everyday life, by 2008 the number of devices connected to the Internet has exceeded the number of inhabitants of the earth. Accordingly, the issue of the processed data security is acute. The relevance of the topic is obvious, since information in modern society is one of the most valuable things in life, requiring protection from unauthorized access by persons who do not have access to it. The information of the operator of fiscal data (CRF) includes most of the information about the users of the monetary system. The most personal data is consumption data. The state must ensure that its citizens trust the system. To do this, the system must function without failures and personal data leaks.

The relevance of the subject is not in doubt, as the issue of confidential information safety in the modern world is quite acute. Therefore, the state took care of the regulation of information protection. The activities of the operator of fiscal data (OFD) are strictly regulated by the law and the main regulations of the Russian Federation which affect the use of cryptographic protection of information in the Russian Federation for OFD.

Activities in the field of cryptography (encryption) are limited in relation to the development, distribution and use of encryption tools in Russia, the import and export of cryptographic (encryption) tools. Regulation of cryptography activities in Russia is carried out by Russian regulatory legal acts, import and export of cryptographic products is regulated by the acts of the Eurasian Economic Commission.

It is important to remember that on the territory of the Russian Federation it is necessary to use cryptographic protection of information tools (CPIT), necessarily pass a special certification procedure that is regulated by the FSS. In brief, the procedure of certification of cryptographic information protection in practice consists of compliance testing for such CPIT with the technical requirements. It implies that the certified means must meet all the security requirements, use only the applicable standards of encryption algorithms and should not have any non-declared capabilities, which on the one hand is good, and on the other hand suggests that the system is static and it can be identified as vulnerable.

2. Literature Review

The question of security of confidential information transmittion has been raised since ancient times. One of the first ways to transmit classified information was to use, not surprisingly, slaves. They were shaved bare, a hidden message was written on the left part of the head and as soon as the hair began to grow, they were sent to the recipient. However, this method became ineffective soon due to the low degree of reliability and waste of time (Sadkhan and Salman, 2018; Grima *et al.*, 2017).

This method was related to steganography. Steganography is a method of protecting confidential information by hiding the very fact of the transmission of such information (Albekov *et al.,* 2017).

The main feature of the science of cryptography – the appearance of public key cryptosystems with a strict mathematical substantiation of the reliability. By the beginning of the 30s, the sections of mathematics were finally formed, which became the scientific basis of cryptology - the theory of probability. Mathematical statistics, number theory and the theory of algorithms and information theory, cybernetics began to dvelop (Babash and Shankin, 2002). The epilogue of the period was the creation of block ciphers in the late 60s, even more stable, but allowing practical implementation only in the form of digital electronic devices. One of such ciphers during the period of computer cryptography was the electronic implementation of block ciphers. In the 70s, the American encryption standard DES was developed, on the basis of which other, more crypto-resistant algorithms were built. In the mid 70s, there was a real breakthrough in modern cryptography - the emergence of asymmetric cryptosystems that did not require the transfer of the secret key between the parties. After all, the advent of such systems has greatly increased the use of cryptography in practice.

Cryptography, as a method of information security, has widely entered the modern world due to the high degree of information security. With the development of information technology cryptographic protection of information (further - CPIT) are introduced in almost all areas of computer use that need information security (Sukhodolskiy and Zapechnikov, 2018). The advent of the accessible Internet has taken cryptography to a new level. Cryptographic techniques have become widely used by individuals in electron ic commerce, telecommunications and many other environments. As it was mentioned earlier, all known encryption algorithms can be divided into symmetric and asymmetric.

3. Methodology and Methods

In accordance with the logic of the theme and research problem and questions concearning cryptographic information protection of the OFD we used a complex of methods. Identification of quality indicators significant for the market of OFD services was carried out using the method of data analysis and systematization. This method helped to carry out the structuring of the materials obtained in the course of analytical stage.

The methods of problems and subproblems` analysis were used within the study of the impact of state paternalism on business. The current management model should dynamically influence the information protection system to prevent possible vulnerabilities in the future (Vinogradova *et al.*, 2015).

The method of abstraction is a theoretical and empirical method that allowed to distract from random, situational, insignificant properties and interrelations of the studied phenomenon in the process of analytical work and to reveal essential characteristics of the phenomenon within the framework of the study.

