MODELS AND ALGORITHMS FOR ENSURING FUNCTIONAL STABILITY AND CYBERSECURITY OF VIRTUAL CLOUD RESOURCES

[1]ALIMSEITOVA ZH., [2]ADRANOVA A., [2]AKHMETOV B., [3]LAKHNO V., [4]ZHILKISHBAYEVA G., [5]SMIRNOV O.A.

[1]Almaty University of Power Engineering and Telecommunications, Kazakhstan
[2]Abai Kazakh National Pedagogical University, Kazakhstan
[3]National University of Life and Environmental Sciences of Ukraine, Ukraine
[4]Yessenov University, Aktau, Kazakhstan
[5]Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

E-mail: [1]zhuldyz_al@mail.ru, [2]assel.adranova@gmail.com , [2]bakhytzhan.akhmetov.54@mail.ru, [3]lva964@gmail.com, [4]gulnaz.zhilkishbayeva@yu.edu.kz, [5]dr.SmirnovOA@gmail.com

ABSTRACT

The article proposes a model that describes the effects of cyber attacks on virtual cloud resources (VCR) of various informatization objects (IO). The developed model served as the basis for an algorithm that allows to analyze threats in the IO cloud environment. The proposed algorithm in this work allows to obtain attack routes, that is achieved by synthesizing the attack graph and the graph of the correlative alert about the state of the IO virtual cloud environment (VCE). There is proposed a model for assessing the state of VCR. This model has become the basis for the algorithm for choosing countermeasures to protect the IO VCE. Ultimately, the proposed solutions allow to obtain a calculated indicator of functional stability (FS) and cybersecurity (CS) of IO virtual resources. And then to form countermeasures for increasing the FS and CS index of IO virtual cloud resources. During the research, there was developed a technique for providing FS and VCE CS based on software-configured networks. The developed technique allows to focus the attention of the protection side on increasing the FS and CS of virtual machines on the basis of the attacks detection and subsequent reconfiguration of virtual networks in VCE.

Keywords: *Attack Graph, Correlation Graph, Software-Configured Network, Virtual Cloud Environment*

1. INTRODUCTION

The modern development of information technology (IT) (for example, in banks, at enterprises, or in the educational processes of many large universities) is characterized by the widespread use of cloud resources located in data processing centers (DPC). Such centers are a collection of servers located on the same site to increase their functional stability (FS) and cybersecurity (CS). In [1], [2] the authors defined cloud computing (CC) in the following way: “This is a model for providing ubiquitous and convenient access through a network to a common pool, including computing resources that must be configured. These resources include: communication networks, servers, data storage means, applications, and services. Resources can be quickly provided with minimal operating costs or with contacting the provider.”

Both large companies that are trying to optimize their enterprise IT infrastructure expenses and small companies that are unable to immediately deploy their own infrastructure have shown active interest in cloud technologies. Ordinary users have also shown interest, primarily in the possibilities for data storage and the use of programs. During the operation of cloud resources, consumers are interested in a significant reduction in capital costs for DPC creation and the purchase of server and network equipment components and in ensuring the continuity and availability of the IT infrastructure of their enterprises. All these resource-intensive and complex issues in using the cloud are transferred from users to cloud service providers—the user only pays for the actual services. Cloud services also provide users with flexibility of configuration. For example, one can independently configure parameters such as processing power, file storage volumes, and software composition. Despite the obvious advantages of CC, there remain problematic questions. The main ones are lack of trust in the service provider; the need to reliably ensure the confidentiality, integrity, and authenticity of information in the cloud; the FS of information at all stages of its existence; guarantees of uninterrupted operation and protection against unauthorized access (UNA); and saving the personal data of users that is transferred to and processed in the cloud.

Confidentiality in working with cloud IT is not only the task of the suppliers, who must ensure both physical and software integrity of the stored data against third parties. Modern cloud DPCs, as a rule, are designed on the basis of the latest standards in the field of CS (including antivirus protection, encryption, and intrusion detection systems [IDS]) [1].

