Problem of Developing an Early-Warning Cybersecurity System for Critically Important Governmental Information Assets

Sergei A. Petrenko, Alexey S. Petrenko
Information Security Department
Saint Petersburg Electrotechnical University "LETI"
St. Petersburg, Russia
s.petrenko@rambler.ru; a.petrenko@rambler.ru

Krystina A. Makoveichuk
Department of Informatics and Information Technologies
Vernadsky Crimean Federal University
Yalta, Russia
christin2003@yandex.ru

***Abstract*—The article considers possible solutions of to the relatively new scientific-technical problem of developing an *early-warning cybersecurity system for critically important governmental information assets*. The solutions proposed are based on the results of exploratory studies conducted by the authors in the areas of Big data acquisition, cognitive information technologies (cogno-technologies), and "computational cognitivism," involving a number of existing models and methods. The results obtained permitted the design of an early-warning cybersecurity system.**

Keywords—Cyberspace; critically important infrastructure; information confrontation; hybrid wars; cyberattacks; information security; cybersecurity system; early-warning; Big Data; Big Data Analytics; cogno-technologies; computational cognitivism; scenarios of an early-warning; synthesize scenarios.

I. Introduction

Nowadays, the information confrontation plays an increasingly important role in modern, "hybrid" wars. Furthermore, victory is often attained not only via military or numerical superiority, but rather by information influence on various social groups or by cyberattacks on critically important governmental infrastructure.

In this regard, means for detecting and preventing information and technical impacts should play a crucial role. Currently, systematic work is being done in Russia to create a National Cyberattack Early-Warning System. A number of state and corporate cybersecurity response system centers have already been organized.

However, the technologies applied in these centers allow only the detection and partial reflection of ongoing IT-attacks, but they do not have the capacity to predict and prevent attacks that are still in the preparation stage [1].

Such a situation requires the creation of fundamentally new information security systems which are capable of controlling the information space, generating and simulating scenarios for the development, prevention and deterrence of destructive information and technical impacts, and to initiate proactive responses to minimize their negative impact. New technologies in big data and deep learning as well as in semantic and cognitive analysis are now capable of proactively identifying the invader's hidden meanings and goals, which the other types of analysis could not discover, will likely play an instrumental role here. This article aims to develop these methods and technologies.

II. PROBLEMS OF DEVELOPING AN EARLY-WARNING CYBERSECURITY SYSTEM

At the same time, it is impossible to implement a National Cyberattack Early Warning System without also tackling a series of related issues. Most notably, this will necessarily entail the creation of an effective computing infrastructure that provides the implementation of new methods and technologies for modeling the development, prevention and deterrence of destructive information and technical impacts in real-time, or even preemptively. Clearly, this problem will not be solved without high-performance computing systems or a supercomputer.

We must confess that Russia currently lags far behind leading Western countries in terms of its supercomputer technology. Cluster supercomputers primarily used in our country are usually based on a CKD assembly from commercially available foreign processing nodes and network switches. It is well-known that this class of supercomputers demonstrates its optimal performance when solving loosely bound problems not requiring intensive data exchange between processor nodes.

The actual performance of cluster supercomputers, however, is significantly reduced when solving. While the solution of tightly bound problems, in particular semantic and cognitive analysis of big data. Moreover, the attempts to increase the cluster system performance by increasing the number of processing nodes have often not only failed to yield positive results, but, on the contrary, have had the opposite effect due to a heightened proportion of non-productive "overhead" in the total solution time which arises not from "useful" processing, but from organizing a parallel calculation process.

These fundamental disadvantages of modern cluster supercomputers are a product of their "hard" architecture, which is implemented at the stage of computer construction and cannot be modified while being used [1-4].

Developed by Russian scientists, the concept of creating a reconfigurable supercomputer made it possible to configure the architecture setup (adjustment) depending on the structure of the task's solution without entailing the aforementioned disadvantages. In this case, a set of field programmable logic devices (FPLG) of a large integration degree comprises the entire computing field and enables the user to create the task-oriented computing structures similar to the graph algorithm of the given task; this is used as a supercomputer computational device, rather than a standard microprocessor. This approach ensures a "granulated" parallel computing process as well as a high degree of time efficiency in organization achieved by adjusting the computing architecture to the applied task.