The method of data analysis and systematization involved the structuring of the obtained analytical materials about consumer preferences, followed by a combination of previously disparate concepts and judgments in the form of qualitatively new way of presenting this information. The method of bibliographic search is a method of searching for the sources of information (documents and publications) that contain or may contain qualitative information confirming statements corresponding to the logic of the studied problem disclosure. The use of this method improved the quality of research, as it allowed you to get all the necessary information during the shortest possible period of time.

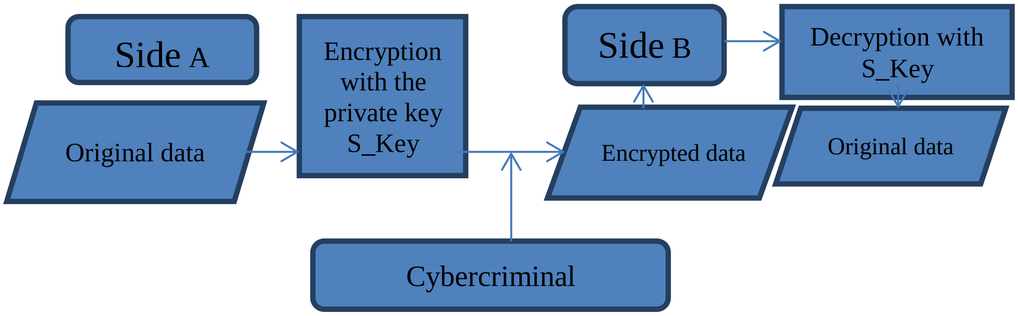
The purpose of this research is to identify the reliability of the OFD encryption algorithm. In accordance with the goal, the following tasks were indicated:

1. to analyze the dependence of the OFD's activity on the legislature;
2. to consider the history of encryption methodology through the analysis of significant approaches;
3. to explore modern encryption algorithms that are used by OFD to service fiscal information and administrative software.

4. Results and Discussion

Symmetric encryption is often referred to as a private key encryption. The development of such systems is referred to the period of scientific cryptography, their cryptographic stability is proved mathematically (Schneier, 2003; Volkov, 2016). The essence is that the parties engaged in information interaction, have a secret key, known only to them, it is used for the encryption and decryption of data .

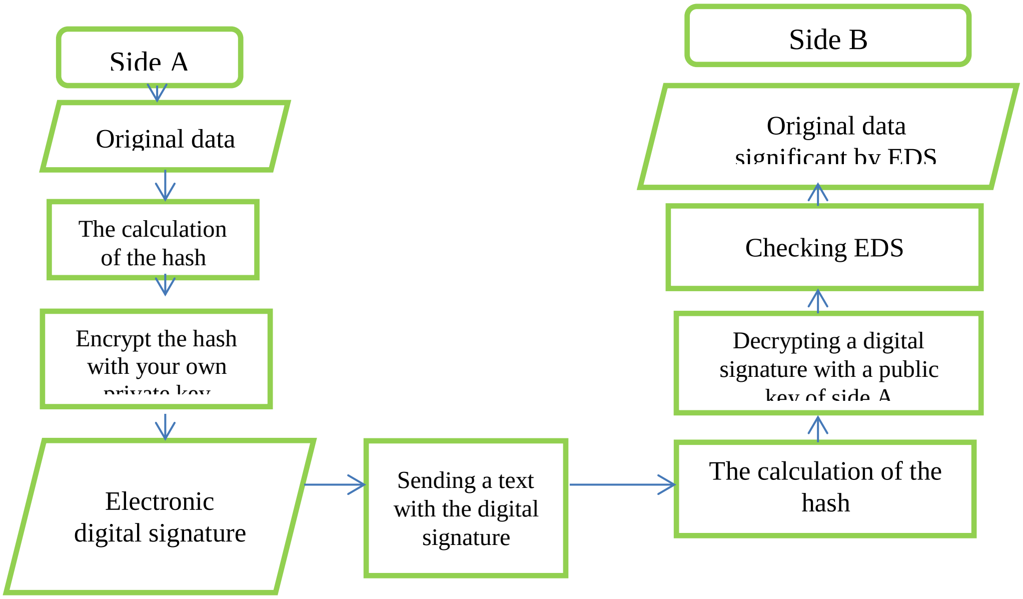
Figure 1. *S_key private key encryption scheme*



Source: *Mao, 2005.*

As shown at Figure 1, when encrypting data, Side A applies the transformation operations according to the specified algorithm using the s_key secret key, and the output is a meaningless set of data, which, when decrypted by Side B using the same s_key, will give the original message. In this case, the mechanism of Electronic digital signature (hereinafter-EDS) is used (Tinyakova *et al.*, 2017; Maloletko *et al.*, 2016).

