ISSN 1814-1196
Научный вестник НГТУ
том 73, № 4, 2018, с. 47–58

http://journals.nstu.ru/vestnik
Science Bulletin of the NSTU
Vol. 73, No. 4, 2018, pp. 47–58

ИНФОРМАТИКА,
ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
И УПРАВЛЕНИЕ

INFORMATICS,
COMPPUTER ENGINEERING
AND CONTROL

УДК 681.518.5+004.457 DOI: 10.17212/1814-1196-2018-4-47-58

An automated system of network and system administration of Windows and Linux family operating systems*

E.A. BASINYA

Novosibirsk State Technical University, 20, K. Marx Prospekt, Novosibirsk, 630073, Russian Federation; Institute of Information and Communication Technologies, 48, Deputatskaya Street, Novosibirsk, 630099, Russian Federation

director@nii-ikt.ru

Abstract

Today, the automation of technological and business processes of an enterprise is one of the key trends in the development of information and communication technologies. As part of the development of management methodology and organization of services in this area, Helpdesk and ServiceDesk user support systems are becoming increasingly popular. However, most existing solutions do not consider the vulnerabilities of the TCP/IP protocol stack as well as the imperfection of software and operating systems, which often complicates the activities of information technology departments by loading them with routine work. This article presents the development of an automated system of network and system administration of Windows and Linux family operating systems, which includes the Helpdesk and ServiceDesk solutions functionality. The signature method of the system operation with the identification of the correlation of events is reviewed. An original approach to creating a knowledge base of the system is described. The solution was implemented using a platform for automated deployment and management of applications in a virtualization environment, which provides an additional level of reliability and fault tolerance. An algorithm for checking third-party software solutions for suspicious malicious activity is proposed, providing a qualitative analysis of the object being investigated: whether functions undeclared by the developer are present, whether any information is being sent to third parties, etc. A comprehensive approach to the management of the enterprise network infrastructure is presented. In order to ensure information security of network communications, encapsulated secure virtual communication channels were used. To ensure the confidentiality of data on the client side, the AES-256 encryption algorithm was used. The proposed approaches are recommended for corporate computer networks which include ten or more hosts operating on the basis of the TCP / IP protocol stack and Windows / Linux family operating systems.

Keywords: technical support, customer requests processing automation, system of user support and request accounting, system and network administration, Helpdesk, ServiceDesk, ITIL, ITSM

* *Received 18 October 2018.*

INTRODUCTION

Automation of technological and business processes of an enterprise is one of the key trends in the development of information and communication technologies. Government agencies and commercial establishments design and implement corporate computer networks based on the TCP/IP protocol stack and Ethernet data link layer technology. The system and network administration of an organization's information infrastructure is not only a creative engineering task, but also an important tool for optimizing an enterprise's business processes. Accordingly, it significantly influences the economic performance of the company, as well as the level of its competitiveness in the market. In the early 1990s, a scientific community developed a unified approach to the management of information technology as a service, which should have an appropriate quality and ensure a consistently high level of user satisfaction. This methodology was described in the IT Infrastructure Library. In May 2007, its third edition was introduced, describing a new format of the services' lifecycle. Based on this library, a method of managing and organizing information technology services ITSM (IT Service Management) was developed, the key element of which was the user support systems: Helpdesk and ServiceDesk. The task of the first system was the accounting and management of user requests [1-3]. Originally, technical requests of a company's employees were being processed by the information technology department. Systems like ServiceDesk were a logical extension of the Helpdesk systems, expanding their functions of managing incidents and service requests in all areas of the company's activities [4]. In these systems, the functionality of providing feedback to users via various communication channels is implemented: e-mail, chat rooms, messengers, social networks, etc. This enabled forming a service-oriented service, which is a single point of interaction between the service provider and the user [5-7].

Under this topic, a lot of research and development work is carried out by Russian and foreign scientists, among them are Zabotina N.N., Zolnikova S.N., Sokolov N.E., TipikinYu.A., Odintsov I.V., Makhnovsky A. and many others [8-19].

It is worth noting that most of the proposed algorithms and methods allow improving the quality of customer service and profitability of economic activity. However, these solutions do not consider the vulnerabilities of the TCP / IP protocol stack and software imperfections, including operating systems. Business interests lower the priority of high-quality technical implementation, which often complicates the activities of information technology departments, loading them with routine work.

Information security issues are an integral part of the task of automating technological and business processes of an enterprise. Potential damage caused by the breach of confidentiality of commercial data may cause irreparable economic harm to the company.