The FS of the servers in DPCs is provided by network and physical protection, as well as by ensuring fault tolerance and reliable power supplies. Nowadays, the market offers a wide range of hardware and software solutions for providing the FS and CS of servers focused on a narrow range of tasks. However, due to the gradual replacement of classical hardware and software systems by virtual platforms, the number of such tasks has increased significantly and continues to grow.

The known types of threat to the integrity of FS and CS (network attacks, vulnerabilities in operating system (OS) applications, and malicious software) have been added to in recent years. Such new threats include the organization of environmental controls (hypervisor), traffic control between guest machines, and difficulties with access rights delimitation. The work of modern DPCs in a number of industries therefore requires increasing the level of technical requirements to ensure their FS. Moreover, this fully applies not only to cloud technologies in education, but also to more serious cloud architecture, such as that used in banks and the transport industry—in other words, in the infrastructure of critical computer systems.

The appearance and development of virtualization technologies has caused a large-scale migration of most systems to virtual machines (VM). At the same time, solving the problems of providing FS and CS for the operation of software in a new environment requires a different approach. Many types of cyber threats are well studied, and appropriate countermeasures and methods have been developed for them. However, such methods must be adapted for use in the cloud. The penetration of platforms based on virtualization technologies has reached a level at which almost all companies using these systems have seriously begun to deal with issues of FS and CS of the cloud.

Many questions on increasing the FS and CS of virtual cloud resources (VCR) have not yet been fully investigated [1], [2]. The solutions to this type of problem based on existing development [2], [3] have significant disadvantages [4]. In particular, a number of researchers [5], [6] have noted the lack of a universal method for providing FS and CS for cloud resources due to 1) constant changes in the capabilities of existing VMs in cloud information systems, 2) the use of insecure application interfaces, and 3) the high resource consumption of existing systems. The topic of this article—solving the scientific and applied tasks of IT development to ensure the FS and CS of VCRs based on software-configured networks—is therefore relevant.

2. REVIEW AND ANALYSIS OF PREVIOUS RESEARCHES

Modern methods of providing FS for VCRs based on software-configured networks are inextricably linked with publications [6], [7], [8], [9], [10]. Publications [7], [8] substantiated the importance and relevance of solving the problem of providing FS and CS for VCRs based on software-configurable networks (SCN). However, these works were mainly of a review nature.

In works [9], [10], the authors analyzed the effectiveness of cloud technologies, on the basis of which it was concluded that their use provides a number of advantages over traditional IT technologies. In [11], the advantages of virtual cloud environments (VCE) in the tasks of efficiently managing an organization's computing resources were shown. Works [9], [11] substantiated the benefits of VCEs in the tasks of reducing the costs of IT infrastructure and informatization object (IO) maintenance personnel and ensuring reliable protection of data from losses and attacks. However, these works did not contain descriptions of specific methods aimed at increasing the FS of VCEs. Works [11], [12] considered the practical aspects of the use of VCEs for the implementation of many types of training activities, monitoring and evaluation, and online testing. However, the tasks associated with VCE CS in educational institutions were not considered.

Publications [13], [14] showed that the FS of VCEs is achieved on the basis of systemic approaches to solving problems by increasing the reliability properties of complex control objects.

Moreover, as was noted in [10], [14], FS is a property fundamentally different from reliability and stability. Methods of providing FS are aimed at a more complete use of the available technical resources of complex technical systems. The task of providing FS and CS for VCEs can be considered one of the urgent scientific problems of modern control theory [15].

Scientific research has shown that the most important factors for cloud users are FS and security [10], [14], [15]. External influence by hackers on VCEs that violates the internal integrity of cloud virtual resources is considered in [10], [16] as a threat to FS. Such influence can exploit vulnerabilities in the cloud and its resources to penetrate the system. In traditional DPCs in which system administrators have full control over the host machines, such external influences can be detected and corrected in a centralized manner. However, measures to ensure FS and CS in DPCs, where cloud users, as a rule, have privileges to manage software on their VMs, cannot work effectively. This, in turn, leads to violations of the requirements of service level agreements (SLA) [10], [17]. Users can also install vulnerable software on VMs in the cloud [14], significantly reducing the FS of the cloud environment. Thus, the task of creating an effective system for identifying and responding to external influences—including of a destructive nature from hackers and other intruders—remains significant and is necessary for timely minimization of the consequences of violations of the FS of cloud virtual resources. The tasks that are mentioned below have not been discussed by other researchers in their publications. In view of the foregoing, the purpose and objectives of this research are highly relevant.

