ISSN 2500-316X (Online)

UDC 004.9
https://doi.org/10.32362/2500-316X-2021-9-6-16-25

RESEARCH ARTICLE

The development of models of an analytical data processing system for monitoring information security of an informatization object using cloud infrastructure

Valerii A. Sizov,
Aleksey D. Kirov @

Plekhanov Russian University of Economics, Moscow, 117997 Russia
@ *Corresponding author, e-mail: kirov.ad@rea.ru*

Abstract. The article is devoted to the problem of developing an analytical data processing system (ADPS) for monitoring information security within the information security management system of modern companies conducting their main activities in cyberspace and using cloud infrastructure. Based on the analysis of modern information technologies related to ensuring information security of cloud infrastructure and the most popular products for ensuring information security of cloud infrastructures, as well as existing scientific approaches, a formalized approach to the synthesis of an ADPS for monitoring the information security of an informatization object using cloud infrastructure is proposed. This approach takes into account the usefulness of the used information technologies from the viewpoint of information security. A general model of the structure of information support of an analytical data processing system for monitoring information security, as well as a model of the dependence of the usefulness of information technology on time and the ratio of the skill level of an information security specialist and an attacker are presented. The quality of the information security monitoring system is used as a criterion in the first optimization model. The following limitations are suggested: limitation on the time of making a decision on an incident; limitation on the degree of quality of analysis of information security events by the analytical data processing system and limitation on the compatibility of data analysis functions with data types about information security events. The cited results of the study of the second model show a logically consistent dependence of the usefulness of information technology on time and the ratio of the skill level of an information security specialist to the skill level of an attacker. The particular models of the structure of the information support of ADPS are presented. They make it possible to determine the rational structure information support of ADPS according to particular criteria. The following particular criteria are used: the maximin criterion of the usefulness of the information support of ADPS for monitoring the information security of an informatization object in the cloud infrastructure; the criterion for the maximum relevance of information support distributed over the nodes of the cloud infrastructure for systems with a low degree of centralization of management.

Keywords: information security, analytical data processing system, cloud infrastructure, computer modeling, mathematical modeling, information security monitoring, object of informatization

• **Submitted:** 25.03.2021 • **Revised:** 11.05.2021 • **Accepted:** 25.07.2021

For citation: Sizov V.A., Kirov A.D. The development of models of an analytical data processing system for monitoring information security of an informatization object using cloud infrastructure. *Russ. Technol. J.* 2021;9(6):16–25. https://doi.org/10.32362/2500316X-2021-9-6-16-25

Financial disclosure: The authors have no a financial or property interest in any material or method mentioned.

The authors declare no conflicts of interest.

НАУЧНАЯ СТАТЬЯ

Разработка моделей аналитической системы обработки данных для мониторинга ИБ объекта информатизации, использующего облачную инфраструктуру

В.А. Сизов,
А.Д. Киров @

Российский экономический университет имени Г.В. Плеханова, Москва, 117997 Россия
@ *Автор для переписки, e-mail: kirov.ad@rea.ru*

Резюме. Статья посвящена разработке аналитической системы обработки данных (АСОД) для мониторинга информационной безопасности (ИБ) в рамках системы менеджмента ИБ современных компаний, ведущих свою основную деятельность в киберпространстве и использующих облачную инфраструктуру. На основе анализа современных информационных технологий (ИТ) и наиболее востребованных продуктов обеспечения ИБ облачных инфраструктур, а также существующих научных подходов предложен формализованный подход к синтезу АСОД для мониторинга ИБ такого объекта информатизации. Этот подход учитывает полезность используемых ИТ с позиции ИБ. Представлена общая модель структуры информационного обеспечения АСОД для мониторинга ИБ, а также модель зависимости полезности ИТ от времени и соотношения уровня квалификации специалиста по ИБ и злоумышленника. В качестве критерия в первой оптимизационной модели используется качество системы мониторинга ИБ. В качестве ограничений предлагаются следующие: ограничение на время принятия решения на инцидент; ограничение на степень качества анализа событий ИБ аналитической системой обработки данных и ограничение на совместимость функций анализа данных с типами данных о событиях ИБ. Приведенные результаты исследования второй модели показывают логически непротиворечивую зависимость полезности ИТ от времени и соотношения уровня квалификации специалиста по ИБ к уровню квалификации злоумышленника. Представлены частные модели структуры информационного обеспечения АСОД, позволяющие определить рациональную структуру информационного обеспечения АСОД по частным критериям. В качестве частных критериев используются следующие: максиминный критерий полезности информационного обеспечения АСОД для мониторинга ИБ объекта информатизации в облачной инфраструктуре и критерий максимума актуальности информационного обеспечения, распределенного по узлам облачной инфраструктуры для систем с невысокой степенью централизации управления.

