Grant of the Russian Science Foundation # 15-11-30029
"Incident management and counteraction against targeted cyber-physical attacks
in distributed large-scaled mission critical systems
taking into account cloud services and networks of the Internet of Things"
Description of the works fulfilled in 2017 and scientific results

1. The architecture and software prototypes of the components for collecting, preprocessing and correlating of security information and events have been developed based on the application of a complex of distributed intelligent sensors and big data technology.

The architecture includes five groups of distributed intelligent sensors and services responsible for: data collection; data storage; aggregation of data; normalization and analysis of data; visualization of data. A separate component of the general architecture is responsible for the implementation of each group. Software prototypes are developed on the basis of a computing cluster for processing big data, formed in two versions: based on Hadoop and on the basis of Spark.

2. The architecture and software prototypes of a reliable, trusted data bus and hybrid storage of security information and events have been developed.

The architecture of a reliable, trusted data bus includes the following levels: cybernetic, physical and systemic. The software prototype of the data bus have been developed based on the I2C protocol. The architecture of the hybrid storage of security information and events contains: a module for downloading of security information from external sources; data normalization module; module for analysis and formation of a hybrid storage model; module for filling the hybrid storage base; module of external interaction with other components of the developed security system. The software prototype of a hybrid repository contains ontological models that on the basis of a logical inference can provide new knowledge about security and perform automatic selection of countermeasures.

3. The architecture and software prototypes of components for real-time detection of complex multi-step attacks based on the technology of intelligent analysis of security information and events have been developed.

The architecture has a four-level data processing mechanism. Software prototypes allow to detect individual attacking activities through the use of technologies for intelligent analysis of security information and events, including those based on neural networks.

4. The architecture and software prototypes of components for calculating primary and integrated security metrics have been developed.

The architecture includes modules that compute metrics in accordance with the previously proposed hierarchical system (topological level, attack level, attacker level, level of events, level of countermeasures and system level). The software prototype implements the following models: service dependencies; Bayesian graph of attacks; events; countermeasures.

5. The architecture and software prototypes of components for analyzing the history of security events, predicting the actions of violators and their consequences have been developed.

The architecture includes a history analysis module that interacts with the incident database and passes the results to the module for calculating security metrics and predicting the actions of violators and their consequences. Software prototypes implement models, techniques and algorithms for analyzing the history of security events, predicting the actions of violators and their consequences (the Bayesian graph model of attacks, the event model, the history analysis technique).

6. The architecture and software prototypes of the components of the automated response to targeted information, software and physical impacts have been developed on the basis of a hybrid storage of security information and events and based on expert knowledge of logical inference.

The architecture covers the following components: data processing; evaluation of security; selection of countermeasures; simulation of attacks; collection of input data. Techniques of using the software prototypes for automated response to targeted information, software and physical impacts on the basis of a hybrid storage of security information and events and based on expert inference-based logic have been developed.

7. The architecture and software prototypes of components of proactive, dynamic and multidimensional management of security incidents of critical objects have been developed taking into account cloud services and Internet of things.

The architecture includes three levels: 1) external data sources (sensors), a reliable and trusted data bus, a security event processing and correlation component, a hybrid data storage, a security event intelligent component, a security metrics calculation component; a component of the choice of countermeasures and external systems implementing the selected countermeasures; 2) components responsible for specific subject areas; 3) services of traditional telecommunication networks analyzed using the security incident management system (SIMS), Internet of things services and cloud services.

8. The scientific and technical proposals for the application of the developed methods, models, techniques, algorithms, architectures and software prototypes of the security incident management system for complex protection of "smart house" elements have been developed.

The implementation of the generalized architecture of a prospective security incident management system of critical objects for the complex protection of smart house elements consists of several main parts: hardware information sources; program sources of information; concentrators; the server of the smart house; module for analytical data processing and visualization (ADPV); as well as a module of integrating with security information and event management systems (SIEMs). Automated response to targeted information, program and physical impacts is carried out through the following operations: 1) notification of the operator about detected incidents, attack scenarios and abnormal activity; 2) notification of the operator about the need to strengthen the physical control of the infrastructure of the system or its individual elements; 3) notification about the need to change the rules for accessing the services of the system. To confirm the correctness of the proposed approach, a prototype of the smart house system have been designed, as well as a number of experiments with it have been performed.

9. The scientific and technical proposals on the application of the developed methods, models, techniques, algorithms, architectures and software prototypes of the security incident management system for the complex protection of Russian Railways objects have been developed.

