INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2020, VOL. 66, NO. 3, PP. 493-498
Manuscript received February 24, 2020; revised July, 2020. DOI: 10.24425/ijet.2020.134004

# Optimization Model of Adaptive Decision Taking Support System for Distributed Systems Cyber Security Facilities Placement

Aliya Kalizhanova, Sultan Akhmetov, Valery Lakhno, Waldemar Wojcik, and Gulnaz Nabiyeva

***Abstract*—An article herein presents an optimization model, designated for computational core of decision-taking support system (DTSS). DTSS is necessary for system analysis and search of optimal versions for cyber security facilities placement and information protection of an enterprise or organization distributed computational network (DCN). DTSS and a model allow automize the analysis of information protection and cyber security systems in different versions. It is possible to consider, how separate elements, influence at DCN protection factors and their combinations. Offered model, in distinction from existing, has allowed implementing both the principles of information protection equivalency to a concrete threat and a system complex approach to forming a highly effective protection system for DCN. Hereby we have presented the outcomes of computational experiments on selecting the rational program algorithm of implementing the developed optimization model. It has been offered to use genetic algorithm modification (GAM). Based on the offered model, there has been implemented the module for adaptive DTSS. DTSS module might be applied upon designing protected DCN, based on preset architecture and available sets of information protection and cyber security systems in the network.**

***Keywords*—distributed computational network, cyber security, optimization, protection facilities placement, decision taking support system**

## I. Introduction

RECENT years statistical researches [1, 2] fix a sustainable tendency to growing the share of information technologies application to different areas of human activity. Today the main IT development trend becomes the transfer to distributed computational networks (DCN). And herein the distributed computational networks application variants might be completely different, starting from constructing virtual organizations [3] and completing with cloud computations [4].

Let's note, that the distributed computational networks specifics is in the fact, that their hardware-software resources [4, 5] and internal structure are supported dynamically. It gives the possibility to modify constantly and expand the distributed computational network structure and configuration at the expense of new IT implementation. But whatever the distributed computational networks' technical advantages are, in conditions of ever-growing destructive impacts number from computer trespassers, the problem of such systems cyber security maintenance is still actual.

As it is shown with researches in the distributed computational networks cyber security maintenance area [6, 7], there are no universal methods and models, which can provide the information protection services specialists with tools for solving the problems of information protection facilities placement optimization. Particularly it is noticed upon scales growth or changes of initially prescribed network architecture. And it is connected, first of all, with constantly changing cyber safety landscape. Thus, the actual scientific-technical task remains the necessity to develop such approach and tools for distributed computational systems cyber security maintenance, which can consider their peculiarities:

1. Necessity of system analysis of cyber threats list, which can be supplemented with new components and occur for each distributed computational network's element, for instance, network equipment (multiplexors, rooters, etc.), distributed computational system's servers, users' local computers, mobile gadgets, etc.;

2. Information protection and cyber security systems selection possibilities, proceeding from available and potential different classes cyber threats;

3. Possibilities of computer support (for example, at the expense of expert or DTSS during the process of distributed computational networks cyber security architectures designing. It is the DTSS, which gives a chance to consider the structure of a certain distributed network. Therefore, there is provided the system approach and versatility of protected distributed computational networks construction mechanisms;

4. Need in integration the paragraphs (1-3) into methods and corresponding models for DTSS. DTSS might be applied in the course of information protection and cyber security systems placement optimization for concrete distributed computational networks. As well, there is possible models adapting and scaling, along with increasing the distributed computational networks sizes and appearing the new cyber threats classes. DTSS will be able, according to user's request, for instance, the distributed computational networks information security administrator, «to give» advices and recommendations on behavior at protection object, being analyzed. At that, the recommendations thereof shall be at the level of an experienced specialist, cyber security and information protection systems designer.

In connection with the above said, we can conclude, that the researches on models, methods and informational technologies, for instance, DTSS on optimizing the

Aliya Kalizhanova, Sultan Akhmetov are with Al-Farabi Kazakh National University and with Almaty University of Power Engineering and Telecommunications, Kazakhstan (kalizhanova_aliya@mail.ru, as_sultan @mail.ru)

Valery Lakhno are with National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine (e-mail: Valss21@ukr.net).

Waldemar Wojcik are with Lublin Technical University, Lublin, Poland (waldemar.wojcik@pollub.pl).