Ключевые слова: информационная безопасность, аналитическая система обработки данных, облачная инфраструктура, компьютерное моделирование, математическое моделирование, мониторинг ИБ, объект информатизации

• **Поступила:** 25.03.2021 • **Доработана:** 11.05.2021 • **Принята к опубликованию:** 25.07.2021

Для цитирования: Сизов В.А., Киров А.Д. Разработка моделей аналитической системы обработки данных для мониторинга ИБ объекта информатизации, использующего облачную инфраструктуру. *Russ. Technol. J.* 2021;9(6):16–25. https://doi.org/10.32362/2500-316X-2021-9-6-16-25

Прозрачность финансовой деятельности: Никто из авторов не имеет финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

INTRODUCTION

Analytical data processing systems (ADPS) for information security (IS) monitoring are a large emerging class of systems operating in the IS management system of modern companies.

Modern companies with main activities in cyberspace, using cloud infrastructure built on the technologies of cloud infrastructure service providers, use these systems to manage IS and to improve processes that implement IS methods, including monitoring processes in real time. The peculiarities of the technical implementation of such analytical systems determine special requirements for the convenience of their use by an IS engineer, efficiency, error-free operation, and quality of data processing in real time. In addition, the potential costs of a cloud service user for the transition from one service provider to another are characterized by the relationship between the consequences in the field of IS arising from cyber attacks, system failures, user errors, and other external factors and the difference in the levels of cybersecurity technologies of providers. Therefore, the level of IS provided by a cloud service provider is subject to the same tough conditions of bilateral market competition, which determines the prices of a cloud service provider and its strategy for providing customers with IS.

New information technologies (IT) actualize the problem of ensuring the security and protection of information for their developers, vendors and consumers. Currently, it is believed that the most effective way to ensure IS for the objects of informatization of the company and/or the cloud infrastructure used by it is the path of development and implementation of secure IT. Their use in cloud infrastructures can further reduce the cost of maintaining corporate information systems. A large number of modern IT used in cloud infrastructure is aimed at a comprehensive solution to the problem of increasing the efficiency of using available resources (Table 1).

The cloud infrastructure used to host corporate information systems is increasingly taking on a hybrid form. Part of the data most critical for the functioning of business processes is placed inside the company's own infrastructure using universal cloud technologies, forming a "private cloud of the company." Other data, in turn, are processed in "public clouds," where infrastructure is provided by cloud providers in an "Infrastructure as a Service," "Platform as a Service," or "Software as a Service" model. This necessitates the use of modern data security technologies in cloud infrastructures. Being integrated with modern data processing technologies, such technologies turn into full-fledged high-tech products offered by the leading companies in the market of IS products for cloud infrastructures. Examples of such products are presented in Table 2.

The analysis of the presented technologies showed their complexity. For their development and improvement, it is necessary to apply a scientific approach, including methods of mathematical and computer simulation.

In [5], an overview of the maturity models of the capabilities and indicators of the security of systems is presented. It is noted that these models are mostly reactive rather than proactive and, therefore, do not

Table 1. The content of modern IT related to the provision of IS in the cloud infrastructure

No.	IT name	Content
1	Data Center Network (DCN) [1]	Network equipment that allows one to automatically allocate the load on local area networks (LANs) of the cloud infrastructure (both on the cloud network equipment itself and on communication channels), provided as a service.
2	Proactive resource allocation [2]	A technology that allows one to automatically allocate cloud infrastructure resources (hardware resources in the form of cloud servers and workstations and software resources in the form of software, including tools for its development and debugging), provided as a service, based on predicting the expected load.
3	Self-diagnosis software [3]	A technology designed to automatically detect and correct errors that occur during the operation of software and the implementation of its functions.
4	Data encryption in cloud infrastructures [4]	A technology designed for distributed data encryption without using a single distribution and certification center.

