ANNOTATION

Thesis of Zhumangaliyeva Nazym on the topic:
«The control technology of anomalous state parameters for intrusion detection systems»
for the degree of doctor (PhD) on the speciality
6D070400 - Computer technology and software.

Relevance of the topic. The intensive development of informational technologies has a positive impact on all spheres of human, society andpublic activities. At the same time, side effects are observed, primarily due to the fact that computer systems and networks are increasingly exposed to threats, new types of which generate new cyber attacks that negatively affecton the security of informational system`s (IS) resources.

Relevance of the topic. The intensive development of information technologies positively influences all spheres of human activity, society, state. At the same time, there are side effects, which are primarily related to the fact that computer systems and networks are increasingly exposed to threats, new types of which generate new cyber attacks that negatively affect the security of information systems (IS) resources.

In this regard, there is a need for security systems that allows the analysis, monitoring, forecasting and blocking of these invasions.One of the most common solutions for the security of IS resources (RIS) are intrusion detection systems (IDS) based on software or firmware, primarily aimed at identifying the facts of unauthorized access through computer networks. As you know, these solutions are based on the signatured (patterned) and anomalous intrusion detection principles. Modern IDS of the abnormal principle are mainly based on mathematical models that require a lot of time to obtain statistical data, implementation of the learning process (for neural network systems) and other complex and lengthy preparatory procedures.More effective in this regard are approaches based on the formalization of the judgments of experts and their use in the decision-making process on the possibility of carrying out attacks on computer systems and networks.

It is known that unauthorized actions on RIS influence the environment and generates certain anomalies in it. It is usually weakly structured, unclearly defined and special models, methods and systems should be used to detect intrusions that have caused anomalies in such environment. Expanding the functionality and increasing the efficiency of network countermeasures systems can be achieved through the use of new, appropriate technical solutions that focus on functioning in fuzzy conditions.

For formalization of information in an unclearly weakly structured environment and effectively implementation of its processing methods and models of fuzzy sets` theory, the foundations of which laid, and for implementation of the decision-making process (for identifying the attacking actions) based on these special methods and models, appropriate means are needed.

In this regard, the development of tools that extends the capabilities of modern IDSs is the creation of appropriate models, methods, technologies and systems for detecting anomalies generated by network of non-signature cyber attacks in fuzzy conditions.

The purpose of the thesis is to develop models and means of identifying abnormal condition, to expand the capabilities of a system for detecting non-signature types of cyber attacks in computer networks.

For achieving this goal, it was necessary to solve the following **tasks**:

1. To investigate the current state of development of the theoretical and practical base using for detection of intrusions in computer systems;

2. To develop a model of base values and a model of reference values for mapping and measuring the anomalous state in environment true to type of a particular type of cyber attack in computer networks;

3. On the basis of the model of base values and the model of reference values to construct a model for determining the rules for detecting anomalous state for the formalization of the process of their formation;

4. To develop on the basis of the model of base values, models of reference values and models of decision rules a technology for detecting anomalous states generated by actions of an unauthorized part;

5. To develop a structural solution for expanding the functionality of intrusion detection systems oriented to non-signature types of network cyber attacksbased on the technology for detecting of abnormal states;

6. To develop and conduct experimental research of new technical solutions that allow to identify attacking actions in computer networks by monitoring activity in the environment.

The object of the researchis the process of revealing the anomalous state generated by the attacking actions in computer networks.

The subject of the researchare models, methods, technologies and systems for detecting anomalies in an indistinctly defined weakly structured environment, generated by attacking activities in computer networks.