Gulnaz Nabiyeva are with Sanzhar Asfendiyarov Kazakh national medical University, Kazakhstan (gulnaz_nc@mail.ru).

information protection and cyber security systems placement for the distributed computational network is an acute scientific and technical problem. At present any information system's priority quality, and, in particular, distributed computational network is its ability to oppose different cyber threats. Cyber security shall be guaranteed with the mechanisms, including various information protection systems. To reach the most effective protection, there is accepted to use mathematical and cybernetic modeling at the stages of the distributed computational networks design, upgrade and maintenance. These methods allow formalize the distributed computational networks cyber security parameters and optimize selection of the most appropriate information protection system's versions. Special software and DTSS, namely, allow consider works certain conditions from the point of view of protection from cyber attacks at the distributed computational network, being analyzed.

And it should be noted, that in optimization tasks on information protection system versions selection, the researches use most different mathematical apparatuses. For instance, in the work [8] there is investigated the task of upgrading the performance in the process of information system security risks management. To solve the problem above, the authors apply a fuzzy logic apparatus. The apparatus is necessary for grounding the protective measures selection. Fuzzy logic is also applied to in the work [9]. Hereby the authors consider a modified method of fuzzy programming and propose the algorithm, which will allow selecting the optimal structures for information complex, consisting of level set. Unfortunately, the authors of the works [8, 9] have not represented the data on practical usage of proposed models.

*Aim of the article* – developing the mathematical model for the system of decision taking support in the process of information protection system placement optimization, which allows forming the cyber safety system proceeding from the list of both actual and new cyber threats for distributed systems.

To reach the set aim it is necessary to solve the following tasks, linked with development and approbation:

- models for solving the tasks on information protection system placement optimization in the distributed computational networks;
- DTSS module in the process of information protection system placement optimization in the distributed computational network.

## II. Methods and Models

Statement of the problem. Distributed computational networks infrastructure of an enterprise or organization from the point of view of cyber safety maintenance and information protection is given on the Figure 1. On default, in the system modules there installed the standard information protection systems: antiviruses; security firewalls; facilities of: 1) cryptographic information protection; 2) access isolation; 3) integrity control; 4) authentication, etc. Clearly, for a certain distributed computational networks the list might be supplemented due to sufficiency lack or shortened due to excessiveness.

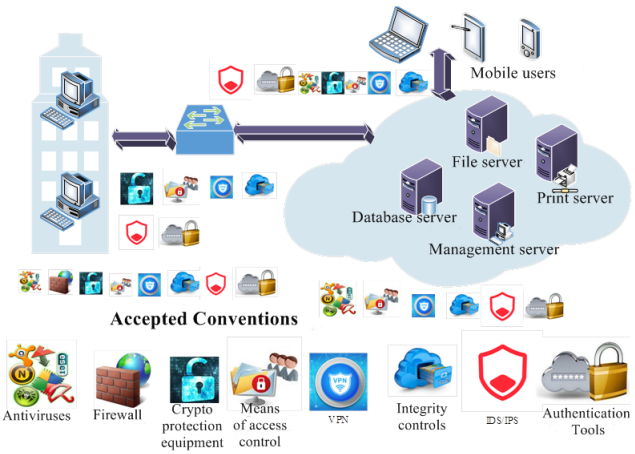


Fig.1. Infrastructure of enterprise or organization distributed computational network in the context of cyber safety maintenance and information protection

Diagram for solving the optimization task of locating the information protection system in the distributed computational network is shown on the Figure 2.

As the initial data there accepted:

- classes set of information protection system for the distributed computational networks;
- modules types of the distributed computational networks;
- types of cyber threats to distributed computational networks;
- others.

Statement of optimization task on information protection system placement, in general, we will formulate as following. There is $P$ – number of classes, modules/points, in which it is necessary to locate the information protection system, see Figure 1, 2. For instance, such points are – servers (storage of database, applications, stamps, etc.); working stations; network equipment (multiplexors, routers).

Denoted classes might be expanded with other elements of the distributed computational networks dependent on specifics of an enterprise or organization business processes. It is obvious, that the network elements classes have own characteristics. Those characteristics can be imposed the limitations. For example, those can be the limitations on functional parameters or cost. Or a feature may have purely informative nature. For instance, informative characteristics is the name (brand) of antivirus software or multiplexor producer. As well, as limitations upon concrete optimization task statement we can use: 1) working memory volume of information protection system elements and cyber safety; 2) sizes of routers tables, etc.

