A System Approach to Information Security in Distributed Ledgers on the Situational Centers Platform

A. A. Grusho, A. A. Zatsarinny, E. E. Timonina

Abstract — **It is considered in the article the implementation issues of one of the digital economy basic directions related to information security concerning the protection of information in distributed ledgers. Any information system has to be constructed on the modern computer platform and uses modern network opportunities. The computer platform provides security of the information system, solves problems of information reservation, and supports the system recovery after failures. Exchange of information through network assumes special facilities for information protection. Cryptography algorithms for enciphering and message authentication codes for control of integrity are used for these purposes. It is shown that within the framework of the digital economy program the distributed ledger technologies have a system forming nature and must be created in conjunction with other technologies, taking into account the principles of a system approach for information networks creation.**

The authors proposed to use the platform and functional resources of the distributed situation centers system as the infrastructure base of the information security subsystem in distributed ledgers. At the same time, it is supposed that the consensus is based on the trust to the protected systems of the situational centers.

Keywords — **Information security infrastructure, system approach, smart ledgers, distributed situation centers.**

I. Introduction

The President of the Russian Federation proposed to "launch a large scale system program for the economy of a new technological generation development – the Digital Economy" [1], [2]. These strategic trends are fully correlated with global trends in the economy, which are presented in a famous book by Klaus Schwab [3].

In the approved program of the Digital Economy of the Russian Federation [4], [5] as end-to-end digital technologies defined: Big Data, Neurotechnology, and Artificial Intelligence, Distributed Ledger Technology (Blockchain).

Surely, the list of such technologies will be changed and supplemented with the appearance of new scientific and practical results.

Note that the special importance of the Distributed Ledger Technology (DLT) in the technologies list, often called "Blockchain" [6], [7]. In our view, this is due to two main factors.

The Digital Economy has a systemic nature and, in fact, involves the solution of three interrelated tasks [8]:

1. creating the unified approach to information ledgers of all resources in the digital economy (materials, technologies, intellectual and human resources, infrastructure and other resources),
2. filling of the ledgers by actual, reliable and objective data in real-time,
3. developing technologies to account for all changes in these resources.

It seems this approach to the concept of the digital economy can ensure the effectiveness of management decisions at all levels by minimizing the human factor and reducing the number of levels in the management system hierarchy.

These tasks create chains of data, components of which reflect economic processes, for example, supply chains, the chain of acquisition of resources for projects, etc. Therefore, DLT may be the basis of such technologies.

The second factor is that the DLT is closely related to the implementation of one of the basic directions of the digital economy such as "information security".

II. Information Security in DLT

DLT is continuously refilled and is protected from changes in any data items. The basis of DLT information security is in creation of a single-linked list of blocks by cryptographic methods, each of them contains records of current transactions with available resources. These transaction records are digitally signed, which makes changes at any previous stage to be a hard problem. In fact, keeping blocks single-connected requires storing of the hash-functions values computed from all information in each block. In turn, this requires the forgery of all digital transaction signatures in each previous block.

Distributed ledgers differ by consensus. The consensus determines the mutual trust of all participants of DLT.

Manuscript received November 27, 2019.

The research is partially supported by Russian Foundation for Basic Research (project 18-29-03124-мк).

A. A. Grusho, Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow State University, Moscow, Russia (e-mail: grusho@yandex.ru).

A. A. Zatsarinny, Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia (e-mail: AZatsarinny@ipiran.ru).

E. E. Timonina, Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow State University, Moscow, Russia (e-mail: eltimon@yandex.ru).

DLT creates new opportunities to search, organize, evaluate and reliable transfer and account of any different types of assets (resources data in distributed ledgers). In fact, it is the new organizational paradigm for the coordination of any kind of human activity. And the implementation of this paradigm has to be linked to requirements of information security [9], [10], either containing state secrets or confidential, especially in terms of personal data protection.

However, this new functionality and technological capabilities produce new security challenges and threats. Security threats by their nature and consequences become increasingly critical.

