European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com

e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.09.02.196

ICEST 2021
II International Conference on Economic and Social Trends for Sustainability of Modern Society

ORGANIZATION OF BUSINESS PROCESSES IN THE FIELD OF INFORMATION SECURITY

A. O. Rukosuev (a), N. T. Avramchikova (b), I. P. Rozhnov (c)*, O. V. Maslova (d)
*Corresponding author

(a) Reshetnev Siberian State University of Science and Technology, Krasnoyarsk 660031, Russia, a9082012551@yandex.ru
(b) Reshetnev Siberian State University of Science and Technology, Krasnoyarsk 660031, Russia, avr-777@yandex.ru
(c) Reshetnev Siberian State University of Science and Technology, Av. Krasnoyarskiy Rabochy 31, Krasnoyarsk 660031, Russia, ris2005@mail.ru
(d) Reshetnev Siberian State University of Science and Technology, Krasnoyarsk 660031, Russia, olga_maslova08@list.ru

Abstract

In Russia, a considerable work on the practical implementation and development of digital services and technologies in public administration is being conducted. The characteristics of business models in the field of digitalization within the framework of the program of the digital economy of Russia are given. It is noted that an integral part of the program is information security and its culture in the life of the population. State and municipal authorities interact with the population using the possibilities of digital technologies. The importance of information security for the implementation of the tasks of regional informatization and the development of economic sectors is revealed. The purpose of organizing business models in the field of digital security of public administration is to achieve the condition of protection of the individual, society and the state from internal and external information threats, which ensures the sovereignty and sustainable socio-economic development of the Russian Federation in the digital economy. The article considers the essence of information security and its influence on the information future of the subject of the Federation and the country as a whole on the example of the departmental centre of GosSOPKA in the Krasnoyarsk Territory. The hierarchy of structures of the GosSOPKA commercial system is given. It is concluded that the information security aspect is the basis for the realization of further progressive national development and increasing the country's competitiveness on the world stage in the field of information technology implementation.

Keywords: Business model, information security, end-to-end digital technologies, critical information infrastructure

https://doi.org/10.15405/epsbs.2021.09.02.196
Corresponding Author: I. P. Rozhnov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The solution of the priority tasks of the socio-economic development of Russia in accordance with the global technological mainstream is possible only with the development, use and widespread dissemination of digital technologies in business processes, public administration and social and social spheres. At the same time, the most popular are digital technologies for the provision of online services in trade, finance, crowdfunding and other technologies. Modernization of traditional mathematical business models in this direction has led to the development of the following categories of new business models (Capgemini, 2018; Kazakovtsev et al., 2020; Vasilieva & Likhacheva, 2012):

1. Models based on attracting external resources: money, people, ideas, etc. (crowdsourcing models) for the implementation of auxiliary functions of business processes for the development of innovations, new products, marketing, sales, etc.
2. Business models, focused on customer requests and needs (outcome based models), the effect of which is achieved through the consumption of complex products and services. Such business models, by analogy with service ones, are often called Product-as-a-Service (PaaS).
3. Business models that expand the possibilities of joint consumption of goods and services and at the same time minimize transaction costs, which becomes possible with direct interaction of partners-suppliers, buyers and sellers.
4. Models and platforms that provide monetization of customer personal data when selling information on paid services using information sources free of charge for users.
5. "As a service" business models based on resource utilization using new varieties of service models. These service models provide personalization of goods and services and enable the client to achieve the desired result while consuming the required product.

2. Problem Statement

State and municipal authorities interact with the population by means of possibilities of digital technologies. In Russia a considerable work is being carried out on the practical implementation and development of digital services and technologies in public administration. The main measures concerning digitalization of public administration are formulated in the federal project "Digital Public Administration" included in the national project "Digital Economy of the Russian Federation" (Digital government, 2021).

In the explanation to this federal project, it is noted that " it is aimed at achieving the national goals defined in paragraph 1 of the Decree of the President of the Russian Federation of May 7, 2018 N 204 "On National Goals and Strategic Objectives of the Development of the Russian Federation for the period up to 2024", and, above all, causes a direct impact on ensuring the accelerated introduction of digital technologies in the economy and social sphere by means of the application of digital technologies and platform solutions in the spheres of public administration and public services, including the interests of the population and business entities, and also provides a qualitative improvement of a number of indicators reflecting the growth of the national economy and social sphere"**.**

The concept of this program envisages that the development of the digital economy in the period up to 2024 will be ensured by achieving the goals, which we spoke about earlier, in the following important areas (Digital economy of the Russian Federation, 2021):

1. Normative regulation.
2. Personnel and education.
3. Formation of research competencies and technical groundwork.
4. Information infrastructure.
5. Information security.