It is necessary to define, by means of the model, which, from potentially possible counter measures on opposing to cyber threats and cyberattacks at the distributed computational networks will be maximum effective according to different criteria, for example, such as:

1) damage minimization from cyber threat likely implementation;
2) cost minimization on countermeasures along the distributed computational networks modules;
3) others.

*Optimization models of minimizing the damage from probable cyber threats implementation and expenses on*

*countermeasures along the distributed computational network modules*

Solution of the problem on searching the optimal strategies for forming the cyber safety for distributed computational networks and locating the components of information protection system and cyber safety corresponding classes along the modules can be executed proceeding from the need to define completely the network safety efficient architecture. That is,

$$Ef = \sum_{i=1}^{P} \sum_{j=1}^{N} \sum_{d \in N_j} e_{ijd} \cdot x_{ijd} \rightarrow \max, \quad (1)$$

where $P-$ number of distributed computational networks modules classes;

$N-$ number of information protection system classes (or cyber safety);

$d_j-$ information protection system (or cyber safety) from class $j$;

$i-$module class (point), for example, server or working station;

$e_{ijd}-$initial performance of information protection system (cyber safety), for instance, percentage of viruses detection for antivirus software;

$x_{ijd}-$fact of fixation of availability in DTSS of the information protection system $d$, which belongs to the class $j$ and which belongs to parent class $i$ of the node, being analyzed;

$N_j-$number of information protection systems in the class $j$.

In the course of the task solution there is traced the observance of the following conditions and general limitations.

General limitation:

$$\forall \psi_{l_1}^{\Psi_n}, \sum_{i=1}^{P} \sum_{j \in N} \sum_{d \in N_j} cnd_{jdl} \cdot x_{ijd} \le \psi_l, \quad (2)$$

where $\psi_l-$general limitation elements set $\Psi = \{\psi_l, l = 1,..., \Psi_n\}$, where $\Psi_n-$ number of general limitations; $cnd_{jdl}-$ index of information protection system according to general limitation $l$.

It is accepted, that general limitations are the factors, for which it is important to control cumulative value magnitude. For instance, such limitations can be: the cost of information protection system, in whole, for the distributed computational network, not for a separate module, see Figure 2. Local limitations:

$$\forall i_1^P, l_1^{LRN} \sum_{j=1}^{N} \sum_{d \in N_j} cnd_{ijdl} \cdot x_{ijd} \le lr_{il}; j \in N, d \in j, \quad (3)$$

where $LR = \{lr_l, l = 1,..., LRN\}$, where $LRN-$ number of local limitations; $lr_{li}-$ local limitation $lr_l$ on the node $i$; $cnd_{ijl}-$ index of information protection system according to local limitation $l$.

In distinction from general, the local limitations should not be computed as aggregate data. It relates to the fact, that local limitations belong only to distributed computational network definite node.

It is accepted, that one and the same information protection system cannot be located more than once in one class point. And, indeed, there is no sense to locate, for instance, two antivirus programs on one working station. That is, the working station under considered task statement has been described as a point of the distributed computational network. That is $\forall x_{ijd} \le 1; i \in P; j \in N; d \in j$.

In the process of developing the adaptive DTSS and searching the definite algorithms for solving an optimization task on selecting countermeasures for the distributed computational network protection one cannot account only one criterion. It is connected with the fact, that in the situation, when it is not possible to find compromise solution, the distributed computational networks cyber safety system developers can face a condition, when a cyber safety system will be cheap, but not efficient. Or, vice versa, the system will be highly effective, but extremely cost-based, and at the same time, extremely demanding to the distributed computational network's hardware resources. The last circumstance, eventually, brings to performance degradation. Consequently, complete solution of the task, having been formulated in the article, might be obtained only in case of using the multicriteria optimization.

In the frame of the article we will restrict ourselves with only two, in our opinion, paramount criteria, which the developers of the distributed computational network shall be governed with: criterion – minimization of the damage from cyber threats implementation at the distributed computational networks; criterion – expenses minimization on information protection system for the distributed computational network in whole. Criterion 1 can be formulated as:

$$vc1 = PD \rightarrow \min, \quad (4)$$

where $vc_1-$ vector criterion 1;

$PD-$ potential damage to the distributed computational networks due to cyberattacks.

