International Journal of Engineering & Technology, 7 (1) (2018) 39-43

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i1.8788
Research paper

Cluster-type models in the logistics industry

A.P. Nyrkov *, S.S. Sokolov, A.S. Karpina, A.V. Chernyakov, V.D. Gaskarov

Admiral Makarov State University of Maritime and Inland Shipping, Saint-Petersburg, Russia
**Corresponding author E-mail: sokolovss@gumrf.ru*

Abstract

The aim of the present article is to detect the basic principles of secure electronic document circulation (EDCS) systems for multi-location structure with multiple non-uniform connections. As far as the object of research is concerned, transport-logistical clusters are used. It is heterogeneous system with implicit classification. In the article were examined the basic stages of designing, methods and models of information security in electronic document circulation systems, operating in distributed network and interacting with other informational systems. The article contains analysis of regulatory and legal base in information security field of Russian Federation. The model of cluster information flows has been created for research purposes, based on hierarchical interaction model of transport-logistical cluster components. We describe transport-logistical cluster subjects, categorized information and supposed information assets. Based on potential threats and system vulnerabilities, mechanisms of EDCS information security have been described. EDCS data exchange process with another system, containing personal data has been described. As a result, a comprehensive set of measures was formed as well as information security tools based on requirements for data protection of personal data, and automated control systemsand transport-logistical cluster information systems at critical objects.

Keywords: *Transport and Logistics Clusters; Electronic Document Workflow Systems; Information Security; Distributed Systems Architecture.*

1. Introduction

As of 2014, according to logistics performance index (LPI) set by World Bank, Russia was at 93rd place among 163 countries [1]. In the same year the new version of Russian Transport Strategy has been issued, in the context of which the new unified information environment (UIE) for interaction of all transport types should be created till 2030 to create the single transport area (STA) and also to raise security level of transport systems [2].

To reach these goals, the government of Russian Federation financed the development of regional scale transport-logistical clusters (TLCs). Their core must be transport and logistical centers (TLCs), built on the base of urban concentration. The issue of transport security is at the center of interest in modern transport system. The rapid development of the IT industry has had a positive impact on the data protection in the transportation sector.TLC is a union of companies, providing services in transportation and freight logistics, aiming to increase quality and speed of service. As it reflected by its name, TLC is complex structure with multiple heterogeneous connections. To create ubiquity secured information exchange zone in Russian transport system, security of every elementary item should be guaranteed.

2. Identification of protection object

Nowadays there is no shared and formally structured knowledge of TLCs. The absence of the formalized object description complicates the process of designing its security system. As a consequence, the first stage of our scientific research was aimed to defining unambiguously the object of our studies and its characteristics. In order to reach this goal, the following tasks have been formulated:

- definition and classification of TLC;
- Detection of interaction patterns in transport-logistical cluster's objects;
- Detection of TLC structure and components;
- Designing of generic model of TLC information flow.

During the research, foreign and domestic experience on the creation of similar structures has been studied. The following foreign clusters have been analyzed: Rotterdam port cluster, Padborg border TLC and the biggest European regional cluster in Frankfurt. Nowadays, there are no fully operation TLCs in Russia, but in many regions, it can be noticed the creation of potential clusters: Ulyanovsk, Samara, Kaluga, Novosibirsk and Yekaterinburg. The research included analysis of current positions and expected results for these clusters, and developed strategies of these regions in Russian Federation.

Furthermore, scientific papers of domestic scientists in this field, such as T.A. Prokofyeva, T.Y. Yevdotyeva, I.G. Smirnova and I.T. Mannibayeva were used to find TLC characteristics, determining the exact type of the cluster.

Consequently at the first stage, TLC hierarchic structure was built, and the ways of data flows were determined [3]. During the process of description of the protected object, it was performed information rating of data processed in TLC information system, and segregated user rights, for whom one or another information category is available.

