УДК 338.246.025.2

MATHEMATICAL MODELING OF CORPORATE NETWORK TOLERANCE TROUBLESHOOTING METHODS

Petrov Anton Alexandrovich[1], Cand. Sc. (Tech.), Assoc. Prof.
Savinskaya Dina Nikolaevna[1], Cand. Sc. (Econ.), Assoc. Prof.
Minina Evgeniya Alexandrovna[2], Cand. Sc. (Econ.)
Dunskaya Lada Konstantinovna[1], M.A. student

[1] Kuban state agrarian University named after I.T. Trubilin, Kalinina st., 13, Krasnodar, Russia, 350044; e-mail: antonpv@mail.ru; savi_dinki@mail.ru; lada.dunskaya@mail.ru

[2] University of Economics and Management, Krymskaya Pravda st., 4, Simferopol, Republic of Crimea, Russia, 295021; e-mail: evgeniyaminina@yandex.ru

Purpose: the article presents the results of mathematical modeling of technique for troubleshooting of network fault tolerance and the developing of methods for fault location search. *Discussion*: since the high performance of corporate networks is provided primarily by the absence of defects and bottlenecks, it becomes necessary to develop a method for diagnosing the fault tolerance of corporate networks, which will help reduce the time spent on Troubleshooting and Troubleshooting. The Troubleshooting method is implemented through a comprehensive analysis of network packet loss and includes the basic formula of the half-division method. Using this method, you can automatically (or manually) detect healthy or faulty nodes in the corporate network. *Results*: it has been introduced the method and algorithm for remote troubleshooting of corporate network fault tolerance through the analysis of packet loss.

Keywords: troubleshooting, fault tolerance, mathematical modeling, troubleshooting algorithm.

DOI: 10.17308/meps.2020.12/2488

Introduction

Widespread use of network infrastructure leads to increased requirements for fault tolerance of corporate networks. High performance network is provided primarily by the absence of defects and bottlenecks that lead to a slowdown in the speed of the network and to the unavailability or fault of communication components. In case of facing any of these problems, we should consider the time spent on a search and recovery of the network system operating ability. The identifying of a space of fault takes, at an average, 90% of the time.

Up to the present time, the solving of LAN's troubleshooting tasks, which includes the scientific task of identifying network faults, still belongs to one of

complicated problems. As network faults are divided into different types, each of them requires various types of diagnostic equipment to be used, as well as various methods, algorithms and methodologies.

To this time, there is no single formalized methodology that can identify any of the types of faults. These problems cause great amount of time wasted on identifying the faults and, also, narrow the range of subjects that provide the correct solution for troubleshooting, what leads to high complexity and difficulty in solving the problem.

The main purpose of this research is to introduce the ways of reducing the complexity, reducing the period of time spent on troubleshooting in corporative networks and eliminating a disability in its operating.

Research methodology

Troubleshooting is divided into two types: preventive (proactive) and reactive. Proactive troubleshooting of the network operation should be carried out every day. The main purpose of preventive troubleshooting is to prevent network operating faults. Reactive troubleshooting is applied when the network has already failed and it is necessary to isolate quickly the source of fault and to find its cause.

If the status check of the object operability gives a negative result, there is a problem in determining the space of fault with the details given to removable block, removable card in a block and a separate element in the circuit. Typically, the process of discovering the space of fault is of long time and complexity, it requires special diagnostic tools. They depend on the efficiency of the process of choosing the right troubleshooting algorithm.

Under the program for discovering the faults it is implied a prearranged and documented sequence of elementary checkups (measuring of controlled parameters) and sequence of the basic checkups analysis, which are performed to determine the cause of fault and fault nodes (nodes, systems, elements etc. – depending on the level of details in identification the spaces of faults).

The most common fault identification programs are divided, for convenience, into two groups: flexible-serial (these include «the program on the maximum information» and «the program on half-splitting»); hard-serial (these include «program on functional scheme» and «program on time-probability»).

Program on functional scheme is based on identifying the spaces of fault by executing the «hard» order (strictly by functional scheme of reply) consecutive elementary checkups. The results of each elementary checkup are analyzed immediately.

Elementary checkup has to be made for every diagnostic parameter (parameters) of each element of the system. The discovering of the fault stops as soon as the analysis of the regular elementary checkup discovers the failing element of the system. Obviously, in the worst case (when the last-checked element of the system failed) the number of elementary checks will be maximized and equal to the number of elements in the system.

