RSF project No. 21-71-20078. Description of the work performed at the 3rd stage and the scientific results obtained

1. **Methods, models, techniques and algorithms for conducting investigations of computer incidents based on analytical processing of large arrays of heterogeneous cybersecurity data** have been developed.

Methods, models, techniques, and algorithms for conducting investigations of computer incidents based on the analytical processing of large volumes of heterogeneous cybersecurity data have been developed. The developed model for conducting computer incident investigations describes the primary sets and subsets of elements of cybercrimes. The developed algorithms and techniques for the stages of investigating computer incidents utilize the stages of the model and its subsets. The developed method for conducting investigations of computer incidents based on the analytical processing of large volumes of heterogeneous cybersecurity data enhances the efficiency of specialists in investigating computer incidents of information security. The method allows for its application to various types of computer incidents as a universal investigative method. The model-algorithmic part of the method specifies procedures used to describe the stages of investigating computer incidents, their composition, and the sequence of actions of the specialist during the investigation. The totality of developed methods, models, techniques, and algorithms for investigating computer incidents forms a comprehensive approach to investigation based on the analytical processing of large volumes of heterogeneous cybersecurity data.

2. **The architecture and software prototypes of real-time attack detection components based on simulation and graph-based modeling** have been developed.

The architecture and software prototypes of real-time attack detection components based on graph-based and simulation modeling have been developed. These components are designed to solve problems of detecting attacks in industrial systems, as well as predicting future system states based on intelligent data analysis with high accuracy and efficiency. The following main software modules have been developed: (1) event preprocessing module, responsible for extracting information features from the input data stream and normalizing them to a unified security event format; (2) event clustering module for constructing a limited number of aggregated system states based on clustering; (3) module for constructing graphs of states and transitions with the determination of permissible transitions between aggregated states of the system; (4) state and transition graph analysis module, responsible for traversing the graph based on the actual flow of events from the system in order to determine the current state of the system; (5) a neural network state prediction module, based on a recurrent neural network and including elements of simulation modeling based on rules and statistics to predict future states. Note, the built software prototypes of attack detection components are also intended for use within other components of the system for analytical processing of large arrays of heterogeneous data on cybersecurity events, particularly in forensics, visualization and decision-making tasks.

3. An **architecture and software prototypes of components for real-time detection of anomalous activity and violations of security criteria and policies** have been developed **based on analytical processing of large arrays of heterogeneous data on cybersecurity events**.

For the software implementation of the developed model-algorithmic part of the component for real-time detection of anomalous activity and violations of security criteria and policies, modules for data preprocessing, anomaly detection, and generation of explanations of decisions given by analytical models were developed using the following Python libraries: TensorFlow and PyTorch for working with deep neural networks, in particular pyOD and pyGOD. The training of the analysis models was performed in the SCC computing environment.

Two types of datasets were selected as input data to perform experimental evaluation of the components of anomalous activity detection and violations of security criteria and policies: a dataset from physical sensors and a dataset with system events from the Windows authentication service.

To analyze system events, we developed a component of their preprocessing, which performs the construction of the event graph for a given time interval Δt and forms a vector of analyzed features, which are represented by both structural and topological characteristics of the graph and statistical characteristics of events.

To detect anomalies in the data stream from physical sensors, we proposed to use a combination of two classifier models: deepSVDD (deep single-class classifier with autoencoder), and a random forest

model that performs multilabel classification. Two local explanation methods, LIME and SHAP, were investigated to explain the prediction of the first model; experiments showed that the SHAP method can be considered applicable in the anomaly explanation task for the SWaT dataset, and its results can be used as additional information in the risk assessment task.

4. **An architecture** has been developed for c**omponents of operational assessment of the security of information, telecommunications and other critical resources based on analytical processing of large arrays of heterogeneous data**.

The developed architecture of components for operational assessment of the security of information, telecommunications and other critical resources based on analytical processing of large arrays of heterogeneous data includes two levels: high and low. The high level consists of modules (subsystems) that directly perform operational assessment of the security of information, telecommunications and other critical resources using the capabilities of the SCC. The high-level structure includes the following modules: network model building module; module for generating risk paths; risk assessment module; high-risk path selection module. Low-level modules include modules that perform supporting (auxiliary) functions. These functions include: collection and preliminary processing of source data; maintaining a working database; interaction with other components; interaction with users.