Figure 2. *Algorithm for creating an electronic digital signature*

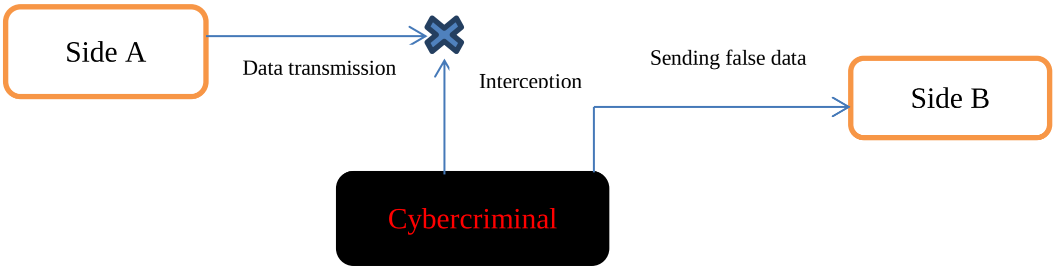

Side A
Original data
The calculation of the hash
Encrypt the hash with your own private key
Electronic digital signature
Sending a text with the digital signature
Side B
Original data significant by EDS
Checking EDS
Decrypting a digital signature with a public key of side A
The calculation of the hash

Source: *Kuzminov, 1997.*

If, in addition to confirming the authenticity of the participants of the information exchange, it is necessary to respect the confidentiality of the transmitted information, each sender encrypts the transmitted data using the public keys of the recipients, who, in turn, as mentioned earlier, decrypt the confidential message with their private key, known only to them (Volkov *et al.*, 2016). The creators of such algorithms also took care of the cryptographic stability of the generated ciphers, significantly reducing the possibility of hacking (Figure 2).

However, these systems are not perfect. As shown at Figure 3, an attacker with access to a data link could easily intercept a secret message by substituting his own and posing as Side A. The problem is solved by the emergence of such bodies as Certification centers (CC). In general, the Certification Authority is an organization that issues certificates of electronic digital signature keys. We will assume that the honesty of the certifying center is undeniable and not subject to doubt.

Figure 3. *Vulnerability of the formation of EDS*



Source: *Zabib et al., 2017.*

The EDS certificate is an electronic document that contains the details and all the necessary information about the owner of such a certificate, as well as its public key (Yashchenko, 2012). That is, Side B, when receiving encrypted information with an electronic signature from Side A on the basis of the certificate of verification of the EDS of Side A, can be sure that the specified sender is them.

The use of this approach in cryptography has made a splash in the field of information security, solving two key problems:

- improving the reliability;
- creation of public key infrastructure.

For the formation of cryptographic protection of information for the operator of fiscal data (OFD) it is important to implement several degrees of protection. In Russia, to become a fiscal data operator, a candidate must meet a number of requirements:

- permission to process fiscal data from the Federal Tax Service(FTS);
- license of the Federal Service for Technical and Export Control (FSTEC) for technical protection of information;
- license of the Federal Security Service (FSS) for the development and production of cryptographic protection;
- FSS license for data protection activities;
- technical means of ownership for the processing of fiscal data - information on the technical equipment of the server space is indicated by FSS;
- technical means for the protection of fiscal data;
- non-residential premises owned or rented.

The importance of different encryption algorithms for the operator of fiscal data is also the fact that it, as a legal entity, acts as a player at the free market. The effectiveness of the information protection characterizes it among other operators providing services to the OFD as a reliable business partner. Stability of business in modern Russia in terms of turbulence is especially important.

Cryptography in digital technologies is one of the key tools to ensure the security of confidential information. It is used to protect against unauthorized access, as a result of which the attacker can perform the following actions with the data of the OFD:

1. unauthorized introduction;
2. intentional violation of integrity or destruction;
3. unwanted with all of the attendant circumstances;
4. falsification.

Cryptographic algorithms based on the use of public key distribution, allowed to create a system of complex information security in large computer networks and information databases. The reason for this is the feature of public key cryptosystems (built on asymmetric encryption algorithms) to use a much smaller number of keys for the same number of users than required by a public key cryptosystem.