Criterion 2 ($vc2 = vc21 + vc21$) includes two sub criteria, which formalized as follows:

$$vc21 = \sum_{i=1}^{NS} \sum_{j=1}^{PC} \sum_{d=1}^{CT} IM_{ijd} \rightarrow \min, \quad (5)$$

$$vc22 = \sum_{i=1}^{NS} \sum_{j=1}^{PC} \sum_{d=1}^{CT} UM_{ijd} \rightarrow \min, \quad (6)$$

where $vc_{21}, vc_{22}-$ vector sub criteria;

$NC-$ number of distributed computational networks modules;

$PC-$ number of information protection system or cyber safety classes;

$CT-$ amount of information protection system or cyber safety facilities, belonging to one class, for instance, number of antiviruses programs, being considered, etc.;

$IM_{ijd}$ – index of information protection system $d$ from class $j$ according to local resource expenditure at the node $i$;

$UM_{ijd}$ – index of information protection system $d$ from class $j$ according to general resources expenditure (for example, financing, operative memory, etc.) at the module $i$.

As vector criteria $vc1, vc2$ are normalized and reduced to minimum, in the mathematical core of an adaptive DTSS we summarize them, by means of weight coefficient to generalized form. With that aim, we have used vector criterion curl method [10]. In compliance with the method herein there has been accounted relative significance according to separate optimality criteria. For that purpose, we construct scalar function, which in reference to a vector criterion is a generalized criterion.

Additive and multiplicative optimality criteria are accordingly:

$$F\left(\bar{y}, vc\left(\bar{x}\right)\right) = \sum_{i=1}^{TC} y_i \cdot vc_i\left(\bar{x}\right), \quad F\left(\bar{y}, vc\left(\bar{x}\right)\right) = \prod_{i=1}^{TC} y_i \cdot vc_i\left(\bar{x}\right), \quad (7)$$

where $\bar{x}$, $\bar{y}$ – accordingly, solutions vector and weight coefficients of solutions significance upon selecting the information protection system for the distributed computational network module;

$TC$ – criteria amount for assessing, for example, with the help of experts $E$ [11];

$F$ – scalar function;

$i$ – sequence number for the criterion under consideration.

As the selection of information protection system optimal locating variant at the distributed computational networks has criteria absolute values, by means of algorithms, used in DTSS, it is expedient to solve the task as multicriterial one. At that, we have used an additive function and procedure of selecting the weight coefficients through expert questionnaire. The solution of the task thereof is discussed thoroughly in the article [11].

Expert assessment lies in the fact, that subsequent to filling in the questionnaires by the experts with indications of information protection system characteristics, there is drawn up the matrix of experts' individual assessments, concerning the accepted criteria, see Table I.

In [11] and in our adaptive DTSS the weight coefficients have been taken into account by the experts upon designing the cyber safety system for the distributed computational networks, based on definite module demands. As well, we analyze, general possibilities and needs of the distributed computational network, proceeding from its specifics.

TABLE I
EXPERTS ASSESSMENT

| | Experts ( $E$ ) | | | |
|---|---|---|---|---|
| Criteria | $E1$ | $E2$ | … | $EEN$ |
| $vc1$ | $vci11$ | $vci12$ | … | $vci1EN$ |
| $vc21$ | $vci211$ | $vci212$ | … | $vci21EN$ |
| $vc22$ | $vci221$ | $vci222$ | … | $vci22EN$ |

In the process of solving the optimization task, as «backpack» there are points of information protection system placement. Those are servers, working stations, multiplexors, routers, etc. As the objects, which are in backpacks, there are antivirus software, firewalls, etc. Then the task, in the context of the cyber safety maintenance is formulated as follows: it is necessary to locate in the «backpack» as many as possible information protection systems.

It follows: 1) to secure the objects best performance; 2) do not exceed the prescribed limitations, for example on the «backpack».

That is, we have the problem statement with multichoice. The main point of the task with multichoice is in the fact, that all objects are broken down into classes. The classes unite only equivalent objects which are similar as intended. It is obligatory to implement an object selection from every available class. That is, for instance, for the solution, considered with the help of DTSS, it is necessary to select one antivirus program from the class of similar software.

*Design and approbation of decision taking support system module to select countermeasures to secure the distributed computational network protection*

Program implementation of the models, being offered in the article, which implement the task solution on searching the optimal strategies of forming the distributed computational network cyber safety, executed in the language C# in Microsoft Visual Studio 2019, see Figure 3, 4.