The following threats are actually in the considered technologies:

- availability;
- integrity (distortion, destruction);
- signature stealing;
- fake blockchain fragments;
- consensus violence.

An unsecure communication system can ambiguously reflect transactions, in particular, delays in payments for performed work or contract default. The integrity violation is in the inability to verify the entire blockchain chain. Stealing signatures may generate false transactions. The blockchain forgery is associated with a lot of computational work. However, it can be done due to collisions of hash functions and other weaknesses of crypto-algorithms and crypto-protocols [11].

One of the implementations of DLT is project support. For projects, it is required tracking of interactions with subcontractors, control of supply chain resources, etc. Hence the necessity of various implementations of DLT has arisen.

The secure implementation of "smart contracts" requires the comparison of the different chains of the blockchain. Let's call the matching process as blockchain clearing. The solution of this task will allow to follow the fulfillment of all parties' obligations and to identify fraudulent schemes.

Ensuring the information security of the DLT requires using secure platforms and securing telecommunications systems. This is called a system approach.

Digital technologies are deeply immersing in the processes of activity (business processes, management processes, service processes) and becoming an integral part of them. Therefore, it isn't enough to make traditional demands for the protection of information. We must have a reliable processing and functional environment. This system must be trusted, which means that it is almost impossible to break blockchain because of its complexity.

Successful solutions to these issues are possible on the basis of a system approach.

III. The essence and the principles of the system approach applied to DLT

Speaking about the system approach, it should be noted that we are speaking about the principles of development, common approaches to the solution to complex problems. That means that we should look at the newly created system as a whole.

At the same time, the more complex the system, the more important is to approach its creation systematically [12].

It is clear that consideration of the "DLT" or "blockchain" concepts should be raised to a higher, systemic level and subsystem of information security in DLT at the same time should be based on system approach principles. These include the principles of system development, its complexity and efficiency, new challenges, development (openness), unification, and standardization, maximum consideration of IT-achievements [13].

We briefly formulate the essence of the principles in relation to a subsystem of information security.

The System Principle assumes a decomposition of the system under the conditional name "Digital Economy" into component parts of structural and technological subsystems. Structural subsystems are determined by the basic directions of the digital economy and technological subsystem by end-to-end technologies. Whereupon with this approach, there is a systems chain as a relation: "Supersystem (DE) - Blockchain system (DLT) Information Security subsystem (ISS)", within which a security policy can be formed, including all its mandatory attributes (threat and intruder models, special technical specifications, etc.) on the basis of the functional requirements of the Supersystem and technological features of the DLT.

The Development principle assumes a possibility of long-term development of the information security subsystem on the basis of new requirements from both infrastructure changes in the system and functional changes in the DLT. Regarding the information security subsystem the implementation of this principle is a very difficult task especially in terms of changing the functionality talking about our experience of creating a row of information systems.

However, this principle in relation to the tasks of the digital economy is imperative. It allows maintaining the integrity and relevance of the information security subsystem without disruption.

The Compatibility principle means the implementation of such systems and organizational solutions of information security subsystem, which provides a possibility of DLT interaction with other technological subsystems of the digital economy. In other words, if the Development principle is about scaling "vertically", the Compatibility principle is about scaling "horizontally".

The Standardization (Unification) principle has two very important aspects. The first is to apply on a maximum standard, unified and standardized components and project solutions that have already been tested in practice when creating an information security subsystem. At the same time, DLTs are new technologies in many ways and therefore the second aspect is very important, which is necessary to standardize newly developed technological and technical solutions. Thanks to this principle, the costs of security subsystem creation, it's maintenance and training of maintenance personnel can be significantly reduced.

The Efficiency principle is to achieve a rational balance between the cost of creation of information security subsystem and the achievement of target indicators. For example, it is necessary to maximum the use of created infrastructure.

In addition, the Efficiency principle must be applied for all stages of the information security subsystem lifecycle (including investigations, design, putting into operation, direct operation, modernization and development).

