Journal of Theoretical and Applied Information Technology
28th February 2021. Vol.99. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

APPLICATION OF BAYESIAN NETWORKS IN THE DECISION SUPPORT SYSTEM DURING THE ANALYSIS OF CYBER THREATS

[1]AKHMETOV B.S., [2]LAKHNO V.A. , [3]YDYRYSHBAYEVA M.B., [4]YAGALIYEVA B.E., [5]BAIGANOVA A.V., [1]AKHANOVA M.B., [5]TASHIMOVA A.K.

[1]Abay Kazakh National Pedagogical University, Almaty , Kazakhstan
[2]National University of Life and Environmental Sciences of Ukraine,
[3]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[4]Yessenov University, Актау, Kazakhstan
[5]Zhubanov Aktobe regional university

E-mail: [1]bakhytzhan.akhmetov.54@mail.ru, [2]lva964@gmail.com, [3]moldir.ydyryshbaeva@gmail.com, [4]bagdat.yag@gmail.com, [5]altynzer_70@mail.ru, [1]madina13.04@mail.ru, [5]anar_6868@mail.ru

ABSTRACT

The article based on the analysis of methods for constructing models of the attacker and cybernetic threats for information objects (OBI), the effectiveness of using the Bayesian network device in intelligent decision support systems for situations with poorly structured data on the types of threats to the OBI.

Implemented a Bayesian network (BN) for the computational core of the DSS. The network is designed to predict the development of cyber threats to the OBI and it's information and communication system (ICS). An example of the BN "Data Modification in an information system" is considered. The Bayesian network allows to operate on a set of random variables and determine the probability of a cybernetic threat to the ICS under given conditions. To improve the efficiency of attack prediction, the network parameters were trained with the EM algorithm (Expectation-maximization algorithm) based on the available statistical data. Alternative networks are also created based on network structure estimation with three different algorithms. The effectiveness of the developed models was checked using test samples that were not previously used in the BN training process. The results obtained indicate the feasibility of using EM and PC (Peter-Clark – PC algorithm) algorithms to obtain a high-quality result of recognizing cybernetic threats for the ICS of informatization objects.

Keywords: *Decision Support System, Modeling And Forecasting, Cyber Threat, Bayesian Networks*

1. INTRODUCTION

Designing modern information security systems (ISS) and creating their security policies requires providing them with accurate source data. An important stage preceding the analysis of information and cyber security risks (IS and CS, respectively), as a key step in building the policy of the ISS, is the creation of a model of violators and threats. The correctness of the built threat model depends on the decisions that will be made at the next stages, as well as the stability of the created ISS to malicious attacks. It should be noted that as the complexity of attack scenarios aimed at information objects (OBI) increases, making decisions in the field of information security and security becomes more and more difficult. Moreover, to solve it, analysts in the field of information security and design often have to be content with rather weakly structured data for analyzing new threats that are little described in the specialized literature or are generally encountered for the first time. As an example of this situation, we can recall the cases of attacks on the components of the so-called Smart City, which began to develop rapidly from the beginning of the 2000s of the XXI century. Software and hardware solutions integrated into Smart City immediately after their appearance in the Smart City infrastructure became objects of cyber attacks, primarily network attacks, by computer attackers [1]. Similar examples can be found in other industries: medicine [2]; industry [3]; banking [4] , etc. In the course of targeted attacks, hackers often use unique malicious programs and methods of penetrating the OBI. It is possible to counter the constant increase in the complexity of illegitimate

impacts on the OBI, in particular, using systems for intelligent recognition of anomalies and cyber attacks, which have integrated modules of decision support systems (DSS) into the structure of information security systems. The DSS architecture usually includes a data mining system (DMS). The inclusion of the DSS in the complexes of ISS for the OBI allows to identify regularities of the dynamics of the state protection of OBI, combining knowledge and experience of decision-making by experts and the computational potential of the DSS.

In complex situations of guaranteed provision of information security and CS OBI, the decision-making process will take place under the condition of active interaction of the ISS with experts. Note that, without computer technology, this work is very time-consuming. Even the initial problem of designing modern complex ISS can be attributed to poorly formalized problems with incomplete information. Similar tasks include situations related to the recognition of long-term targeted cyber attacks that are not accompanied by obvious signs.

Therefore, the subject of the research devoted to the development of models for DSS in poorly structured and difficult to formalize tasks, as well as to improve the quality of estimates of the probability of implementing malicious threats for the OBI, seems relevant.

2. REVIEW AND ANALYSIS OF LITERATURE

The increasing number of cyber attacks on the OBI in recent years has aroused interest in the development of effective ISS [1, 2]. A promising and fairly new area of research in this area has been the development of methods, models and software complexes of the DSS [5] and expert systems (ES) [6] in the field of information security and CS.