As a result, near-peak performance of the computing system is achieved and its linear growth is provided, when the hardware resources of the FPLG computational field are increased [5-8].

Today, reconfigurable FPLG-based computing systems are increasingly finding use in solving a number of topical applied tasks, primarily computationally labor-intensive and "tightly coupled" streaming tasks that require mass data processing (streams), as well as tasks that require the processing of non-standard data formats or variable number of bit (e.g. applied fields of big data semantic and cognitive analysis, cryptography, images processing and recognition, etc.).

This allows us to estimate the prospects of using reconfigurable supercomputers technology when establishing a National Cyberattack Early-Warning System [1].

III. OF NATIONAL SUPERCOMPUTER GRID NETWORK

At the same time, one supercomputer, even the most productive one, is not enough to create the computing infrastructure of the National Cyberattack Early-Warning System.

Obviously, such a system should be built based on a network of supercomputer centers, with each unit having its owntask focus, while preserving the possibility to combine all the units into a single computing resource; this would, *de facto*, provide a solution to computationally labor-intensive tasks of real-time and preemptive modeling development scenarios for prevention and deterrence of the destructive information and technical impacts. In other words, the National Cyberattack Early Warning System should be based on a certain segment (possibly secured from outside users) of the National Supercomputer GRID network.

Furthermore, establishing a National Supercomputer GRID-Network evokes a complex problem of optimal distribution (dispatching) of computational resources while solving a stream of tasks on modeling development scenarios for cyberattack prevention and deterrence [9].

Nowadays, the problem of dispatching distributed computer networks is being solved with uniquely allocated server nodes. However, such centralized dispatching is effective when working with a small computational capacity or nearly homogenous computational resources. However, in cases of numerous, heterogeneous network resources, the operational distribution (also redistribution) of tasks, not to mention of informationally relevant subtasks via a single central dispatcher becomes difficult to implement. Moreover, using a centralized dispatcher significantly reduces the reliability and fault tolerance of the GRID network, since a failure on the part of the service server node that implements the dispatcher functions will lead to disastrous consequences for the entire network.

These disadvantages can be avoided by using the principles of decentralized multi-agent resource management of the GRID network. In this case, software agents which are physically implemented in each computational resource as part of the GRID network play the main role in the dispatching process and represent their *interests* in the dispatching process. Each agent will *know* the computing capabilities of "its own" resource, as well as responsively track all changes (e.g. performance degradation owing to the failure of numerous computing nodes).

Given this information, the agent can "allocate" its resource for solving tasks where "its" resource will prove most effective. If the computing resource of one agent is not enough to solve the problem in the given time duration, then a community of agents will be created, with each one providing its resources for solving the various parts of a single task.

The benefits of a decentralized multi-agent dispatching system in a National Supercomputer GRID-network are manifold:

- Ensure efficient loading of all computational resources included in the GRID network, by using up-to-date information about their current status and task focus;
- Ensure the adaptation of the computational process to all resource changes in the cloud environment;
- Reduce the overhead costs for GRID network organization due to the absence of the need to include special service servers as a central dispatcher;
- Increase the reliability and fault tolerance of the GRID network and, as a result, dependable computing, since the system will not have any elements whose failure may lead to disastrous consequences for the entire network [4, 7-8].

IV. DEVELOPMENT EARLY-WARNING CYBER-SECURITY SYSTEM

As a technological basis for solving this problem, it is proposed to consider modern software and hardware systems for analyzing and processing information security events [10]. In international practice, these complexes are developed as part of specialized security centers, known as the *Computer Emergency Response Team* (*CERT*) or the *Computer Security Incident Response Team* (*CSIRT*), or the *Security Operation Center* (*SOC*). *Computer Emergency Response Team* (*CERT*) or *Computer Security Incident Response Team* (*CSIRT*), or *Security Operation Center* (*SOC*).