The above principles can be attributed to system engineering. Besides them, organizational principles of system approach are highlighted often, actual for large systems especially. These principles are discussed in detail in [13, 14].

Thus, in a concentrated form the essence of a system approach to the creation of the information security subsystem in DLT is to choose the most effective organizational and system solutions, including:

- formation of DLT infrastructure;
- formalized representation of the information security subsystem, including all its components (technical, software, infrastructure, organizational);
- substantiation of the threat and intruder model in the system of distributed ledgers technologies;
- formation of alternatives of information security subsystem design (including all above components);
- selection of the alternative with the highest efficiency (according to the selected indicator).

With this approach, the information security subsystem is "deeply immersed" in DLT as in subsystem of the Digital economy.

IV. Consensus based on trust in the state

Let's consider an example of consensus which is possible in the digital economy for small and medium enterprises. A consensus is proposed which ensures the trust of the parties based on the state support system. The state structure provides systemic resources for the organization of DLT. The state provides DLT-secured platform for block creation and blockchain building, provides secured telecommunications services and secured storage for filled ledgers, provides backup and recovery.

It should be noted that protection against insider attacks to blockchain is provided by cryptography, and is easily detected by the state information security structure. In order to provide documentary evidence of fulfilled obligations, subcontractors fill their blockchains with confirmations of messages received by communication, which security is guaranteed by the protocols of non-repudiation. A disagreement of data is considered by the arbitration.

V. The situation centers system as a platform for the implementation of information security in distributed ledgers

Let's consider one of the most important components of the information security subsystem infrastructure. Certainly, the creation of separate infrastructure for DLT implementation would not be justified obviously. In this regard, it seems appropriate and very attractive to use the platform of distributed situation centers (DSSC) as an infrastructure component of the DLT information security subsystem. The system is currently being created in accordance with regulatory documents at the level of President RF Decrees and Government resolutions [15].

The DSSC should cover the situation centers (SC) of the Supreme bodies of state power, departments and ministries, regions as well as large business structures. The most important feature of the DSSC is the subject to unify multifunctional SC with different departmental and regional affiliations, which were created as an integral part of the management system of a certain organizational system. Another feature of the DSSC is the need to process information of different categories (transfer of information from "open" circuit to "confidential" and "closed" circuits and a joint display of information from different circuits).

To solve such large-scale problems the DSSC is created as a multi-level geographically distributed system, where situation centers are integrated on the basis of system forming components that allow interaction of participants (existing and created SC). These include (Fig. 1):

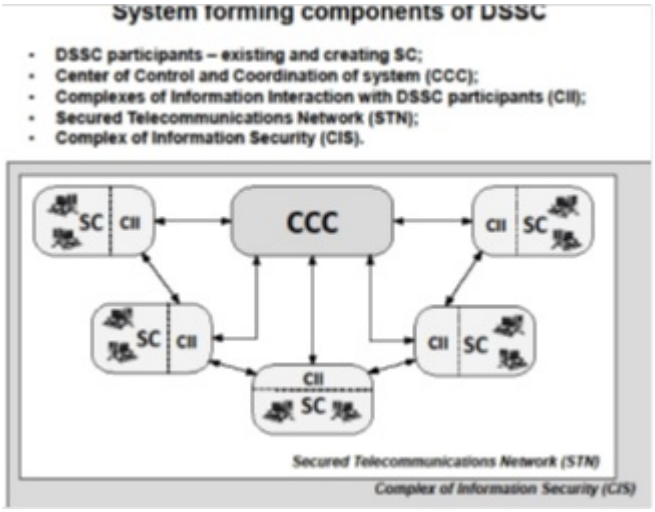

Fig. 1. System forming components of DSSC

- Center of Control and Coordination of system (CCC), distributed data warehouse (DDW);
- Complexes of Information Interaction (CII);
- Secured Telecommunications Network (STN);
- Complex of Information Security (CIS) [11]. CIS of the DSSC performs the function of collecting and processing information about a status and security breaches to come up with solutions in information security, information exchange in action implementation for information security;
- administration of protection against unauthorized access;
- organization of routine maintenance and preventive works on ISS;
- identification, prevention, repelling and neutralization of security violations,
- as well as the functions of the certifying center, antivirus center, the center for monitoring of computer attacks on the resources of the DSSC, as well as administrative functions for its management.