In [7, 8] are considered Data Mining technologies in the problems of IS and CS. The emphasis in these studies is placed on the task of identifying patterns of evolution of the situation that is associated with the provision CS of the OBI. The considered works had no practical implementation, in the form of software packages.

In [9, 10] are analyzed the methodology of intelligent modeling in the problems CS of the OBI. The methodology proposed by the authors is intended for analysis and decision-making in insufficiently structured information security situations. However, these studies are not brought to hardware or software implementation.

Complex to analyze and support decision-making in CS tasks are poorly formalized and structured tasks of ensuring CS when new classes of attacks appear [11]. In this case, the state parameters CS of the OBI can be represented by qualitative indicators [12]. The latter is not always appropriate.

According to the authors [13, 14], analysis of the degree of security of the OBI and the development of plans to counter targeted cyber attacks should be preceded by the stage of identifying the main threats. The authors point out that it is problematic to solve such a problem qualitatively without appropriate DSS. In particular, the DSS is necessary in order to describe the not always formalized links between threats and vulnerabilities in the conceptual and functional aspects IS and CS of the OBI.

Today, a number of empirical and formal methods have been developed that solve the problem of synthesis (construction) of ISS. The logical-probabilistic approach [12], game theory [15], mathematical programming methods [14], and other approaches [16-18] are used.

Analysis of the current state of research in the field of IS indicates that there are shortcomings associated, first of all, with the effective use of accumulated statistical and other data together with subjective expert assessments and developed mathematical models. However, there are still no approaches that combine the advantages of each group of methods. In practice, either expert-based methods (the Saati hierarchy analysis method, the «Delphi» method of consistent estimates, and the preference criterion) or statistical methods (time series analysis) are used to analyze the probability of CS threats to the OBI. Each group of methods has its own advantages, but for complex OBI and their complex ISS, the probability of expert error increases, while statistical data may be unsuitable for use due to its incompleteness or lack of structure.

In [19, 20], it was shown that these aspects of the construction of ISS can be taken into account in the approach based on the applied Bayesian networks (further BN). Compared to existing data analysis methods, they provide a clear and intuitive explanation of their findings. Bayesian networks also involve logical interpretation and modification of the structure of relations between variables of the problem. Additionally, it is possible to use the empirical frequency of occurrence of different values of variables as input data. You can also take into account the subjective assessments of experts and theoretical ideas about the mathematical probabilities of certain consequences of cyber attacks with a priori information.

The representation of the BN in the form of a graph makes it a convenient tool for solving the problem of assessing the probability of

implementing cybernetic threats, for example, for the ICS of OBI.

Thus, taking into account the controversy in the considered works, it is obvious that it is necessary to continue research on practical solutions for DSS in the field CS of the OBI. Such research, in particular, should be aimed at solving complex and atypical problems of information security (IS), for example, in the implementation of multi-stage targeted cyber attacks.

3. THE PURPOSE AND OBJECTIVES OF THE STUDY

The aim of this work is to improve the quality of estimates of the probability of implementing malicious threats for OBI by developing an approach based on the use of Bayesian networks.

To achieve this goal, you must complete the following tasks:

– perform analysis of variables related to cybernetic threats to the ICS of OBI;

– build a probabilistic model in the form of a Bayesian network to estimate the probability of a cybernetic threat to the OBI;

– perform computational experiments to study the adequacy of the constructed probabilistic models, which will allow integrating these models at the next stages of research into the computational core of the DSS and develop a model for describing meta knowledge for the DSS about weakly structured situations related to the cyber security of the OBI.

4. MODELS AND METHODS

The computational core of the DSS is based on probabilistic models that can describe processes in conditions where data is poorly structured or insufficient for, for example, statistical analysis. Tasks that can be solved through the application of probabilistic models obviously have to use the procedure of probabilistic inference. Various processes that take place in the ICS of OBI generate their own data sequences. Accordingly, these data sequences should be reflected in the description of each process.

For example, the process of invading the ICS will manifest itself in changing the sequences of network traffic, system calls to the operating system kernel, and user behavior profiles.

Building a BN begins with defining the variables $a_i \in V$, that are involved in solving the problem. Here, $a_i, V -$ respectively, the variable and vertex of a directed acyclic graph. Among the set of all variables, select the target values and describe their possible values. In the next step, based on experience and available information, we will use experts to determine the a priori probabilities of the values of these variables $p(a_i)$. Then we describe the cause-and-effect relationships between the variables as directed edges of the graph $\{a_i, a_j\} \in E$, placing the variables in the nodes of the problem. The state of all parent variables for a_i vertex is denoted by $pa(a_i)$. For a set of graph variables, the Markov condition is met, according to which each variable a_i in the graph does not depend on all variables, except the parent ones $pa(a_i)$.

