Journal of Theoretical and Applied Information Technology
15th July 2021. Vol.99. No 13

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

INTELLIGENT SUPPORT IN MAKING TECHNICAL DECISIONS IN THE ENTERPRISE INFORMATION INFRASTRUCTURE

[1]A.B.ZAKIROVA, [2]E.A.BASINYA, [1]M.A.KANTUREYEVA, [1]A.ZH.AKHMETOVA, [1]ZH.B.AKHAYEVA

[1] L.N.Gumilyov Eurasian National University, Department of Information Systems, Astana, Kazakhstan
[2] Novosibirsk State Technical University, Department of Automation, Novosibirsk, Russia

E-mail: [1]alma_zakirova@mail.ru, [2]director@nii-ikt.ru, [1]ma_khantore@mail.ru, [1]akhmetova_azh@mail.ru, [1]ahaeva07@mail.ru

ABSTRACT

Today, intelligent information technology can act as a catalyst for the development of almost all areas of society. The article discusses the current state of affairs in the field of management and maintenance of the information infrastructure of the enterprise. The problems of system and network administration of technical objects and systems are described. The shortcomings of the existing systems of intellectual support for engineers involved in their support are described. The method of providing intellectual support when making technical decisions in the enterprise's information infrastructure, operating on the basis of the TCP / IP protocol stack and the operating systems of the Windows and Linux family, is submitted for review. The scientific novelty of the proposed solution lies in the intellectual support in making technical and managerial decisions based on previous experience and the ability to predict the state of the system. Unlike existing approaches, safe forecasting of the reaction of a technical object to certain external, internal or local influences and changes, including those set forth in a declarative form, is provided. The continuous operation of the object during its research and forecasting with the possibility of applying influences / changes to the real system with successful iterative testing is ensured. Optional parallelization of testing and research processes in an isolated and safe environment is performed. The knowledge base of system and network administration of the enterprise information infrastructure is being formed, which allows solving complex and complex incidents. These provisions are achieved by creating many model objects in stealth mode (for example, by a volume shadow copy service) in an isolated environment based on the ESXI hypervisor with virtual segmentation of VLAN traffic and technology for automatic deployment and configuration of user and server solutions (including Ansible). The method is integrated with the previously developed by the author system of intellectual adaptive management of the enterprise information infrastructure.

Keywords: *Intellectual Support, Forecasting, Automation Of System And Network Administration, Shadow Copying, Cloning, Model Objects, Hypervisor, Feedback, Intelligent Adaptive Management, Knowledge Base.*

1. INTRODUCTION

Improvement of intellectual information technologies is an integral part of the strategy of scientific and technological development of the Russian Federation. Successful development, implementation and application of these technologies can significantly improve the quality of solving problems of analysis, management and processing of information in various areas of the company's activities. The result is the level of competitiveness of companies and the state in the international economic and political arena. It is impossible to consider the creation of algorithms, methods, or technologies for working with data in isolation from information security. Violation of this concept leads to significant costs. Only at the beginning of April, the personal data of 4,934,863 residents of Georgia became publicly available, according to research by Under the Breach. In addition, the Marriott hotel chain reported a leak of information about 5.2 million people who used the

company's loyalty app. Unfortunately, it is not always possible to objectively assess the total material and moral damage caused by such malicious actions.

Each business entity (enterprise) has an information infrastructure (IIP), which must be maintained by a qualified technical specialist, including to ensure a high level of security of information resources. Automation of system and network administration processes with the provision of intellectual support for making managerial and technical decisions in technical systems simplifies this process. At the same time, depending on the economic activity, scale and organization of business processes, each company searches for a cost-effective technical solution with a balance of information security, automation efficiency and functionality. For example, small businesses can make do with a standard package of custom software and typical network devices of the small/home office class (English: SOHO, Small office/home office). Medium and large businesses need specialized intrusion detection and prevention systems, data leaks, automated incident processing, and many other tools. The expediency of their application is not subject to doubt in the context of the economic profitability of maintaining the life of the enterprise and leveling potential threats and their consequences. In this paper, we will focus in more detail on intellectual support for technical decision - making by system and network administrators and information security engineers.

The international scientific community develops specialized algorithms and methods for solving a wide range of problems in this field. The works of Xiaoqing Z., Zhiyong Z., Jianqiong X., Jiaxiu S. offer the introduction of a simplified layer of abstraction for the representation of knowledge models, while presenting only theoretical research without practical implementation with no possibility of application for the entire IIP. Authors presented new decision-support system that integrates data warehouse, knowledge warehouse and model warehouse [1]. Proceedings Of Chatterjee P., Cymberknop L. J., Armentano R. L., Changhui Y., Tianxiang F., Gang C., Yifan Z. they are focused on narrow subject areas, solve atomic problems and do not allow scaling, and do not provide correct collaboration with existing technology stacks. The authors propose IoT-based decision support system for intelligent healthcare using seamless data exchange, as well as Emergency Logistics Decision Support System Design under Data Mining and Web GIS Technology [2-4]. The proposed projects close atomic tasks and do not allow scaling, do not provide correct collaboration with existing technology stacks and objects of the enterprise information infrastructure.