It seems that the wide functionality of CIS along with geographically distributed secure telecommunication networks of the DSSC will allow its usage in interests of information security subsystems in distributed ledgers.

VI. Conclusion

Technologies of the distributed ledgers are of a system forming nature and require an information protection.

Based on the principles of the system approach, the information security subsystem in distributed ledgers may be created using the infrastructure and technological capabilities of the State platform of distributed situation centers.

REFERENCES

[1] The Missive from President RF Vladimir Putin to the Federal Assembly, (Dec 01, 2016). Available: http://kremlin.ru/events/president/news/copy/53379.

[2] The Strategy of scientific and technological development of the Russian Federation (approved by presidential decree 642, Dec 01, 2016). Available: http://static.kremlin.ru/media/events/files/ru/uZiATIOJiq5tZsJgqcZLY9YyL8PWTXQb.pdf.

[3] Schwab, K. *The fourth industrial revolution.* Eksmo, Moscow, 2016.

[4] National goals and strategic objectives of development of the Russian Federation until 2024, the decree of the President of the Russian Federation No. 204, (May 07, 2018). Available: http://static.kremlin.ru/media/acts/files/0001201805070038.pdf.

[5] The Program "Digital Economy of the Russian Federation" (approved by Order 1632-p of the Government of the Russian Federation, (Jul 28, 2017). Available: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.

[6] Swan, Melanie. *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2015.

[7] Leloup, Laurent. *Blockchain: La revolution de la confiance*. Groupe Eyrolles, 2017

[8] Zatsarinny, A. A., Kiselyov, E. V., Kozlov, S. V., Colin, K. K. *Information space of digital economy of Russia. Conceptual bases and problems of formation*. Zatsarinny, A.A. (eds.), FRC CSC RAS, Moscow, 2018

[9] Grusho, A. A., Grusho, N. A., Timonina, E. E. "Information security architecture synthesis in distributed information computation systems", *Automatic Control and Computer Sciences*, V. 51, no. 8, P. 799-804, 2017.

[10] Grusho, A., Grusho, N., Levykin, M., Timonina E. "Analysis of information security of distributed information systems", in *9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops* (ICUMT 2017), 2017, pp. 96-100.

[11] Grusho, A. A., Primenko, Ed. A., Timonina, E. E. *Theoretical bases of computer security*. Publishing Center Academy, Moscow, 2009.

[12] Prangishvili, I.V. *System approach and system-wide regularities*. Sinteg, Moscow, 2000.

[13] Zatsarinny, A.A. "The basic principles of system approach at design, introduction and development of modern corporate networks", *Systems and means of informatics*, V. 12, pp. 58-66, 2002.

[14] Zatsarinny, A.A., Colin, K.K. "Methodological bases of system approach to creation of information systems in the conditions of globalization of society", *Strategic priorities*, V. 1, no. 17, pp. 38-61, 2018.

[15] *Socio-humanistic aspects of the situational centers of development*. Lepsky, V.E., Raykov, A.N. (eds.), Kogito-center, Moscow, 2017.

Alexander A. Grusho is Doctor of Science in physics and mathematics, Professor. He is principal scientist at Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences and Professor of Moscow State University.

Research interests: probability theory and mathematical statistics, information security, discrete mathematics, computer sciences.

Alexander A. Zatsarinny is Doctor in Technical Science, Professor. Now he works as Deputy Director in Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences.

Research interests: informatization of science, education and production.

Elena E. Timonina is Doctor in Technical Science, Professor. Now she works as leading scientist in Institute of Informatics Problems, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences.

Research interests: probability theory and mathematical statistics, information security, cryptography, computer sciences.