The «the program on time-probability» can be used only when the huge experience on faults in this type of equipment is already accumulated and the experience on its operating is systematized, and in particular the experience of searching the space of fault.

Obviously, this program allows to checkup firsthand those elements of the system, whose fault probability is maximal and the time for elementary checkup is minimal. As a result, the total time for identifying the location of system fault is significantly less than using the above mentioned «program on functional scheme».

Program on the maximum information can be applied only when the equipment fault search experience has been accumulated and some experience of its operation has been systematized, especially, when the degree of probability of fault for every single element of the system is already known.

The program on the maximum information is based on identifying the space of fault by performing serial elementary checkups of groups of elements in the «soft» manner. In some cases, the group may be presented by one element.

The search of the fault space stops as soon the results of the next checkup shows failed element. This program allows performing the most basic informative checkups, which results in significant reduction of the number of elementary checkups as well as the overall time for searching the fault.

The discussion of the results

We introduce the method for diagnostics of corporate network fault tolerance (see Fig. 1), grounded on above considered methods for troubleshooting the network and methods for identifying the space of fault. This method is based on the analysis of packet loss.

Fig. 1. Corporate network

This method is developed by using the methodology of active and passive testing, i.e. troubleshooting starts with checkup of the presence or absence of

signals in some points (nodes) of network through bombarding the network nodes by 32 bytes package.

Method for remote diagnostics of corporate network fault tolerance through analyzing the packet loss is a permanent (or as needed) observation for the state of network and recording any changes in its behavior.

On the basis of these observations, the administrator can draw conclusions about the necessity to replace the active equipment or the network architecture.

Record

$$z=\Psi(X,Y,t) \quad (1)$$

is regarded as some graphical, tabular representation of the system transfer function of ready-to-operate facility of the diagnosed object, which reflect the dependence of output functions, realized by object *Z*, from its input variables *X*, initial value *Y* of internal variables and the time *t*. The system (1) is a mathematical model of the item (corporate network) in good working order.

The symbol *M* denotes the set of all considered (not necessarily all possible) single and multiple faults of object, the symbol *B* – the set of its single faults. Hence, $M \in V$.

So we say that by the presence of the fault in the object, $m_i \in M$, $i = 1,2, ..., |M|$, or, $b_i \in B$, $i = 1,2, ..., |B|$ the object is in the i-defective condition or is *i*-faulty.

The object of troubleshooting that is in i-defective condition, carries out the system of transfer functions

$$Z^i=\Psi^i (X^i,Y^i,t) \quad (2)$$

is presented in the same form as the transfer functions (1).

The initial value of *Y* and *X* in *i*-faulty object may be different from their initial value of *Y* and *X* in object in good working order. The system (2) for a fixed i is a mathematical model of *i*-faulty object.

The system (1) and the set of systems (2) form a clear model of the object of troubleshooting. We denote this model by record $(\Psi, \{\Psi^i\})$.

Let us letter the symbol P for the set of all admissible elementary checkups of the object πj, j = 1,2, ..., | P |, i.e. those object's checkups that are physically implemented in the specific conditions of the process of troubleshooting.

Each elementary checkup, by definition, is characterized by the impact made on the object in the event of implementation the elementary checkup, and the response of the object to this impact.

Figure 2 shows the treelike graph of type G (V, E) corporate network.

With the help of treelike graph of corporate network we draw the table of routing for nodes (K12, B11), for visual demonstration of the system (1).

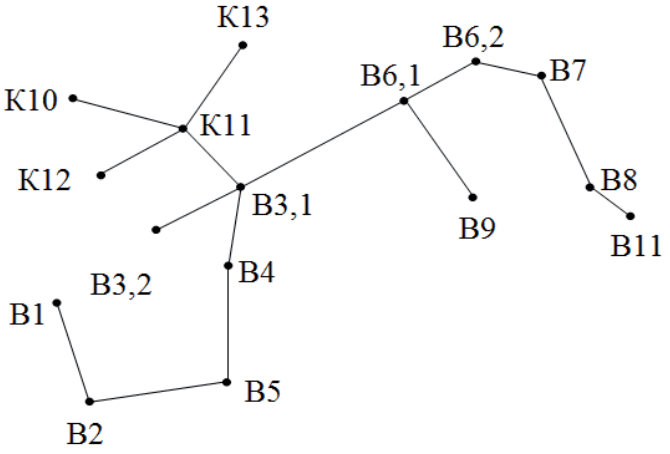

Fig. 2. Treelike graph of corporate network

To find the system (2) we use the routing table of nodes and the following formula:

to calculate the value of limit *a*, $a_0 = 0$ by the formula

$$a_{\pi_j} = a_{\pi_{j-1}} + p_{\pi_{j-1}} \quad (3)$$

where π_j – the number of checkup.