C. S., Prabhavathi C. N., Ilieva R., Anguelov K., Gashurova D. correspond to the methodology of ITIL (it Infrastructure Library) and develop the efficiency of Service Desk systems. The authors propose Administration based on Network Computing for Enterprise Systems using a modification of the computer network architecture and program structure, as well as an approach to analyzing and improving the performance of e-Services in IT Service Desk Systems [5-6]. There are no unified methods or products to support technical decision-making within the information infrastructure of an enterprise; the presented approaches solve only atomic functionality. However, a common key disadvantage of existing approaches is the lack of ability to predict host responses to internal, external, or local impacts / changes with automatic self-learning of the knowledge base without the potential risk of violating its normal operation.

The statement of the key problem lies in the fact that the existing systems of support for making technical decisions by engineers of information infrastructures of enterprises are not able to function effectively and efficiently when processing complex complex events / incidents. At the same time, significant time and human resources are required to carry out computational experiments and form a knowledge base in manual mode. A technician who wants to make certain changes to the server (including installing and configuring a new software module) will not be able to get the correct support when making a technical decision. Existing systems will be able to provide only general recommendations that do not take into account all the parameters and settings of the current host with various software operating on it. Ultimately, this can lead to a violation of the normal operating mode and the failure of both a separate service and the entire facility.

Low efficiency and lack of automation are due to a wide range of key disadvantages of existing solutions:

1) the inability to predict the reaction and state of a host under control of operating systems of the Windows / Linux family of client and server versions after making changes to the configuration of the OS or various software;

2) unattainability of an objective assessment of the correctness of the client or server after the proposed software update;

3) the complexity of the examination of the compatibility of the installed software module with working services / services;
4) difficulty in the process of reproducing the experiment and creating a reference initial sample, especially in online mode without stopping the combat server;

5) lack of confirmation and support of hypotheses by introducing an additive test signal (generating additional legitimate traffic of functioning services and services, as well as introducing additional activity of information processes). Such checks could improve the quality and reliability of the decisions made, confirming the absence of errors and failures in the normal functioning of all information processes of the host.

Accordingly, the development of new methods and systems for providing intellectual support for technical decision-making by information and communication technology specialists is becoming more urgent.

2. PROBLEM STATEMENT AND RESEARCH GOAL

The goal was to develop and programmatically implement a method for providing intellectual support for technical decision - making in the enterprise information infrastructure that operates on the basis of the TCP / IP Protocol stack and Windows and Linux operating systems.

Providing the following functions formed the provisions of scientific novelty and were the key tasks:

1) the ability to predict the reaction of a technical object to certain impacts and changes, including those set out in a declarative form;

2) maintaining the continuous operation of the object during its research and forecasting;

3) formation of the knowledge base of system and network administration of the enterprise information infrastructure;

4) the ability to apply impacts / changes to the real system during successful iterative testing;

5) intelligent support for making technical decisions based on previously accumulated experience and the ability to predict the state of the system;

6) optional parallelization of testing and research in an isolated and secure environment;

7) integration with the previously developed system of intelligent adaptive management of enterprise information infrastructure (SIAU IIP) [7].

The software implementation of the proposed method also includes a standard set of Service Desk systems functionality to provide a single point of interaction with users and processing requests. Due to the standard functionality of such products, the emphasis on these points is not made in this article.

3. METHOD OF PROVIDING INTELLECTUAL SUPPORT FOR MAKING TECHNICAL DECISIONS IN THE ENTERPRISE INFORMATION INFRASTRUCTURE

To achieve these goals, a method for providing intellectual support for making technical decisions in the information infrastructure of an enterprise was developed and software implemented, which involves performing a sequence of actions illustrated in Figure 1.

Brief essence of the proposed method: a technician wants to make changes to the configuration of a working server or install new software. It formalizes the desired actions and specifies the data for accessing the server. The authoring system creates its reference clones online without interruption and without interfering with the operation of the object. Then, in an isolated environment, it performs the specified actions and tests the assembly performance with the introduction of legitimate actions and monitoring of all services and services. Based on the data obtained, the decision support system issues to the technician recommendations for applying changes (including in automatic mode) or rejecting them due to potential errors. By accumulating experience, the system learns itself and establishes relationships between various types of impacts, methods of neutralizing and processing them, as well as the state of the operating system and its components. In the future, the system additionally monitors the state of the host and offers the administrator to automatically neutralize the problems of system and network administration of the information infrastructure of the enterprise.