Table 2. Purpose of modern products for IS of cloud infrastructures

No.	Product name for IS in cloud infrastructures	Manufacturer of IS product in cloud infrastructures	Purpose
1	MVision Cloud	McAfee	Creation of a "dynamic protection perimeter" capable of adapting to the dynamic conditions of the external environment. Create security policies and apply them to SaaS, PaaS, IaaS solutions, containers and virtual cloud components.
2	Cisco Cloud Security	Cisco	Protect users, data, and applications in the cloud from compromised account attacks, malware, and data leaks, no matter where they are or where they access the Internet. Neutralizing malware before it spreads to the network or endpoints and shortens recovery time from infection.
3	FortiGate-VM	FortiNet	High-speed VPN connections are used to protect data. Security policies are enforced in all environments. Cloud Security Center provides a centralized and consistent implementation of corporate network security and communications, and maintains secure connectivity of networks, locations, clouds, and data centers.
4	Kaspersky Security for virtual and loud environments	Kaspersky Laboratory	Simultaneous implementation of both the protection of the work environment and the concept of "security as code," which ensures continuous integration of workflows and bridging the cybersecurity gap in development environments.
5	CheckPoint CloudGuard	CheckPoint	Support of the widest range of cloud infrastructures including AWS, Microsoft Azure and Azure Stack, Google Cloud Platform, VMware Cloud on AWS, and more. Automatic provisioning and automatic scaling, along with automatic policy updates, ensures that defenses keep up with changes in your cloud. One unified console provides consistent visibility, policy management, logging, reporting, and control across all cloud environments and networks.

provide adequate measures to assess the overall security of the cloud system. Therefore, this paper proposes a Cloud Security Capabilities Maturity Model that augments existing cybersecurity models with a security metric. In [6], a methodology is presented to determine the best security measures for multi-cloud applications whose components are deployed in heterogeneous clouds. The methodology is based on application decomposition and threat modeling on components, followed by risk analysis along with capturing cloud business and security requirements. However, in these works, insufficient attention is paid to the processes and technologies of IS monitoring, which significantly affect the quality of its output information (completeness, relevance, timeliness, etc.).

The output information generated by ADPS is a collection of data obtained as a result of performing sets of data analytics functions included in its composition with a certain structure or several possible types of structures. Such collections of data can be used either in the current system, or redirected to other systems present in this cloud infrastructure. The quality of the ADPS output information is the degree of its suitability for use in detecting and investigating IS incidents by a security officer.

Computer modeling is one of the main methods proposed to improve the quality of data obtained as a result of the analysis of IS monitoring data using ADPS.

PROBLEM STATEMENT

Modern IS monitoring systems are created to ensure the possibility of an adequate and timely response to cyber attacks aimed at the information infrastructure of the electronic document management system and IS management of the company, which is the main component necessary for a prompt and strategic response to current threats, in accordance with the company's IS policy. Such infrastructure can be built on the basis of LAN technologies, constituting a "private cloud of the company" and/or in the form of cloud infrastructures provided by cloud service providers, constituting a "public cloud of the company."

To create an effective IS management system, a company needs to automate its management functions as much as possible, taking into account modern requirements for IS monitoring and the characteristics of hybrid cloud infrastructures.

Thus, the task of developing models of an analytical data processing system for monitoring the IS of an informatization object using cloud infrastructure is urgent. It is advisable to divide this task into a number of subtasks.

The first subtask is to develop a general model of the structure of the information support of the analytical data processing system for IS monitoring. The solution of this problem allows one to determine rational solutions close to the optimal, which are certain sets of information elements distributed over the nodes of the ADPS computer network.

The second subtask is to determine the nature and degree of dependence of the usefulness of information technology on time and the ratio of the qualification level of an IS specialist and the skill level of an attacker. The solution to this problem allows us to identify the conditions under which the utility of IT will be the best.

The third subtask is the development of a set of private models of the ADPS information support structure for monitoring the IS of an informatization object in a cloud infrastructure. The solution to this problem allows us to determine the rational structure of information support for ADPS according to particular criteria [7, 8].

DEVELOPMENT OF A GENERAL MODEL OF THE INFORMATION SUPPORT STRUCTURE OF THE ADPS FOR MONITORING IS

Let:

$$\theta = F(\delta, t), \tag{1}$$

where θ is the quality of the IS monitoring system; F is the quality function of the IS monitoring system; $\delta = G(R)$, where δ is the quality of the analysis of events of the ADPS IS; t is the time required for the analytical data processing system to make a decision on how likely it is that a particular IS event or their combination is an IS incident; G is a function of the quality of the analysis of events of the ADPS IS;

$$R = H(S),$$

where R is the degree of compatibility of data analysis procedures with data types about IS events; H is a function of the degree of compatibility of data analysis procedures with data types about IS events; S is the structure of information support for ADPS (sets of information elements distributed over the nodes of the ADPS computer network: data on IS events, additional data for the analysis and investigation of IS incidents).