Системный Подход к Информационной Безопасности в Распределенных Бухгалтерских Книгах на Платформе Ситуационных Центров

А. А. Грушо, А. А. Зацаринный, Е. Е. Тимонина

***Аннотация* — В статье рассматриваются вопросы внедрения одного из основных направлений цифровой экономики, связанных с информационной безопасностью, в отношении защиты информации в распределенных бухгалтерских книгах. Любая информационная система должна быть построена на современной компьютерной платформе и использовать современные сетевые возможности. Компьютерная платформа обеспечивает безопасность информационной системы, решает проблемы резервирования информации, а также поддерживает восстановление системы после сбоев. Обмен информацией через сеть предполагает специальные средства защиты информации. Для этих целей используются криптографические алгоритмы для шифрования и коды аутентификации сообщений для контроля целостности. Показано, что в рамках программы цифровой экономики технологии распределенной бухгалтерской книги имеют системообразующую природу и должны создаваться совместно с другими технологиями с учетом принципов системного подхода к созданию информационных сетей.**

Авторы предложили использовать платформу и функциональные ресурсы системы распределенных ситуационных центров в качестве инфраструктурной базы подсистемы информационной безопасности в распределенных бухгалтерских книгах. При этом предполагается, что консенсус основан на доверии к защищенным системам ситуационных центров.

***Ключевые слова* — Инфраструктура информационной безопасности, системный подход, интеллектуальная бухгалтерская книга, распределенные ситуационные центры.**

Библиография

[1] Послание Президента РФ В.В. Путина Федеральному Собранию, 1 декабря 2016 года. Available: http://kremlin.ru/events/president/news/copy/53379.

[2] Стратегия научно-технологического развития Российской Федерации (утверждена Указом Президента РФ №642 от 01.12.2016. Available: http://static.kremlin.ru/media/events/files/ru/uZiATIOJiq5tZsJgqcZLY9YyL8PWTXQb.pdf.

[3] Шваб К. *Четвертая промышленная революция*. М.: Эксмо, 2016.

[4] «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», Указ Президента РФ №204 от 07.05.2018. Available: http://static.kremlin.ru/media/acts/files/0001201805070038.pdf.

[5] Программа «Цифровая экономика Российской Федерации» (утв. Распоряжением Правительства РФ от 28.07.2017 №1632-р). Available: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.

[6] Swan, Melanie. *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2015.

[7] Leloup, Laurent. *Blockchain: La revolution de la confiance*. Groupe Eyrolles, 2017

[8] Зацаринный А. А., Киселев Э. В., Козлов С. В., Колин К. К. *Информационное пространство цифровой экономики России. Концептуальные основы и проблемы формирования* / Под общей редакцией А. А. Зацаринного. - М.: ФИЦ ИУ РАН, 2018.

[9] Grusho, A. A., Grusho, N. A., Timonina, E. E. "Information security architecture synthesis in distributed information computation systems", *Automatic Control and Computer Sciences*, V. 51, no. 8, P. 799-804, 2017.

[10] Grusho, A., Grusho, N., Levykin, M., Timonina E. "Analysis of information security of distributed information systems", in *9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops* (ICUMT 2017), 2017, pp. 96-100.

[11] Грушо А. А., Применко Э. А., Тимонина Е.Е. *Теоретические основы компьютерной безопасности*. М.: Академия, 2009.,

[12] Прангишвили И. В. *Системный подход и общесистемные закономерности*. М.: Синтег, 2000.

[13] Зацаринный А. А. "Основные принципы системного подхода при проектировании, внедрении и развитии современных корпоративных сетей", *Системы и средства информатики*, Вып. 12, С. 58-66, 2002.

[14] Зацаринный А. А., Колин К. К. "Методологические основы системного подхода к созданию информационных систем в условиях глобализации общества", *Стратегические приоритеты*, Т. 17, №. 1, pp. 38-61, 2018.

[15] *Социогуманитарные аспекты ситуационных центров развития* / Под ред. В.Е. Лепского, А.Н. Райкова. М.: Когито-Центр, 2017.