The target variables in the BN $x_k \in V$ under consideration will be potential threats to which the ICS may be vulnerable. All variables in the model are discrete. Each variable (or threat) can take one of five values, each of which corresponds to the probability of its implementation: *trivial, low, medium, high, critical* (respectively, insignificant, low, medium, high, critical).

The other variables in the BN are characteristics that will allow you to identify the threat and determine its probability. These variables were divided into categories that classify IS (CS) threats or describe different types of computer attackers:

1. The purpose of unauthorized access (UAA) to the ICS of OBI. Violation of confidentiality (*p_confidentiality*), integrity (*p_integrity*), or availability (*p_availability*) of OBI information resources is considered.
2. The position of the source UAA (*n_network*). Three source categories are accepted: intra-segment, inter-segment, and external.
3. The need for authentication to implement the threat (*a_ authentication*).
4. Attacker qualification (*a_qualification*): high, medium, low.

Having defined all the BN variables, it is necessary to describe the cause-and-effect relationships between them. It is necessary to determine which characteristics affect which threats, as well as the relationship between the characteristics, if any.

A table of conditional probabilities $p(y_1 | b_l, ..., b_i, ..., b_n)$ is assigned to each

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

descendant variable y_l with parent variables $b_l,...,b_i,...,b_n$. If the variable has no ancestors, then an unconditional probability is used instead of a conditional probability $p(y_1)$.

Both target variables x_k and characteristic variables a_i can act as descendants and parent variables, depending on the BN topology.

After determining all the variables and the cause-and-effect relationships between them (figure 1), it is necessary to determine the probabilities of different values of variables for a set of parent variables. There are a number of methods for determining these probabilities, including: expert (setting probabilities by a qualified specialist); statistical (training the network based on accumulated data about implemented threats); mathematical (determining formal relationships between variables).

When constructing this network, empirical and statistical approaches were used to obtain initial data, but the main method is the statistical method [13]. In this paper, the conditional probability tables were determined through BN training using the expected maximization algorithm [21].

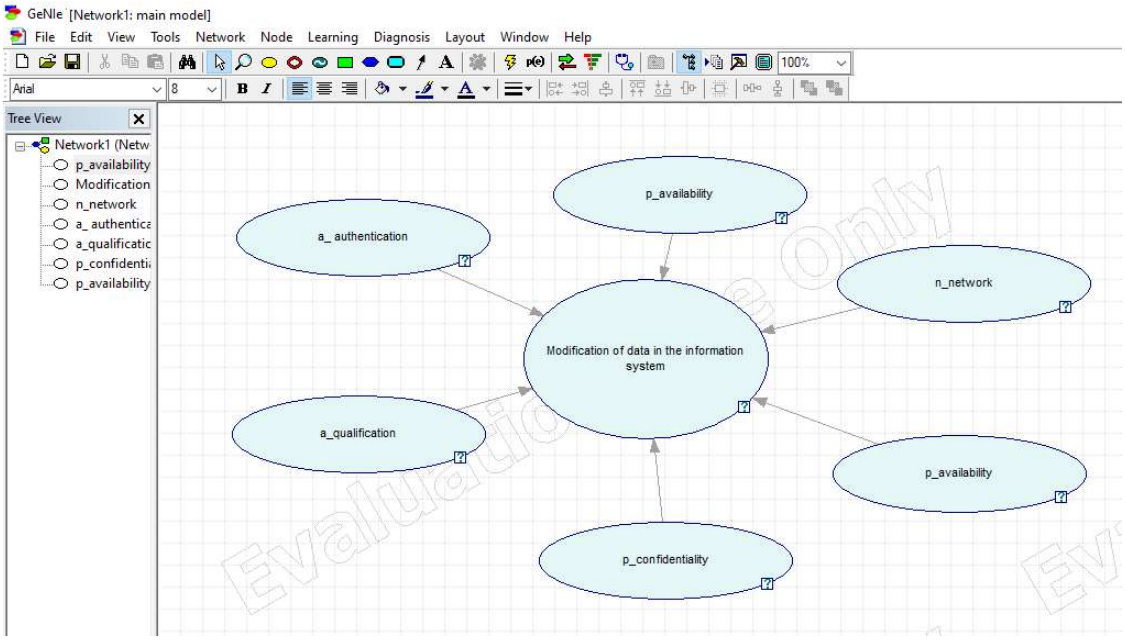


Figure 1: Example BN for the threat "Data modification in the information system" (GeNIe Modeler Editor)

BN training was based on statistical data [17]. Training can be divided into two stages: training network parameters and its structure.

