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 2016 and scientific results

1. The general architecture of the perspective security incident management system for mission critical objects was developed. On the basis of the analysis of the applicability of the principles of proactivity, dynamism and multidimensionality for the management of security incidents of mission important objects the following components of the security incident management system were highlighted: (1) external data sources (sensors); (2) a reliable and trusted data bus; (3) a component of processing and correlation of security events; (4) a hybrid data storage; (5) a component of intelligent analysis of security events; (6) a component for calculating the security metrics; (7) a component of countermeasure selection; (8) external systems which implement the selected countermeasures.

2. The methods, models, techniques and algorithms for collection, preprocessing and correlation of security information and events on the basis of applying the complex of distributed intelligent sensors and the concept of Big Data are developed. The methods, models, techniques and algorithms of collection and preprocessing of information and security events of critical objects were developed. The task of ensuring of aggregation of information and security events was formulated, which is decomposed into two subtasks: determining the sequence of performing the operators of streaming data processing which implement the required queries for aggregation; distribution of operators in the transport network nodes which provide parallel processing of sequences of operators of streaming data processing. In order to solve both problems it is proposed to use an approach based on the Complex Event Processing technology. The software system Spark Streaming is investigated and used as a tool platform. The methods, models, techniques and algorithms of information and security event correlation were developed which are based on a combination of several approaches: the finite state machine, the rule-based approach, the method of reasoning based on precedents, Bayesian networks, artificial neural networks.

3. The methods, models, techniques and algorithms of functioning of a trusted data bus and a hybrid storage of information and security events were developed. Requirements for the data bus are specified which necessitate to ensure the reliability of data transmission under the impact of computer attacks, the reliability of transmitted data, which excludes the possibility of a third-party and (or) an unauthorized implementation, and operativeness of data transmission under near real time conditions. On this basis the methods, models, techniques and algorithms were identified for operation of the trusted data bus. The methods, models, techniques and algorithms for a hybrid storage of information and security events were defined which include the methods of representation of information and security events, the technique of constructing the hybrid storage, the technique of selection of a tool for creating the hybrid storage, as well as models and algorithms for access control to the hybrid storage.

4. The methods, models, techniques and algorithms for detecting the complex multistage targeted attacks in a real time based on the technology of intelligent analysis of information and security events were developed. The models and methods of detecting the targeted attacks based on the technology of intelligent analysis of information and security events were proposed: the model of a two-layer neural network as a binary classifier for detecting the targeted attacks; the model of a neuro-fuzzy classifier based on Takagi-Sugeno fuzzy inference; the method of attack detection based on a support vector machine. For real-time detection of complex multistage targeted attacks the technique was developed

which is based on analytical modeling which uses information about security incidents received from the proposed models, methods and algorithms of targeted attack detection.

5. The methods, models, techniques and algorithms for calculation of primary and integrated security metrics were developed. The methods, techniques and algorithms for calculation of the various metrics (on the topological level, on the level of the attack graph, on the attacker's level, on the event level, on the level of countermeasures and on the integrated level) were proposed. The models (including the model of attacks in the form of a Bayesian graph of attacks, the model of dependencies between network services, the service model, the attacker model, the event model and the model of countermeasures), techniques and algorithms for calculating the indicators of security included in the taxonomy.

6. The methods, models, techniques and algorithms for the analysis of security events history, prediction of malefactor actions and their consequences were developed. Processed events come from the correlation subsystem and indicate a compromise of the network host (i.e. violation of the properties of confidentiality / integrity / accessibility or illegitimate getting access rights). To analyze events we applied the developed models of attacks, attacker and event. Changing elements of these models' state allows predicting the next steps of the malefactor. The event model determines the time the event occurred in, the host it was registered on and event type (that is the consequences for the system). To fix the state changes in the attack model (Bayesian attack graph) and the malefactor a relationship between these models and the event model is introduced. The communication is carried out via the host and the consequences (type of compromise of the host). The current position of the malefactor on the system is determined on the base of these data and the developed technique. Besides, the information on the previously recorded events is taken into account considering their temporal and spatial characteristics to assign events to a single attack or several different multi-stage attacks.