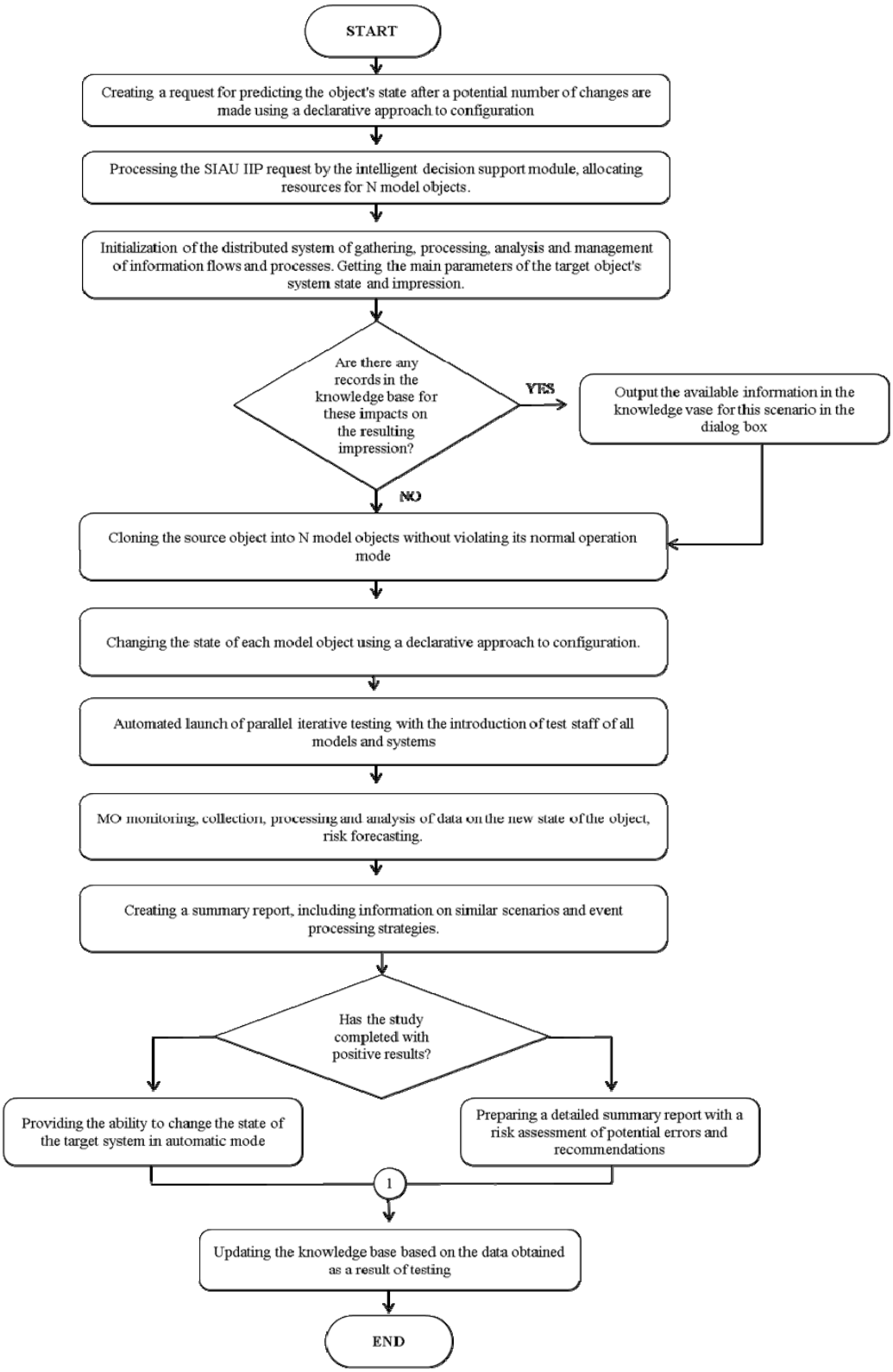

Figure 1:Flowchart Of The Method For Providing Intellectual Support In Making Technical Decisions In The Enterprise Information Infrastructure

Let's consider the method in more detail. At the first stage, a request is formed to forecast the object's state in response to external, internal, or local influences, or after a potential number of changes are made using a declarative approach to configuration. At this stage, to formalize actions, we use the technology of automated deployment and configuration of ansible user and server solutions in combination with the Researcher program and the framework of the same name. The platform has been prepared in the form of a web interface with a wide range of basic scripts, playbooks and the ability to configure them, as well as combine and create new instances. The key programming languages are Python and YAML. For remote machines, you must specify data for successful authentication and authorization: from IP addresses, ports, remote access protocols/technologies to usernames and passwords with specific information security settings (up to modification of the port tapping technology and system parameters of a self-organizing virtual secure communication channel).

Then the legitimate SIAU IIP request is processed by the intelligent decision support module, and resources are allocated for N model objects. Each model object represents a virtual machine in the ESXI hypervisor space, including isolated traffic segmentation VLAN (virtual Local Area Network) virtual managed switch L2+. The number of model objects is balanced depending on the load of the ESXI server computing cluster and is optionally configured by the engineer in the administration panel when requested.

Then SIAU IIP initializes a distributed system for collecting, processing, analyzing and managing information flows and processes (Ssoaiu), which operates on the basis of a client-server model. It is organized to get the main state parameters and a snapshot of the entire operating system (OS) and application software of the target object. After receiving the data, the System and network administration knowledge base is accessed. If it contains records and statistics on the specified impacts on a similar OS impression, then the output of available information for this scenario is organized for analysis by a technical specialist. In this case, as in the case of no records, the source object is cloned to N model objects without violating its normal operation mode.