To train the network parameters with the fixed structure used Expectation-maximization (EM) algorithm. The purpose of this algorithm is to clarify the a priori assumptions of the expert regarding the values of the parameters . The problem in this case reduces to the determination of the most probable threat level for ICS - $tr \in TR$ at known m the set of factors $a_1,...,a_n \in A$ that can lead to the realization of this threat. Mathematically, it can be written like this :

$$tr = \arg\max_{TR} P(TR|A_i). \quad (1)$$

EM algorithm is used to find the maximum ratings th reliability parameters of the probabilistic model and provides an opportunity to reach a global extremum. In this case, Bayes' formula (2) is taken again. This makes it possible to solve the search $P(TR|A_i)$ problem by switching to indirect probabilities.

$$P(TR|A_i) = \frac{P(A_i|TR) \cdot P(TR)}{P(A_i)}. \quad (2)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Algorithms for learning the BN structure provide for the search for conditional independence between variables and the selection of the appropriate graph structure.

Table 1 shows the results of network training using the EM algorithm.

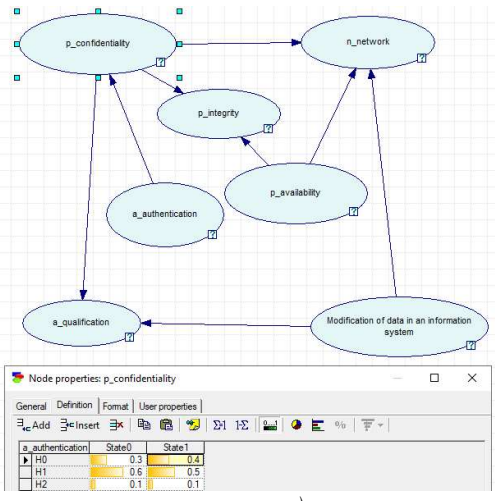
Table 1: Example Of A Part Of The Conditional Probability Table For The Threat «Data Modification In The Information System» (Calculation Using The EM Algorithm)

Factors	*p_availability*	**Full**					
	p_integrity	**Full**					
	p_confidentiality	**Full**					
	n_network	**Intersegment**					
	a_authentication	**Is absent**		**Weak**			
	a _ qualification	**Low**	**With Independent user**	**High**	**Low**	**With Independent user**	**High**
Threat level	*trivial*	0.0005 9	0.0005 9	0.025	0.0074	0.0074	0.025
	low	0.0005 9	0.0005 9	0.025	0.0074	0.0074	0.025
	medium	0.0005 9	0.0005 9	0.9	0.0074	0.0074	0.9
	high	0.99 8	0.99 8	0.025	0.97	0.97	0.025
	critical	0.0005 9	0.0005 9	0.025	0.0074	0.0074	0.025

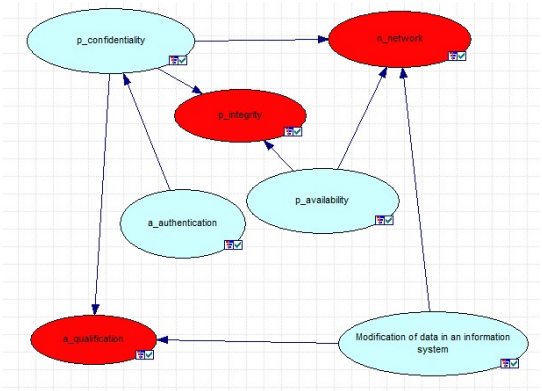
As can be seen from the table, some situations are equally likely. This indicates the incompleteness of statistical data for the computational experiment. The network structure was also trained to predict the probability of threat implementation using the algorithms mentioned above.

5. COMPUTATIONAL EXPERIMENTS

To create a BN, a priori conditional probabilities of occurrence of certain events are set, see Fig. 2 and 3. after that, the network was trained based on statistical data [22]. The data is based on information on the website of the USA national vulnerability Database [22]. The page contains information about current vulnerabilities of the ICS, the conditions of their occurrence and the consequences (threats) that these vulnerabilities can lead to.



a)



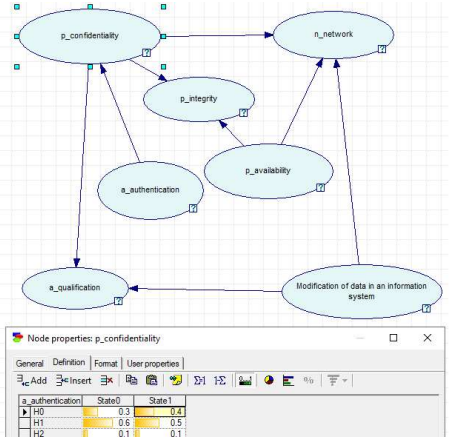
б)

a-network design.
b-visualization of simulation results in the Genie package (v2. 0)