7. The methods, models, techniques, algorithms, architectures and software prototypes of components of automated response on the targeted cyber and physical attacks, based on the hybrid storage of security information and events and on expert knowledge inference, were developed. The component of the response based on a hybrid repository of information and security events uses the event calculus and temporal logic for inference. The component of the response based on expert knowledge uses indicators of security and implements the method of countermeasure selection based on their analysis. The component of the response based on a fuzzy inference provides a decision support about the presence of anomalous system behavior using the Mamdani fuzzy inference method.

8. The methods, models, techniques, algorithms, architecture, and software prototypes of components of proactive, dynamic and multidimensional security incident management for critical objects taking into account cloud services and networks of the Internet of Things were developed. The proposed results are realized by the example of the access control system in an office building with the use of a programmable microcontroller Arduino Yun, digital RFID sensors, workstations, server and network equipment.

9. The models of the specific subject areas (smart house, Russian Railways, power-and water supply system, mobile communication network of support and operational management in emergency situations) as a security incident management objects were developed.

The proposed integrated model of a smart house system includes three levels of representation. The lower level is represented by the models of software and hardware information sources designed for modeling of the certain aspects of the concept of Internet of Things. At the intermediate level modeling

a network infrastructure is performed that combines the individual hardware and software information sources into a unified system of collection, storage and preprocessing of information and security events. The upper level contains a model of a smart house as a security incident management object.

A physical model of the systems for centralization, signaling and blocking for Russian Railway consists of four levels. The first level (level of operator) is represented by a graphical user interface, which is used to display information on the status of objects of railway automation, supervisory control and centralization. The second level (level of computing) is represented in the model as a personal computer serving to perform functions of collecting, storing, processing and transmitting information on the current state of the objects of centralization and diagnostics of the centralization system. The third level (level of management and control of the flow based equipment) is modeled as a system of Arduino based controllers. For the fourth level modeling (physical level of railway automation devices) we used a model of railway digitally controlled by equipment from Piko company.

A developed physical model of a dam comprises a number of hydraulic devices, namely water tanks, sensors, switches, hoses working in conjunction with a microcontroller Arduino Yun. This equipment at the physical level allows modeling of water flow processes, opening and closing of locks, excess of the established restrictions of water levels, etc. The software and information based part of the system is responsible for the collection, processing, analysis and display to the user of mission-critical events and dam security incidents.

As a basis for a prototype of a mobile communication network for support and operational emergency management the XBee s2 embedded devices were proposed. These devices allow organizing wireless communication on the base ZigBee protocol. The hardware and software implementation of the protocol on the physical devices of the network allows ensuring its self-organization and self-recoverability after the failure of one of the nodes or in case of downgrade of communication quality.

Models of security incidents for these systems were constructed. Possible attacks at all levels of the system were considered, examples of the modeled security incidents were obtained.

10. Three certificates of state registration of computer programs were obtained. We published six papers (and one paper was accepted for publication) in scientific journals indexed in the databases Web of Science and Scopus. Ten publications in scientific journals indexed in the RSCI were published.

11. Preparatory works on organization of the 25th anniversary International Conference on Parallel, Distributed and Network-based Processing (PDP 2017) were carried out. The conference will be held on March 6-8, 2017, in St. Petersburg, Russian Federation. In particular we developed a website of the conference (http: //pdp2017.org), co-chairs, the program and organizing committees were formed. The review and selection processes of submitted scientific papers from more than 20 different countries were conducted. We signed an agreement and started cooperation with Conference Publishing Services (CPS), namely IEEE International Association for the publication of the conference proceedings.

12. A school of young scientists was carried out with an invitation of leading Russian and foreign scientists as lecturers on the subject of the project. Name of the scientific school - "Incident management and countering targeted cyber-physical attacks in distributed large-scale critical systems", IM&CTCPA 2016. Dates of the school – October 31 - November 2, 2016. The school location - St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Saint-Petersburg. The school was attended by 79 participants, including 13 Russian and 6 foreign

scientists and lecturers (including from France, Sweden, Finland, Belarus and Ukraine), as well as 9 Russian young scientists aged under 35 years old, 51 PhD students and undergraduate students.

13. The presentations were made in 19 Russian and international scientific conferences, where the issues relating to the project were discussed.

Information resources on the Internet devoted to the project:

- information about the RNF project:

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

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

- information about the full-time international scientific conference:

http://www.pdp2017.org/

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

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

- information about the School of Young Scientists (with presentations of lectures):

http://www.comsec.spb.ru/ru/imctcpa16/

http://www.comsec.spb.ru/imctcpa16/