The Russian Federation has already established a number of state and corporate centers for detecting, preventing, and recovering from cyber-attacks or centers for responding to cyber security incidents, which are similar to foreign CERT / CSIRT / SOC in their functionality. In domestic practice, they are known as SOPCA. Some examples include, inter alia, GOV-CERT.RU (FSS of Russia), SOPCA of the Ministry of Defense of Russia, FinCERT (Bank of Russia), Rostechnologies CERT, Gazprom SOC, etc.

The Russian Federation Presidential Decree No 31c of January 15, 2013 “On the establishment of a state system for detecting, preventing, and recovering from cyber-attacks on Russian information resources” establishes that the Russian FSS is making methodological recommendations on the organization of protection of the critical information infrastructure of the Russian Federation and organizes work on the creation of a State and corporate segments of Monitoring in the Detection, Prevention and Cyber Security Incident Response (SOPCA).

The concept of a state system for detecting, preventing, and recovering from cyber-attacks on Russian information resources No K 1274, was approved by the President of the Russian Federation on December 12, 2014, defines the state SOPCA system image based on special centers for detecting, preventing, and recovering from cyber-attacks, divided into centers:

- Russian *FSS* (created to protect information resources of the public authorities);
- State and commercial organizations (created to protect their own information resources).

In addition, these centers are coordinated by the National Coordinating Center for Computer Crimes under the FSS of Russia.

At the same time, in practice, the task to develop a cognitive early warning system for cyber-attacks on the information resources of the Russian Federation was far from being trivial.

It was necessary to conduct appropriate scientific research and solve a series of complex scientific and technical problems – e.g. input data classification, identifying primary and secondary signs of cyber-attack, early cyber-attacks detection, multifactor prediction of cyber-attacks, modeling of cyber-attack spread, training, new knowledge generation on quantitative patterns of information confrontation – many of which did not have ready standard solutions [11].

In addition, it was essential to ensure the collection, processing, storage of big data, as well as carrying out analytical calculations on extremely large amounts of structured and unstructured information from a variety of Internet / Intranet and IoT / IIoT sources (big data and big data analytics) [17]. A possible list of requirements for such cognitive systems is represented in Table 1.

TABLE I. REQUIREMENTS FOR COGNITIVE SYSTEMS

Requirements for such cognitive systems is represented	
While implementation of SHC “Warning-2016”, there were a number of general requirements: - monitoring a large number of objects number real time (1000000+); - low delay level in event processing (less than 10 ms); - distributed storage and fast access to data for petabyte data volumes; - a high reliability degree of data and knowledge storages able to operate 24 hours a day, 7 days a week, without risk of interruption or loss of information in the event of server failure (one or more); - ability to scale (including the means of the underlying software) for the performance and volume of processed information without modifying the installed software by upgrading / scaling the used set of hardware; - indicator of the SHC availability level should be at least 99% per year; - possibility of SHC integration with third-party systems: the complex architecture should be created, taking into account the openness and ease of introducing interaction modules with external systems. Creating the data storage of SHC “Warning-2016” is implemented taking into account the following requirements: • data, stored in the repository is a series of records characterized by a time stamp (time series), thus, the repository should be optimized for storing time series; • high speed of data recording; • high speed of Map Reduce operation with preliminary selection on time intervals; • ability to work with data with a coordinate as one of its properties (mobile sensors); • low requirements for data consistency (Eventually Consistency); • immutable data, without need to conduct distributed transactions or synchronization. **Requirements for data and knowledge collection, preliminary processing and analysis subsystem:** • receiving data on various information interaction protocols, i. e. ZMQ (zeromq), TCP / IP, RAW TCP / IP, HTTP (REST-requests processing), AMQP, SMTP, etc; • receiving data in XML, JSON / BSON, PlainText formats;	average value change over a certain time interval; - change in characteristics of events occurrence frequency, etc .; • use of machine learning models to identify correlations and detect incidents (i.e. the application of multivariate analysis, clustering and classification methods); • identification of various kinds of templates in text messages described by regular expressions, and applying the above-mentioned statistical functions to them; • correlation of data from various sources; • combination of parameters from various sources with subsequent application of the above-mentioned statistical methods; • testing of the models for detecting new incidents, etc .; • giving notification to users of incidents detected by sending messages to the visualization and administration subsystem or other IS. **Requirements of the data storage and knowledge subsystem:** - support for structured and unstructured data types; - support for data index to speed up data search and retrieval; - ability to work with time series; - ability to create queries in the MapReduce paradigm; - implementation of aggregation and statistical queries on the time series in the data storage location; - ability to automatically remove outdated data of time series; - availability of libraries for accessing storage functions for Java, Python; - library for accessing storage system functions through specialized drivers (e.g. Django database engine); - knowledge support for working with new models of neurophysics and classical methods of artificial intelligence. The modeling, decision-making, visualization, and administration subsystem needed to support models and methods of neurophysics, artificial intelligence, and mathematical logic, including cognitive agents and artificial neural networks of direct distribution [12], trained by the Levenberg-Marquardt method, and so on. The visualization and administration subsystem needed to support: - statistical reports on incidents and stored time series; - density distribution function graphs; - cybersecurity values distribution histograms; - series graphs with different characteristics (mean, extrapolation, etc.); - correlation models for performing