3. PURPOSE OF THE ARTICLE

This research examines approaches to increasing the FS and CS of VCRs of various IOs based on monitoring their state and assessing ways to counter intrusions. Some aspects of the influence of the proposed solutions on the FS of the cloud environment and the possibility of automated control of software-configured networks are also discussed.

During the process of the research, the following tasks were solved:

1) the development of an attack model of VCRs in the form of an attack graph that will describe and predict the behavior of an attacker;

2) the development of a model for choosing countermeasures, for security indicator monitoring, and for assessing the state of the VCRs of an IO;

3) the development of a methodology for ensuring FS and CS of a VCE based on software-configured networks; and

4) an experimental assessment of the effectiveness of using the developed methodology for automated decision-making on countering intrusions into a VCE.

4. METHODS AND MODELS

During the process of the research, the model describing the cyberattack influence on VCRs was improved. The model differs from the existing ones in that, for constructing edges in the alert correlation graph (ACG) [18], a function that takes into account the time difference between the arrival of alerts from neighboring nodes ($D(Alert)$ and $Alert$) in the system is used:

$$T = D(Alert) \bigcup Alert, \tag{1}$$

A graph of attacks on VCEs was developed that allows gathering of information about all known vulnerabilities in the system and shows, in real time, the status of the FS and CS of the system. This makes it possible to predict possible threats and attacks by correlating the identified events.

The graph scenario (hereinafter referred to as GRS) can be submitted in the tuple format:

$$SC_{ga} = \langle VR, ED \rangle, \tag{2}$$

where $VR -$ is a set of vertices of the attack graph (AG) and $ED -$ is a set of directed edges connecting the vertices of the AG.

The vertices of the AG can be of three types: $NO_{co} -$ nodes of the conjunction (to display vulnerabilities), $NO_{di} -$ nodes of the disjunction (to indicate the result of exploiting the vulnerability by an attacker), and the root node $NO_{ro} -$ (to indicate the initial stage of the attack scenario).

The set of AG vertices VR is defined as follows:

$$VR = NO_{co} \cup NO_{dt} \cup NO_{ro}. \tag{3}$$

A set of edges reflects which of the NO_{dt} must be met in order to achieve NO_{co}. The edge means that the nodes NO_{dt} must be obtained for nodes NO_{co} to be met.

Then it is fairly

$$ED = ED_{pre} \cup ED_{post}, \tag{4}$$

where ED_{pre} – represents the AG edges, which reflect the relationship between the result of exploiting the vulnerability in the previous node and the vulnerability itself in the next node, and ED_{post} – represents the edges that reflect the relationship between vulnerabilities in the previous node and possible results of exploiting the vulnerabilities in the next node.

The ACG will be presented as a tuple of the form

$$G_{cev} = \langle AL, ED, SR \rangle, \tag{5}$$

where $\{AL\}$ – is a set containing all alerts $(Alert)$—an alert $al \in AL$ is a data structure that includes the source and destination IP addresses, the type of alert, and timestamps—and SR – is a set of attack paths in the ACG.

Each alert refers to a pair of vertices $(vr_c; vr_d)$ in the GRS. In alerts, a function $map(al)$ is used that reflects an improved model of the attack influence on the VCRs:

$$map(al): al \to \left\{ (vr_c, vr_d) \middle| \begin{array}{l} (al.sour.addr.alert \in vr_{c.host}) \wedge \\ (al.dest.addr.alert \in vr_{d.host}) \wedge \\ (al.alert.cl = vr_{c.vul}) \end{array} \right\}, \tag{6}$$

where vr_c – is a vertex that reflects a vulnerability; vr_d – is a vertex that reflects the exploitation of the vulnerability; $al.sour.addr.alert$ – is an alert with the IP address of a source; $vr_{c.host}$ – is a vertex that corresponds to a particular node in the cloud environment, an alert with the IP address of the destination node, and a vertex that corresponds to a particular node in the VCE associated with; $al.alert.cl$ – is an alert with a vulnerability class; $vr_{c.vul}$ – is a vulnerability in the analyzed node; c – is a vulnerability index; and d – is a vulnerability exploitation index.