TLC consists of 4 levels. Based on its level, restricted information is distributed and processed by participant companies. The lowest (the first) level is a cluster core, it consist of companies providing major transportation and storage services. Cluster core is a big company or group of companies that are in charge of the over whole development of the cluster. Core companies could be huge freight forwarders, railroad departments, seaports, and logistics

Copyright © 2018 A.P. Nyrkov et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

hub stations or logistics centers. All constituents of the aforementioned level share information freely among one another.
The second level consists of servicing objects, companies, which are crucial to the right functioning of the cluster. These objects handle tasks, which must be performed daily in order to sustain the operational ability of the whole structure. Such companies include repair services, storages, finance institutions, freight terminal handlers, etc. A constituent of the second level has access only to its own information as well as information of clients from the first level.
The third level consists of auxiliary objects. These are such companies, which bear no importance on TLC business process. They can be the part of a cluster, but in case of their absence, TLC can rely on outsourcing companies. These are such companies as insurance firms, security companies, advertisement agencies, etc. Information access for this level is restricted and is provided by the first level on demand.
The last component is the fourth level, consisting of companies that form the innovation input. These are scientific laboratories, institutes, techno-parks, technology cities, innovation centers and other companies taking part in science development. This level has access only to information, which is used for its own activity.
Connection of all levels with the core is performed based on following scheme: from the core level to single company and from single company to the core level. It means there is no face-to-face interaction between single companies of the lower levels with each other. It is suggested that the fourth level operates within its segment (face-to-face interaction).

3. Methods

After highlighting the characteristics of protected object, methods and models of information security were analyzed. Based on resource presumption for the information system, the generic model of information security system of EDCS in TLC was developed. According to presumed resources, possible exposures and threats were determined [4], [5].
There are eight categories of attackers:

- Hackers, competitors, criminal organizations – N1;
- Former workers – N2;
- Technical staff without access to IS and EDCS; clients and partners of TLC – N3;
- legitimate IS user – N4;
- legitimate EDCS user – N5;
- IS administrator – N6;
- EDCS administrator – N7;
- Information security administrator – N8.

These attackers differ in level of knowledge, training, technical equipment and possible attack zone. Within IS and EDCS of TLC, attack could be carried out on the following functional levels: physical, internet, network services level, OS level, information system database level, and the user level. Information security model was developed using the Standard of Bank Rossii STO BR IRBS-1.0-2014 “Information security in companies of banking sector of Russia” [6].
Analyzing the possible attackers, it was determined that the most dangerous attacker category is inner attackers. For simplification of construction of secured workflow system, the “Prisoner dilemma” was applied to cluster structure components. Using the principles of this dilemma, inter-cluster loyalty could be raised. TLC will benefit from this situation because of its unique structure.
Since TLC is a community of several divided companies, their interaction will be performed through Internet. Several possible network attacks were analyzed, including mail-bombing, DoS and DDoS, brute force, root-kits and breaches in EDCS, code injection, malware, man in the middle attacks, packet sniffing, IP-spoofing, network reconnaissance [5]. The result of the second stage is a list of threats and exposures, attacker types shown in Table 1. It was used as a base for creating the complex of protection tools.

Table 1: Model with Total Intersection for EDCS TLC

Resource	Threat	Exposure	Attacker type	Prevention tools
E-mail server	server unauthorized access, theft and server destruction	weak access control arrangements	N6, N8	physical protection and organization preventive measurescertified
	remote connection	errors in operating system or EDCS application, configuration errors	N1, N2, N8	EDCS (Microsoft Exchange Server 2013 Enterprise, Windows Server Standard 2012), FW, IDS/IPS
	denial of service	absence of monitoring in resource distribution (resources limitation)	N1, N2, N4,N6	FW, IDS/IPS
back-up servers	server unauthorized access, theft and server destruction	weak access control arrangements	N6, N8	physical and organization preventive measures
	remote connection	errors in operating system or application, configuration errors	N1, N8	certified EDCS
EDCS servers	server unauthorized access, theft and server destruction	weak access control arrangements	N7, N8	physical and organization preventive measures
	remote connection	errors in operating system or EDCS application, configuration errors	N1, N2, N5, N7	certified EDCS (Windows Server Datacenter 2012), FW, IDS/IPS ,«E1 EUPHRATES»
	denial of service	absence of monitoring in resource distribution (resources limitation)	N1, N2, N5, N6	FW, IDS/AIS
	undesirable modifications	incompetence, disloyalty	N5	organization measures, back-up tools
users’ workstations	unauthorized access to EDCS network	weak authentication mechanisms	N1	forced authentication
	unauthorized physical access	weak access control arrangements	N2, N4-N8	physical and organization preventive measures

net infrastructure	server unauthorized access, theft and server destruction	weak access control arrangements	N3-N8	physical and organization preventive measures
	remote connection	errors in operating system, configuration errors	N1, N2, N8	certified EDCS, FW, IDS/IPS, VPN
	denial of service	absence of monitoring in resource distribution (resources limitation)	N1, N2, N8	FW, IDS/IPS
SW (Inc. OS)	server unauthorized access, theft and server destruction	weak authentication methods, ignoring information security policies	N4-N8	physical and organization preventive measures
	remote connection	errors in operating system or EDCS application, configuration errors	N1, N2, N6-N8	OS Windows 8 Enterprise, Kaspersky antivirus, FW, IDS/IPS, VPN, forced authentication
physical information holders (PIH)	theft, deletion or password compromising of physical keys	ignoring information security policies	N2-N8	physical and organization preventive measures