There are many ready-made encryption algorithms that have high cryptographic strength, the encoder can only create its own unique key to give the information the necessary cryptographic qualities (Roslyakov, 2006; Turkov and Volkov, 2018). The key is used for both encryption and decryption.

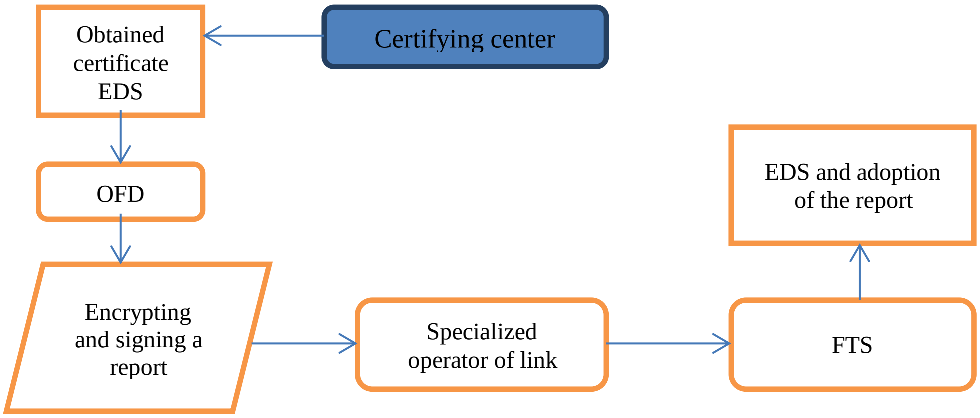
The introduction of electronic document management systems (EDMS), allows to gain great flexibility in the storage, processing and transmission of information and makes the bureaucratic system work faster and with greater efficiency. At the same time, EDMS causes new risks, and neglect of protection will necessarily lead to the new threats with the confidentiality of information.

The OFD is required to report to the FTS using electronic reporting. This information, as well as information about user transactions, must be protected. Today it is difficult to imagine any organization that would not use such services. All key supervisory bodies of the Russian Federation, such as the Federal Tax Service, the Pension Fund of Russia, the Federal Social Service accept reports via electronic channels. It solves a number of problems, reduces the load caused by endless standing in queues and also decreases the load from the regulatory authorities. Thanks to the development of cryptography, the exchange of electronic documents can be considered safe.

Of course, in practice it is a little more complicated. And encryption requires special cryptographic software. Cryptographic Service Provider (CSP) is an independent module that allows to perform cryptographic operations with information arrays. It is an intermediary between the operating system, which can manage it using standard functions, and the executor of cryptographic operations (it can be both a program and a hardware complex).

In addition to the cryptoprovider, it is also necessary to have specialized software for creating such reporting and working with the cryptoprovider, for example, Russian analogues of SBIS++ or 1S-reporting.

Figure 4. *Electronic reporting mechanism*


Obtained certificate EDS
Certifying center
OFD
EDS and adoption of the report
Encrypting and signing a report
Specialized operator of link
FTS

Source: *Sharma and Kaur, 2017.*

To create unified information systems large organizations use geographically distributed corporate networks to connect individual branch networks and remote employees with the network of the Central office (Figure 4). To solve these problems, the service of virtual private VPN (Virtual Private Network) can be used. A virtual private network is built on the basis of logical connections between certain corporate users through the public Internet. Simply put, 2 objects that can be located in different parts of the city or country create a virtual communication channel between them, in which data is encrypted Internet traffic. This technology can be considered as a potential analogue for the state document flow, or in the framework of support exclusively OFD.

5. Conclusion

The operators of fiscal data in the Russian Federation must follow the instructions of the state regulators. In order not to be a weak link in the chain of state control and security of citizens, the OFD is obliged to provide a maximum protection of information. Information security today plays a huge role in the modern world of information technology.

The popularity of this theme has served as a good service for the theory of cryptographic protection of information. In the age of information technology, it is important that such galloping jumps allow protecting the data of economic entities. In a turbulent business environment, the latest data protection technologies are vital.

In our opinion, the static nature of the legislative system with regard to the organization of security is a weak point of the organization of data security of the operator of fiscal data. The resources of operators across Russia can be useful in reforming information security systems. Additional resources in the field of protection can be used without additional funding from the public sector such as the OFD and so commercialize their businesses within the philosophy of the marginal utility.