1. PROBLEM STATEMENT

The aim of the work was to develop and study an automated system of network and system administration of the Windows and Linux family operating systems, including the functionality of the Helpdesk and ServiceDesk solutions.

An algorithm for checking third-party software solutions for suspicious malicious activity needed to be developed and included in the system. In this context particular importance was given to the potential absence of antiviral agents on the client side. It was necessary to ensure both the security of network communications and the confidentiality of data on the client side

2. DESIGN AND IMPLEMENTATION OF THE SYSTEM

The development and software implementation of the proposed network and system administration system of the Windows and Linux family operating systems was carried out in two versions. The first version was presented as an independent end product commissioned by a commercial holding. The second version was designed and implemented as a module of the system of intellectual and adaptive management of an enterprise's network infrastructure developed by the author.

This article presents the material of the second project implementation. At the design stage, the following functions of the developed system were embedded:

- receiving and processing requests through various communication channels (e-mail, online chat rooms, messengers, social networks, etc.), primary communication with customers or employees of the company;
- semantic analysis of the query text, an attempt to automatically solve the problem or provide a suitable article from the knowledge base;
- evaluation of the request, delegation to the most appropriate specialist in the absence of the possibility of applying the solution in automatic mode;
- accounting and tracking of requests and incidents;
- informing customers/employees about the status of requests and the progress of their execution;
- monitoring the level of service in accordance with the SLA agreement (Service Level Agreement);
- management of the lifecycle of incidents and requests, including their closure and verification;
- alerting, informing and coordinating employees and customers;
- providing tools of a flexible project maintenance methodology;
- processing and analysis of logs of the operating system and installed software in the enterprise corporate computer network;
- providing tools to verify third-party software solutions for suspicious malicious activity in corporate computer network;
- automatic identification and solution of local technical problems;
- monitoring network infrastructure of the enterprise;
- monitoring employee activity on personal computers;
- and many others.

The proposed original solutions in the field of system and network administration are worth considering in more detail. At first sight, processing and analyzing the logs of the operating system and the installed software is a rather trivial task. However, a simple example of the remote work of the user of the host A on the host B for one hour using the Remote Desktop Protocol (RDP) should be given. In the event log of the Windows operating system EVTX (XML Event Log) there

may appear more than 60 entries of entry/exit events with identical id instead of the expected two.

Another interesting example is the work with the volume shadow copy service, which can be accessed by various applications and services, including over the network. If this service fails, the number of events per minute can exceed 500 units, cyclically referring to each other. To compile an objective picture of what happened, it is necessary to collect additional information from the system, parse, process and analyze it. In order to meet such objectives, an enhanced signature approach with the identification of event correlation was integrated with the system. The initial knowledge base was compiled in a virtualization environment based on the ESXi hypervisor, which had more than 10 copies of each of the popular Windows and Linux family operating systems being deployed. Next, the tools of testing, passive and active analysis of operating systems and applications were used. For local testing, additional scripts which caused failures and malfunctions were written to check the reliability and fault tolerance of the software. During one hundred iterations of each individual network/local disturbance, the client-server model tracked the events being recorded and identified the correlation. Thus, the initial knowledge base was being compiled.

Importantly, each iteration was carried out towards the reference image of the operating system, a return to which was driven through snapshots system. Adding new entries to the general knowledge base of the corporate solution is being carried out only on the basis of similar results from 50% of clients with the number of hosts with identical software from 10 units.

This approach allowed us to perform automatic identification and solution of local technical problems. The situation with the problem of the receipt of the TCP/IP protocol stack settings by the host can serve as a simple example. The system identifies the failure of the DHCP-client service, tracks its dependencies on other services and finds the one being stopped. After that the system launches them in the correct order and restoring the full functioning of the service.

To implement the verification of third-party software solutions for suspicious malicious activity, an original algorithm was developed, shown in Figure 1.

This algorithm provides the technician and/or technically competent user with a qualitative analysis of the object being investigated: whether functions undeclared by the developer are present, whether any information is being sent to third parties, etc. However, it is important to note that the algorithm does not replace a full-fledged audit of the program code (including that being carried out through disassembly). It is also not possible to detect in a closed source code a tool for hidden data collection or information management (backdoor), if it was in passive ("sleeping") mode.

Monitoring of the enterprise network infrastructure is being carried out using network management protocols and a decentralized knowledge base of participants in the interaction of the corporate computer network. This includes control of the versions of the installed software and the hardware solutions used on each device. This functionality is fully implemented by the system of intellectual adaptive management of the enterprise network infrastructure, developed by the author. As noted previously, the network and system administration system of the Windows and Linux family operating systems is its integral part. The components of the client part of the system are illustrated in Figure 2.