Within the framework of the federal project "Digital State Administration", two main directions have been defined:

1. Introduction of digital technologies and platform solutions in the field of public administration and provision of public services, including the interests of the population and business entities.
2. Development and introduction of the national mechanism of the implementation of the coordinated policy of the member states of the Eurasian Economic Union in the realization of plans of the digital economy development.

In the national program "Digital Economy of the Russian Federation" nine "end-to-end" digital technologies (EtoEDT) are distinguished, which are used for collecting, storing, processing, searching, transmitting and presenting data in electronic form, the functioning of which is based on software and hardware tools and systems, demanded in all sectors of the economy and creating new markets and changing business processes (Digital economy of the Russian Federation, 2021).

1. Big data are technologies for collecting, processing and storing structured and unstructured information arrays, characterized by a significant volume and high rate of changing (including in Real time mode), what requires special instruments and methods of dealing with them.
2. Artificial intelligence — a system of software and/or hardware tools, which is able to acquire information with a certain degree of autonomy, learn and take decisions based on big data analyses, including human behavior simulation.

Neuroethologies are cyber-physical systems which partially or completely replace / supplement the functioning of the nervous system of a biological object, including those based on artificial intelligence.

3. Distributed Ledger Technologies (block chain) - algorithms and protocols for the decentralized storage and processing of transactions, structured as a sequence of linked blocks without the possibility of their subsequent change.
4. Quantum technologies are technologies for creating computing systems based on new principles (quantum effects) allowing radically change the ways of transmitting and processing big data.

https://doi.org/10.15405/epsbs.2021.09.02.196
Corresponding Author: I. P. Rozhnov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

5. New production technologies are technologies for the digitalization of production processes, which ensure an increase of the efficiency of resource use, design and manufacture of individual objects, the cost of which is comparable with the cost of mass-produced goods.

Additive technologies are technologies of layer-by-layer creation of three-dimensional objects on the basis of their digital models ("twins"), allowing to manufacture products of complex geometric forms and profiles. Supercomputer technologies are technologies, which provide high-performance computations due to the application of the principles of parallel and distributed (grid) data processing and high throughput.

Computer engineering are technologies for digital modeling and design of objects and production processes throughout the life cycle.

6. Industrial Internet are data transmission networks which unite devices in the manufacturing sector, equipped with sensors and capable to interact between each other and/or with the external environment without human intervention.
7. Components of robotics (industrial robots) - production systems with three or more degrees of mobility (freedom), built on the basis of sensors and artificial intelligence, able to perceive the environment, control their own actions and adapt to its changes.
8. Sensorics - technologies for creating devices, which collect and transmit information about the state of the environment through data transmission networks.
9. Technologies of wireless communication are technologies of data transmission by means of a standardized radio interface without a wired connection to the network application.
10. 5G is the fifth generation wireless communication technology characterized by high bandwidth (at least 10 Gbp/s), network reliability and security, low data transmission latency (no more than one millisecond), what results in effective big data application.
11. Technologies of virtual reality - technologies of computer modeling of a three-dimensional image or space, through which a person interacts with a synthetic ("virtual") environment with the subsequent sensory feedback.

Augmented reality technologies are visualization technologies based on adding information or visual effects to the physical world by overlaying graphic and/or sound content for improving user experience and interactivity. The proposed set of "end-to-end" technologies is not well-founded, unfortunately. For example, the use of distributed ledger systems has got a very limited application and cannot be recommended for all basic directions. At the same time, because of the lack of practical results in the sphere of quantum technologies, it seems to be very difficult to imagine the practical implementation of quantum technologies, quantum cryptography, technology for creating trusted environments and other technologies of this direction in the foreseeable future (Novikova & Strogonova, 2020). To achieve this goal, the program has identified a number of tasks, which can be divided into the following directions:

1. Ensure the technological independence and security of the hardware and data processing infrastructure (paragraphs 5.1 and 5.2 of the program);
2. Ensure the security of the functioning of the Russian segment of the Internet;
3. Develop regulatory mechanisms for the functioning of the CPS in the digital economy (paragraphs 5.5-5.8, 5.10-5.12);
4. Create the basis for building a trusted environment for the functioning of the CPS;

5. Ensure the stability and safety of the functioning of information systems and technologies (paragraphs 5.4 of the program);
6. Ensure international cooperation on information security issues in the digital economy.

