ANNOTATION

Ph.D. dissertation of doctoral candidate PhD specialty 6D070400 - "Computer Science and Software" Beketova G.S. on the theme "Models and methods of intelligent recognition of cyber threats in critical computer systems"

The relevance of the research topic. The widespread use of computer systems and information and communication technologies contributes to higher labor productivity, lower material inputs and improve product quality and living standards. Computer systems and IT play a important role in the deployment, operation and maintenance of critical infrastructures responsible for the timely delivery of energy, water, food, transport services and communications to consumers. The most important element of such critical infrastructures are computerized systems, the malfunctioning of which can lead to serious or even explosive social and economic consequences on a national or regional scale, which is due to a strong systemic relationship between the various components of KVKS and life support systems. To ensure the high availability, reliability and security of critical computer systems (hereinafter –“CCS”), it is necessary to preventively solve problems related to their information security (hereinafter – “IS”) and cyber defense.The active expansion of the use of CCS, especially in the segment of mobile, distributed and wireless information technologies, is accompanied by the emergence of new threats to the IS, as evidenced by the rapid growth in the number of incidents related to IS and cyber defense CCS, as well as identified vulnerabilities in their software (hereinafter – “SO”) . Threats are quite real, since criminals can get the opportunity to intercept passwords, separate files, geolocation information, broadcast audio and video data, monitor Wi-Fi networks, web cameras, placards, etc. The seriousness of the problem can be judged, if only by repeated facts, when one or more intruders, having access to CCS data, could completely paralyze the work of large enterprises or companies in a matter of minutes.

Thus, the relevance of research aimed at further development of models and methods of protection based on intellectual recognition of CCS threats and providing there is one of the key problems of cyber defense of the critical infrastructure of the state.

The aim and goals of the research. The aim of the thesis is the development of models and methods for the protection of critical computer systems based on intelligent recognition of cyber threats in the conditions of constant increase in the number of destabilizing effects on the confidentiality, integrity and availability of information.

To achieve this goal, it is necessary to solve the following tasks:

1. To develop a method of intellectual recognition of threats, anomalies and cyber attacks, allowing to ensure cyber security of CCS based on the use of innovative intelligent cyber defense systems to increase the resistance of CCS to cyber attacks.

2. Develop a model of intelligent recognition using logical procedures for the detection of anomalies and cyber attacks, based on the coverings of the feature

matrices (hereinafter – “MP”) and the concept of the elementary classifier (hereinafter – “EC”).

3. Minimize the number of training samples for features located in the repository of an intelligent threat, abnormality and cyber attack detection system.

4. Improve models for determining the structural and technological reserve of software and information support (software and IO) CCS, taking into account the criticality of their modules to increase the level of information security, as well as a model that allows selecting the rational composition of the information security system, taking into account its effect on the functional parameters of CCS.

5. Perform simulation of the main components of CCS and the cyber defense subsystem, based on the proposed models of intellectual recognition of threats, anomalies and cyber attacks in CCS.

The object of the research is the processes of intellectual recognition of cyber threats for CCS.

The subject of the research is methods and models for the protection of critical computer systems.

Methods of research. In the course of the research, taking into account the features of the subject area and formulated problems, Boolean algebra and fuzzy set theory were used to develop a model for intelligent recognition and detection of anomalies, cyber attacks and cyber threats; discrete optimization method - to effectively solve the problems of providing cyber securityCCS; methods and means of simulation for the implementation of the developed models; principles and methods of object-oriented programming for the creation of application software products.

Research results scientific novelty

1. For the first time developed:

- the method of intellectual recognition of cyber threats, based on the definition of conjunctions for matrix coatings containing binary informative characteristics of attributes for classes of threats, anomalies and cyber attacks, and differing from the existing application of logical functions and fuzzy sets of signs of cyber attacks, which allows creating effective analytical, circuit and software solutions information security system for CCS;

- model of recognition and formation of a decisive rule for logical procedures for the identification of cyber threats and attacks, based on the procedure for analyzing the criticality of individual components of CCS, coatings of matrices of binary features and the concept of an elementary classifier, and unlike existing ones, providing the possibility of intelligent recognition with a minimum of errors, and, account is difficult to explain the signs of anomalies, threats and cyber attacks;

2. Improved:

- Optimization models of structural, technological and virtual-redundant backup, as well as software and information support for CCS, which differ from existing ones, using the criterion of maximum probability of successfully hindering the system of threat, anomaly and cyber attack detection, which allows assessing the functionality and stability of GIS to various classes of cyber attacks at the design stage.