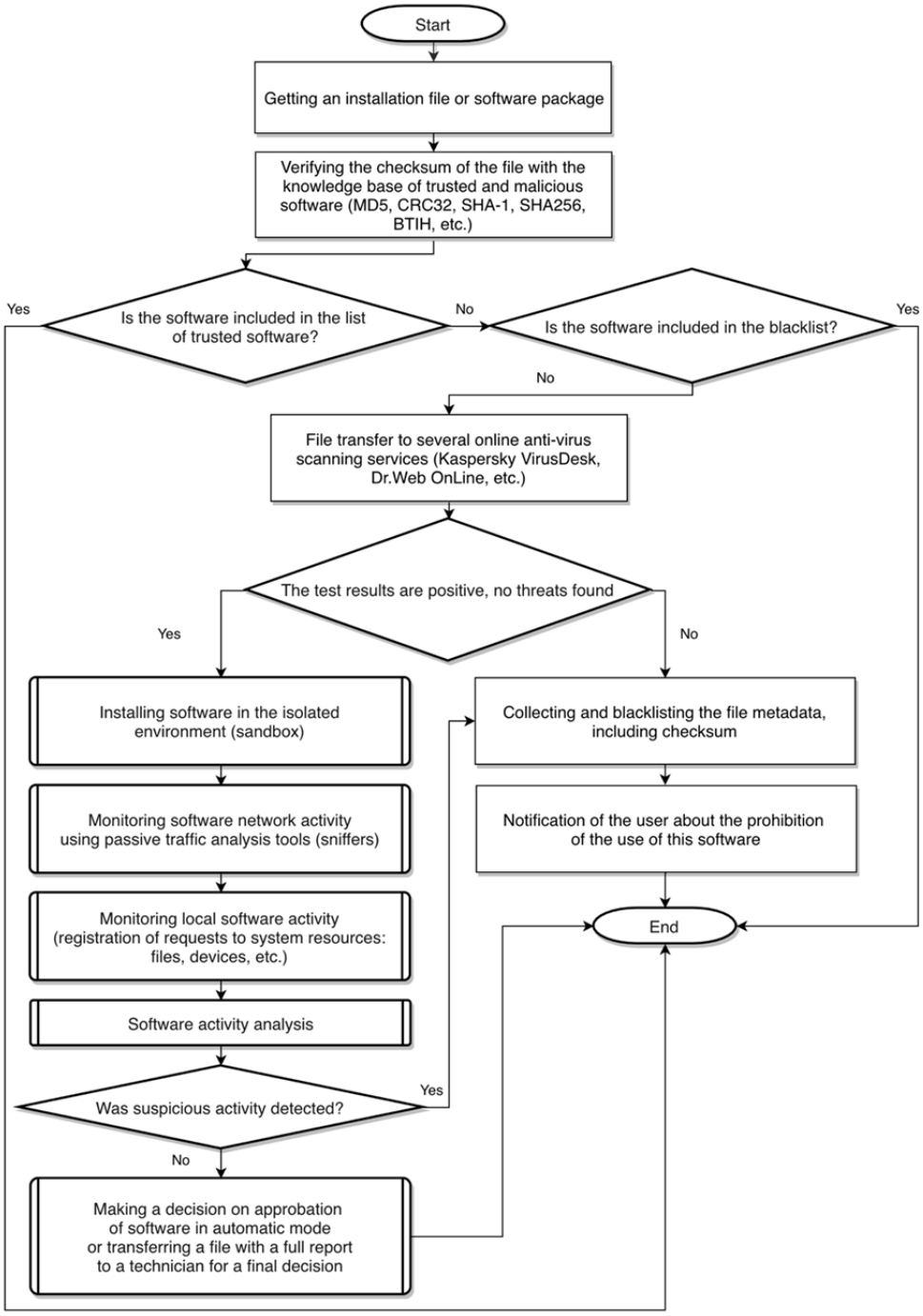

Fig. 1. An algorithm for checking third-party software solutions for suspicious malicious activity