To calculate the value of the *b*, $b_0 = N$ by the formula

$$b_{\pi_j} = p_{\pi_{j-1}} \quad (4)$$

where N – the quantity of nodes in the network.

To calculate the bias in the routing table of nodes *h* by the formula

$$h_{\pi_j} = \frac{b_{\pi_j} - a_{\pi_j}}{2} \quad (5)$$

finding the node number for identifying IP-addresses by ordinal number *p*, $p_0 = 0$ by the formula

$$p_{\pi_j} = p_{\pi_j - 1} + h_{\pi_j}. \quad (6)$$

The example of practical application of the method for remote troubleshooting of corporate network fault tolerance by analyzing packet loss, regarding items (K12, B11) of the system (1) with equally-reliable elements is given on Fig. 3.

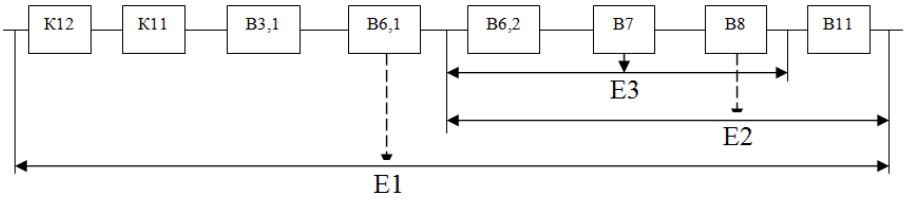

Fig. 3. Troubleshooting algorithm

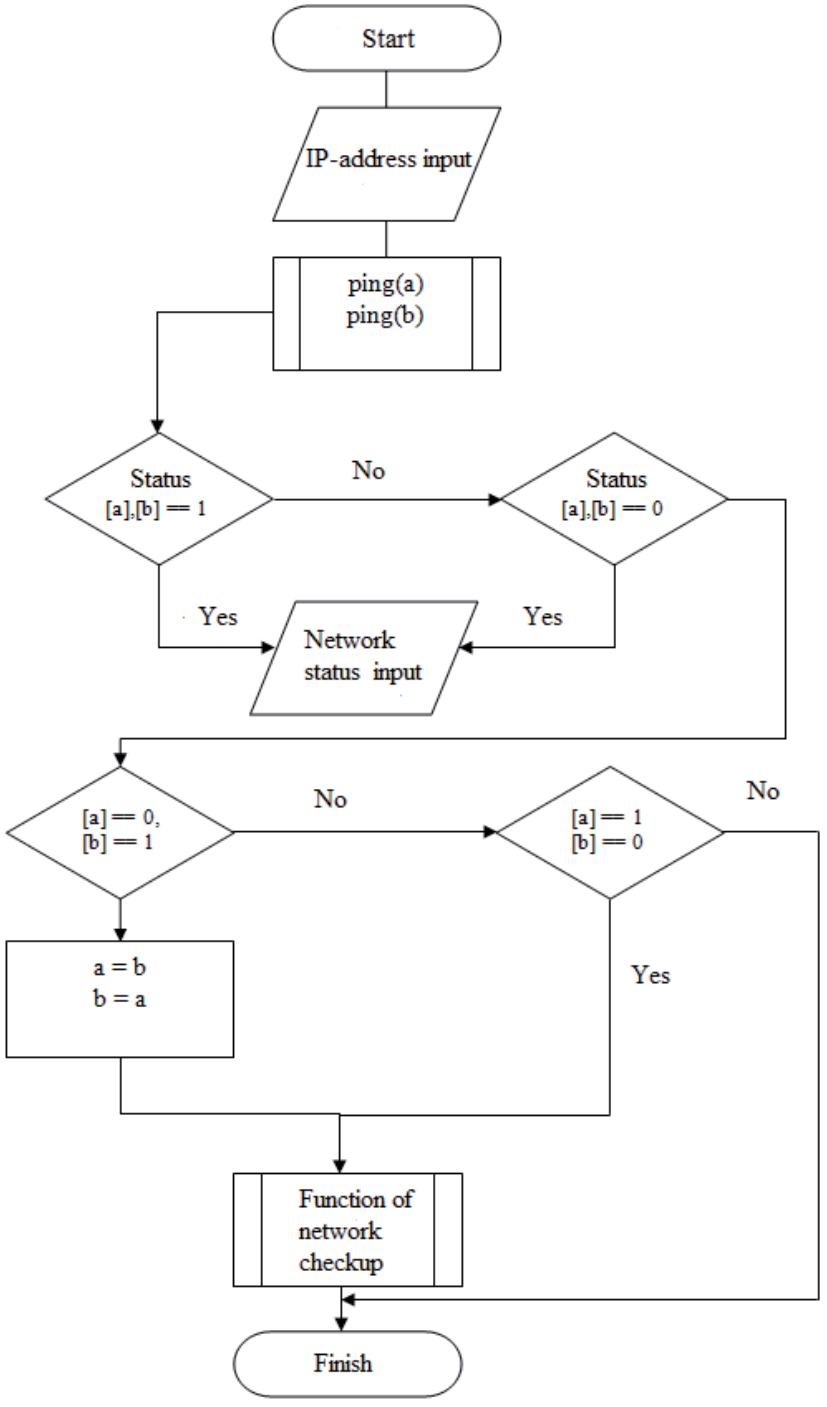

Fig. 4. Flowchart 1. IP-address checkup

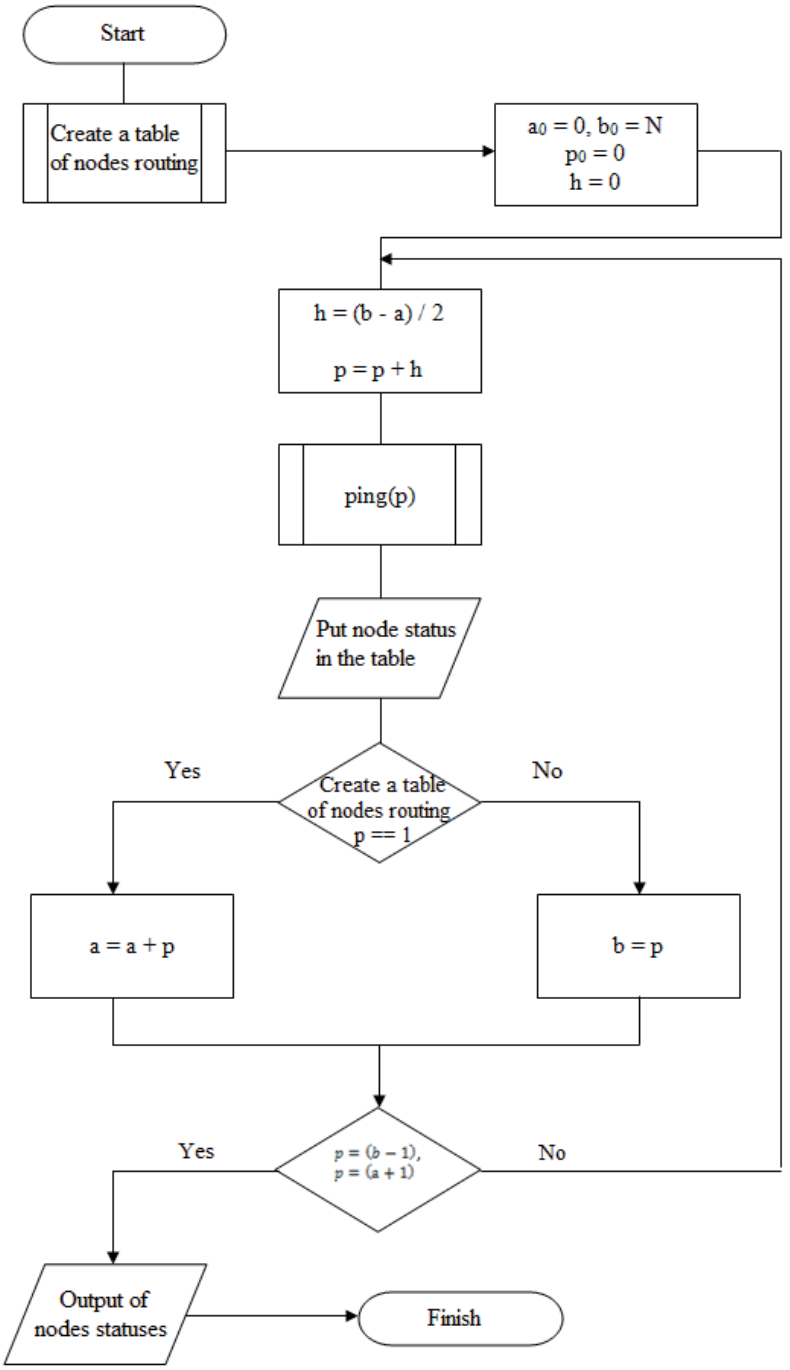

Fig. 5. Flowchart 2. Functions of network checkup

On this figure, vertical lines that represent the basic checkups are placed under the scheme. It is necessary to divide between elementary checkups performed immediately after the inspection, with, positive and negative results respectively.

However, in spite of the all positive sides there are some drawbacks: in some cases, identifying failed nodes may take longer period of time than searching them manually by using the utilities ping and traceroute.

For more visual representation, the troubleshooting algorithm is shown on the flowchart.

Method for remote troubleshooting of corporate network fault tolerance through analyzing the losses is divided into two flowcharts.

The last figure shows the main functions of the simulated remote Troubleshooting method in the corporate network.