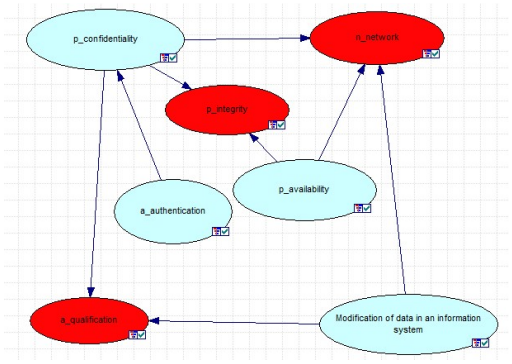
Figure 2: Bayesian search

Journal of Theoretical and Applied Information Technology
28th February 2021. Vol.99. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



a)



b)

a - network design;
b - visualization of simulation results in the Genie package (v 2.0)

Figure 2.1: Bayesian search

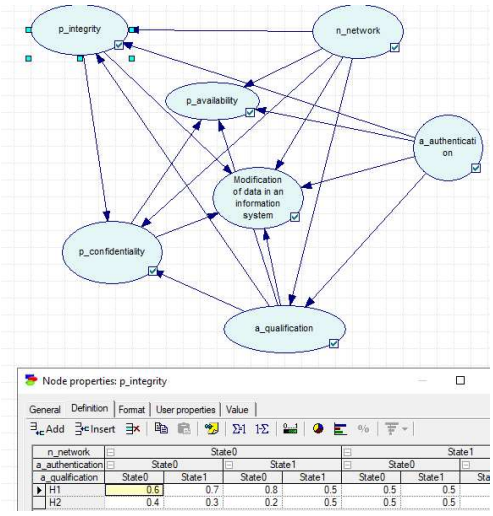
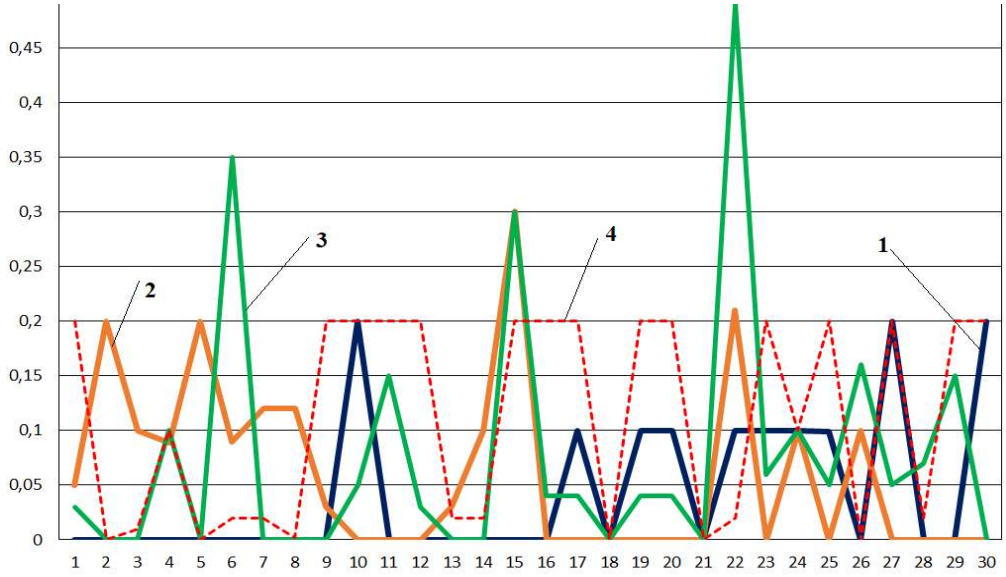


Figure 3: Algorithm of Peter- Clarke - PC

Figures 4 and 5 show the results of modeling the probabilities of correctly determining and interpreting threats using the DSS (errors of the 1st kind, respectively) for networks that were trained: using the PC algorithm (line 1); naive Bayesian classifier (line 2), Bayesian search (line 3); EM algorithm (line 4).