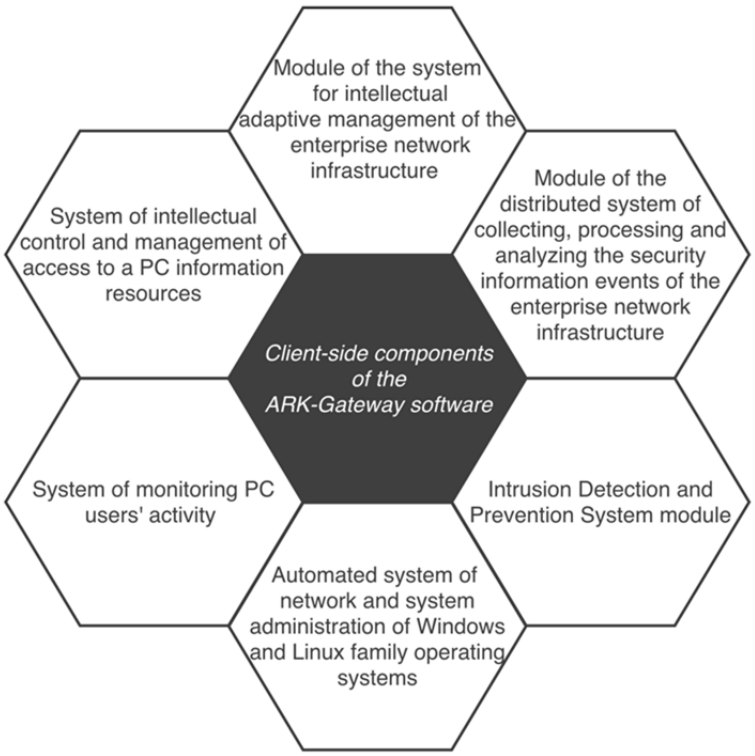

Fig. 2. The components of the client part of the system

The decision to use different components in the same client software implementation was made taking into account two factors. The first is the necessity of ensuring the comprehensive intelligent adaptive management of the enterprise network infrastructure. The second is the willingness to optimize the use of the computational power pool, since most components have overlapping functionality and access to the same resources. It is firstly referred to the operating system and application logs, however, in some cases, to the access to equipment. Thus, the system of intellectual control and management of access to information resources of a personal computer controls the connected data storage devices and used data transmission networks. The purpose of these actions is to prevent illegal copying of information. At the same time, an automated network and system administration system monitors the operation of hardware resources in order to provide reliable and fault-tolerant functioning of the host.

During the work, the architecture of the server part of the system was designed and implemented, as shown in Figure 3.

The software solution was created using the platform for applications automated deployment and management in a virtualization environment. This ensures a high level of reliability and fault tolerance of the system.