Then the general model of the structure of the information support of the analytical data processing system for IS monitoring is as follows:

Find $\max\limits_{\{S\}} \theta$ under constraints:

$$t1 < t2;\ \delta 1 < \delta < \delta 2;\ R1 < R < R2, \tag{2}$$

where $t1$–$t2$ is the time period for which it is necessary to make a decision as to how likely it is that a particular IS event or their combination is an IS incident for the most effective response to this incident and its investigation;

$\delta 1$–$\delta 2$ are the limits of the degree of quality of the analysis of IS events by the analytical data processing system, which make it possible to make a decision as to how likely it is that a particular IS event or their combination is an IS incident with the required degree of reliability;

$R1$–$R2$ are the limits of the degree of compatibility of data analysis functions with types of data on IS events, in which it is possible to make a decision as to how likely it is that a particular IS event or their combination is an IS incident.

DEVELOPMENT OF A MODEL OF DEPENDENCE OF THE USEFULNESS OF INFORMATION TECHNOLOGY ON TIME AND THE RATIO OF THE QUALIFICATION LEVEL OF AN IS SPECIALIST AND AN ATTACKER

To develop a model of the dependence of usefulness of information technology on time and the ratio of the skill level of an IS specialist and an attacker, it is proposed to use an analytical model based on the Rayleigh statistical distribution [9]. The ratio of the skill level of an IS specialist who eliminates vulnerabilities in software and hardware to the skill level of an attacker who attacks software and hardware that implements IT is used as a parameter of the Rayleigh distribution scale.

The assessment of the dependence of the utility of information technology on time and the ratio of skill levels of these categories is as follows:

$$P(t,\sigma) = 1 - \frac{t}{\sigma^2} \mathrm{e}^{-\frac{t}{2\sigma^2}},\ t \geq 0,\ \sigma > 0, \tag{3}$$

where P is the level of IT usefulness at time t; σ is the ratio of the quantitative evaluation of the qualification level of an IS specialist to the skill level of the attacker.

The correspondence between quantitative and qualitative assessment of the qualification levels of an IS specialist and an attacker is given in Tables 3 and 4, respectively. In the case when the opposing sides are groups of people, it is necessary to apply group quantitative assessments of the level of their qualifications to them [10]. The final matrix of relationships between quantitative assessments of the qualification levels of an IS specialist and the skill level of an attacker is presented in Table 5.

The analysis of graphs in Fig. 1 shows that with an increase in the skill level of an attacker, the usefulness of IT for users decreases faster, and with an increase in the level of qualification of an IS specialist, the usefulness of IT for users quickly returns to the maximum value, which corresponds to reality.

Table 3. Correspondence of quantitative and qualitative assessments of qualification levels of an IS specialist

IS specialist class	Qualitative assessment of the qualification level of an IS specialist	Quantitative assessment of the qualification level of an IS specialist
Highly qualified specialist	High	1
Ordinary specialist	Intermediate	2
Low-skilled specialist	Low	3

Table 4. Correspondence of quantitative and qualitative assessments of the attacker's skill levels

Attacker's class	Qualitative assessment of the qualification level of an attacker	Quantitative assessment of the qualification level of an attacker
Highly qualified specialist	High	3
Ordinary specialist	Intermediate	2
Low-skilled specialist	Low	1

Table 5. The final matrix of relationships between quantitative assessments of the qualification levels of an IS specialist and the skill level of an attacker

IS specialist's class Attacker's class	Highly qualified specialist	Ordinary specialist	Low-skilled specialist
Highly qualified specialist	0.33	0.5	1
Ordinary specialist	0.66	1	2
Low-skilled specialist	1	1.5	3