Requirements for such cognitive systems is represented	
• detection of incidents and security threats by applying the following models to the incoming data stream: - various parameters excess / decrease detection, setting thresholds for these parameters; - detection of deviation from normal values for various parameters; - detection of statistical deviations from standard behavior for various parameters in the time window;	multifactor analysis; - parameters correlation and incidents on selected time interval graphs; - classification models to detect correlation of parameters from various sources with incident occurrence; - clustering models for detecting parameters correlation over a given time interval, etc.

Appropriate technological solutions for creating a cognitive early warning for cyber-attacks on Russia's information resources are represented in [1].

Here, the choice and implementation of the *big data* processing component represented an important task.

Another important task was the structure of big data storage structure. Many known solutions (e.g. *Cassandra* or *HBase*), proved to be of little use due to the following limitations:

- Lack of database components to ensure efficient storage and retrieval by time series (most known solutions do not contain integration tools due to their closeness, and those available (e.g. *InfluxDB*) do not have a high level of work stability);
- Absence of the logical connections between the interfaces of business logic and the database;
- System functionality duplication due to the database and the processing logic being separated in a heterogeneous solution environment;
- Limited performance of the *HBase* solution, associated with the architectural solution features;
- Significant overhead *Cassandra*, associated with the synchronization of data on various nodes, etc.

TABLE 2. KNOWN SOLUTIONS FOR STREMING AND BATCH DATA PROCESSING

Solution	Developer	Type	Description
Storm	Twitter	Packaged	New solution for Big Data streaming analysis by Twitter
S4	Yahoo!	Packaged	Distributed streaming processing platform by Yahoo!
Hadoop	Apache	Packaged	First open source paradigm MapReduce realization
Spark	UC Berkeley AMPLab	Packaged	New analytic platform supporting data sets in RAM: has high failure safety level.
Disco	Nokia	Packaged	MapReduce distributed environment
HPCC	LexisNexis	Packaged	HPC-cluster for Big Data

Possible system architecture of the cognitive early warning system for cyber-attacks on information resources of the Russian Federation based on NBIC technologies is presented in [1]. The positive experience gained in the creation of a cognitive early warning system for cyber-attacks of SHC “Warning-2018” speaks to the expediency of a methodical approach to solving the task.

Stage 1. Developing the technical component of a traditional *SOPCA* based on big data technologies is the creation of a high-performance corporate (state) segment of detecting, preventing, and recovering from cyber-attacks.

Stage 2. Creation of the SOPCA analytical component based on “computational cognitivism” is the realization of the cognitive component of the cyber-attack early warning system capable of independently extracting and generating useful knowledge from large volumes of structured and unstructured information for SOPCA operational support.