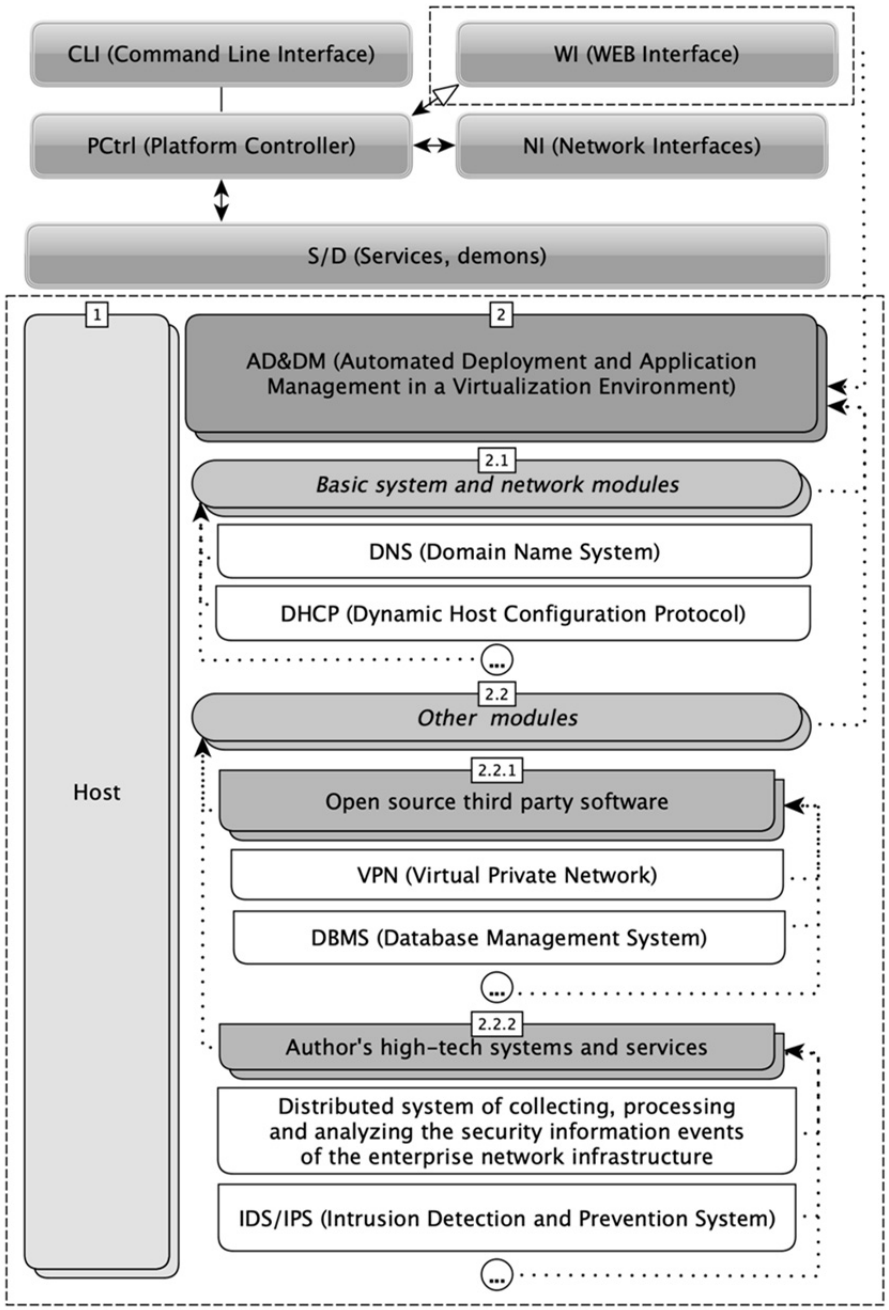

Fig. 3. The architecture of the server part of the system

The software implementation of the server part was performed using Python, Flask, C ++, Bash, Docker, Ansible on the basis of AlpineLinux OS. The client module for Windows family operating systems was written in the C# programming language using native controls from the Windows Forms .NET library. For the Linux family, Python and the Qt framework were used. Encapsulated virtual secure communication channels (VPN, Virtual Private Network) helped to ensure the protection of data transmission over the network. Depending on the project build, the

following technologies were used: Gate VPN, GoVPN, Tinc, Wire Guard, Free-LAN, Open VPN, IPsec and others. Secure local data storage was provided by the symmetric block encryption algorithm AES-256 (Advanced Encryption Standard).

Both during the development and afterwards, manual and automated testing of the developed software product (client and server parts, as well as their interaction) was performed.

The developed solution significantly extends the existing systems such as Helpdesk and ServiceDesk. The integration of the first version of the system at the customer's enterprise (with a number of hosts of more than 500 units) allowed to optimize the work of the information technology department and to reduce the time costs for system and network administration of the existing infrastructure of the company by 70%.The general knowledge base of the system is not updated in enterprises with fewer than ten hosts, which may be mentioned as a disadvantage of the proposed approach. Adding new entries to the general knowledge base of the corporate solution is carried out only on the basis of similar results from 50% of clients with the number of hosts with identical software from 10 units. The described development has been registered as an object of intellectual property [20].

CONCLUSION

In this paper the design and implementation of an automated network and system administration system for Windows and Linux family operating systems, which includes the Helpdesk and ServiceDesk solutions functionality, is presented. The signature method of the operation of the system with the identification of the correlation of events is reviewed. An original approach to creating a knowledge base of the system is described. The solution was implemented using a platform for automated deployment and management of applications in a virtualization environment, which provides an additional level of reliability and fault tolerance. An algorithm for checking third-party software solutions for suspicious malicious activity is proposed, providing a qualitative analysis of the object being investigated: respective of whether functions undeclared by the developer are present or whether any information is being sent to third parties, etc. A comprehensive approach to the management of an enterprise network infrastructure is also reviewed. In order to ensure information security of network communications, encapsulated secure virtual communication channels were used, while the AES-256 encryption algorithm was used to ensure data privacy on the client side.

The proposed approaches are recommended for use in enterprise network infrastructure management systems with a number of hosts from ten units operating on the basis of the TCP/IP protocol stack and the Windows/Linux family operating systems.

REFERENCES

1. Glushenko S.A., Dolzhenko A.I., Maleev D.V. Razrabotka sistemy Helpdesk dlya otdela soprovozhdeniya OOO "Elektronnaya meditsina" [Development system Helpdesk for maintenance department of "Electronic medicine"]. *Vestnik Rostovskogo gosudarstvennogo ekonomicheskogo universiteta (RINKh) – Vestnik of Rostov state university of economics (RINH)*, 2016, no. 2 (54), pp. 93–102.

2. Nikiforov O.Yu. Pokazateli effektivnosti vnedreniya sistemy Help Desk i edinoi uchetnoi zapisi [Performance indicators for the implementation of the help desk system and a single account]. *Novaum.ru*, 2018, no. 12, pp. 24–26. (In Russian).