This is achieved by the volume shadow copy service or its analogues, depending on the version and operating system family. Such services are initially intended for backup of individual files without suspending the normal operation of the object even when documents are open, but they are fully suitable for solving the problem of full-fledged cloning of model objects.

The next stage of SIAU IIP is to make external, internal, or local impacts, or make changes to the state of each model object using the previously described declarative approach to configuring user and server solutions. The automated launch of parallel iterative testing with the introduction of standard test actions, tracking the status of all modules and systems. At the same time, the state of model objects is continuously monitored, data on the new state of the object is collected, processed and analyzed, and risks are forecast through the Ssoaiu. A summary report is generated and information about similar scenarios and event processing strategies is included.

If the research and testing iterations are completed with positive results (all services, services, and components continue to operate normally, and no failures, failures, errors, over-quotas, or other problems are detected), the technician is provided with a report and the ability to change the state of the target system in automatic mode using the previously described declarative approach.

Otherwise, the engineer is issued a detailed summary report with a risk assessment of potential errors and recommendations for their elimination. The final stage of the method is to update the knowledge base, taking into account the data obtained as a result of testing and research. The generalized scheme of the knowledge base with elements of the semantic network is illustrated in Fig. 2

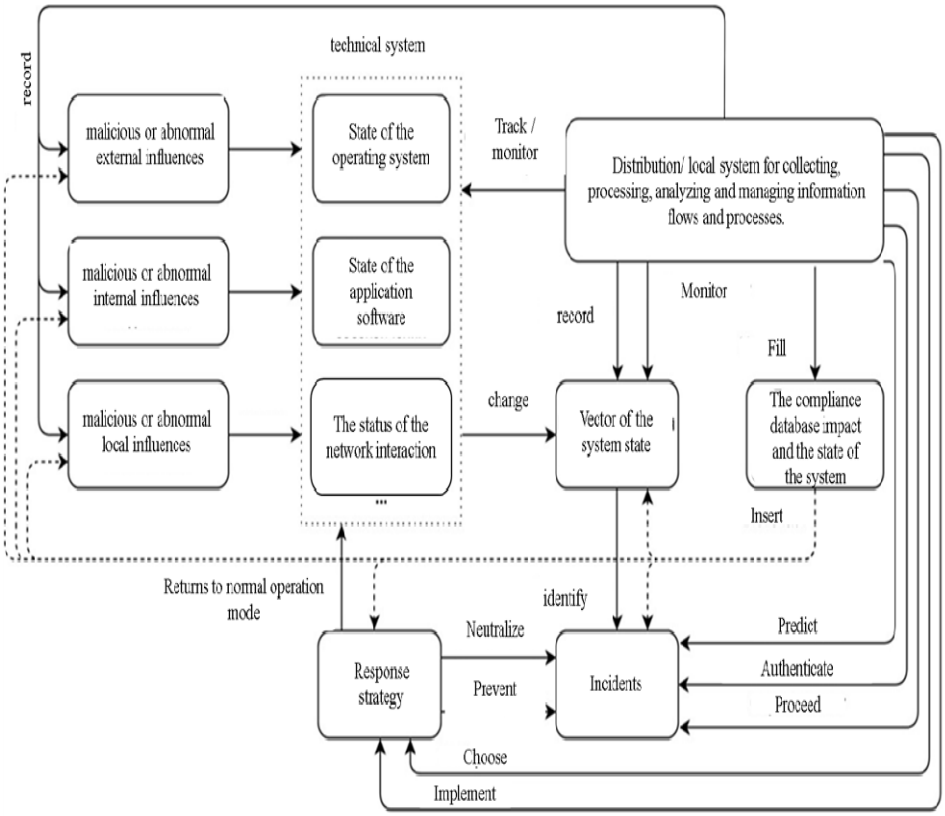

Figure 2:Generalized Scheme Of The Knowledge Base With Semantic Network Elements

As an example of how this method works, it is necessary to provide intelligent decision support when installing new software on the target system (Fig. 3). This scenario applies to an information security engineer who needs to study the impact of certain scripts on the object of the real enterprise infrastructure, or to a system administrator who is tasked with studying the compatibility of updates and correct application collaboration.