4. Projecting the Secured EDCS

The third stage is projecting of secured EDCS in TLC, included: Existing solutions analysis;

i). Formulating the requirements for EDCS;

ii). Analysis of mechanisms of ensuring the legal validity of ED;

iii). Formulation of the requirements for security measures.

During projecting of EDC system, its existing products were analyzed. As a basis for projected system, the following systems were considered: DocsVision, Directum, E1 EUPHRATES. The systems were compared by stated criteria: application features, information security, economic efficiency. From the viewpoint of information security, it can be separated based on the following criteria: used database server, electronic signature support, data encryption, access rights separation, ability of setting authorization rules for different parts of document, user activity log, authentication schemes, back-up tools and data recovery, remote access, software certifications, compliance to requirements of federal laws and GOSTs. On top of that, EDCS system must satisfy business needs. At the present stage, the important characteristics are: possibility of remote access, presence of mobile application, friendly interface, full-text search, workstation customization features.

Using given criteria as a basis for secured EDCS projecting, the complex "E1 EUPHRATES" has been chosen. In spite of the fact that full compliance with information security standards and GOSTs in all of the systems, this complex was chosen because of lowest price and rich functionality. Both DocsVision and Directum offer lower degree of customizing and less remote access features. After choosing the EDC software complex, full architecture of TLC information system has been formulated, including hardware backbone and information security policies. Interaction with user is made by client application and web interface. Access to server is performed through public data transfer channels, encrypted with TLS. On user device, copies of accessed documents are stored in cache. Front-end "E1 EUPHRATES" is set on Microsoft IIS web-server and is used like interface for user, accessing system with web-browser. For clients, working through application on PCs, server offers application public interface.

Server back-end performs user requests processing, access isolation, information integrity control. EDCS's basic logic is focused here. With the aim of raising the number of concurrent connections and parallel user sessions, several front-end servers could be connected to single back-end. Cognitive Nexus platform allows utilization different SQL-servers, which can be united in clusters [7]. In case of big distributed systems, clusters can be connected with replication relations "master-to-master" type, with the help of which data consistency between SQL-clusters is assured. It means, that all changes on servers of one company will be automatically spread on servers of another companies. As for EDCS validity, the electronic signature (ES) should be used. In EDCS, documents interchange occurs only between TLCs own organizations. That is why in isolated systems of transport-logistical cluster, it will be enough to use self-validated ES [8]. Described EDCS is, by its design, an information system of company's personal data (hereinafter – ISPD).

As to Order of Government of Russian Federation of the 1st of November, 2012 n.1119, threats, which will be applicable for our IS, are of the second type [9]. The fist type was excluded, being that it was determined earlier that operation system (hereinafter – OS), used on LC, belongs to Microsoft Windows family. Beyond that, many OS of this company have FSTEC certificates. As to which, on the base of these operation systems it can be designed automated systems up to 1G protection class. It must be chosen such OS, which is authorized and certified as to legislation about personal data (hereinafter – PD). It is supposed that EDCS may store data about staff in companies consisting cluster, including photos and biometric PD, giving an ability to unequivocally identify the person. It was concluded on the base of explanations of Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications as to questions of photos attribution to biometric PD. Clients PD belongs to 'other' PD category, as to Order of Government of Russian Federation of the 1st of November 2012 n.1119. It means ISPD system of EDCS TLC requires maintaining the 2nd level of data security.

On different levels of TLC structure model, different companies will have different ACS, interacting between each other through EDCS. All information, received in the process of ACS operation of one company on EDCS, must be constantly accessible to all another TLC participant with granted access to it. This process runs through information resources, includes information, is the result of all ACS operations. As to Methodology of classification of state and non-state property to critically important objects: "companies, providing infrastructure of railway, air and sea transport, can be part of crucially important objects" [10]. It means that some companies of TLC could be seen as "crucially important objects", in which airports, railway stations and sea ports are included. Nevertheless, every regional TLC will have at least one critically important object (hereinafter – CIO). By the way, TLC itself will be crucially important for the Russian Federation.