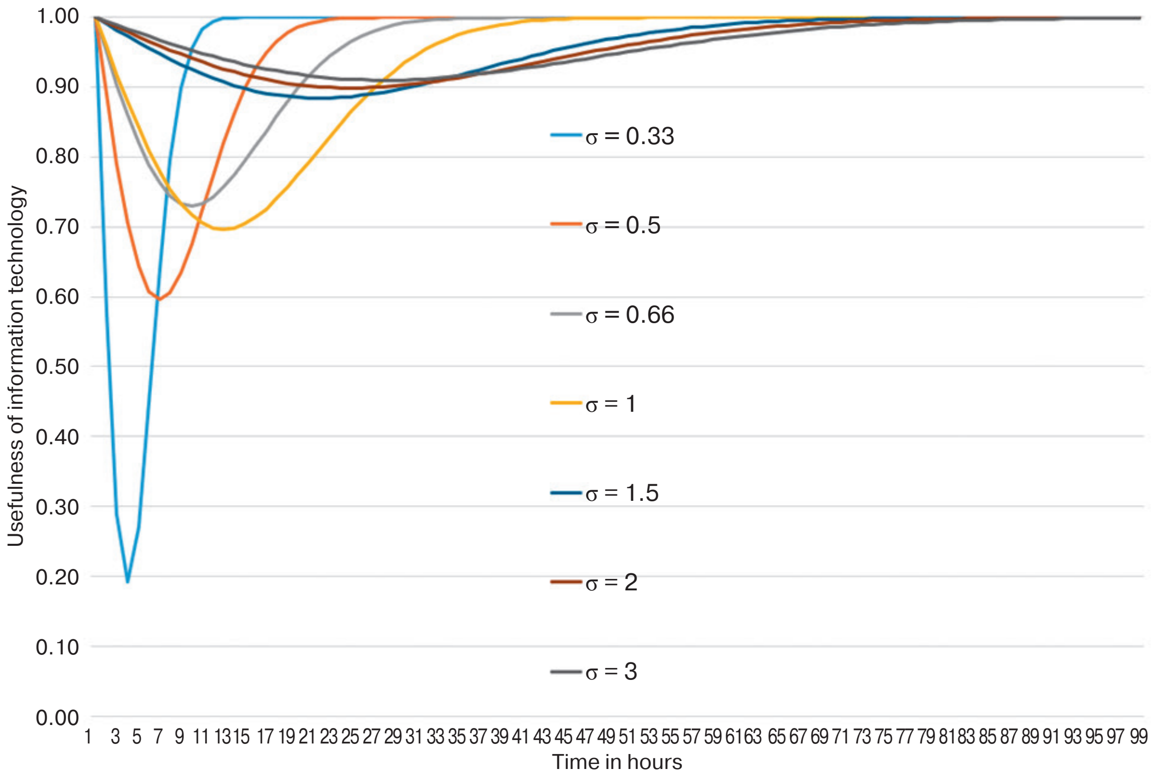

Fig. 1. Dependence of the usefulness of information technology on time and the ratio of the qualification levels of an IS specialist and an attacker

DEVELOPMENT OF PARTICULAR MODELS OF THE INFORMATION SUPPORT STRUCTURE OF THE ADPS FOR MONITORING SECURITY OF THE INFORMATIZATION OBJECT IN THE CLOUD INFRASTRUCTURE

Currently, in the field of IS management of modern informatization objects in cloud infrastructures, a group of IS incident management tasks is distinguished, which includes the following main tasks: monitoring IS events of informatization objects in cloud infrastructures and identifying IS incidents; registration of IS incidents; analysis of IS incidents; informing the administration of cloud infrastructure service providers about all cases of IS violations; collection of evidence for responding to incidents of IS in cloud infrastructures and others. From a practical point of view, one of the most effective ways to creating IS monitoring is the use of systems of the security information and event management (SIEM) class [11–14].

Solutions of the SIEM class are designed to provide the following functions:

- management of information and security events, including those in cloud infrastructures;
- collection and storage of registered security events;
- processing and analysis of IS events stored in internal databases using a system of rules created and managed by a security officer and unique for each cloud infrastructure.

The implementation of the above functions allows for the identification and analysis of incidents, as well as verification of the compliance of the IS management system with existing requirements and norms that are part of the standards, recommendations, orders and other regulatory and guidance documents in this area [15]. The implementation of the above functions assumes the presence of ADPS in systems of the SIEM class, the principles of construction of which were indicated earlier, or, at least, its key components.

However, the main disadvantage of such systems is the relatively long period of time required for them to analyze the data and make a decision about whether this IS event or their combination is an IS incident or not [16–18].

This drawback is based on the contradiction between the distributed nature of information sources about an IS event in cloud infrastructures (as a rule, these sources are IS tools integrated in cloud infrastructures) and a centralized way of deciding on actions with IS incidents. To resolve this contradiction, it is necessary, on the one hand, to provide the decision-making process with the most complete information, and on the other hand, this information must be relevant. Taking into account the large volumes of data on IS events in ADPS, it is necessary to optimize the structure of information support for ADPS, taking into account the structure and technical characteristics of the LAN.

The peculiarities of the functioning of ADPS for monitoring the IS of an informatization object based on cloud infrastructure allow for solving problems of improving the quality of output information using computer modeling, using the methods of utility theory, which make it possible to assess the useful effect of placing information elements in certain computing nodes of the cloud infrastructure [17]. Modern ADPS makes it possible to establish the degree of information reliability, taking into account not only the degree of completeness and accuracy of the data (the sufficiency of data for solving the problem and the correspondence of the structure and content of the data to the systems, the use of which is optimal for solving the assigned tasks), but also the degree of relevance of the data (the ability of information to reflect the real state of objects at the current time).