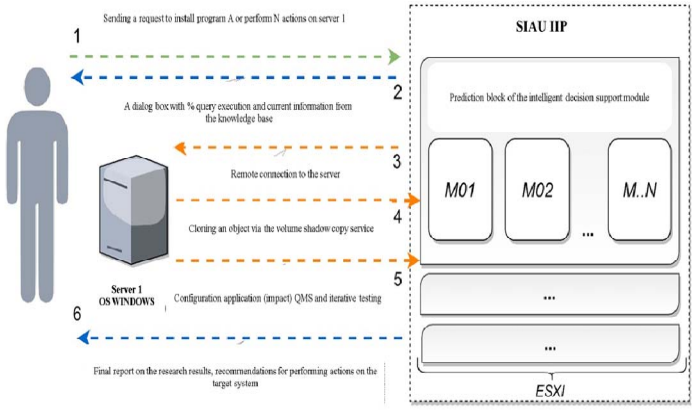

Figure 3. Results Of Working Neural Network

This process includes the following steps:

1) the specialist sends a declarative request to the intelligent decision support module, indicating that you need to install program A or perform actions N on server 1, specifying its IP address and data for authentication and authorization;

2) SIAU IIP in the dialog window displays the progress of query execution, as well as information stored in the knowledge base about earlier testing of the installation of this program A on a cast of the target system with the passed parameters;

3) the intelligent decision support module based on SIAU IIP initiates a connection to a server running on the Windows Server 2019 operating system;

4) initiates cloning of the entire object in hidden mode without violating the normal operation mode via the Windows volume shadow copy service. Copying is performed on separate VMS that act as model objects within the ESXI hypervisor. Isolation of model objects is achieved including virtual traffic segmentation on a virtual managed hypervisor switch;

5) the target system configuration is applied to the MOD. Parallel integration testing is launched on model objects with the introduction of standard effects. The reaction of all systems and modules is tracked, and statistical data on new ones is collected and analyzed object States. To achieve these goals, a distributed / local system for collecting, processing, analyzing, and managing information flows and processes is used, as described earlier;

6) a detailed summary report is generated with the results of research and testing, including information from the knowledge base for similar scenarios and event processing strategy. It also includes information with an error risk assessment and recommendations for installing software on the target system.

If you receive positive research results (there are no technical failures or problems), you can change the state of the target system automatically. Of course, the technician is also given the opportunity to work with model objects in manual mode.

The interaction of the intelligent decision support module with the knowledge base and a distributed system for collecting, processing, analyzing and managing information flows and processes is shown in figure 4.

It is worth noting that the event collection and analysis system not only expands the database, but also uses its knowledge to manage information flows and processes (incident processing) [8].

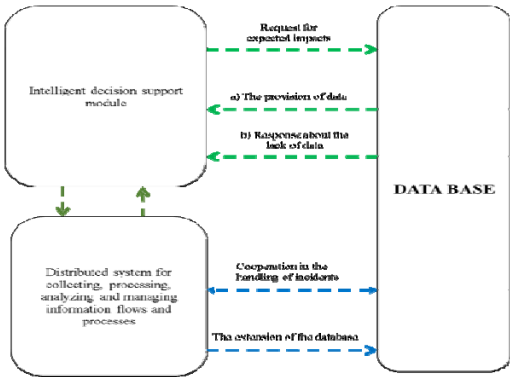

Figure 4: Interaction Of The Intelligent Decision Support Module With The Knowledge Base And A Distributed System For Collecting, Processing, Analyzing And Managing Information Flows And Processes Work

The software implementation of the proposed method used a well-established technological pipeline of software production using the methodology of continuous integration and deployment (CI / CD, Continuous integration & Continuous delivery). The DevOps line was built in the context of industry standards [9-10]. It is important to note that each stage of development was covered by autotests, which made it possible to eliminate errors and shortcomings in the final version of the project.

To evaluate the effectiveness of the developed method, experimental studies were conducted both in the test environment and within the real information infrastructures of enterprises. In one of them, the SIAU IIP was deployed in the space of a dedicated physical server with the following characteristics: Intel Xeon E-2176G processor with six cores, 12 threads, a base clock frequency of 3.70 GHz, 64 GB ddr4 ECC RAM, 3 x SSD 960 GB, 100 Gbit/s bandwidth. The delay inside the corporate computer network did not exceed 2 MS, the volume of target systems under study did not exceed 100 GB, and the number of

model objects ranged from 3 to 9 units (since corporate server solutions also functioned in the virtual infrastructure).

During the year of applying the method of providing intellectual support for technical decision-making in the enterprise information infrastructure, automated parallel cloning and launching of model objects did not exceed 59 minutes and 17 seconds (the worst value was due to the pulsating loading of the communication channel with low bandwidth, which falls to 200 Mbit/s in

short periods), while the average value was 6 minutes 19 seconds, and the best indicator for an object inside the hypervisor was 1 minute 56 seconds. The process of parallel testing and research ranged from 3 minutes and 5 seconds to 64 minutes and 48 seconds, depending on the number of model objects, as well as the scale and volume of the selected tests. It is important to note that all stages of the method were always worked out correctly, and there were no errors in forecasting and Analytics.

4. DISCUSSION OF RESULTS AND CONCLUSIONS

As part of the discussion of the results of scientific and practical research, it is worth starting from a comparative analysis with existing methods and approaches, and then proceed to assessing the experimental indicators and describing the scientific novelty of the method.

Approaches to the formation of decision support systems proposed by Xiaoqing Z., Zhiyong Z., Chatterjee P., Cymberknop LJ, Yifan Z are improved by bringing self-learning to the system by predicting the state of the host after making changes on model objects with reinforcement through testing and research [1-4].