The scientific novelty of the work is as follows:

1. The model of basic values and the model of reference values have been further developed due to the introduced sets of possible intrusions and values, and on their basisthe sets of pairs "intrusion: values" and "invasion: the set of conjugate pairs" which allows to display and measure the anomalous state in environment and formalize the process of building standards of fuzzy variables, characteristic of a certain set of network intrusions;

2. The model of decisive rules has been further developed due to the set of reference values and formed by the expert evaluation methods of initialization matrices for conjugated pairs and fuzzy identifiers which allows to formalize the process of forming sets of decisive rules for revealing anomalous state in computer networks expertly;

3. For the first time a method of forming linguistic standards for intrusion detection systems was developed based on the model of base values and the model of reference values, which, due to the use of sets of identifiers of linguistic estimates and identifiers of intervals, the base and derivative matrix of the frequencies of mapping experts' judgments of current states of quantities, as well as the processes of the formation at specified intervals of frequencies of the occurrence of expert assessments and subsets of fuzzy terms, allow us to formalize the procedure for obtaining reference values for the values of given groups of linguistic variables

that characterize under various conditions of anomaly a particular heterogeneous parametric environment;

4.On thebasis of the model of base values, the model of reference values and the model of decisive rules, a technology was developed for detecting anomalous states generated by the actions of an unauthorized part that allows the creation of means for identifying non-signature types of cyberattacks on the basis of an expert approach and generated fuzzy current values;

5. A structural solution for intrusion detection systems has been further developed with the help of the implemented technology for detecting anomalous states due to the fuzzy arithmetic module and subsystems; formation of fuzzy standards of network values; the formation of decisive rules and primary processing which allows by monitoring the activity in the environment to expand the functionality of modern intrusion detection systems.

Research methods are based on theories of fuzziness, sets, decision-making, algorithms, modeling of information processor structures, as well as methods of expert evaluation and soft calculations.

The introduction reveals the urgency, specifies the problems associated with the topic under study. The idea of work, the purpose and tasks of the research, the scientific novelty and practical value of the work, the methods of research are given.

In the first chapter was made an analysis of the methods and means for implementing attacks (intrusions) and was determined that they constitute a fairly wide range which are continuously improved, updated and used to implement unauthorized actions with respect to computer systems and networks. The most common IDSs are mainly focused on the use of statistical methods and neural network approaches.The reliability of the operation of such systems is quite sensitive to insufficient sampling of statistical data, unexpected changes in the environment, errors in the training of systems, unknown attacks (for example, "zero day") and modification of known ones leads to certain intrusion detection difficulties.

The second chapter is devoted to the development of models for detecting anomalous state for IDS. Forbuilding of the model of base values (MBV) a lot of possible intrusion of the model of reference values (MRV) has been introduced. On the basis of the proposed MBV, model of reference values (MRVs) is formed taking into account the chosen MFP. The process of identifying anomalies caused by intrusions on computer systems and networks which requires the determination of the necessary quantities and their properties. model of decisive rules (MDR). For building of a model of decisive rules (MDR), many fuzzy identifiers have been introduced.

The third chapteris devoted to the development of technology for detecting anomalous state and new structural solutions for anomaly detection systems generated by network attacks. The proposed technology is based on the mathematical models developed in the second chapter and the methods of fuzzy logic analyzed in the first section and the determination of the coefficient of importance (CI). It contains eight basic steps that reveal the process of detecting an abnormal state generated by a particular type of cyberattacks.

The fourth chapter is devoted to practical implementations and studies of anomaly detectors in computer networks. On the basis of the proposed algorithmic support and a typical system for detecting anomalies generated by port scanning was developed and carried out an experimental study of a software system for detecting scanning means and an application system for detecting anomalies generated by attacking actions. Also, with concrete examples, the main essence of the work of the system implementing the proposed method is illustrated.A graphical interpretation of the obtained anomalous states for different types of cyber attacks is presented

and the basic experiment was carried out by modelling 1500 intrusions (attacks) on workstations of the Department of Information Technology Security of the National Aviation University.

The experiment showed that the detected cyber attacks in 29.3% of the cases were initiated by the rule SR_{15} = "If $\sim^{t_{VCA}}$ the closest to $\sim^{Y^e}$ entering $\sim^{T^e_{VCA}}$ and $\sim^{t_{NVC}}$ closest to $\sim^{VB^e}$ and one entering in $\sim^{T^e_{NVC}}$, then the level of the anomalous state generated by SCANNING will be LIMITS," and in 38.7% and 32% according to rules SR14 and SR13. On the basis of the results of the verification, it was established that all intrusions (attacks) were detected by different rules and reflect a different degree of confidence of the expert and it was also determined that the implementation of the proposed models and systems adequately reflect the reactions to the simulated actions.