In this case, the above-mentioned technical component of *SOPCA* based on big data technologies should be appropriately allocated with the following functions:

- Big data on the information security state in controlled information resources collection;
- Data detection and recovery after cyber-attacks on information resources;
- Software and technical tools for IS events monitoring support;
- Interaction with the state *SOPCA* centers;
- Information on the detection, prevention, and recovery from cyber-attacks, etc. (Fig. 1. Technical component of SHC “Warning-2016”

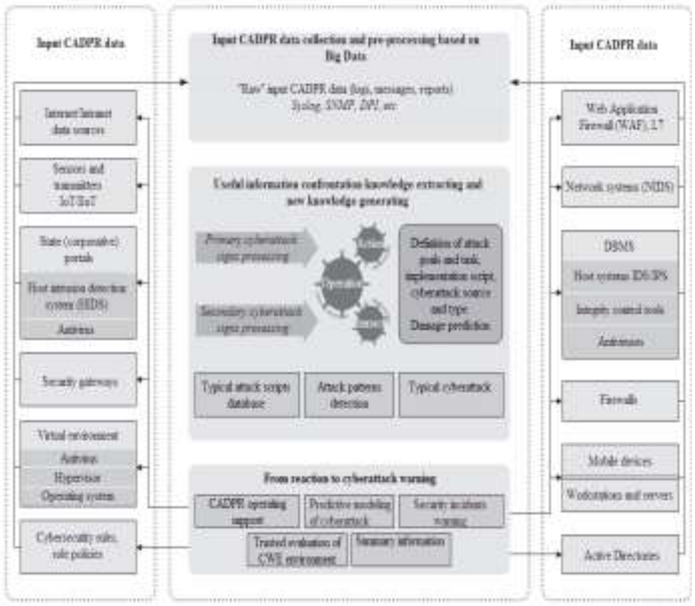
Input CADPR data
Input CADPR data collection and pre-processing based on Big Data
"Raw" input CADPR data (logs, messages, reports)
Syslog, SNMP, DPI, etc
Input CADPR data
Internet/Intranet data sources
Sensors and transmitters IoT/IIoT
State (corporative) portals
Host intrusion detection system (HIDS)
Antivirus
Security gateways
Virtual environment
Antivirus
Hypervisor
Operating system
Cybersecurity rules, rule policies
Useful information confrontation knowledge extracting and new knowledge generating
Primary cyberattack signs processing
Secondary cyberattack signs processing
Definition of attack goals and task; implementation script, cyberattack source and type. Damage prediction
Typical attack scripts database
Attack patterns detection
Typical cyberattack
From reaction to cyberattack warning
CADPR operating support
Predictive modeling of cyberattack
Security incidents warning
Trusted evaluation of CWE environment
Summary information
Web Application Firewall (WAF), L7
Network systems (NIDS)
DBMS
Host systems IDS/IPS
Integrity control tools
Antiviruses
Firewalls
Mobile devices
Workstations and servers
Active Directories

Fig. 1. Technical component of SHC "Warning-2016"

The analytical component based on "computational cognitivism" should be appropriately allocated with the following functions:

- An early warning system for cyber-attacks on information resources;
- Identification and generation of new useful knowledge about qualitative characteristics and quantitative patterns of information confrontation;
- Prediction of security incidents caused by known and previously unknown cyber-attacks;
- Preparation of scenarios for deterring a cyber-opposition and planning a response, adequate computer aggression.

In the following sections on this issue, the practice of using big data technologies to organize a streaming process of cybersecurity data, as well as practical questions of semantic Master Data Management (MDM) will be considered for building the SOPCA knowledge base.

The development of a new functional model of a cognitive high performance supercomputer will also be justified, possible prototypes of software and hardware complexes for the early detection and prevention of cyber-attacks will be presented, examples of solutions to classification and regression problems will be given, as will be solutions to the search for associative rules and clustering and possible directions for the development of artificial cognitive cybersecurity systems (Table III).