The method for determining the optimal computing nodes of the cloud infrastructure from the point of view of monitoring IS for placing certain types of information elements in them and distributing these elements among the nodes is based on computer modeling of the cloud infrastructure, in which IS is monitored and the application of the utility theory methods for assessing the degree of type correspondence information elements to one or another computing node of the cloud infrastructure. The specificity of IS incident management involves working with data arrays, which makes it possible to select the necessary data sets that can be distributed among the nodes of the cloud infrastructure based on the model [16–19]. Consequently, particular models should be used, among other things, to determine the structure and volumes of information exchange between nodes of the cloud infrastructure. The information support of ADPS for monitoring the IS of an informatization object in the cloud infrastructure can include both the data about the state of the IS of the informatization object in the cloud infrastructure, obtained directly from the IS tools deployed inside the cloud infrastructure, as well as their copies and/or prehistories received in the nodes cloud infrastructure in the places of their use ADPS for monitoring the IS of the object of informatization. It is advisable to use as particular criteria of these models: the maximin criterion of the usefulness of information support of ADPS for monitoring the IS of an informatization object in a cloud infrastructure; the criterion for the maximum relevance of information support distributed over the nodes of the cloud infrastructure for complex systems with a low degree of centralization of management [7, 8].

The result of solving the problem of developing the structure of the information support of the analytical data processing system for monitoring the IS of the informatization object is the optimal composition, according to given criteria, of the information support components of the ADPS and their placement on the nodes of the cloud infrastructure.

CONCLUSIONS

This article has analyzed the problem of determining a rational structure of information support for ADPS for monitoring the IS of an informatization object in a cloud infrastructure. At the same time, the ISMS, built on the basis of modern SIEM-systems, were considered, and a formalized approach based on the development and use of methods of mathematical and computer modeling was proposed.

The formalization and solution of this problem is based on the methods of utility theory and operations research, which allow using computer modeling to determine the optimal composition of the information support of ADPS and their distribution among the nodes of the cloud infrastructure in terms of the general usefulness of information, taking into account the analytical information technologies used in these nodes to identify IS incidents.

In general, this approach makes it possible to increase the efficiency of the procedure for identifying IS incidents by organizing a rational exchange of information between nodes of the cloud infrastructure (information protection means), taking into account the characteristics of analytical data processing procedures, and, in general, the quality of the IS monitoring system.

Authors’ contribution. All authors equally contributed to the research work.

REFERENCES

1. Liu Z., Zhao A., Liang M. A port-based forwarding load-balancing scheduling approach for cloud datacenter networks. *J. Cloud Comp*. 2021;10(1):13. https://doi.org/10.1186/s13677-021-00226-w
2. Chen J., Wang Y., Liu T. A proactive resource allocation method based on adaptive prediction of resource requests in cloud computing. *J. Wireless Com. Network*. 2021;24. https://doi.org/10.1186/s13638-021-01912-8
3. Wang J., Zhang G., Wang W., Zhang K., Sheng Y. Cloud-based intelligent self-diagnosis and department recommendation service using Chinese medical BERT. *J. Cloud Comp.: Advances, Systems and Applications*. 2021;10(1):4. https://doi.org/10.1186/s13677-020-00218-2
4. Chen Y., Liu H., Wang B., Sonompil B., Ping Y., Zhang Z. A threshold hybrid encryption method for integrity audit without trusted center. *J. Cloud Comp.: Advances, Systems and Applications*. 2021;10(1):3. https://doi.org/10.1186/s13677-020-00222-6
5. Ngoc T.L., Doan B.H. Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing: Practice and Experience*. 2017;18(4):277–290. https://doi.org/10.12694/scpe.v18i4.1329
6. Afolaranmi S.O., Moctezuma L.E.G., Rak M., Casola V., Rios E., Lastra J.L.M. Methodology to Obtain the Security Controls in Multi-cloud Applications. In: *Proceedings of the 6th International Conference on Cloud Computing and Services Science* (*CLOSER 2016*). V.1. 2016, p. 327–332. http://doi.org/10.5220/0005912603270332
7. Sizov V.A. Development of models for improving the efficiency of data safety in a distributed computing environment based on dynamic data reservation. In: *Advances in Science and Technology*: *Collection of articles of the XXI International Scientific and Practical Conference*. 2019, p. 96–100. (in Russ.).
8. Sizov V.A. Models and methods of virtual-recovered redundancy of data of automatic information-control systems under extreme conditions. *Autom. Remote Control*. 1998;59(7):1047–1053.