In **conclusion**partthe main results and conclusions of the dissertation work are reflected.

The practical significanceof the work is as follows:

• On the basis of the created models and technology, the laboratory work and lecture material was used in the training process of training specialists in the field of knowledge 1701 - "Information Security". The practical use of the results of the dissertation research is confirmed by the acts of introduction into the educational process of the National Aviation University (Ukraine, Kiev) from 17.02.2017.

•On the basis of the proposed technology for detecting anomalous state, the computer program "Detection of ports based on fuzzy logic" was developed, which allows in an indistinctly weakly structured environment to identify cyber attacks on information systems resources, which made it possible to improve the degree of protection of the information system and optimize the performance indicators of the network protection system, which is confirmed by the act of introduction into the activities of OOO "Sifer BIS" from 03.02.2017.

Approbation of work. The main provisions of the thesis were reported, as well as discussed at the following scientific and technical and scientific-practical conferences:

• International scientific and technical conference "Modern information and telecommunication technologies" (Ukraine, Kiev, 2015);

• II International Scientific and Practical Conference "Information and Telecommunication Technologies: Education, Science, Practice" (Kazakhstan, Almaty, 2015);

• 16th International Conference on Control, Automation and Systems / ICCAS.2016.7832298 Gyeongju, South Korea, 2016

• II and III International scientific and practical conferences "Actual issues of ensuring cybersecurity and information protection" (Ukraine, Kiev, 2016, 2017);

• VI International Scientific and Technical Conference ITSEC (Ukraine, Kiev, 2016);

• "Status and improvement of the security of information and telecommunication systems" (SITS-2016) (Ukraine, Nikolaev-Koblevo 2016).

Publications. The main provisions of the thesis are published in 12 scientific papers, 4articles of which 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; 2 articles are published in publications indexed in the Scopus database; 2 articles are published in scientific journals and collections of scientific papers (Ukraine); 3 articles were published in the collections of international conferences (Ukraine), 1 article was published in the materials of the international conference (Kazakhstan).

Structure and scope of the dissertation. The thesis consists of an introduction, four chapters, general conclusions, applications, a list of used resources and has 165 pages of body text, 41 drawings, 23 tables, 13 pages of applications. The list of literature contains 113 titles and occupies 14 pages. The total workload of 192 pages.

On the topic of the thesis 17 publications were published:

1.Akhmetov B.S. Using of fuzzy sets in intrusion detection systems Akhmetov, A.A. Korchenko, N.K. Zhumangaliyeva // Information of bezpeka. - 2014. - No. 1 (13); №2 (14).- p. 42-55.

2. Using of expert assessment methods in intrusion detection systems. Akhmetov, A.A. Korchenko, S.T. Akhmetova, N.K. Zhumangaliyeva // Information of bezpeka. - 2014. - No. 3 (15); № 4 (16).- p. 34-43.

3. Akhmetov B.S. Analysis of methods of fuzzy sets for the construction of intrusion detection systems. Akhmetov, A.A. Korchenko, N.K. Zhumangaliyeva // "Modern Information and Telecommunication Technologies": Intern. nauch.-teh. Conf. : Mater. of Conf. - K .: GUT, November 17-20, 2015. - p. 38-40.

4. Base models of reference values for intrusion detection systems / B.S. Akhmetov, RBAbdrakhmanov, AAKorchenko, N.K. Zhumangaliyeva // Bulletin of the International Kazakh-Turkish University. A.Yasavi. - 2015. - № 5-6 (97-98). - p. 15-26

5. Analysis of the methods of expert evaluation for intrusion detection systems / B.S. Akhmetov, A.A. Korchenko, S.T. Akhmetova, N.K. Zhumangaliyeva // "Information and telecommunication technologies: education, science, practice": II intern. scientific-practical. Conf. : Works. - Almaty, Kazakhstan, December 3-4, Volume II. - 2015 year. - p. 28-31.