The directed edges represent the correlation between two alerts (al, al') if the following criteria are true:

$$(al.time < al'.time) \wedge (al'.time - al.time < threshold \quad value) \tag{7}$$

where an alert with a time stamp in the previous node and $al'.time$ – is an alert with a time stamp in the next node.

$$\exists (vr_c, vr_d) \in ED_{pre} : \wedge \begin{pmatrix} (al.dest.addralert \in vr_{d.host}) \wedge \\ (al.'sour.addralert \in vr_{c.host}) \end{pmatrix}. \tag{8}$$

A route $RO_i \subset SR$ is a set of related alerts in chronological order that belong to the same attack scenario.

An AG is used to predict the behavior of an attacker. Based on it, an algorithm for analyzing threats in the cloud environment is created; see Fig. 1.

According to the algorithm, for each alert, one or more attack routes RO_i are detected and returned. For each alert that is received from an IDS, a new vertex is added to the ACG if it does not exist. For this new alert, we should find the corresponding vertex in the GRS using the function $map(al)$. For this vertex in the GRS, alerts associated with its vertices of the type NO_{co} are correlated. This creates either a new set of vertices that relate to the route RO_i in the ACG or a new route $RO_i + 1$. At the end of the work of the threat analysis algorithm in the VCE, we add the alert attribute to the corresponding vertex in the GRS. The result of the algorithm is to obtain one or more routes of attack on the VCE.

During the research process, the model for assessing the state of VCRs was improved. The model is described by the expressions (9)–(12) and differs from the existing ones in that, for choosing the countermeasure $(cm \in CM)$, the indicator characterizing the negative effect $(cm.ef)$ of the countermeasure on the SLA (or) is used as well as the indicator of the costs required to use the countermeasure in terms of resources and operational complexity.

To assess a VM from the point of view of FS, it is proposed that, as the indicator of the FS of the VM, the following be used:

$$FS_{VM} = A_{VM} + A_{U_{VM}}, \tag{9}$$

where $A_{U_{VM}}$ - is assessment of the use of VM vulnerabilities in the VCE and A_{VM} is assessment of the VM vulnerabilities.

It is assumed that

$$A_{VM} = \min \left\{ 10, \ln \sum e^{BL(vm)} \right\}, \tag{10}$$

where $BL -$ is the average base score for each vulnerability of a particular VM termed $vm.$

An assessment of the VM vulnerabilities exploit can be obtained as follows:

$$A_{U_{VM}} = \left(\min \left\{ 10, \ln \sum e^{W(vm)} \right\} \right) \left(\frac{N(vm)}{Q(vm)} \right), \tag{11}$$

where $W(vm) -$ is the average vulnerability exploit score of each of the vulnerabilities of a particular VM, $N_{(vm)} -$ is the number of services provided by the VM, and $Q_{(vm)} -$ is the number of services that can be provided by a VM in the VCE.

Therefore, the parameter A_{VM} takes into account the basic assessments of all VM vulnerabilities, and each basic vulnerability assessment takes into account the attacker's ability to exploit that vulnerability. One can also take into account the amount of damage that an attacker can inflict. The exponential sum of the basic indicators allows assessment of the deviations of their values on a logarithmic scale based on the number of vulnerabilities.

On the other hand, a vulnerability assessment of a virtual machine $A_{U_{VM}}$ reflects an attacker's ability to exploit VM vulnerabilities and depends on the ratio of the number of used network services to the total number of possible network services. A high assessment FS_{VM} means that, for the vulnerabilities, there are a large number of possible ways to achieve an attacker's goal.