3. Have received the further development:

- Simulation models of cyber attacks on elements of CCS, allowing choosing rational ways of preventing and neutralizing their consequences, to perform analysis of complex, combined types of cyber attacks on CCS.

Scientific results in the framework of requirements for dissertations.

In the introduction disclosed the relevance of specific issues associated with the studied problem. Given the idea of work, the aims and goals of the research, scientific novelty and practical value of the work.

In the first section, the analysis of scientific works devoted to the study of cyber attacks on critical computer systems. The most common classes and types of cyber attacks on CCS conducted a review and analysis of previous researches and also work performed at the direction of synthesis of systems of recognition of intrusions on the basis of intelligent technologies for pattern recognition.

In the second section it is shown that application components of an intelligent adaptive information security CCS may be based on the use of logical procedures and the concept of an elementary classifier for anomalies, cyber threats and vulnerabilities CCS. The proposed model to detect threats, anomalies and cyber attacks in CCS based on constructing coverings of classes and the elementary classifiers. The basic approaches to the design of logical procedures for threat recognition using the apparatus of logic functions that will allow us to create effective analytical, circuit and software solutions information security system for CCS. The developed methodology decision rules for logical procedures for threat recognition that allows you to perform sensing in the framework of a certain class, with a minimum number of errors.

In the third section the proposed refinements to the models used to solve optimization problems of complex information security solutions for CCS. The specification of the models affects the aspect of the pre-decomposition information security system for CCS on critical and non-critical components, which are provided with the backup procedure.The problems of optimizing the composition of the SLC complexes of CCS are considered.The optimization model of the structural and technological reserve of information and software arrays for CCS has been clarified, and the specifics of the application of discrete optimization methods for solving problems of ensuring cyber security of CCS are considered.

In the fourth section, we analyzed the possibility of writing and connecting our own modules in the MATLAB and Simulink environment for implementing models describing the probabilistic states of the system during the implementation by the attacker of various scenarios of cyber attacks on CCS. The developed models in MATLAB and Simulink, allow reducing the time of debugging of cyber defense projects by 25-30% due to simulation of cyber attacks on CCS modules.

In conclusion, the main results of the dissertation work and information on the practical application of the research results are reflected.

Approbationof research results.

The main provisions and results of the researchwere discussed at the seminars of the Chair "Computer and Software Engineering" of the Kazakh National Research Technical University named after K. Satpaev (hereinafter – “KazNRTU”); seminars of the Chair "Information Security Technologies" of the National Aviation University of Ukraine and were reported at: International Satpaev Readings "The Role and Place of Young Scientists in Implementing the New Economic Policy of Kazakhstan" (Almaty, 2015); II International Scientific and Practical Conference "Actual issues of ensuring cybersecurity and information protection", (Kiev, 2016); International Scientific and Practical Conference ITSEC - National Aviation University (Kiev, 2016); International scientific-practical conference "The state and improvement of the security of information and telecommunication systems". SITS-2016 (Ukraine, 2016); X International Scientific and Practical Conference "Modern Information and Communication Technologies in Transport, Industry and Education", (Dnepro, 2016); International scientific and practical online conference "Energy and resource-saving technologies: experiences and perspectives" (Kyzylorda, 2017); International Scientific and Practical Conference "Integration of Science, Education and Production - the Basis for the Implementation of the Nation Plan" No. 9 Saginov Readings (Karaganda, 2017).

The results of the dissertation research were highly appreciated by Kaspersky Lab's LLP in Central Asia and Mongolia; are used in the educational process of the departments "Computer Science and Information Systems" of Kyzylorda State University named after Korkyt Ata and "Information Technology Security" of the National Aviation University of Ukraine; have been tested in LLP "Sipher BIC" (Kiev) and LLP "QUARES" (Almaty).

The dissertation was made at the Computer and Software Engineering Department of the Institute of Information and Telecommunication Technologies of KazNRTU named after K.Satpaev.

Publications. 21 papers have been published on the topic of the dissertation, of which 8 were published in publications recommended by the Committee for Control in Education and Science of the Ministry of Education and Science of the Republic of Kazakhstan, 3 articles were published in the edition included in the Scopus database, 1 article was published in foreign journals, 9 articles were published in collections international scientific and practical conferences.

Structure and size of the dissertation. The dissertation consists of an introduction, four parts, a conclusion, a list of bibliography and applications, contains 135 pages of the main text (64 figures, 14 tables). The bibliography contains 90 references of literature.