6. Akhmetov B.S. Model of base values for monitoring of the anomalous state of the environment. Akhmetov, A.A. Korchenko, N.K. Zhumangaliyeva // News of the National Academy of Sciences of the Republic of Kazakhstan. A series of physics and mathematics. - 2016. - No. 1 (305).- p. 26-33.

7. Akhmetov B.S. A model of decision rules for the detection of anomalies in information systems. Akhmetov, A.A. Korchenko, N.K. Zhumangaliyeva // News of the National Academy of Sciences of the Republic of Kazakhstan. Series-physics and mathematics. - 2016. - No. 4 (308).- p. 91-100.

8. Method of constructing conditional detection expressions for systems of detection of cyber attacks / N.P. Karpinsky, A.A. Korchenko, S.T. Akhmetova, N.K.Жумангалиева /Актуальніпитаннязабезпеченнякібербезпекитазахистуінформації: II міжнар. Sciences-practical. Conf. :Thesi add. - Київ, 24-27 лютого 2016 року - With.65-69.

9. Akhmetov B.S. Technology for detecting an anomalous state for intrusion detection systems. Akhmetov, A.A. Korchenko, N.K. Zhumangaliyeva // Vestnik of the KAFU. A series of mathematics, mechanics, computer science. - 2016. - No. 1 (88). - P. 106-113

10. Akhmetov Bakhytzhan, KorchenkoAnna, AkhmetovaSanzira, ZhumangalievaNazym. Improved method for the formation of linguistic and ards for intrusion detection systems.Journal of Theoretical and Applied Information Technology, 2016.Vol.87. №2. - Pp. 221-232.

11. Korchenko A.A. The construction of linguistic standards for the detection of sniffing attacks / A.A. Korchenko, N.K. Zhumangaliyeva, P.A. Vikulov // Actualinipitanniyazabezpechennyakiberbezpeki ta zahistuinformatsiї: III міжнар. Sciences-practical. Conf. :Thesi add. - Київ, 22-25 лютого 2017 року - p. 93-97.

12. Akhmetov B., Ivanov A., Alibieva Zh., Mukapil K., Beketova G. Prospects for Multiple Reductions in Test Samples with a Multivariate, Multicriteria, The Neural Network Statistical

Analysis of Biometric Data // Medwell Journals, 2015 Research Journal Applied Scienses 10(12) 2015 956-967

13. Mikolaj Karpinski, Vasyl Martsenyuk, Iryna Gvozdetska, Bakhytzhan Akhmetov, Zhumangalieva Nazym. Estimation Problem for Network Model at State and Measurements Attacks and Information Cost Criterion// 16th International Conference on Control, Automation and Systems / ICCAS.2016.7832298 Gyeongju, South Korea, 2016, pp. 45-50.doi: 10.1109/

14. Aleksandra Kłos-Witkowska; Bakhytzhan Akhmetov; Volodymyr Karpinskyi; Tomasz Gancarczyk. Bovine Serum Albumin stability in the context of biosensors//2016 16th International Conference on Control, Automation and Systems ICCAS)//Year:016//Pages: 976 80, DOI: 10.1109/ICCAS.2016.7832427EEE Conference Publications

15. Akhmetov BS, Korchenko AA Smagulov SK, Zhumangaliyeva N.K. Models of base fluctuation values for monitoring the state of the information system // The State University named after Shakarim in Semey city, 2016 № 2 (74) -C. 87 -91 ISSN 1607-2774

16. Akhmetov BS, Korchenko AA Smagulov SK, Zhumangaliyeva N.K. Basic models of anomaly control of the information system // The State University named after Shakarim of the city of Semey № 1 (77) 2017 C 111-115 ISSN 1607-2774

17. B. Akhmetov, A. Korchenko, J. Kultan, N.Zhumangalieva,. Model decision rules to detect anomalies in Information Systems// Informational Technology Application, Словакия, №1, 2016 126-136 ISSN 13386468