3. Research Questions

The purpose of business models organisation in the field of digital security of public administration is to achieve a state of protection of the individual, society and the state from internal and external information threats, which ensures the realisation of constitutional rights and freedoms of a man and a citizen, a decent quality and standard of living of citizens, sovereignty and sustainable social-economic development of the Russian Federation in the digital economy (Sidorenko et al., 2019). To realize the tasks of regional informatization and development of economic sectors, it is important to create innovations, solutions and effective practices in the IT industry. In this regard, in accordance with federal law from 26.07. №187-FL "On the security of the critical information infrastructure of the Russian Federation", GosSOPKA are being created in the regions (Federal Law N 187-FZ…, 2017). By the end of 2018, the National Coordination Centre for Computer Incidents (NCCforCI of the FSB of Russia) concluded more than a dozen agreements with organizations on their participation in the system as GosSOPKA centres. The GosSOPKA system is a commercial system organised for collecting and exchanging information concerning computer attacks on the territory of the Russian Federation.

In the subjects of the Russian Federation, as a part of ensuring the security of significant objects of the critical information infrastructure of the Russian Federation in the protection system basic measures, aimed at countering computer attacks, should be realised (Rozhnov et al., 2020). Critical information infrastructure (hereinafter CII) refers to information systems, information and telecommunications networks, automated control systems of CII subjects, as well as telecommunication networks used to organize their interaction. The hierarchy of the structures of the GosSOPKA commercial system is shown in Figure 1.

State regulators underline that the protection of the CII object from computer attacks is the duty and responsibility of the CII subject itself: the state does not intend to share this responsibility with it, in any way confirming the sufficiency of the protection measures taken by the subject. This implies the possibility (inevitability) of mistakes made by the subjects of the CII when protecting their information systems. Therefore, FL87 allows that, despite the implemented security measures, incidents in significant CII objects are possible. In accordance with the law, the owner of a significant CII object independently decides how exactly he will protect the system from computer attacks, i.e. prevent the possibility of attacks, detect and localize attacks, not allowing them to develop into an incident. But this freedom lasts exactly until the moment an incident happens, that is, until the subject turns out to be unable to cope with the attack. In this case, he is obliged to inform the FSB about the incident and must follow the instructions of the department on responding the attack. From this moment, helping the subject in responding to the attack becomes the task of the GosSOPKA. The GosSOPKA centres, serving their clients, act as intermediaries between the subjects of CII and NCCforCI.

https://doi.org/10.15405/epsbs.2021.09.02.196
Corresponding Author: I. P. Rozhnov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