Conceptually, there has been implemented the DTSS module, which allows, based on available data on the distributed computational networks architecture and information protection system cyber safety aggregate, automatically fulfill selecting the optimal variant of locating available facilities. At the research's present stage there is a possibility to select from three algorithms: 1) modified genetic [12] (GMA); 2) based on the method of branches and boundaries [13] and 3) «greedy» (taking locally optimal decision at every stage of selecting the information protection system for distributed computational networks, based on the assumption, that final decision is, as well, optimal [13]).

For example, in the frame of «greedy» algorithm implementation there is shown below the fragment of program code, implementing the class objects, see 3 I.

«SUBJECT» CLASS IMPLEMENTATION FOR MULTICHOICE TASK, BEING SOLVED BY MEANS OF «GREEDY ALGORITHM»

```
namespace BackpackTask
{
  class Item
  {
    public string name {get; set;}
    public double efficiency {get; set;}
    public double price {get; set;}
    public Item (string _name, double _ efficiency, double _price)
    {
      name = _name;
      efficiency = _ efficiency;
      price = _price;
  } } }
```

Distributed computational systems classes, for which there is solved the task on information protection system selection optimization.

TABLE III
INFORMATION PROTECTION FACILITIES CLASSES

| Symbols | Name | Criteria (levels) | *CR* | UOM. |
|---|---|---|---|---|
| N1 | Antiviruses | protection from viruses | *CR*11 | % |
| | | absence of false alarms | *CR*12 | % |
| N2 | Security firewalls | protection from external attacks | … | % |
| | | protection from internal attacks | … | % |
| N3 | Data reserve systems | module self-protection or DCN protection from hacking | … | % |
| | | system running speed | … | % |

Further by means of built-in into DTSS the algorithms of solving the task on selecting the object, we define the most appropriate protection facility, which is available in every class. For example, for the class – antivirus software, the result will be as follows, see table III.

TABLE IV
OBJECT SELECTION FROM CLASS

| Name | Values per criteria | | Cost, conventional unit | Parameter complexity | Connectivity coefficient |
|---|---|---|---|---|---|
| Antivirus #1 | *CR*11 | 87 | 15 | Да | 0 |
| | *CR*12 | 98 | | | |
| Antivirus #1 | *CR*11 | 95 | 18 | Да | 0 |
| | *CR*12 | 95 | | | |
| Antivirus #1 | *CR*11 | 98 | 10 | Нет | 0 |
| | *CR*12 | 94 | | | |
| … | … | … | … | … | .. |

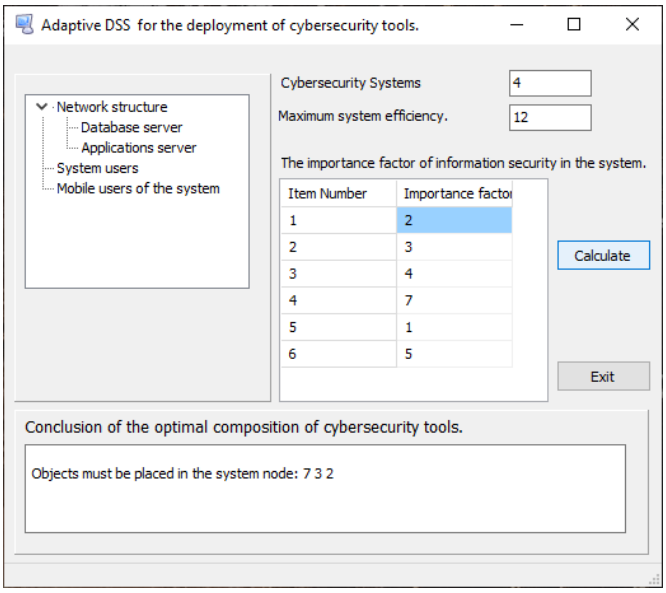


Fig.3. Interface of DTSS module on selecting the countermeasures to secure the distributed computational network protection («greedy»)

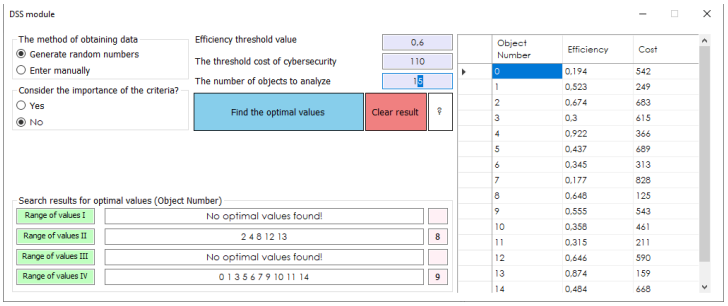


Fig. 4. General view of DTSS module for searching the optimal strategies of forming the distributed computational network cyber safety, using GAM