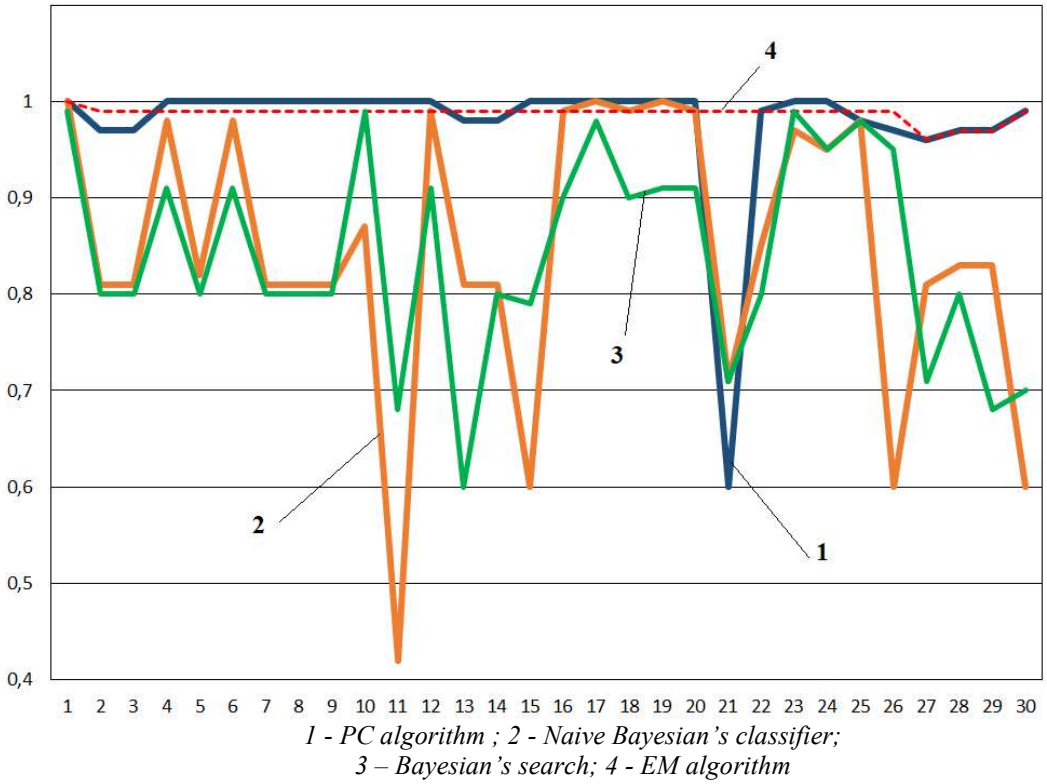
In this article, only the results of modeling and interpretation of the threat – "Data Modification in the information system" - developed by the DSS are considered.

The test sample included 30 records.



1 - PC algorithm; 2 - Naive the Bayesian's classifier;
3 – Bayesian's search; 4 - EM algorithm

Figure 4: The Probability Of Correctly Determining The Error Of The 1-St Kind When Interpreting The Threat To The BN Using The DSS For Networks That Were Trained Using Various Algorithms.



1 - PC algorithm ; 2 - Naive Bayesian's classifier;
3 – Bayesian's search; 4 - EM algorithm

Figure 5: Probability Of Correctly Determining The Threat (2nd Kind Of Error) For BN That Were Trained Using Various Algorithms

6. DISCUSSION OF THE RESULTS OF THE COMPUTATIONAL EXPERIMENT

The obtained BN are shown in Fig. 2 and 3, the results of computational experiments in Fig. 4 and 5. The structure of the network for training which the naive Bayesian classifier was used coincides with Fig. 1, except for the fact that the edges are directed in the opposite direction.

The Genie software (v2.0) was used to build the BN and train them. This made it possible to determine variables and relationships between them, to train the parameters and structure of the network, and to make probabilistic conclusions based on the data obtained.

As can be seen from the generated BN (Fig. 2 and Fig. 3), there is a complex relationship between the variables in comparison with the previously described result (see Fig. 1), which was obtained using the expert method. The resulting network should highlight a number of features. In particular, attacks aimed at violating the integrity of information resources in the ICS OBI also lead to a violation of confidentiality and availability. This point was not reflected in the expert model in figure 1.

It is also worth noting that almost 74-77% of attacks from the local OBI network lead to a violation of availability. At the same time, attacks from a remote network showed results at the level of 45-46%. It is interesting that more "simple" attacks can lead to a larger amount of losses. This is due to the fact that such attacks do not require high training of the attacker.

Further analysis of the simulation results for the obtained BN was carried out in the direction of estimating errors of the 1-st and 2-nd kind. Of the 60 records that were used in the DSS and did not participate in the BN training, the first 30 records are correct data for checking that an existing threat was missed (type 2 error). The remaining 30 entries were used to check for false positives (type 1 error). Figure 4 and figure 5 show errors of the 2-nd and 1-st kind, respectively. The most effective were PC and EM algorithms that correctly determined the

probability of the analyzed threat implementation with more than 94-95% accuracy – data Modification in the information system.

Thus, computational experiments confirm that Bayesian reasoning makes it possible to determine the probable representation for each component in the diagram. Moreover, this representation is given relative to the knowledge and experience of a particular user.

Note that the DSS does not guarantee that the resulting presentation of explanations will meet the information needs of users.