For this reason, the security of all interacted ACS TP and ACSP, consisting TLC information system must be guaranteed. In view of the fact that automated controlling systems over technological processes operates at critically important objects, for making models of information security, for this research the order of FSTEC on March 14, 2014 No.31 was used [11]. As previously indicated, by means of this document, not only ACS in CIO should be provided with the necessary level of security, but also in other organizations in TLC. This is a necessary measure as far as security and unification of the protected system are concerned. As to this order, the level of importance of the information is determined by the extent of possible damage from the violation of one of the information security properties. The extent of possible damage to the TLC is an average, because the violation of any of the

properties (integrity, confidentiality, accessibility) may lead to emergency situations of a regional impact and has a negative aftereffect in various fields (economic, political, etc.). For this reason, on the base of FSTEC order of the 14th of March, 2014 No.31, ACS protection class is defined as the second. On the base of FSTEC No.21 orders of the18th of February, 2013 and No.31 of the 14th of March, 2014, for providing the 2nd level of protection of ISPD EDCS on transport-logistical cluster and the second class of ACS security, these measures should be performed:

i). computer technology - Class 5 or above;
ii). intrusion detection tools, system intrusion prevention and antivirus tools - Class 4 or above;
iii). trusted boot and control over removable media - Class 4 or above;
iv). antivirus protection - Class 4 or above;
v). FW – Class 3 or above [11], [12].

5. Protective tools of EDCS TLC

The final stage was the choice of comprehensive protection, based on the requirements for ISPD, ACS and TLC information system. All sorts of tools, combating network attacks, have been analyzed. In order to eliminate the possibility of unauthorized access to the system and to minimize possible damage to the structure of EDC, at least one countermeasure should be used, opposed to every single type of attack. It is the principle of information security model "with a full overlap". The data storing architecture in TLC is following. At the first level, all information is stored in the data-centers of large companies, because large companies have more resources to maintain such setups and more resources to guarantee physical protection. Access to public servers will be differentiated by “E1 EUPHRATES” embedded tools. Private servers in companies of any level are available to the company only. In fact, these servers are not part of EDCS, but they are the part of IS TLC. Since the EDCS core is located on the first structural level of TLC model, the back-up system will be deployed only to this level. For security reasons, backup data is stored in physically remote data-centers.

In EDC TLC system, back-up will utilize an multi-level scheme. Incremental backup will be performed daily, differential - weekly and full backup will be created monthly. This will ensure the recoverability of the data for a period not exceeding 24 hours. For some particularly crucial data, continuous data protection technology can be applied in order to recover the data for 15 minutes. On all major TLC companies, regardless of level, should be deployed the server version of “E1 EUPHRATES”. Databases of EDCS core are replicated with “master-master” relation, the reasoning was previously described. The rest of the companies in TLC are clients to core infrastructure. EDCS does not provide secure communication for users in different organizations. It must be performed by other security mechanisms. We need to secure data transmission channel that would adequately fit into the infrastructure of computer network. Building a separate line would be excessively expensive, however in the case of TLC and because of the distances between organizations; it took place to ensure the physical protection is nearly impossible. Beyond that, some regional TLC, where several ports are present on opposite sides of the open reservoirs, building the fiber-optic communication line is not feasible. For this reason the network is built on top of existing public data exchange networks using VPN technology [13], [14].

Inside the company, the network consists of two levels, represented by separate network segments. In one segment, user’s workstations and servers for generic use are located. The other is a server farm with EDCS of TLC. With the aim to secure interaction between segments, the process should be performed using the firewalls. Company resources, such as enterprise mail, access to which is required from the intranet and the Internet, are located in a separate segment. In order to ensure proactive protection of information, networks’ computer security against network attacks is necessary to use specialized software and hardware components, such as scanners, intrusion detection and prevention toolkits. Deploying these on every single workstation is economically ineffective. It is much more profitable to buy additional modules for firewalls. As a consequence, the monitoring of management will be centralized and, therefore, more effective.

In addition to the internal network, workstations should have access to the external public network. For this reason, additional protective tools for personal computers should be installed. As for those computers that does not have access to ECDS, there is still should be installed scanners and security tools, detecting and preventing intrusions. For TLC functioning, corporate e-mail service is used. It was decided to make use of the following protective tools against mailbombing: grey-listing and black lists. Grey-listing technology is effective for high-volume servers of large companies. It allows you to keep a record of legitimate sender, and make separate decisions about e-mail delivery from known or unknown senders. At the same time, also popular measures are the “black lists”. They are populated with IP-addresses and domain names, previously marked as spam. During the session of receiving e-mails, server will check sender’s name against black lists, and only then tries to use grey-listing technologies.