Conclusions

Thus, on the basis of the described methods of network diagnostics and identification of fault locations, the authors have developed a method for troubleshooting a corporate network. Based on active and passive testing methodology, this method is easy to use and reduces the time spent troubleshooting nodes in corporate networks. However, the only drawback of the developed method is that on small networks it may take longer to find disconnected hosts than to manually identify them using the ping and traceroute utilities.

References

1. Baranovskaya T.P., Popova E.V., Zamotailova D.A. Approaches to multi-criteria analysis of the activities of management organizations of the housing and communal complex. *Materials of the international scientific and practical conference "National economies in the context of global and local transformations"*, 2018, pp. 10-14.

2. Gorkavoy P.G., Zamotailova D.A. Features of forecasting and multi-criteria analysis in social spheres. *Materials of the 75th scientific and practical conference of students on the results of research for 2019 "Scientific support of the agro-industrial complex"*, Krasnodar, 2020, pp. 653-655.

3. Olifer V.G., Olifer N.A. *Fundamentals of computer networking*. St. Petersburg, Piter, 2009.

4. Fundamentals of technical diagnostics. In 2 volumes. Book 1. *Object models, methods and algorithms for Troubleshooting.* Ed. By P. P. Parkhomenko, Moscow, Energia, 1976.

5. Parkhomenko P.P., Sagomonyan E.S. *Fundamentals of technical diagnostics*. B.

2. Optimization of diagnostic algorithms and hardware. Ed. By P. P. Parkhomenko. Moscow, Energia, 1981