However, as proposed in our research approach to develop models of BN and the corresponding model for cores of DSS will enable users to use information technology and relevant software to support the tasks of explanation for situations in which data on threats and vulnerabilities rather poorly structured or the number is small for proper statistical evaluation.

At the moment, research is ongoing and work is underway to expand the base of Bayesian network models, algorithmize the described models and implement them into the computational core of the DSS.

7. CONCEPTUAL DIAGRAM OF THE INTRUSION DETECTION SYSTEM MODEL WITH INTEGRATED DSS IN ITS ARCHITECTURE BASED ON THE USE OF BAYESIAN NETWORKS

Thus, the computational results performed, as well as taking into account the results of other authors works [7-12], we can say that BN are able to provide a fairly accurate interpretation of anomalies and attacks using DSS. As previously mentioned, integrating the DSS into the intrusion detection system (IDS) architecture can provide a solid Foundation for simplifying the computing core of the IDS. The conceptual scheme of the IDS model with integrated DSS in its architecture based on the use of Bayesian networks is shown in Fig. 6.

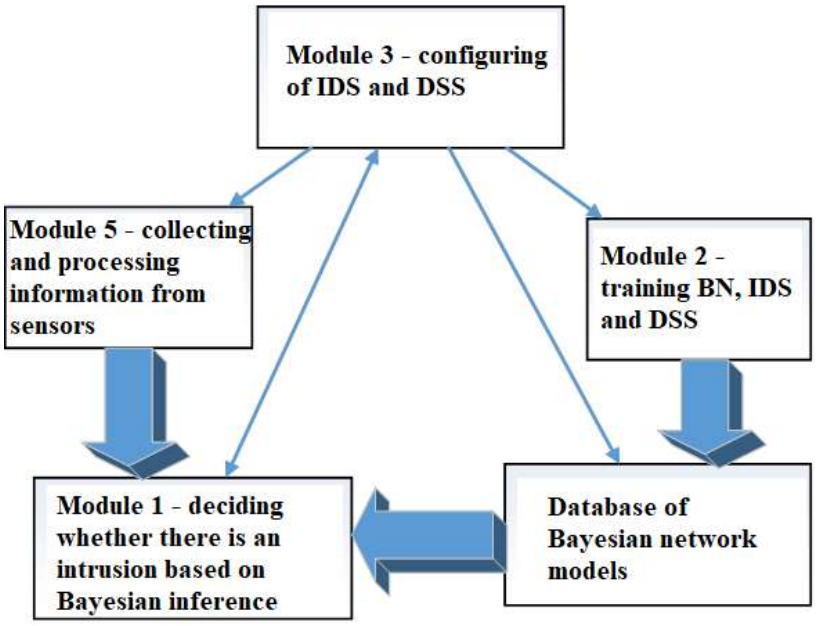


Figure 6: Conceptual Scheme Of The Intrusion Detection System Model With Integrated DSS In Its Architecture Based On The Use Of Bayesian Networks

The architecture is a modular structure. A brief description of the tasks solved by each of the modules is provided below.

Module 1 - deciding whether there is an intrusion based on Bayesian inference. Data is collected from sensors that record the properties of network sessions in the IDS.

Module 2 - designed for training BN and DSS in General. The choice of the effectiveness of the training criterion is described in more detail in [23].

Module 3 - configuration of IDS and DSS. It is intended for adaptive selection of algorithms for training IDS and DSS [23].

Module 4 - contains a database with Bayesian network models for various classes of attacks on the OBI ICS.

Module 5 - collection and processing of information from sensors located in key ICS nodes

8. THANKS

The research was carried out within the framework of grant funding for the AP05132723 project "Development of adaptive expert systems in the field of cybersecurity of critical information objects" (Republic of Kazakhstan). The authors Express their gratitude to the team of project participants for their assistance in preparing and processing experimental data.

9. CONCLUSIONS

Based on the analysis of methods for constructing models of the attacker and cybernetic threats to the object of Informatization, the effectiveness of using the Bayesian network apparatus in decision support systems for situations with poorly structured data on the types of threats to the OBI is justified.

A Bayesian network was developed for the computing core of the DSS in the course of predicting threats to the OBI and their information and communication system (ICS). The Bayesian network allows you to operate on a set of random variables and determine the probability of a cyber threat under given conditions. To improve the effectiveness of attack prediction, the network parameters were trained with an EM algorithm based on the available statistical data. Alternative networks are also created based on network structure estimation with three different algorithms.

The effectiveness of the developed models was tested on test samples that were not previously used in training. The results obtained indicate the feasibility of using the EM algorithm to obtain a high-quality result for recognizing cybernetic threats to the ICS.

Further development of the work provides for the expansion of the model by introducing additional criteria and factors that affect the occurrence of cyber threats to the OBI.