At the following stages of adaptive DTSS implementation we plan to broaden the list of algorithms, offered for tasks solutions. As well, it will be possible to consider the specifics of a definite distributed computational network. For instance, the distributed computational networks specifics accountancy can be supplemented with introducing into the model such additional criteria as: minimal probability, that computer trespassers (extremal or internal) will reach their aims; minimal level of information loss in the distributed computational networks in the issuance of computer trespassers destructive interference; maximum high probability, that the information protection system and cyber safety will successfully oppose to implementation of all trespassers' aims; minimal value of integral index «cost-risk», etc. Let's note, that some of mentioned criteria are especially significant for critically important information distributed systems, for instance, for banks, traffic management, etc.

## III. COMPUTATIONAL EXPERIMENT

To check the model and adaptive DTSS module adequacy according to the information protection system and cyber safety multicriterial optimal placement in the distributed computational networks nodes, there have been carried out corresponding computational experiments, see Figure 5, 6.

Computational experiments are executed for randomly generated set of information protection systems and distributed computational networks elements. There has been compared the work performance of three algorithms, denoted above.

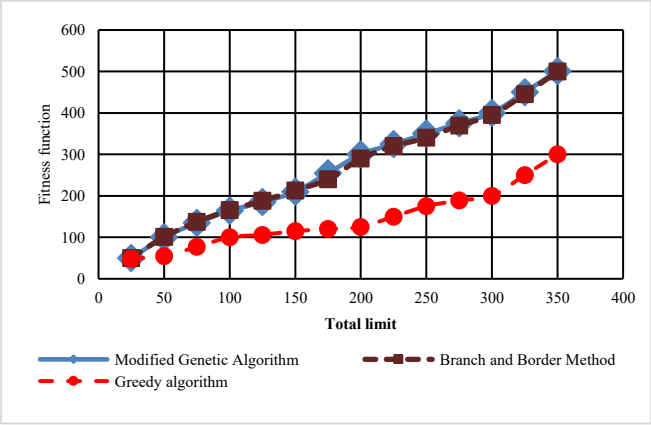


Fig. 5. Outcomes of computational experiments comparing to efficiency of algorithms, used in the adaptive DTSS

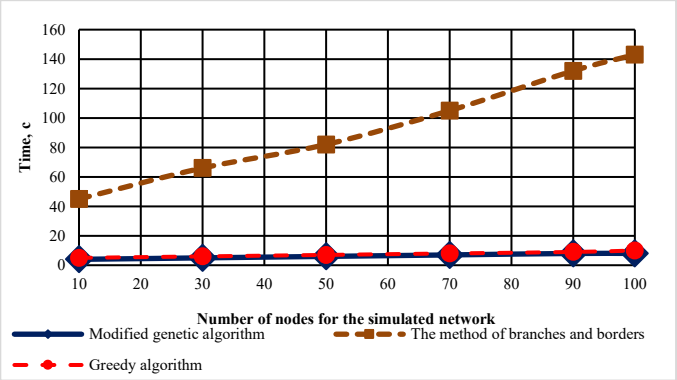


Fig. 6. Outcomes of computational experiments comparing to algorithms operation time

Below there is an analysis of the results.

## IV. Discussion of computational experiments and DTSS testing outcomes

Computational experiments outcomes have shown, that the method of branches and boundaries and GAM demonstrate approximately the same efficiency. At that, maximum error has constituted 3,1-3,3 %.

During the computational experiments there has been stated, that GAM has high enough performance and speed capability. It has been established, that the time, spent for the task solution, using GAM, is approximately 17-25 times less, comparing to indices of branches and boundaries method. That circumstance allows, ultimately, upon adaptive DTSS further development, to choose, particularly, the algorithm thereof.

Certain shortages of the research at present stage of its conducting is the fact, that not all possible task solution algorithms have been analyzed. In particular, while the DTSS module does not allow solve the task, based on modified D. Whitley model [36] or methanoic algorithm [37]. At present there have being conducted the works on including those algorithms into the list of accessible in the adaptive DTSS. It will make DTSS more functional for solving the task under consideration.