6. Popova E.V., Savinskaya D.N. Specificity of distribution on HOD market. *Collection of scientific papers SWorld*, 2011, Vol. 11, no. 2, pp. 21-22.

7. Savinskaya D.N. *Modeling and forecasting of small and medium-sized businesses in the HOD market dissertation for the degree of candidate of economic Sciences*. Voronezh state University, Krasnodar, 2012.

8. Savinskaya D.N., Tankayan A. Information security of a personal computer and modern types of threats to data loss in the collection: Information society: current state and prospects for development. *Collection of materials of the XI international student forum*, 2018, pp. 114-116.

9. Safarbakov A.M., Lukyanov A.V., Pakhomov S.V. *Fundamentals of technical diagnostics*: textbook. Irkutsk, The Irkutsk State University Of Communications, 2006.

10. Uditsky S., Borisenko V., Ovchinnikov O. Fundamentals of network diagnostics // *LAN./ Journal of network solutions*, 1988, December.

11. Litvinenko A., Maslovsky B., Glazok O., & Petrov A. (2020). Method of optimal planning of cyberprotection actions for a corporate information system // *CEUR Workshop Proceedings*, 2654, pp. 60-71. Scopus.

12. Petrov A., Karpinski M., & Petrov O. (2018). Development of methodological basis of management of information protection in the segment of corporate information systems. *International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management*, SGEM, 18(2.1), pp. 317-324.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ МЕТОДОВ ДИАГНОСТИКИ ОТКАЗОУСТОЙЧИВОСТИ КОРПОРАТИВНЫХ СЕТЕЙ

Петров Антон Александрович[1], канд. техн. наук, доц.
Савинская Дина Николаевна[1], канд. экон. наук, доц.
Минина Евгения Александровна[2], канд. экон. наук
Дунская Лада Константиновна[1], маг.