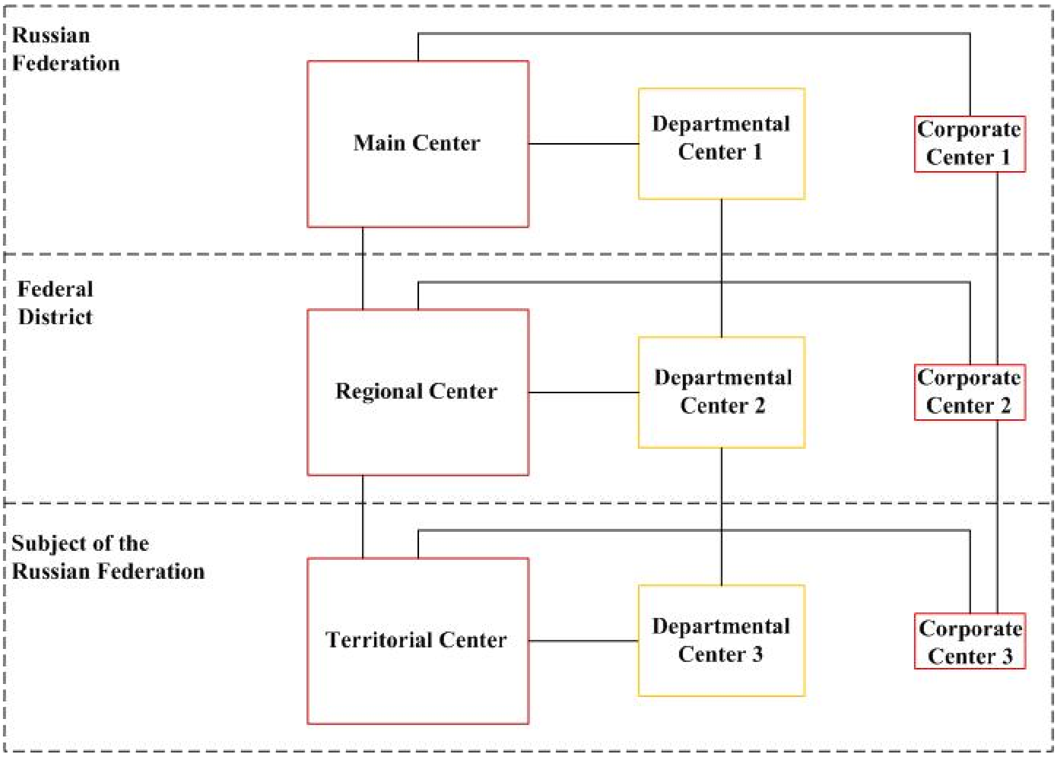

Figure 1. Hierarchy of structures of the GosSOPKA commercial system

4. Purpose of the Study

In the Krasnoyarsk Territory a departmental centre of the state system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation is being built. As a part of the realization of this goal the "Security System of Significant Objects of Critical Information Infrastructure of the Regional State Public Institution "Centre for Information Technologies of the Krasnoyarsk Territory "- the Departmental Centre GosSOPKA was created in the region. The purpose of the system is:

1. Ensuring of information security of the electronic government of the Krasnoyarsk Territory, executive authorities of the Krasnoyarsk Territory and their subordinate organizations.
2. Ensuring of a continuous process for identifying any events which could influence the safety.
3. Ensuring of an adequate response to the events which have occurred.
4. Operational liquidation of the consequences of an incident (including control over the restoration of the normal functioning of resources in case of computer incidents caused by computer attacks).
5. Preventing the repetition of incidents.

In particular, for the creation of the Security System of the SOofCII RSPI "CIT", it is necessary to consistently solve the following tasks:

1. Perform the analysis of information security threats and develop requirements for ensuring the security of SOofCII.
2. Develop a project of the SOofCII security system.

3. Regulate the rules and procedures for ensuring the safety of SOofCII.
4. Realize the construction of the departmental centre of GosSOPKA.

5. Research Methods

To build the Departmental Centre of GosSOPKA, it is proposed to introduce software products from "Positive Technologies": MaxPatrol SIEM and "PT Departmental Centre". MaxPatrol SIEM is a real-time information security event monitoring and correlation system which collects and analyses security events from various sources, compares them with the rules and correlates security events from various sources and hardware and software configurations. The data obtained allow to make an assessment of the security with immediate information of the responsible employees.

MaxPatrol SIEM solves the following tasks:

1. Providing inventory and analysis of configurations of information assets.
2. Detection and collection of IS events from IS elements.
3. Operational control of the security of IS elements.
4. Correlation of events and detection of information security incidents.
5. Management of information security incidents.
6. Making reports on the results of work.
7. Providing storage of initial and normalized information security events.

"PT Departmental Centre" is an incident management system. It automates the process of reacting to incidents and informs the National Coordination Centre for Computer Incidents - the main centre of GosSOPKA. Information about incidents comes from MaxPatrol SIEM and from users of information systems.

6. Findings

The departmental centre of GosSOPKA solves the following tasks:

1. Formation and keeping up actual data about information resources of RSPI "CIT".
2. Formation and keeping up actual information about computer incidents.
3. Formation of tasks for the investigation of computer incidents.
4. Sending information about computer incidents to NCCforCI.
5. Accounting of the information sent to the NCCforCI.

The implementation of the DC will allow:

1. To organize the process of investigating computer incidents.
2. To send information about the investigation of computer incidents to the NCCforCI in the required exchange format.

3. To receive methodological recommendations and information messages from NCCforCI.
4. To keep records of information sent to the NCCforCI;.
5. To reduce incident response time by automating incident registration and processing.
6. Analyze the results of incident response using reporting and visualization tools.

All interaction between the Departmental Centre and the main centre of GosSOPKA on the Internet is carried out using cryptographic information security tools certified by the FSB of Russia.

Within the framework of the exchange via the Internet, the following interaction methods are supported:

1. Exchange of information through specialized systems, such as a portal, or automated data exchange of automated subsystems and components of GosSOPKA.
2. Exchange of information and access to reference information using interaction automation tools.
3. E-mail correspondence.