3. Prakhin D. Sistema vsDesk. Bol'shoi pomoshchnik malen'kogo IT-otdela [VSDESK system. A great assistant to a small IT department]. *Sistemnyi administrator – System Administrator*, 2015, no. 10 (155), pp. 9–15.

4. Golosov D. ManageEngine ServiceDesk Plus. Ch. 2. Obzor vozmozhnostei [ManageEngine ServiceDesk Plus. Pt. 2. Overview of features]. *Sistemnyi administrator – System Administrator*, 2015, no. 12 (157), pp. 14–20.

5. Lyamukov S. Universal'nyi ITSM [Universal ITSM]. *Otkrytye sistemy. SUBD – Open Systems. DBMS*, 2014, no. 3, pp. 22–26.

6. Sterlyagov S.P., Bezmaternykh N.A. Sovershenstvovanie deyatel'nosti otdela informatsionnykh tekhnologii nalogovoi inspektsii na osnove metodologii ITSM/ITIL [Improvement of the activity of the information technology department of the tax inspection on the basis of the ITSM/ITIL methodology]. *Internet-zhurnal Naukovedenie – Online journal science research*, 2017, vol. 9, no. 3, pp. 1–13.

7. Golosov D. Avtomatizatsiya raboty IT-podrazdeleniya s pomoshch'yu ITSM-sistemy [Automation of the IT department using ITSM-system]. *Sistemnyi administrator – System Administrator*, 2015, no. 7–8 (152–153), pp. 9–13.

8. Zabotina N.N., Vasil'kov Yu.V., Gushchina L.S. Upravlenie intsidentami v IT-infrastrukture predpriyatiya [Incident management in the enterprise IT infrastructure]. *Informatizatsiya i svyaz' – Informatization and communication,* 2016, no. 2, pp. 31–35.

9. Malaev A.N. Kachestvo operativnogo upravleniya v sfere tekhnicheskoi podderzhki bankovskikh ustroistv samoobsluzhivaniya [Quality of operational management in the field of technical support of self-service banking devices]. *Izvestiya Orenburgskogo gosudarstvennogo agrarnogo universiteta – Izvestia Orenburg State Agrarian University*, 2015, no. 1 (51), pp. 223–225.

10. Zol'nikova S.N., Deberdieva E.M. Povyshenie effektivnosti deyatel'nosti IT-podrazdeleniya [Improving the efficiency of the IT department]. *Ekonomika i predprinimatel'stvo – Journal of Economy and Entrepreneurship*, 2014, no. 11-3 (52), pp. 364–368.

11. Kokunov V.A., Sokolov N.E., Sharabaeva L.Yu. Problemy vnedreniya i soprovozhdeniya informatsionnykh sistem [Problems of implementation and maintenance of information systems]. *Upravlencheskoe konsul'tirovanie – Administrative Consulting*, 2014, no. 9 (69), pp. 146–153.

12. Sergeeva A. Raspredelennye virtual'nye stendy dlya testirovaniya veb-servernykh prilozhenii [Distributed virtual stands for testing web server applications]. *Sistemnyi administrator – System Administrator*, 2014, no. 11 (144), pp. 78–84.

13. Yuzhanin N.V., Tipikin Yu.A., Gankevich I.G., Zolotarev V.I. Computational task tracking complex in the scientific project informational support system. *Komp'yuternye issledovaniya i modelirovanie – Computer Research and Modeling*, 2015, vol. 7, no. 3, pp. 615–620.

14. Ponachugin A.V., Odintsov I.V. Sistema kontrolya za nesanktsionirovannoi deyatel'nost'yu pol'zovatelei komp'yuternoi seti [Control system for unauthorized activity of computer network users]. *Programmnye sistemy i vychislitel'nye metody – Software systems and computational methods*, 2016, no. 1, pp. 23–31.

15. Latypova O.Yu., Agievich V.A., Nagoryanskii O.N. Primenenie sistemy pokazatelei dlya sovershenstvovaniya protsessa upravleniya podderzhkoi pol'zovatelei na osnove metodologii COBIT 5 [Application of the scorecard to improve the process of managing user support based on the COBIT 5 methodology]. *Vestnik kibernetiki – Proceedings in Cybernetics*, 2015, no. 3 (19), pp. 186–192.

16. Efremova L.I., Kurganov A.N. Formirovanie portfelya prikladnykh sistem dlya predpriyatiya gazodobyvayushchei otrasli [Formation of a portfolio of application systems for the gas industry]. *Informatsionnye sistemy i tekhnologii – Information Systems and Technologies*, 2017, no. 3 (101), pp. 57–66.