The studies carried out improve the efficiency of the methods of functioning of Service Desk Systems and Administration based on Network Computing, proposed by Govindaraju CS, Prabhavathi CN, Ilieva R., Anguelov K., Gashurova D., in the information infrastructures of the enterprise using the family of operating systems of the Linux / Windows family [5 , 6]. This is achieved by introducing the automation of system and network administration processes and automated processing of emerging or predicted incidents.

As noted earlier, no unified product in this subject area has previously been presented. And the results of the experiment, given the fundamentally new functionality, is not possible to compare with the existing methods. However, conducting a computational experiment clearly demonstrated the key drawback of the developed system - increased requirements for computing power. The minimum system requirements are increased several times due to the need to use a hypervisor: from a processor with hardware support for virtualization and AES encryption algorithm, DDR4 RAM with support for ECC (Error Correction Code Memory) technology, to a high-speed enterprise-class SSD.

The experience of industrial operation showed that the maximum duration of the parallel testing and research process was 64 minutes and 48 seconds. It would be difficult to carry out such research manually without stopping the production server or client, and would also take from 53 working hours of a technician. The effectiveness of automation is beyond doubt. The disadvantage in the form of high requirements for computing power is a relatively low price to pay for improving the quality and efficiency of the enterprise's information infrastructure, achieved by scientific and practical novelty.

The scientific novelty of the developed method is to provide intellectual support in making technical and managerial decisions in the information infrastructure of the enterprise. In contrast to existing approaches, a safe automated prediction of the object's response to various changes, external, internal or local influences in the space of model objects is performed with parallelization of the study without the slightest risk of harming the desired technical system or suspending regular work. Forms knowledge base of system and network administration of enterprise information infrastructure for identification and neutralization of incidents.

If a technical specialist wants to test certain actions or integration of new modules, the method (or a System based on it) can offer iterative research on model objects with the introduction of standard test signals and tracking the reaction. In this case, the System will first provide information about the records available in the knowledge base about the expected impact on objects with the specified parameters. Upon completion of testing, a detailed report with risk assessment and recommendations will be provided to the system administrator. In case of successful testing and stable positive results, it will be possible to perform automatic actions on the target system. It is worth noting that the results of testing automatically update the knowledge base.

The ability to predict the response of a technical object to certain impacts and changes, including those set out in declarative form, is achieved using virtualization technology and tools for automated deployment and configuration of server solutions. The ESXI hypervisor is used to create model objects in the form of virtual machines, which are configured by the Ansible configuration management system. The latest technology allows you to apply impacts / changes to the actual system during successful iterative

testing. The multiplicity of model objects in the hypervisor space allows you to optionally parallelize testing and research in an isolated and secure environment.

Maintaining the continuous operation of the object during its research and forecasting is provided by cloning the source system in a hidden and seamless mode. For example, using the volume shadow copy service for Windows operating systems.

Intelligent support for making technical and managerial decisions based on previously accumulated experience and the ability to predict the state of the system is supplemented by a knowledge base of system and network administration of the enterprise's information infrastructure for identifying and neutralizing incidents.

The results of the experimental study on modern server capacities demonstrated acceptable indicators: error - free operation of the method in the implementation of intellectual support for technical decision - making on for typical user and server solutions up to 100 GB in size, the time interval is from 5 minutes and 1 second to 124 minutes and 5 seconds. These indicators are sufficient for effective maintenance of even medium and large enterprise information infrastructure. Optimization of the method is achieved by increasing the server's computing power and bandwidth of communication channels. Taking into account the provided functionality, the method has not only scientific novelty, but also significant practical significance for applied technical specialists.

In conclusion, I would like to note that the analysis, scientific and practical research and software implementation of the method can be used in information infrastructures of enterprises operating on the basis of the TCP / IP technology stack and the Windows / Linux family of client and server versions to improve the quality and efficiency of their functioning. Prediction mechanisms on model objects with the introduction of an additive test signal, iterative testing and object research can be used in other subject areas. As well as approaches to filling and forming a knowledge base of a decision support system with elements of self-learning.

REFRENCES:

[1] Xiaoqing Z., Zhiyong Z., Jianqiong X., Jiaxiu S. Research and Application of an Intelligent Decision Support System // In Proceedings of the International Conference on Computer Network, Electronic and Automation (ICCNEA). Xi'an, China, 23-25 September 2017. pp. 186-189.

[2] Chatterjee P., Cymberknop L. J., Armentano R. L. IoT-based decision support system for intelligent healthcare — applied to cardiovascular diseases // In Proceedings of the 7th International Conference on Communication Systems and Network Technologies (CSNT). Nagpur, India, 11-13 November 2017. pp. 362-366.

[3] Changhui Y. Research on Emergency Logistics Decision Support System Design under Data Ming & WebGIS Technology // In Proceedings of the International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS). Changsha, China, 17-18 December 2016. pp. 375-378.