To calculate the cost of the necessary hardware, it should be presumed the number of users, who will have access to the EDCS, as well as the total number of workstations on the TLC. Such averaged parameters were selected [17-20]:

i). Number of employees in small companies - 80, while 60 of them have a workstation with an Internet access, 40 of them have the access to EDCS;
ii). Number of employees in middle companies - 120, while 80 of them have a workstation with an Internet access, 90 of them have the access to EDCS;
iii). Number of employees in big companies - 500, while 400 of them have a workstation with an Internet access, 320 of them have the access to EDCS;

Total in TLC: 7 large companies, 20 medium-sized enterprises and 27 small businesses. Total staff: 8300, of whom 6140 - staff with workstation and Internet access, 4640 - users of EDCS. In Tables 2-4 protective tools are indicated, needed for maintaining information security of EDCS. Selected software and hardware products have been certified by FSTEC and can be used in PD IS 2 class and in ACS Class 2 security [15], [16].

Table 2: Protective Tools of EDCS with Prices

Tools	Quantity, pcs.
User License of EDCS “EUPHRATES E1”	4 640
Technical support (per year)	–
Training price	–
WindowsServerDatacenter2012	42
Firewall with VPN D-linkDFL-2560	14
Firewall with VPN D-linkDFL-1660E	26
Firewall with VPN D-linkDFL-260E	21
Advanced subscription for IDS/IPS per year for D-link DFL-2560 + antivirus protection	14
Advanced Subscription IDS/IPS per year for D-link DFL-1660E + antivirus protection	26
Advanced Subscription IDS/IPS per year for D-link DFL-260E + antivirus protection	21

Table 3: Protective Tools of Enterprise E-Mail with Prices

Tools	Quantity, pcs.
Microsoft Exchange Server 2013 Enterprise	7
Windows ServerStandard 2012	7
Firewall with VPN D-link DFL-2560	7
Advanced Subscription IDS/IPS per year D-link DFL-2560 + antivirus protection	7

Table 4: Protective Tools for Workstations with Prices

Tools	Quantity, pcs.
OS Windows 8 Enterprise	6140
Kaspersky antivirus for workstations (per year)	6140

In accordance with the FSTEC order No.31 of the 14th of March, 2014, on workstation with installed ACS, it must be also

installed tools of trusted boot and control tools of removable media above Class 4. As preferred solution, certified hardware-software module "Sobol" could be used.

6. Basic results

One of the most important results of the study is the differentiation of cluster members on the levels of their importance and subsequent integration levels obtained in a coupled system of information flows, to simplify audit procedures. Particular attention was paid to the problem of interaction between geographically distributed organizations within a single information space. As information security model for the construction of the protection system, the model with complete overlap was chosen. This model is based on three sets (resource-vulnerability-threat) that had been identified unambiguously.

The coherent set of technical means of information was chosen, including:

- Tools, providing EDCS operation in secured environment;
- Protective tools for enterprise mail;
- Protective tools for server back-up;
- Protective tools for workstations [18].

The cost of back-up solution was not calculated, because it depends on the volume and rate of information growth. Calculation for the cost of the hardware servers and client workstations in this study also not included, as their market value can vary greatly, depending on the executable functions and tasks. In addition to the aforementioned, system owners should pay special attention to the organizational information protection measures. No technical solution in the field of information security will be effective if the staff ignores security policies. Arrangements significantly reduce the risk of unauthorized access, disclosure and leakage of confidential information. With regular and methodical work with the staff, the errors from incompetence and negligence could be reduced. Measures aimed to increase employees' loyalty need to be performed constantly. The loyalty should be increased not only to their company, but also to other companies in the TLC. Competent organization and access control, protection of the perimeter and the location eliminates access for physical attacker to the information in the TLC. With the right combination of physical and organizational methods, many of the proposed technical measures presented in this paper will be redundant.

7. Conclusion

The next step of this research is developing integrative model of information protection system, based on math models that can estimate security of studied object. Based on it, software will be built, including the following functions:

i). Calculation of possibility for threats realization and information risks of different type, depending on existing system protective tools;

ii). Time calculation of threats realization and time of its detection;

iii). Statements creation and recommendations as to modernization of existing or projecting system. The program output depends on which exposures are used by attacker, its qualification and equipment level. At the same time, it will be developed projection scheme of physic protection of transport-logistical cluster. Therefore, all aspects of complex information protection will be considered.