[1] Кубанский государственный аграрный университет им. И.Т. Трубилина, ул. Калинина, 13, Краснодар, Россия, 350044; e-mail: petrov.a@kubsau.ru; savi_dinki@mail.ru; lada.dunskaya@mail.ru

[2] АНО «ООВО» «Университет экономики и управления, ул. Крымской Правды, 4, Симферополь, Республика Крым, Россия, 295021; e-mail: evgeniyaminina@yandex.ru

Цель: в статье представлены результаты математического моделирования приемов диагностики отказоустойчивости сети и разработки методов поиска места повреждения. *Обсуждение*: так как высокая производительность корпоративных сетей обеспечивается, прежде всего, отсутствием дефектов и узких мест, то появляется необходимость в разработке метода диагностики отказоустойчивости корпоративных сетей, который поможет сократить время, затрачиваемое на поиск неисправностей и их устранение. Метод устранения неполадок реализуется посредством комплексного анализа потери сетевых пакетов и включает базовую формулу метода половинного деления. Применяя этот метод, можно автоматически (или вручную) обнаруживать исправные или неисправные узлы в корпоративной сети. *Результаты*: представлен метод и алгоритм удаленного устранения неполадок отказоустойчивости корпоративной сети посредством анализа потери пакетов.

Ключевые слова: устранение неисправностей, отказоустойчивость, математическое моделирование, алгоритм устранения неисправностей.

Список источников

1. Барановская Т.П., Попова Е.В., Замотайлова Д.А. Подходы к многокритериальному анализу деятельности управляющих организаций жилищно-коммунального комплекса // *Материалы Международной научно-практической конференции «Национальные экономики в условиях глобальных и локальных трансформаций»*, 2018, с. 10-14.

2. Горкавой П.Г., Замотайлова Д.А. Особенности прогнозирования и многокритериального анализа в социальных сферах // *Материалы 75-й науч.-практ. конф. студентов по итогам НИР за 2019 год «Научное обеспечение агропромышленного комплекса»*. Краснодар, 2020, с. 653-655.

3. Олифер В.Г., Олифер Н.А. *Основы*

компьютерных сетей. Санкт-Петебург, Питер, 2009.

4. Пархоменко П.П. *Основы технической диагностики*. В 2-х томах. Книга 1. Объектные модели, методы и алгоритмы устранения неисправностей. Москва, Энергия, 1976.

5. Пархоменко П.П., Сагомонян Е.С. *Основы технической диагностики*. Б. 2. Оптимизация алгоритмов диагностики, аппаратных средств. Эд. П.П. Пархоменко. Москва, Энергия, 1981.

6. Попова Е.В., Савинская Д.Н. Specificity of distributorship on HOD market // *Сборник научных трудов SWorld,* 2011, Т. 11, no. 2, с. 21-22.

7. Савинская Д.Н. *Моделирование и прогнозирование деятельности предприятий малого и среднего бизнеса на рынке HOD:* диссертация на соискание ученой степени кандидата экономических наук. Воронежский государственный университет, Краснодар, 2012.

8. Савинская Д.Н., Танкаян А.И. Информационная безопасность персонального компьютера и современные виды угроз потери данных // *В сборнике: Информационное общество: современное состояние и перспективы развития. Сборник материалов XI международного студенческого форума*, 2018, с. 114-116.

9. Сафарбаков А.М., Лукьянов А.В., Пахомов С.В. *Основы технической диагностики*: учебное пособие. Иркутск, ИрГУПС, 2006.

10. Юдицкий С., Борисенко В., Овчинников О. Основы сетевой диагностики // *LAN. Журнал сетевых решений*, 1988, декабрь.

11. Litvinenko A., Maslovsky B., Glazok O. & Petrov A. (2020). Method of optimal planning of cyberprotection actions for a corporate information system // *CEUR Workshop Proceedings*, 2654, pp. 60-71. Scopus.

12. Petrov A., Karpinski M. & Petrov O. (2018). Development of methodological basis of management of information protection in the segment of corporate information systems // *International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management,* SGEM, 18(2.1), pp. 317-324.