СПИСОК ЛИТЕРАТУРЫ

1. Liu Z., Zhao A., Liang M. A port-based forwarding load-balancing scheduling approach for cloud datacenter networks. *J. Cloud Comp*. 2021;10(1):13. https://doi.org/10.1186/s13677-021-00226-w
2. Chen J., Wang Y., Liu T. A proactive resource allocation method based on adaptive prediction of resource requests in cloud computing. *J. Wireless Com. Network*. 2021;24. https://doi.org/10.1186/s13638-021-01912-8
3. Wang J., Zhang G., Wang W., Zhang K., Sheng Y. Cloud-based intelligent self-diagnosis and department recommendation service using Chinese medical BERT. *J. Cloud Comp.: Advances, Systems and Applications*. 2021;10(1):4. https://doi.org/10.1186/s13677-020-00218-2
4. Chen Y., Liu H., Wang B., Sonompil B., Ping Y., Zhang Z. A threshold hybrid encryption method for integrity audit without trusted center. *J. Cloud Comp.: Advances, Systems and Applications*. 2021;10(1):3. https://doi.org/10.1186/s13677-020-00222-6
5. Ngoc T.L., Doan B.H. Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing: Practice and Experience*. 2017;18(4):277–290. https://doi.org/10.12694/scpe.v18i4.1329
6. Afolaranmi S.O., Moctezuma L.E.G., Rak M., Casola V., Rios E., Lastra J.L.M. Methodology to Obtain the Security Controls in Multi-cloud Applications. In: *Proceedings of the 6th International Conference on Cloud Computing and Services Science* (*CLOSER 2016*). 2016. V.1. p. 327–332. http://doi.org/10.5220/0005912603270332
7. Сизов В.А. Разработка моделей повышения эффективности сохранности данных в распределенной вычислительной среде на основе динамического резервирования данных. В сб.: *Advances in Science and Technology*: *сб. статей XXI международной научно-практической конференции*. М.: «Актуальность. РФ», 2019. С. 96–100.
8. Сизов В.А. Модели и методы виртуально-восстановительного резервирования данных автоматизированных информационно-управляющих систем в условиях

[Sizov V.A. Models and methods of virtual-recovered redundancy of data of automatic information-control systems under extreme conditions. *Automat. i Telemekh*. 1998;(7):176–184 (in Russ.).]

9. Arce D.G. Cybersecurity and platform competition in the cloud. *Computers & Security*. 2020;93:101774. https://doi.org/10.1016/j.cose.2020.101774
10. Dzhincharadze G.R. Methodological aspects of the organization of the personnel assessment procedure. *Inzhenernyi Vestnik Dona = Engineering journal of Don*. 2012;2(20):340–345 (in Russ.). Available from URL: https://cyberleninka.ru/article/n/metodicheskie-aspekty-organizatsii-protsedury-otsenki-personala
11. Sizov V.A., Kirov A.D. Problems of implementation SIEM-systems in the practice of managing information security of economic entities. *Otkrytoe obrazovanie = Open Education*. 2020;24(1):69–79 (in Russ.). https://doi.org/10.21686/1818-4243-2020-1-69-79
12. Lee J., Kim Y.S., Kim J.H., Kim I.K. Toward the SIEM architecture for cloud-based security services. In: *2017 IEEE Conference on Communications and Network Security (CNS)*. https://doi.org/10.1109/CNS.2017.8228696
13. Granadillo G.G., El-Barboni M., Debar H. New Types of Alert Correlation for Security Information and Event Management Systems. In: *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. 2016. https://doi.org/10.1109/NTMS.2016.7792462
14. Kavanagh M., Rochford O. *Magic Quadrant for Security Information and Event Management.* Gartner technical report. 2015. 15 p.
15. Markov A.S., Tsirlov V.L. Structured content of information security requirements. *Monitoring pravoprimeneniya = Monitoring of Law Enforcement*. 2017;1(22):53–61 (in Russ.). https://doi.org/10.21681/2412-8163-2017-1-53-61
16. Nabil M., Soukainat S., Lakbabi A., Ghizlane O. SIEM selection criteria for an efficient contextual security. In: *2017 International Symposium on Networks, Computers and Communications (ISNCC)*. https://doi.org/10.1109/ISNCC.2017.8072035
17. Kirsanov K.K. The theory of utility in the period of change of conceptual provisions. *Naukovedenie* (*The Eurasian Journal*). 2015;7(2):38 (in Russ.). Available from URL: http://naukovedenie.ru/PDF/37EVN215.pdf
18. Kotenko I.V., Fedorchenko A.V., Saenko I.B., Kushnerevich A.G. Big data technologies for security event correlation based on event type accounting. *Voprosy kiberbezopasnosti = Cybersecurity issues*. 2017;5(24):2–16 (in Russ.). https://doi.org/10.21681/2311-3456-2017-5-2-16
19. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. An Analysis of Security Event Correlation Techniques in SIEM-Systems. Part 2. *Trudy SPIIRAN = SPIIRAS Proceedings*. 2016;6(49):209–225 (in Russ.). https://doi.org/10.15622/sp.49.11