Summing up the results of the research, we can say with confidence that cryptography as a guarantor of the preservation of confidential data not only has the right to exist, but also simply must be used in all spheres of human activity, where information with limited access appears.

6. Acknowledgements

The research is carried out within the framework of the implementation of research work № RDW-0116 from October 1, 2016 with the financial support of the Ministry of Education of the Russian Federation under the agreement N 03.G25.31.0236 from March 3, 2017.

References:

Albekov, U.A., Vovchenko, N., Andreeva, G., Vladimirovna, O. and Sichev, R.A. 2017. Block Chain and Financial Controlling in the System of Technological Provision of Large Corporations. European Research Studies Journal, 20(3B), 3-12.

Babash, A.V., Shankin G.P. 2002. History of cryptography. Part I-M: Helios ARV.

Grima, S., Seychell, S. and Bezzina, H.F. 2017. Investigating Factors Predicting Derivative Mishandling: A Sociological Perspective. European Research Studies Journal, 20(4A), 3-17.

Kuzminov, T.V. 1997.Cryptographic methods of information security. Moscow – Novosibirsk: NSU.

Maloletko, A.N., Vinogradova, M.V., Yudina, T.N., Dolgorukova, I.V., Tanatova, D.K., Kaurova, O.V., Mazayev, Y.N., Fomichev, T.V., Kireev, E.Yu., Korolev, I.V., Babakaev, S.V., Kulyamina, O.S., Shendrik, G.N., Timoshina, E.N., Akhtyan, A.G., Glotova, T.A., Vasilkevic, E.I., Kuzmin, S.N., Friesen A.G., Volkov, D.V. 2016. Annual sociological study of the level of satisfaction of citizens with quality of public and municipal services provided by the bodies of state power and local self-government. Available at: http://rgsu.net/about/science/minek-socopros/

Mao, B. 2005. Modern cryptography. Theory and practice. Moscow: Williams.

Roslyakov, A.V. 2006. Virtual private networks. Fundamentals of construction and application. Mocow: Eco-Trend.

Sadkhan, S.B., Salman, A.O. 2018. A survey on lightweight-cryptography status and future challenges. In International Conference on Advances in Sustainable Engineering and Applications, ICASEA 2018 - Proceedings, 105-108.

Schneier, B. 2003. Applied cryptography. Protocols, algorithms, source code in C language. Moscow: Triumph.

Sharma, S., Kaur, N. 2018. Hybridization of ICA based on arnold cat map using reversible cellular automata for faster cryptographic speed. In 4th International Conference on Image Information Processing, ICIIP 2017, 563-566.

Sukhodolskiy, I., Zapechnikov, S. 2018. A blockchain-based access control system for cloud storage. In Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018, 1575-1578.

Tinyakova, V.I., Maloletko, A.N., Kaurova, O.V., Vinogradova, M.V., Larionova, A.A. 2017. Model of evaluation of influence of globalization on the national stock market. In E.G. Popkova (Ed.). Russia and the European Union: Development and Perspectives, 261-272.

Turkov, M.M., Volkov, D.V. 2018. Building an adequate method of streaming microsegmentation of the internet audience on the basis of data on quality consumer characteristics. Contemporary Problems of Social Work, 4(2), 20-30.

Vinogradova, M.V., Kulyamina, O.S., Koroleva, V.A., Larionova, A.A. 2015. The impact of migration processes on the national security system of russia. Mediterranean Journal of Social Sciences, 6(3), 161-168.

Volkov, D.V., Akhtian, A.G., Semennikova, A.I., Dgibabov, M.R., Kusina, O.A. 2016. Effective use of human capital through reduction of working time. International Journal of Environmental and Science Education, 11(18), 12995-13005.

Volkov, D.V. 2016. Analysis of the structure of the modern monetary system. Economy: Yesterday, Today, Tomorrow, 6(10A), 161-170.

Yashchenko, V.V. 2012. Introduction to cryptography. Moscow: Publishing house of MCNMO.

Zabib, D.Z., Levi, I., Fish, A., Keren, O. 2018. Secured Dual-Rail-Precharge Mux-based (DPMUX) symmetric-logic for low voltage applications. In 2017 IEEE SOI-3D-Subthreshold Microelectronics Unified Conference, S3S 2017, 1-2.