17. Filippov O. Instrumenty tekhnicheskoi podderzhki filial'noi seti [Branch network technical support tools]. *Sistemnyi administrator – System Administrator*, 2017, no. 4 (173), pp. 34–37.

18. Grishakov V.G., Frolov D.V. Modelirovanie v sisteme tekhnicheskoi podderzhki vychislitel'nykh klasterov [Modeling in the system of technical support for computing clusters]. *Programmnye produkty i sistemy – Software & Systems*, 2014, no. 3, pp. 72–78.

19. Makhnovskii A. Integratsiya IDM v IT-infrastrukturu predpriyatiya [IDM integration into enterprise IT infrastructure]. *Zashchita informatsii. Insaid*, 2015, no. 1 (61), pp. 18–19. (In Russian).

20. Basinya E.A. *Avtomatizirovannaya sistema setevogo i sistemnogo administrirovaniya operatsionnykh sistem semeistva Windows i Linux* [Automated system of network and system administration of Windows and Linux family operating systems]. The Certificate on official registration of the computer program. No. 2018662438, 2018.

Басыня Евгений Александрович, кандидат технических наук, доцент кафедры автоматики Новосибирского государственного технического университета, директор Научно-исследовательского института информационно-коммуникационных технологий. Основные направления научных исследований: сетевая информационная безопасность, оверлейные технологии, автоматизация и управление в области информационных технологий. Имеет более 30 публикаций. E-mail:director@nii-ikt.ru

Basinya Evgeny Alexandrovich, PhD (Eng.), an associate professor at the automation department in the Novosibirsk State Technical University, director of the Research InstiIute of information-Communication Technologies. His research interests are focused on network information security, overlay technologies, automation and management in the field of information technologies. He has published more than 30 scientific papers. E-mail:director@nii-ikt.ru

DOI: 10.17212/1814-1196-2018-4-47-58

Автоматизированная система сетевого и системного администрирования операционных систем семейства Windows и Linux[*]

Е.А. БАСЫНЯ

630073, РФ, г. Новосибирск, пр-т К. Маркса, 20, Новосибирский государственный технический университет; 630099, РФ, г. Новосибирск, ул. Депутатская, 48, Научно-исследовательский институт информационно-коммуникационных технологий

director@nii-ikt.ru

На сегодняшний день автоматизация технологических и бизнес-процессов предприятия является одним из ключевых трендов развития информационно-коммуникационных технологий. В рамках развития методологии управления и организации услуг в данной сфере все большую популярность приобретают системы поддержки пользователей Helpdesk и ServiceDesk. Однако большинство существующих решений не учитывают уязвимости стека протоколов TCP/IP и несовершенство программного обеспечения, в том числе и операционных систем, что зачастую усложняет деятельность отделов информационных технологий. В данной статье представлена разработка автоматизированной системы сетевого и системного администрирования операционных систем семейства Windows и Linux, включающей функционал Helpdesk и ServiceDesk решений. На обзор вынесен сигнатурный метод ее функционирования с идентификацией корреляции событий. Описан оригинальный подход составления базы знаний

[*] *Статья получена 18 октября 2018 г.*

системы. Решение выполнено с использованием платформы автоматизации развертывания и управления приложениями в среде виртуализации, что предоставляет дополнительный уровень надежности и отказоустойчивости. Предложен алгоритм проверки программных решений сторонних разработчиков на предмет подозрительной вредоносной активности, предоставляющий качественный анализ исследуемого объекта: присутствуют ли незадекларированные разработчиком функции, отсылается ли какая-то информация третьим лицам и т. д. Представлен комплексный подход к управлению сетевой инфраструктурой предприятия. Для обеспечения информационной безопасности сетевых коммуникаций использовались инкапсулированные защищенные виртуальные каналы связи. Для обеспечения конфиденциальности данных на стороне клиента был задействован алгоритм шифрования AES-256. Предложенные подходы рекомендуются к применению в корпоративных вычислительных сетях с количеством хостов от десяти единиц, функционирующих на основе стека протоколов TCP/IP, и операционных системах семейства Windows/Linux.

Ключевые слова: техническая поддержка, автоматизация обработки запросов клиентов, системы поддержки пользователей и учета заявок, системное и сетевое администрирование, Helpdesk, ServiceDesk, ITIL, ITSM

СПИСОК ЛИТЕРАТУРЫ

1. *Глушенко С.А., Долженко А.И., Малеев Д.В.* Разработка системы Helpdesk для отдела сопровождения ООО «Электронная медицина» // Вестник Ростовского государственного экономического университета (РИНХ). – 2016. – № 2 (54). – С. 93–102.