чрезвычайных ситуаций. *Автоматика и телемеханика*. 1998;7:176–184.

9. Arce D.G. Cybersecurity and platform competition in the cloud. *Computers & Security*. 2020;93:101774. https://doi.org/10.1016/j.cose.2020.101774
10. Джинчарадзе Г.Р. Методические аспекты организации процедуры оценки персонала. *Инженерный Вестник Дона*. 2012;2(20):340–345. URL: https://cyberleninka.ru/article/n/metodicheskie-aspekty-organizatsii-protsedury-otsenki-personala
11. Сизов В.А., Киров А.Д. Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности. *Открытое образование*. 2020;24(1):69–79. https://doi.org/10.21686/1818-4243-2020-1-69-79
12. Lee J., Kim Y.S., Kim J.H., Kim I.K. Toward the SIEM architecture for cloud-based security services. In: *2017 IEEE Conference on Communications and Network Security* (*CNS*). https://doi.org/10.1109/CNS.2017.8228696
13. Granadillo G.G., El-Barboni M., Debar H. New types of alert correlation for security information and event management systems. In: *2016 8th IFIP International Conference on New Technologies, Mobility and Security* (*NTMS*). 2016. https://doi.org/10.1109/NTMS.2016.7792462
14. Kavanagh M., Rochford O. *Magic Quadrant for Security Information and Event Management.* Gartner technical report. 2015. 15 p.
15. Марков А.С., Цирлов В.Л. Структурное содержание требований информационной безопасности. *Мониторинг правоприменения*. 2017;1(22):53–61.
16. Nabil M., Soukainat S., Lakbabi A., Ghizlane O. SIEM selection criteria for an efficient contextual security. In: *2017 International Symposium on Networks, Computers and Communications* (*ISNCC*). 2017. https://doi.org/10.1109/ISNCC.2017.8072035
17. Кирсанов К.К. Теория полезности в период смены концептуальных положений. *Науковедение* (*Вестник Евразийской науки)*. 2015;7(2):38. URL: http://naukovedenie.ru/PDF/37EVN215.pdf
18. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей. *Вопросы кибербезопасности*. 2017;5(24):2–16. https://doi.org/10.21681/2311-3456-2017-5-2-16
19. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2. *Труды СПИИРАН*. 2016;6(49):208–225. https://doi.org/10.15622/sp.49.11

About the authors

Valerii A. Sizov, Dr. Sci. (Eng.), Professor, Department of Applied Informatics and Information Security, Institute of Mathematics, Information Systems and Digital Economy, Plekhanov Russian University of Economics (36, Stremyanny per., Moscow, 117997 Russia). E-mail: sizov.va@rea.ru. https://orcid.org/0000-0002-4844-4714

Aleksey D. Kirov, Specialist, Specialized Educational and Scientific Laboratory on Information Confrontation in Business, Department of Applied Informatics and Information Security, Institute of Mathematics, Information Systems and Digital Economy, Plekhanov Russian University of Economics (36, Stremyanny per., Moscow, 117997 Russia). E-mail: kirov.ad@rea.ru. https://orcid.org/0000-0002-8424-3071

Об авторах

Сизов Валерий Александрович, д.т.н., профессор, кафедра Прикладной информатики и информационной безопасности Института математики, информационных систем и цифровой экономики ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова» (117997, Россия, Москва, Стремянный пер., 36). E-mail: sizov.va@rea.ru. https://orcid.org/0000-0002-4844-4714

Киров Алексей Дмитриевич, специалист, специализированная учебно-научная лаборатория по информационному противоборству в бизнесе, кафедра Прикладной информатики и информационной безопасности Института математики, информационных систем и цифровой экономики ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова» (117997, Россия, Москва, Стремянный пер., 36). E-mail: kirov.ad@rea.ru. https://orcid.org/0000-0002-8424-3071

Translated by E. Shklovskii