[4] Tianxiang F., Gang C., Bo C., Yifan Z. Intelligent Student Services Administration System in the Context of Collegiate System // In Proceedings of the 13th International Conference on Computer Science & Education (ICCSE). Colombo, Sri Lanka, 8-11 August 2018. P. 1-4.

[5] Govindaraju C. S., Prabhavathi C. N. Administration based on network computing for enterprise systems: Enhancing the efficiency of network based administration // In Proceedings of the International Conference on Circuits, Controls, and Communications (CCUBE). Bangalore, India, 15-16 December 2017. P. 91-94.

[6] Ilieva R., Anguelov K., Gashurova D. Monitoring and optimization of e-Services in IT Service Desk Systems // In Proceedings of the 19th International Symposium on Electrical Apparatus and Technologies (SIELA). Bourgas, Bulgaria, 29 May-1 June 2016. P. 1-4.

[7] Basynya E. A. Method of intellectual and adaptive management of enterprise information infrastructure / / Information technologies. – 2020. - № 3 (26). – pp. 185-191.

[8] Basynya EA Software implementation and research of the system for intellectually adaptive management of the enterprise information infrastructure = Software implementation and research of the system for

intellectually adaptive management of the enterprise information infrastructure / EA Basynya // Bulletin of the Samara State Technical University. Series: Engineering = Vestnik of Camara state techmical university. Technical sciences series. - 2020. - T. 28, No. 1 (65). - S. 6-21.

[9] Basynya EA The system of intelligent-adaptive management of the information infrastructure of the enterprise / EA Basynya // Information technologies = Informatsionnye tekhnologii: scientific and technical. zhurn. - 2020. - No. 5 (26). - S. 283–289. - DOI: 10.17587 / it.26.283-289. - The work was carried out: with the support of the Russian Foundation for Basic Research (No. 18-00-00238).

[10] Basinya E. A. Automatic traffic control system for SOHO computer networks / E. A. Basinya, A. A. Rudkovskiy // Studies in Systems, Decision and Control. - 2019. - Vol. 119 : Recent Research in Control Engineering and Decision Making. ICIT 2019. - P. 743-754. - DOI: 10.1007/978-3-030-12072-6_60.

[11] Basinya E. A. Countermeasure method against unauthorized and anonymous information system data collection [Electronic resource] / E. A. Basinya, V. E. Khitsenko, A. A. Rudkovskiy // Dynamics of systems, mechanisms and machines (DYNAMICS) : proc., 13 intern. sci. and techn. conf., Omsk, 5–7 Nov. 2019. – IEEE, 2019. – 6 p. - Mode of access: https://ieeexplore.ieee.org/document/8944715/ authors#authors. - Title from screen - ISBN 978-1-7281-0970-1. - DOI: 10.1109/Dynamics47113.2019.8944715.B

[12] Basinya E. A. Development of a comprehensive security system [Electronic resource] / E. A. Basinya, A. A. Yushmanov // Dynamics of systems, mechanisms and machines (DYNAMICS) : proc., 13 intern. sci. and techn. conf., Omsk, 5–7 Nov. 2019. – IEEE, 2019. – 7 p. - Mode of access: https://ieeexplore.ieee.org/document/8944700/ authors#authors. - Title from screen - DOI: 10.1109/Dynamics47113.2019.8944700.

[13] Basynya E. A. Method for forming a decentralized registry of the enterprise information infrastructure events / E. A. Basynya, A. V. Safronov // Bulletin of the Ural Federal District. Information security = Journal of the Ural Federal District Information security. - 2019. - No. 4 (34). - S. 35-44.

[14] Basynya E.A. Method to identify cybercriminals using network analysis of information systems with anonymization / E. A. Basynya, V. E. Khitsenko, A. A. Rudkovsky // Reports of the Tomsk State University of Control Systems and Radioelectronics. - 2019. - T. 22, No. 2. - P. 45–51. - DOI: 10.21293 / 1818-0442-2019-22-2-45-51.

[15] Basinya E. A. Implementation of an intrusion detection and prevention system module for corporate network traffic management / E. A. Basinya, Y. K. Ravtovich // Актуальные проблемы электронного приборостроения (АПЭП–2018) = Actual problems of electronic instrument engineering (APEIE–2018) : тр. 14 междунар. науч.-техн. конф., Новосибирск, 2–6 окт. 2018 г. : в 8 т. – Новосибирск : Изд-во НГТУ, 2018. – Т. 1, ч. 6. – С. 178-183. - 45 экз. - ISBN (NSTU) 978-5-7782-3614-1.

[16] Basinya E. A. Personal computer user`s activity monitoring software development for the enterprise business process optimizing / E. A. Basinya, S. V. Kazarbin // Актуальные проблемы электронного приборостроения (АПЭП–2018) = Actual problems of electronic instrument engineering (APEIE–2018) : тр. 14 междунар. науч.-техн. конф., Новосибирск, 2–6 окт. 2018 г. : в 8 т. – Новосибирск : Изд-во НГТУ, 2018. – Т. 1, ч. 6. – С. 174-177. - ISBN (NSTU) 978-5-7782-3614-1.