V. CONCLUSIONS

The article shares valuable insight gained during the process of designing and constructing open segment prototypesof an early-warning cybersecurity system for critical national infrastructure in the Russian Federation. The results obtained permitted the design of an early-warning cybersecurity system.

In addition, prototypes were developed and tested for software and hardware complexes of stream pre-processing and processing as well as *big data* storage security, which surpass the well-known solutions based on Cassandra and HBase in terms of performance characteristics.

As such, it became possible, for the first time ever, to synthesize scenarios of an *early-warning cybersecurity system* in cyberspace on extra-large volumes of structured and unstructured data from a variety of sources: Internet/Intranet and IoT/IIoT (*Big Data and Big Data Analytics*) [16].

TABLE III. EXAMPLE SHC COMPONENT "WARNING-2018"

Cognitive subsystem of early warning system for cyber-attacks on Russian information resources
1. Development of traditional SOPCA components based on big data technologies 2. Creation of analytical SOPCA component based on "computational cognitivism" 3. Monitoring the security and sustainability state of critically important infrastructure operation in cyberspace: • Introducing the informatization CWE passport (inventory, categorization, classification, definition of requirements, etc.); • Creating priority action plans, etc.; • Certifying the information security tools (facility attestation for safety requirements [13-15]); • Monitoring safety criteria and indicators and stability of the given facilities' operation; • Maintaining a database of cybersecurity incidents. 4. Identification of preliminary signs of cyber-attacks on Russian Federation information resources: • Recognizing structural, invariant, and correlation features of cyber-attacks; • Adding primary signs of cyber-attacks to the database; • Clarifying cyber-attack scenarios; • Developing adequate measures for deterrence and compensation. 5. Identification of secondary signs of cyber-attacks on Russian Federation information resources: • Identifying correlation links and dependencies between the signs; • Adding secondary signs of cyber-attacks to the database; • Clarifying cyber-attack scenarios; • Developing adequate measures for deterrence and compensation. 6. From detection to prevention: • Early warning for a cyber-attack on Russian information resources; • Prediction of cyber - attack from a cyber-enemy; • Assessing possible damage in case of cyber-attack; • Preparing scenarios of deterrence and coercion response to the cyberworld preparation. 7. Extraction of useful knowledge and generation of new knowledge in the field of information confrontation based on: • New NBIC models: • Neuromorphic, similar to the living nervous system structure; • Corticomorphous, similar to the cerebral cortex structure; • Genomorphic, similar to genetic and epigenetic mechanisms of living organisms' reproduction and development; • Models and methods of mathematical logic and artificial intelligence; • Cognitive agents; • Artificial neural networks of direct distribution, trained according to the Levenberg-Marquardt method; • Educable, hierarchically ordered neural networks and binary neural networks; • Various representations of dynamic thresholds and classifiers of network packets based on the Euclidean-Mahalanobis metric and the support

vectors method;

- Statistical (correlation) and invariant profilers;
- Complex poly-model representations, etc.

8. Development of guidelines for work with cognitive SOPCA

9. Cyber-training organization to develop skills of early warning for cyber-attacks on information resources of the Russian Federation

10. Development of the necessary normative documents

11. Training and retraining of employees on issues relating to the early warning for cyber-attacks on information resources of the Russian Federation

12. Elaboration of proposals for the development of a national (and international) regulatory framework for cyber-attack early warning.

REFERENCES

[1] Petrenko S.A., Stupin D.D. Natsional'naya sistema rannego preduprezhdeniya o komp'yuternom napadenii [National system of advance computer attacks alerting]. Innopolis, Afina Publ., 2017. 440 p. *(In Russ.).*

[2] Guarino, N. Services as Activities: Towards a Unified Definition for (Public) Services. In Proc. Enterprise Distributed Object Computing Workshop (EDOCW), 2017 IEEE 21st International. Quebec City, QC, Canada, 10-13 Oct., 2017, pp. 102 - 105. DOI: 10.1109/EDOCW.2017.25.