The component prototype is implemented in Python using such libraries as networkx, psycopg2, joblib and pickle. PostgreSQL DBMS is used to store data. The Flask framework is used for integration with the operational visualization component. To be able to test the prototype component on data from large network information systems, a generator of network graphs of such systems was additionally developed.

5. **The architecture and software prototypes of components for operational analysis and information security risk management** have been developed **based on analytical processing of large arrays of heterogeneous data on cybersecurity events**.

The architecture of the operational analysis and information security risk management component has been developed. Within the architecture, the following functional modules of the component are identified: module for generating an integral risk assessment in static mode; module for generating an integrated risk assessment in dynamic mode; module for comparing the integral assessment with the criterion; module for setting tasks for attack and anomaly detection components; module for setting a task for the decision support component. Connections with other system components (components of data collection, risk assessment, attack and anomaly detection, and decision support), as well as a high-performance cluster for performing computing tasks, are defined. Input data formats have been clarified, including security events, device and user profiles, and relationships between them, calculated values of security metrics for devices and for users, data on the number and type of anomalies, data on the number and type of cyber attacks, historical information on risk assessments entered Expert criteria for risk levels. Based on the developed architecture, a software prototype was implemented in Python, implementing the models, methods and algorithms developed at this stage of the project. The SWaT dataset was used to test the developed prototype. Experiments were carried out to validate the proposed models, techniques and algorithms and determine their parameters.

6. The **architecture and software prototypes of components for operational visualization of large arrays of heterogeneous data on cybersecurity events** have been developed **in the interests of status assessment, decision support and incident investigation**.

This result is intended for further implementation of manual visual analysis of data on information security events when displaying large volumes of heterogeneous source data, displaying user authentication logs, assessing the security status of a computer network and displaying metrics for risk assessment purposes.

The developed architecture assumes the order of pairing the modules of the decision support system with the operational visualization module to solve problems of visual search for anomalies in the data of each module.

The developed software prototypes of operational visualization components can be included in decision support systems and will be used to enable the operator to visually search for anomalies in data when solving assigned information security problems.

7. The **architecture of the system for analytical processing of large arrays of heterogeneous data on cybersecurity events, using the capabilities of the SCC**, has been clarified**.**

To solve optimization problems, refinements to the system architecture were proposed. The following subsystems were developed: (1) control subsystem, (2) experimental environment subsystem, (3) engineering subsystem, (4) subsystem for creating, training and validating models, (5) subsystem for operating and retraining models. The proposed architecture refinements ensure the launch into the production cycle and commissioning of solutions built on the basis of machine learning, and guarantee feedback, as well as controlled automation, end-to-end integration with new methods, models, algorithms, and software components developed for the analytical processing of large arrays of heterogeneous data on cybersecurity events.

Various approaches to building information security event management systems have been studied. As a result of research during the project, elements and technology stacks were selected that provide high levels of performance and resource efficiency for monitoring systems. So ClickHouse was chosen as the main DBMS. Data sets are loaded into it, with which anomaly and attack detection models work. Information about incidents (alerts, information security events, etc.) is also loaded into it. Data cubes are formed in it, on which visual analytics in the system is subsequently built. To manage flows, the Apache Kafka technology was chosen, with which the MongoDB DBMS (unification and normalization) is associated. To unify data, the project created unification models for Users and Hosts, the latter including cyber-physical devices. Data received from external systems, for example, IOC indicators of compromise, information about vulnerabilities, and security assessments are also stored in an online storage built on the MongoDB DBMS.

The research results were published in 15 articles indexed in WoS and Scopus (including 2 Q1 articles), 2 articles indexed in RSCI (on WoS platform), and 20 articles and abstracts of reports indexed in the Russian platform – eLIBRARY.RU.

During the implementation of the project, exclusive rights to intellectual property were obtained: 1 patent for an invention, 5 certificates of state registration of computer programs.

Members of the team participated in testing the results at 14 Russian and international conferences and seminars.

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