## Conclusion

Thus, the work results are:

1. Optimization model, designated for the computational core of the decisions taking support system (DTSS), made in the process of the system analysis of cyber safety and information protection optimal placement variants of the distributed computational networks of an enterprise or organization. In distinction from the existing, this model allows automize the analysis of information protection system and cyber safety different variants. As well, the model permits to consider, how separate factors influence at the protection indices of the distributed computational networks and their combinations. Those factors might be: architecture variants of the distributed computational networks; characteristics of definite equipment of organizations and enterprises distributed computational networks; classes of threats to cyber safety; threats parameters, for instance, potential damage from threat and/or probability of its occurrence; etc. Such approach has allowed implement both equivalency principles of the information protection system to a concrete threat, and system complex approach to forming the highly effective protection system for the distributed computational networks.

2. In the article, there have been fulfilled the computational experiments on selecting the rational program algorithm for the model implementation. As a rational variant there has been offered to use the genetic algorithm modification (GAM). It has been shown, that GAM implementation in the adaptive DTSS module allows accelerate searching optimal versions of cyber safety and information protection facilities locating for the distributed computational networks for more, than 25 times. The given advantage permits to fulfill not only quick search of different variants of hardware-software information protection system and their combinations for distributed computational networks, but also in the future to unite the model, given in the article with the available models and algorithms to detect cyberattacks. Potentially such uniting of models and algorithms will give the possibility to reconstruct quickly the distributed computational networks protection, adapting them to the information about the possibility to implement the new cyber threats, in particular, based on dynamically changing data on the distributed computational networks state.

3. On the basis of the models having been analyzed, there has been developed the model for adaptive DTSS in the process of designing the protected distributed computational networks, using prescribed network architecture and available sets of information protection system and cyber safety.

## References

[1] Avgerou, C., & Walsham, G. (Eds.). (2017). Information technology in context: Studies from the perspective of developing countries: Studies from the perspective of developing countries. Routledge.

[2] Clarkson, A. (2019). Toward effective strategic analysis: new applications of information technology. Routledge.

[3] Grabowski, M., & Roberts, K. H. (2019). Reliability seeking virtual organizations: Challenges for high reliability organizations and resilience engineering. Safety science, 117, 512-522.

[4] Sabi, H. M., Uzoka, F. M. E., Langmia, K., & Njeh, F. N. (2016). Conceptualizing a model for adoption of cloud computing in education. International Journal of Information Management, 36(2), 183-191.

[5] Zadeh, A. H., Akinyemi, B. A., Jeyaraj, A., & Zolbanin, H. M. (2018). Cloud ERP Systems for Small-and-Medium Enterprises: A Case Study in the Food Industry. Journal of Cases on Information Technology (JCIT), 20(4), 53-70.

[6] Wang, K., Zhang, Y., Guo, S., Dong, M., Hu, R. Q., & He, L. (2018). IEEE Access Special Section Editorial: The Internet of Energy: Architectures, Cyber Security, and Applications. IEEE access, 6, 79272-79275.

[7] Deng, S., Zhou, A. H., Yue, D., Hu, B., & Zhu, L. P. (2017). Distributed intrusion detection based on hybrid gene expression programming and cloud computing in a cyber physical power system. IET Control Theory & Applications, 11(11), 1822-1829.

[8] Sallam, H. (2015). Cyber security risk assessment using multi fuzzy inference system. IJEIT, 4(8), 13-19.

[9] Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security, 74, 323-339.

[10] Erdogmus, D., & Principe, J. C. (2002). Generalized information potential criterion for adaptive system training. IEEE Transactions on Neural Networks, 13(5), 1035-1044.

[11] Akhmetov, B., Lakhno, V., Akhmetov, B., & Alimseitova, Z. (2018, September). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity. In Proceedings of the Computational Methods in Systems and Software (pp. 162-171). Springer, Cham.

[12] Zhang, Peng, et al. Pattern mining model based on improved neural network and modified genetic algorithm for cloud mobile networks. Cluster Computing, 2019, 22.4: 9651-9660.

[13] Lakhno, V., Tsiutsiura, S., Ryndych, Y., Blozva, A., Desiatko, A., Usov, Y., & Kaznadiy, S. (2019). Optimization of information and communication transport systems protection tasks. International Journal of Civil Engineering and Technology, 10(1), 2019.