Implementation of the generalized architecture of a prospective security incident management system of critical objects for the complex protection of Russian Railways objects consists of several main parts: a data collection module; data management module; a central processing unit and an information panel. Application of the obtained results will allow implementing a dynamic approach to incident management through the use of distributed cloud services, which allow maintaining the following knowledge bases up-to-date: 1) knowledge bases of the rules of the process of correlation of security events; 2) knowledge bases of multi-step attack patterns; 3) knowledge base of possible conflicts between the elements of the system.

10. The scientific and technical proposals for the application of the developed methods, models, techniques, algorithms, architectures and software prototypes of the security incident management system for complex protection of objects of energy and water supply system have been developed.

The results obtained in the project can be applied to the construction of a security incident management system for objects of energy and water supply system, where the processes of accumulation, distribution, transmission, accounting of volume of water resources are implemented as target processes. The main objects of the infrastructure includes reservoirs and channels for transferring water between producers and consumers of water, as well as energy generating capacities. The developed proposals take into account the varieties of physical sensors and activating elements, incl. water level sensors, water flow sensors, water pressure sensors, electromechanical closures (simulated by ball valves with an energy drive) and other elements.

11. The scientific and technical proposals for the application of the developed methods, models, techniques, algorithms, architectures and software prototypes of the security incident management system for complex protection of the telecommunication system of the infrastructure of a mobile communication network of support and operational management in emergency situations have been developed.

The results obtained in the project can be used to build a security incident management system of the telecommunication infrastructure of a mobile communication network of support and operational management in emergency situations. The developed proposals take into account the variety of available communication interfaces, physical sensors and activating elements.

12. Theoretical and experimental evaluation of the effectiveness of methods, models, techniques, algorithms and architectures for analytical processing of big data for managing the incidents and counteracting to targeted cyber-physical attacks in mission-critical distributed systems, taking into account cloud services and Internet of things.

An experimental evaluation of the data processing time has shown that the usage of parallel computations makes it possible to realize the requirements for realizing this process in real or near real time. For security events correlation tasks, acceleration was achieved more than 1.5 times with OpenMP and more than 1000 times with Cuda. Time of construction and analysis of attack patterns did not exceed 1 minute for a network of 1000 hosts. Experiments have shown that the functional and non-functional requirements are met. It is shown that the greatest gain is achieved in the case of implementation of countermeasures after the first incident. The average gain for test computer networks was 80% compared to the situation of the absence of countermeasures.

13. 8 certificates of state registration of computer programs were received and 17 papers have been published in scientific publications indexed in the Web of Science and Scopus databases as well as 11 publications – in scientific publications indexed in the "RSCI" (Russian scientific citation index).

14. One monograph have been prepared and submitted to the publishing house. Also, based on the results of the project, two monographs have been prepared for publication.

15. 25th Anniversary Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2017) was organized and held March 6-8, 2017 in St. Petersburg, Russian Federation. Particularly a web-site of the conference https: // www.pdp2017.org was created. The co-chairmens, program and organizing committees of the conference was defined, eight special sections of the conference were prepared. The proceedings of the conference were published in cooperation with the Conference Publishing Services (CPS) of the International Association IEEE. The proceedings of the conference are indexed into international citing Scopus and Web of Science.

16. A third school of young scientists was organized in the field of the project. Leading Russian and foreign scientists were invited as lecturers. The name of the school is "Incident management and countering targeted cyber-physical attacks in distributed large-scale critical systems" (IM & CTCPA 2016). The dates of the school are December 18 - 21, 2017. The venue is SPIIRAN and ITMO University, St. Petersburg. 150 participants took part in the school, including: 13 Russian and 11 foreign scientific lecturers (from France, Ukraine, Italy, Germany, the Czech Republic and other countries).

17. Presentations at 20 international and Russian scientific conferences were made by the participants of the project, where questions in the project field were discussed.

Information resources in the Internet, which are connected to the project:

- information on the RNS project:

http://www.comsec.spb.ru/en/projects

http://www.comsec.spb.ru/en/projects/

- information on the full-time international scientific conference:

https://www.pdp2017.org/

http://www.comsec.spb.ru/en/pdp2017/

http://www.comsec.spb.ru/pdp2017/

- information on the school of young scientists (with presentations of the lectures):

http://www.comsec.spb.ru/en/imctcpa17/

http://www.comsec.spb.ru/imctcpa17/