References

[1] *The World Bank. LPI Global Rankings 2014*. http://lpi.worldbank.org/international/global

[2] *Transport Strategy of Russian Federation for 2030* / Transport Department of Russia. Moscow, 2014.http://www.mintrans.ru/upload/iblock/3cc/ts_proekt_16102008.pdf.

[3] Prokofyeva, T.A.; Klymenko, V.V. *Logistics and Supply Chain Management*. 2011, *No. 6*, 31–41.

[4] Dosmukhamedov, B.R. *ASTU Reports. Series: Management, Computer Science and Informatics*. 2009, *No. 2*, 140–143.

[5] Yong, Wu; Gengzhong, Feng; Nengmin, Wang; Huigang, Liang. *Game of Information Security Investment: Impact of Attack Types and Network Vulnerability*. 2015, *vol. 36(1)*, 25–34.

[6] *Information Security Providing of Bank System of Russian Federation. Common Aspects: Russia Standard Bank STO BR IRBS-1.0-2014* / Russia Bank Order of 17.05.2014 No. P-399. http://www.consultant.ru/document/cons_doc_LAW_163762

[7] *EDCS Architecture "E1 Euphrates"*http://www.evfrat.ru/about/architecture/.

[8] Sokolov, S.S.; Karpina,A.S. In: "*Scientific Student Community of XXI century. Technical Sciences": Electronic Essays Collection as to Materials of XIX International Student Research-to-Practice Conference*. Novosibirsk: SIRAK. 2014, *No. 4(19)*, 50–56 (in Russian).

[9] *On Adoption of Personal Data Security Requirements through their Processing in Personal Data of Information System: Order of Russian Federation Government. 01st November, 2012 No, 1119* // Official Gazette of Russian Federation. 2012, No. 45, 6257.

[10] *Classification Methodology of Government and Non-government Object Properties to Extra Important Objects* / EMERCOM of Russia, 2012.

[11] http://central.mchs.ru/upload/site4/files/bea08465669b520c2603f73058fe188a.pdf.

[12] Order of FSTEC of Russia, 18th February, 2013 No. 21 "*On Adoption of Content of Organization and Technical EDCS Measures as to Providing Data Safety through their Processing in Personal Data of Information Systems*".

[13] Sokolov, S.S. *Modern Science and Education Questions*. 2015, *No. 1*.

[14] www.science-education.ru/121-18583.

[15] Sokolov, S.S.; Karpina,A.S. In: *Reports of Materials of the III International Research-to-Practice Conference "Information Management Systems and Technologies"*. Odessa: Odessa National Sea University. 2014, 277 (in Russian).

[16] Chernyi, S., & Budnik, V. (2017). Methods for optimizing solutions when considering group arguments by team of experts. https://doi.org/10.1063/1.5009873.

[17] Kovalnogova, N. M.; Sokolov, S. S.; Nyrkov, A. P. In: *IOP Conference Series: Materials Science and Engineering*, *vol. 124*, https://doi.org/10.1088/1757-899X/124/1/012066.

[18] Boriev, Z.; Nyrkov, A.; Sokolov, S.; Chernyi, S. In: *IOP Conference Series: Materials Science and Engineering*, *vol. 124*, https://doi.org/10.1088/1757-899X/124/1/012006.

[19] Sokolov, S.S.; Malov, S.S.; Karpina, A.S. Vestnik of Admiral Makarov State University of Maritime and Inland Shipping. 2014, *No. 5(27)*, 148-157 (in Russian).

[20] Nyrkov, A.; Sokolov, S.; Zhilenkov, A.; Chernyi, S. In: *Proceedings of the 2016 IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference*, EIConRusNW. 2016, https://doi.org/10.1109/EIConRusNW.2016.7448264.

[21] Kukushkin, I.; Sokolov, S.; Nyrkov, A.; Pavlova, L. In: *Proceedings of the 2016 IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference*, EIConRusNW 2016, https://doi.org/10.1109/EIConRusNW.2016.7448166.

[22] Boriev Z.; Nyrkov A.; Sokolov S; Chernyi S. In: IOP Conference Series: Materials Science and Engineering, vol. 124, p. 012006, 2016. https://doi.org/10.1088/1757-899X/124/1/012006.