REFERENCES:

[1] Al Hadidi, M., Ibrahim, Y. K., Lakhno, V., Korchenko, A., Tereshchuk, A., & Pereverzev, A. Intelligent systems for monitoring and recognition of cyber attacks on information and communication systems of transport. *International Review on Computers and Software*, *11*(12), 2016, pp. 1167-1177.

[2] Meng, W., Li, W., Wang, Y., & Au, M. H. Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. *Future Generation Computer Systems*, *108*, 2020, pp. 1258-1266.

[3] Urbina, D. I., Giraldo, J. A., Cardenas, A. A., Tippenhauer, N. O., Valente, J., Faisal, M., ... & Sandberg, H. Limiting the impact of stealthy attacks on industrial control systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, October, 2016* pp. 1092-1105.

[4] Lekha, K. C., & Prakasam, S. Data mining techniques in detecting and predicting cyber crimes in banking sector. In *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS),* August, 2017, IEEE, pp. 1639-1643.

[5] Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. Decision support approaches for cyber security investment, Decision Support Systems, Vol. 86, 2016, pp. 13-23.

[6] Gamal, M.M., Hasan, B., Hegazy, A.F. A Security Analysis Framework Powered by an Expert System, International Journal of Computer Science and Security (IJCSS), Vol. 4, No. 6, 2011, pp. 505–527.

[7] Dua S., Du, X. Data Mining and Machine Learning in Cybersecurity, CRC press, 2016, p. 225.

[8] Buczak, A. L., Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Communications Surveys & Tutorials, Vol. 18, Iss. 2, 2016, pp. 1153 – 1176.

[9] Larionov, I. P., Khorev, P.B. Problemy sozdaniya i osnovnye zadachi ekspertnoy sistemy podderzhki proektirovaniya kompleksnoy sistemy zashchity informatsii, Internet-zhurnal NAUKOVYEDYENIYE», 2016, Tom 8, №2. available at: http://naukovedenie.ru/PDF/117TVN216.pdf. DOI: 10.15862/117TVN216

[10] Ben–Asher, N., Gonzalez, C. Effects of cyber security knowledge on attack detection, Computers in Human Behavior, Vol. 48, 2015, pp. 51–61.

[11] Goztepe, K. Designing Fuzzy Rule Based Expert System for Cyber Security, International Journal of Information Security Science, Vol. 1, No 1, 2012, pp.13–19.

[12] Gamal, M.M., Hasan, B., Hegazy, A.F. A Security Analysis Framework Powered by an

Expert System, International Journal of Computer Science and Security (IJCSS), Vol. 4, No. 6, 2011, pp. 505–527.

[13] Li-Yun Chang, Zne-Jung Lee. Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system, International Conference on Fuzzy Theory and Its Applications (iFUZZY) , 2013, pp. 346 – 351.

phase issues, Soft Computing and Intelligent Systems (SCIS), Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), 2014, pp. 896 – 900.

[15] Akhmetov, B. B., Lakhno, V. A., Akhmetov, B. S., & Malyukov, V. P. The choice of protection strategies during the bilinear quality game on cyber security financing. *Bulletin of The National Academy of Sciences of the Republic of Kazakhstan*, (3), 2018, pp. 6-14.

[16] Pan, S., Morris, T., Adhikari, U. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems, IEEE Transactions on Smart Grid, Vol. 6, Iss. 6, P. 3104 – 3113.

[17] Lakhno, V., Kazmirchuk, S., Kovalenko, Y., Myrutenko, L., Zhmurko, T. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features, Eastern-European Journal of Enterprise Technologies, No 3/9 (81), 2016, pp. 30–38.

[18] Louvieris, P., Clewley, N., Liu, X. Effects-based feature identification for network intrusion detection. Neurocomputing, Vol. 121, Iss. 9, 2015, pp. 265–273.

[19] Xie, P., Li, J. H., Ou, X., Liu, P., & Levy, R. Using Bayesian networks for cyber security analysis. In *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, June, 2010, pp. 211-220, IEEE.

[20] Shin, J., Son, H., & Heo, G. Development of a cyber security risk model using Bayesian networks. *Reliability Engineering & System Safety*, *134*, 2015, pp. 208–217.

[21] David Heckerman. A Tutorial on Learning With Bayesian Networks // Tecnical Report. – Redmond: Microsoft Research. – 1995. – 58 p.

[22] US National Vulnerability Database - https://nvd.nist.gov/

[23] Lakhno, V., Zaitsev, S., Tkach, Y., Petrenko, T. Adaptive expert systems development for cyber attacks recognition in information educational systems on the basis of signs' clustering, Advances in Intelligent Systems and Computing, Vol 754, 2019, pp. 673-682.

[14] Kanatov, M., Atymtayeva, L., Yagaliyeva, B. Expert systems for information security management and audit, Implementation