Specialized systems of information exchange should provide the possibility of interaction both in manual mode (operator actions) and in automated mode (via the API). To carry out the work of the Certification Centre, a license from the FSB of Russia was obtained for the development of protection means.

At the moment, outsourcing services are being purchased and put into commercial exploitation with the connection of facilities not related to the ministry on the basis of agreements. It is necessary to form a separate division, obtain licenses from the FSTEC of Russia and the FSB of Russia, develop a package of organizational documentation and consolidate powers in the regulation on the ministry and the charter of the organization. In particular, the creation of the Departmental Centre GosSOPKA in the Krasnoyarsk Territory will contribute to the solution of the following tasks in the field of information security:

1. Prevention of illegal access to information, destruction of such information, its modification, blocking, copying, provision and distribution, as well as other illegal actions in relation to such information.
2. Prevention of impact on technical means of information processing.
3. Carrying out measures to assess the degree of security of controlled information resources.
4. Carrying out activities to establish the reasons of computer incidents caused by computer attacks on controlled information resources.
5. Collection and analysis of data on the state of information security in controlled information resources.
6. Informing interested parties in the sphere of responsibility of the DC on the detection, prevention and liquidation of the consequences of computer attacks.
7. Formation and keeping up in actual state information about controlled information resources.
8. Providing the ability to connect third-party CII subjects to the DC.

The structure of the DC GosSOPKA generates a kind of public-private partnership in countering computer attacks issues. The threat of hacker attacks is relevant both to government authorities and to business, but in the spheres, defined by the law, they are of a particular danger to the society (Yakutin, 2017). Not everyone is able to defend himself against such attacks on his own. Within the framework of GosSOPKA, the concentration of competencies necessary to prevent attacks and respond to them is ensured, and both representatives of large business and small companies and even individual entrepreneurs can make use of such competencies. At the same time, the state, represented by the NKTsKI, acts as the guarantor of the integrity of the GOSOPKA centres, establishing the requirements for their activities, exercising supervision of these activities.

7. Conclusion

The distribution of the national digital economy program mostly depends on information security and the level of realization of the state of security of objects and subjects of the information system. Today the processed information is of great value for all spheres of the population's activity. That is why the aspect of information security plays an important role in the further development of this program and is the basis for the realisation of further progressive national development and increasing the country's competitiveness on the world arena in the field of introducing information technologies. Moreover, the application of the program will lead to the improvement of the regional government bodies functioning.

References

Capgemini. (2018). *World Wealth Report*. https://www.capgemini.com/service/world-wealth-report-2018/

Digital economy of the Russian Federation. (2021). https://digital.gov.ru/ru/activity/directions/858/

Digital government. (2021). https://digital.gov.ru/ru/activity/directions/882/

Federal Law N 187-FZ dated July 26. (2017). "On the Security of the Critical Information Infrastructure of the Russian Federation". http://www.consultant.ru/document/cons_doc_LAW_220885/

Kazakovtsev, L., Rozhnov, I., Popov, A., & Tovbis, E. (2020). Self-adjusting variable neighborhood search algorithm for near-optimal k-means clustering. *Computation*, *8*(4), 90. https://doi.org/10.3390/computation8040090

Novikova, N. V., & Strogonova, E. V. (2020). Regional aspects of studying the digital economy in the system of economic growth drivers. *Journal of New Economy, 21,* 76-93. https://doi.org/10.29141/2658-5081-2020-21-2-5

Rozhnov, I. P., Avramchikova, N. T., Maslova, O. V., Lapunova, E. V., & Bezrucov, M. A. (2020, November). Digital technologies in the regional management information system. In *Journal of Physics: Conference Series* (Vol. 1679, No. 3, p. 032004). IOP Publishing. https://doi.org/10.1088/1742-6596/1679/3/032004

Sidorenko, E. L., Bartsits, I. N., & Khisamova, Z. I. (2019). The effectiveness of digital public administration: theoretical and applied aspects. *Issues of state and municipal administration, 2,* 93-111.

Vasilieva, Z. A., & Likhacheva, T. P. (2012). *Innovative Factors of Economic Growth of Territories*. Sib. Feder. Un.

Yakutin, Yu. V. (2017). The Russian economy: a strategy for digital transformation (Constructive criticism of the government programme "Digital economy of the Russian Federation"). *Management and Business Administration*, *4*, 27-52.