2. *Никифоров О.Ю.* Показатели эффективности внедрения системы Help Desk и единой учетной записи // Novaum.ru. – 2018. – № 12. – С. 24–26.

3. *Прахин Д.* Система vsDesk. Большой помощник маленького ИТ-отдела // Системный администратор. – 2015. – № 10 (155). – С. 9–15.

4. *Голосов Д.* ManageEngine ServiceDesk Plus. Ч. 2. Обзор возможностей // Системный администратор. – 2015. – № 12 (157). – С. 14–20.

5. *Лямуков С.* Универсальный ITSM // Открытые системы. СУБД. – 2014. – № 3. – С. 22–26.

6. *Стерлягов С.П., Безматерных Н.А.* Совершенствование деятельности отдела информационных технологий налоговой инспекции на основе методологии ITSM/ITIL // Интернет-журнал «Науковедение». – 2017. – Т. 9, № 3. – С. 1–13.

7. *Голосов Д.* Автоматизация работы ИТ-подразделения с помощью ITSM-системы // Системный администратор. – 2015. – № 7–8 (152–153). – С. 9–13.

8. *Заботина Н.Н., Васильков Ю.В., Гущина Л.С.* Управление инцидентами в ИТ-инфраструктуре предприятия // Информатизация и связь. – 2016. – № 2. – С. 31–35.

9. *Малаев А.Н.* Качество оперативного управления в сфере технической поддержки банковских устройств самообслуживания // Известия Оренбургского государственного аграрного университета. – 2015. – № 1 (51). – С. 223–225.

10. *Зольникова С.Н., Дебердиева Е.М.* Повышение эффективности деятельности ИТ-подразделения // Экономика и предпринимательство. – 2014. – № 11-3 (52). – С. 364–368.

11. *Кокунов В.А., Соколов Н.Е., Шарабаева Л.Ю.* Проблемы внедрения и сопровождения информационных систем // Управленческое консультирование. – 2014. – № 9 (69). – С. 146–153.

12. *Сергеева А.* Распределенные виртуальные стенды для тестирования веб-серверных приложений // Системный администратор. – 2014. – № 11 (144). – С. 78–84.

13. Computational task tracking complex in the scientific project informational support system / N.V. Yuzhanin, Yu.A. Tipikin, I.G. Gankevich, V.I. Zolotarev // Компьютерные исследования и моделирование. – 2015. – Т. 7, № 3. – С. 615–620.

14. *Поначугин А.В., Одинцов И.В.* Система контроля за несанкционированной деятельностью пользователей компьютерной сети // Программные системы и вычислительные методы. – 2016. – № 1. – С. 23–31.

15. *Латыпова О.Ю., Агиевич В.А., Нагорянский О.Н.* Применение системы показателей для совершенствования процесса управления поддержкой пользователей на основе методологии COBIT 5 // Вестник кибернетики. – 2015. – № 3 (19). – С. 186–192.

16. *Ефремова Л.И., Курганов А.Н.* Формирование портфеля прикладных систем для предприятия газодобывающей отрасли // Информационные системы и технологии. – 2017. – № 3 (101). – С. 57–66.

17. *Филиппов О.* Инструменты технической поддержки филиальной сети // Системный администратор. – 2017. – № 4 (173). – С. 34–37.

18. *Гришаков В.Г., Фролов Д.В.* Моделирование в системе технической поддержки вычислительных кластеров // Программные продукты и системы. – 2014. – № 3. – С. 72–78.

19. *Махновский А.* Интеграция IDM в ИТ-инфраструктуру предприятия // Защита информации. Инсайд. – 2015. – № 1 (61). – С. 18–19.

20. Автоматизированная система сетевого и системного администрирования операционных систем семейства Windows и Linux: свидетельство о гос. регистрации программы для ЭВМ № 2018662438 / Е.А. Басыня. – Зарег. 08.10.2018.

For citation:

Basinya E.A. Avtomatizirovannaya sistema setevogo i sistemnogo administrirovaniya operatsionnykh sistem semeistva Windows i Linux [An automated system of network and system administration of Windows and Linux family operating systems]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Science bulletin of the Novosibirsk state technical university*, 2018, no. 4 (73), pp. 47–58. doi: 10.17212/1814-1196-2018-4-47-58.

Для цитирования:

Басыня Е.А. Автоматизированная система сетевого и системного администрирования операционных систем семейства Windows и Linux // Научный вестник НГТУ. – 2018. – № 4 (73). – С. 47–58. – Яз. англ. – doi: 10.17212/1814-1196-2018-4-47-58.