[17] Y. Lan, Y. Sun, S. Liu and Z. Ma, "A real-time network traffic analysis and QoS management platform", *Proceedings of the IEEE 9th International Conference on Communication Software and Networks (ICCSN)*, pp. 266-270, 2017.

[18] Basinya E. A. Design and study of the system of computer network traffic using the secure virtual communication channel technology / E. A. Basinya, A. V. Safronov // Актуальные проблемы электронного приборостроения (АПЭП–2016) = Actual problems of electronic instrument engineering (APEIE–2016) : тр. 13 междунар. науч.-техн. конф., Новосибирск, 3–6 окт. 2016 г. : в 12 т. – Новосибирск : Изд-во НГТУ, 2016. – Т. 1, ч. 3. – С. 132-134. - 60 экз. - ISBN 978-5-7782-2991-4.

[19] Basynya E.A., Safronov A.V. Development and research of a traffic control system for computer networks using the technology of secure virtual communication channels / E. A. Basynya, A. V. Safronov // Actual problems of electronic instrument engineering (APEP – 2016) = Actual problems of electronic instrument engineering (APEIE – 2016): tr. 13 int. scientific and technical Conf., Novosibirsk,

October 3–6. 2016: in 12 volumes - Novosibirsk: Publishing house of NSTU, 2016 .-- T. 10. - P. 163-165. - 50 copies. - ISBN 978-5-7782-2991-4.

[20] Basynya E. A. Development of a module for intrusion detection and prevention / E. A. Basynya, Yu. K. Ravtovich // Modern materials, equipment and technologies. - 2016. - No. 2 (5). - S. 26–32.

[21] L. Nie, "Traffic matrix estimation approach based on partial direct measurements in large-scale IP backbone networks", *Proceedings of the IEEE 5th International Conference on Electronics Information and Emergency Communication*, pp. 178-181, 2015.

[22] Basynya E.A.Method of traffic control at the gateways of local area networks / E. A. Basynya // Bulletin of the Samara Scientific Center of the Russian Academy of Sciences. - 2014. - T 16, No. 4 (3). - S. 507-511.

[23] Basynya EA Problems of traffic management of a packet-switched computer network based on the TCP / IP protocol stack. / EA Basynya // Technique and technology: new development prospects. - 2014. - No. 15. - S. 48-57. - The work was carried out with the financial support of the Ministry of Education and Science of the Russian Federation under state assignment No. 2014/138, the topic of the project is "New structures, models and algorithms for breakthrough methods of managing technical systems based on science-intensive results of intellectual activity."

[24] Basinya E. A. Methods of self-organization in providing network security / E. A. Basinya, G. A. Frantsuzova, A. V. Gunko // Global Science and Innovation : materials of the 1 intern. sci. conf., USA, Chicago, 17–18 Dec. 2013. – Chicago : Accent Graphics communications 2013. – Vol. 2. – P. 386-389.

[25] Basynya E. A. Optimal regulation of the throughput of a computer network by a self-organizing traffic control system / E. A. Basynya, G. A. Frantsuzova, A. V. Gun'ko // Modern trends in education and science: collection of articles. scientific. tr. based on materials from international. scientific-practical conf., 31 oct. 2013: at 26 o'clock - Tambov: Business Science-Society, 2013. - Part 5. - P. 13-14.

[26] Frantsuzova G.A. Application of artificial intelligence in the field of network information security / G. A. Frantsuzova, A. V. Gunko, E. A. Basynya // Artificial intelligence: philosophy, methodology, innovations: collection of articles. tr. 7 Vseros. conf. students, graduate students and young scientists, Moscow, November 13–15, 2013 - Moscow: Radio and Communication, 2013. - Part 2. Sections 4–6. - S. 110-115.

[27] Basynya E. A. Technology of traffic control of a computer network based on self-organizing systems / E. A. Basynya; scientific. hands. G. A. Frantsuzova; consultant A. V. Gun'ko // New information technologies in scientific research (NIT -2013): materials of the 18th All-Russian. scientific and technical conf. students, young scientists and specialists. - Ryazan: Publishing house of RGRTU, 2013 .-- P. 181-183.

[28] Frantsuzova G. A. Self-organizing traffic control system of a computer network: protection mechanisms against scanning and probing / G. A. Frantsuzova, A. V. Gunko, E. A. Basynya // Collection of scientific works Sworld. - 2013 .-- T. 9, no. 4. - P. 75–78. - Topic of issue. Promising innovations in science, education, production and transport – 2013.

[29] Gunko A.V. Stochastic methods of ensuring information network security / A.V. Gun'ko, E. A. Basynya // Actual problems of electronic instrumentation. Materials of the XI International Conference in 7 volumes. - Novosibirsk: Publishing house of NSTU, 2012.Vol. 7.P. 47-49

[30] Gunko A.V., Basynya E.A. Stochastic methods of traffic control of a computer network with packet switching / A. V. Gun'ko, E. A. Basynya // Nonlinear dynamic systems: modeling and optimization of control. Collection of abstracts of the International Youth Conference, pp. 5 - 7.