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 2015 and scientific results

1. A construction conception and architecture of a security incident management system for mission critical objects were developed. Conditions of implementation of both targeted information/software and physical impacts in cloud-based systems and Internet of Things networks were analyzed. Various approaches to understand the term "targeted attacks" offered by various security means developers, which define various features of this attack class manifestation, were considered. Examples of targeted attacks as well as their characteristics were given. In accordance with the formed criteria of the targeted attacks their comparison to mass attacks was performed. As a result of the comparison a list of the distinctive features of targeted attacks was formed as well as their essence was exposed. The sequence and content of the stages of the targeted attacks were defined. The direction vectors of the targeted attacks were analyzed. The necessity of creating a security incident management system (SIMS) to successfully implement the measures to protect mission critical objects (MCO) was substantiated. Tasks solved by SIMS for MCO were selected. The purpose and the basic principles of SIMS construction for MCO, namely proactivity, dynamicity and multidimensionality, were defined. A set of tasks, SIMS should solve to implement the declared principles, was substantiated. Disadvantages of existing SIMSs, not allowing to realize these principles, were identified. A conception of building SIMS for MCO on the base of proactivity, dynamicity and multidimensionality principles was formed. It includes general statements, principles of security incident management, goals and objectives of SIMS, MCO features as objects of protection, mechanisms for security incidents management, general description of the architecture of the SIMS for MCO.

2. A common approach and requirements to the components of the collection, pre-processing, correlation of information and security events through the use of the complex of distributed intelligent sensors and Big Data were developed. The place and role of components of collection, pre-processing and correlation of information and security events in SIMS for MCO were substantiated. The location of these components is expected to be at the end and intermediate nodes of the MCO infrastructure, as well as in the center of information collection and processing. Two types of basic elements forming the base for the components at the end and intermediate nodes, intelligent sensors and aggregators were identified. A common approach and requirements to construct the components of data collection through the use of distributed intelligent sensors were described. A general scheme of intelligent sensor location in SIMS for MCO was proposed. The necessity of the implementation of the normalization procedure during data collection was substantiated. The requirements imposed on the information collection components in SIMS for MCO were formed. A common approach and requirements to build the components of pre-processing of data through the use of distributed intelligent sensors were defined. It was shown that the components of the SIMS for MCO involved in the direct data pre-processing are aggregators. The general location scheme for aggregators in SIMS for MCO, allowing demonstration of the principles of their location, taking into account the conception of processing large data streams was formed. The requirements imposed on the components of data pre-processing in SIMS for MCO necessary for correct operation in real-time mode, taking into consideration the conception of Big Data, were formed. A common approach and requirements to construct the components for data correlation on the base of the use of distributed intelligent sensor were defined. Correlation components functions were described. It was shown the main correlation component is a data center that can be represented by one or more connected hosts of an appropriate level. Requirements to components of security events correlation in SIMS for MCO were formed.

3. A common approach and the requirements to reliable trusted data bus and hybrid storage of information and security events were developed. Requirements to the reliable trusted data bus, such as high bus reliability, high accuracy and high operativeness of information processing, were substantiated. The features that have cloud systems and Internet of Things networks as a medium to disseminate through the data bus were defined. The place of the data bus was determined in SIMS for MCO, as well as its connections with other system components were established. The common approach to the construction of the reliable trusted data bus was substantiated. For this purpose, first of all, attacks influencing the bus were analyzed and their characteristic were given. To improve the reliability of the data bus in conditions of the presence of the considered attacks types we proposed an approach that focuses on the use not only of proactive protection methods, but also a posteriori information protection strategies. Requirements to hybrid storage of information and security events were substantiated. In the first place, the storage place in the SIMS structure was determined. At that the storage requirements were divided into two groups: the requirements from users and ones from the other components of the SIMS. The common approach to the construction of the hybrid storage of information and security events was substantiated. At that, first of all, we selected the most promising and widely used standards for security data representation (events, incidents, attacks, etc.). It was substantiated a need to supplement the relational format of data in the storage by XML and RDF formats. To implement this approach an architecture of ontological data repository in SIMS for MCO was proposed.

4. A common approach and requirements for the components of the real-time detection of complex multistep attacks based on intelligent analysis of information and security events were developed. To determine the requirements to a detection system of multistep targeted attacks the existing implementations of such systems were analyzed. Based on this analysis we formulated the main functional and non-functional requirements for the components of the detection of multistep targeted attacks. In the process of developing a common approach to building the components of targeted attacks detection, different strategies were analyzed, which are used by companies to protect against targeted attacks. The specialized methods to detect such attacks were considered, which allow to detect their existence both on the stage of the attack, and while investigating of already occurred incidents. The standard protection components were considered, which are the basis for systems of detection of complex multistep targeted attacks. The following protection components were considered: firewalls; intrusion detection systems; intrusion prevention systems; Internet gateways; email gateways; honynets; network traffic analyzers. Besides the protection components, that are directly involved in the process of detecting the targeted attacks, components were highlighted, which have an indirect impact on the detection, but allow to enhance the effectiveness of standard components and complex components of protection. Thus, to counteract usage of vulnerabilities the following protection components were analyzed: automatic updating of installed software; automatic testing of installed software; analysis of network infrastructure; network access control. The basic principles were highlighted that distinguish the proposed approach to build the components of protection from existing analogues: the principle of multi-level structure and the principle of heterogeneity. It is concluded that the usage of such components enable to increase significantly the probability of detection and reduce the possible risks.

5. A common approach and requirements for components of calculating the primary and integrated metrics of security were developed. To develop this scientific result we carried out a detailed analysis of the metrics, which are used for security assessment and support of decision-making, and techniques of their calculation. This analysis allowed to reveal the main results and trends in the field, the advantages and disadvantages of existing solutions, and provided the opportunity to offer the basic requirements for primary and integrated security metrics. These requirements were formulated taking into account the standard requirements to metrics, the requirements to security metrics based on the analysis and the requirements on the part of the analyzed system. The classification of security metrics was proposed, which is formed according to the data used to calculate the security metrics and allows to define a multi-level approach to the calculation of primary and integrated security metrics. A common approach to calculation of security metrics includes three stages: gathering the input data; calculating the security metrics; determining the level of security and choice of countermeasures. The peculiarity of the proposed approach is the possibility of determining the level of security and choice of countermeasures at various levels of functioning of the protected system and taking into account the input data available at the time of the analysis.

6. A common approach and requirements for the history analysis components of security events, forecasting the actions of intruders and their effects, were developed. During the preparation of the scientific result we formulated the main requirements to the functional and non-functional characteristics of the history analysis of security events, forecasting the actions of intruders and their effects. An approach was developed which is based on the operational formation, modification and analysis of attack models, which allows to predict the actions of intruders and their consequences for near real-time. Due to the complex analysis of the multistep attack, this approach allows to identify groups of events, among which an element of the multistep attack was perhaps not detected. This makes it possible to detect zero-day vulnerability exploitation and other covert actions of intruder.

7. 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 2015. Dates of the school – November 26-28, 2015. The school location - St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), Saint-Petersburg. The school was attended by 12 Russian and 6 foreign scientists and lecturers (including from Germany, Italy, Finland and Belarus), as well as 37 listeners - Russian young scientists aged under 35 years old inclusive and students, PhD students and undergraduate students.

Information resources on the Internet devoted to the project:

- information about the project RNF:
  http://www.comsec.spb.ru/ru/projects
  http://www.comsec.spb.ru/en/projects/
- information about a full-time international scientific conference:
  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/imctcpa15/
  http://www.comsec.spb.ru/imctcpa15/