[3] Nardi J., Falbo R., Almeida J., Guizzardi G., Pires L., Sinderen M., Guarino N. An Ontological Analysis of Value Propositions. In: Enterprise Distributed Object Computing Conference (EDOC), 2017 IEEE 21st International. Quebec City, QC, Canada, 10-13 Oct. 2017, pp. 184 - 193. DOI: 10.1109/EDOC.2017.32.

[4] Pashchenko I. N., Vasilyev V. I., Guzairov M. B. Smart Grid security system on the basis of intelligent technologies: rule base design. Izvestiya SFedU. Engineering Sciences *[News of SFedU. Technical science]*, 2015, pp. 28–37. (In Russ.).

[5] Pospelov D.A. Introduction to applied semiotics. News of Artificial Intelligence, 2002, no. 6. (In Russ.).

[6] Pospelov G.S. Artificial intelligence is the basis of the new information technology. Moscow, Nauka, 1988. 280 p. (In Russ.).

[7] Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K. Organization of the entrusted calculations in crucial objects of informatization under uncertainty. In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24-26 May 2017, St. Petersburg, Russia). SCM 2017, 2017, pp. 299 - 300. DOI: 10.1109/SCM.2017.7970566.

[8] Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K. Analysis of computer security incidents using fuzzy logic. In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24-26 May 2017, St. Petersburg, Russia). SCM 2017, 2017, pp. 369 - 371. DOI: 10.1109/SCM.2017.7970587.

[9] Massel L., Voropay N., Senderov S., Massel A. Cyber Danger as One of the Strategic Threats to Russia's Energy Security. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2016. No 4 (17), pp. 2-10. DOI: https://doi.org/10.21681/2311-3456-2016-4-2-10.

[10] Dorofeev A.V., Markov A.S., Tsirlov V.L. Social Media in Identifying Threats to Ensure Safe Life in a Modern City, Communications in Computer and Information Science, 2016, vol. 674, pp. 441-449. DOI: 10.1007/978-3-319-49700-6_44.

[11] Sheremet I. A. Augmented Post Systems: The Mathematical Framework for Data and Knowledge Engineering in Network-centric Environment. Berlin, 2013. 395 p.

[12] Starodubtsev Yu.I., Grechishnikov E.V., Komolov D.V. Use of neural networks to ensure stability of communication networks in conditions of external impacts. Telecommunications and Radio Engineering. 2011. V. 70. N 14. P. 1263-1275.

[13] Kozachok A., Bochkov M., Lai M.T., Kochetkov E. First Order Logic for Program Code Functional Requirements Description. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2017. N 3 (21), pp. 2-7. DOI: 10.21681/2311-3456-2017-3-2-7.

[14] Reber, G., Malmquist, K., Shcherbakov, A. 2014. Mapping the Application Security Terrain. Voprosy kiberbezopasnosti *[Cybersecurity issues]*. 2014. N 1(2). P. 36-39. DOI: 10.21681/2311-3456-2014-2-36-39.

[15] Barabanov A., Markov A., Tsirlov V. Procedure for Substantiated Development of Measures to Design Secure Software for Automated Process Control Systems. In Proceedings of the 12th International Siberian Conference on Control and Communications (Moscow, Russia, May 12-14, 2016). SIBCON 2016. IEEE, 7491660, 1-4. DOI: 10.1109/SIBCON.2016.7491660.

[16] Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V., Petrenko A.S. About Readiness for Digital Economy. In Proceedings of the 2017 IEEE II International Conference on Control in Technical Systems, IEEE, CTS, 2017, pp. 96–99. DOI: 10.1109/CTSYS.2017.8109498.

[17] Petrenko A.S., Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V. The IIoT/IoT device control model based on narrow-band IoT (NB-IoT). In Proceedings of the the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (29 Jan.-1 Feb. 2018, Moscow and St. Petersburg, Russia) EIConRus, IEEE, 2018, pp. 950-953. DOI: 10.1109/EIConRus.2018.8317246.