Therefore, the indicator of functional stability FS_{VM} is a quantitative assessment of the level of FS and CS of each VM in a VCE. The functional stability index FS_{VM} can be used to determine the level of FS and CS for each VM in a VCE. To prevent cyber threats from a compromised VM impacting VMs with higher values of FS_{VM}, the protection side needs to use more effective means of CS. To reduce the value FS_{VM}, there are substantiated strategies for reducing the influence of the attack, depending on the value of the negative impact of attackers on a VCE.

We should note that the choice of countermeasures is a complex task that includes purely technical countermeasures, such as ending a session with an attack source node, sending an alert to the user, blocking access to the server in the network, or changing the configuration of security services to block an IP. However, the choice of a rational strategy for technical means requires financing, and the task of choosing such a strategy can be considered independent; both our research [22], [23] and the work of other authors [24], [25] are devoted to a solution.

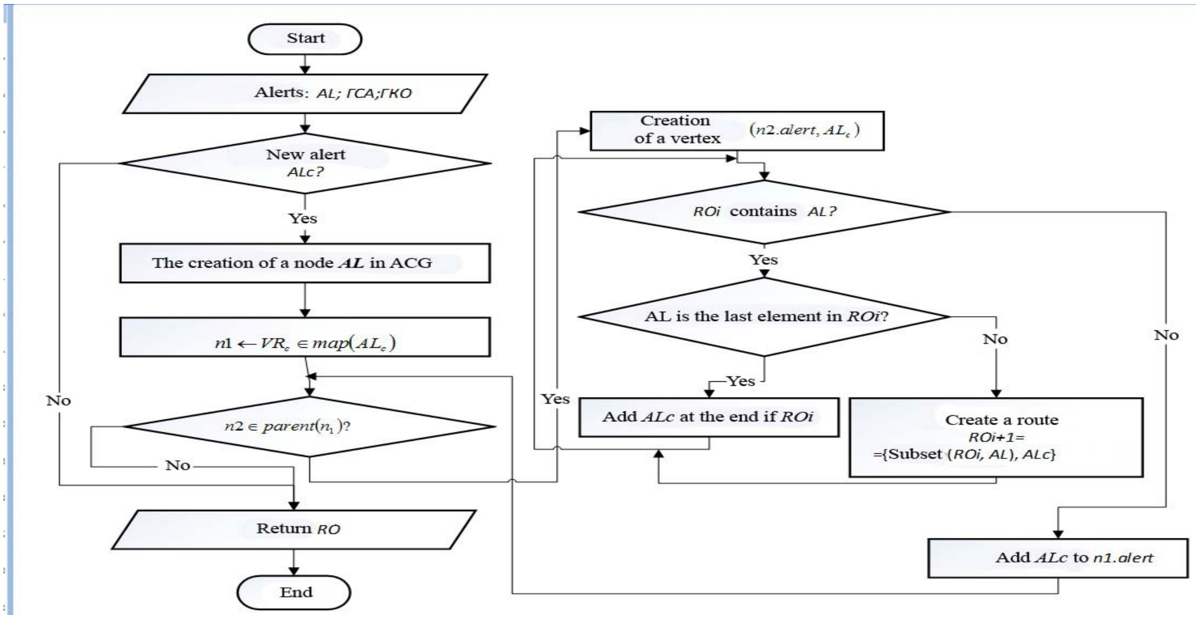

Figure 1: Cyberthreats analysis algorithm in VCE

On the basis of the obtained results, a countermeasure selection algorithm using an example of an attack of the Probe type is proposed; see Fig. 2. The meaning of the algorithm is as follows:

Countermeasures $(cm \in CM)$ are selected for a specific cyberattack scenario. The input data for the algorithm comprises alarm alerts from a network analyzer (Alert), an AG, and a database containing possible countermeasures (a set containing possible countermeasures for VCE protection). The operation of the algorithm begins with the selection of a node in the ACG, which is responsible for the alerts received from the network analyzer. For this alert, the time distance to the target node is calculated. If the obtained value is greater than the threshold (th_val), then the selection of countermeasures cm is not performed. Next, the ACG is updated and new alerts in the system are monitored.

The countermeasure that gives the smallest value of the complex indicator of the countermeasure choice is defined as in demand. AG and ACG scenarios are also updated before the completion of the algorithm.

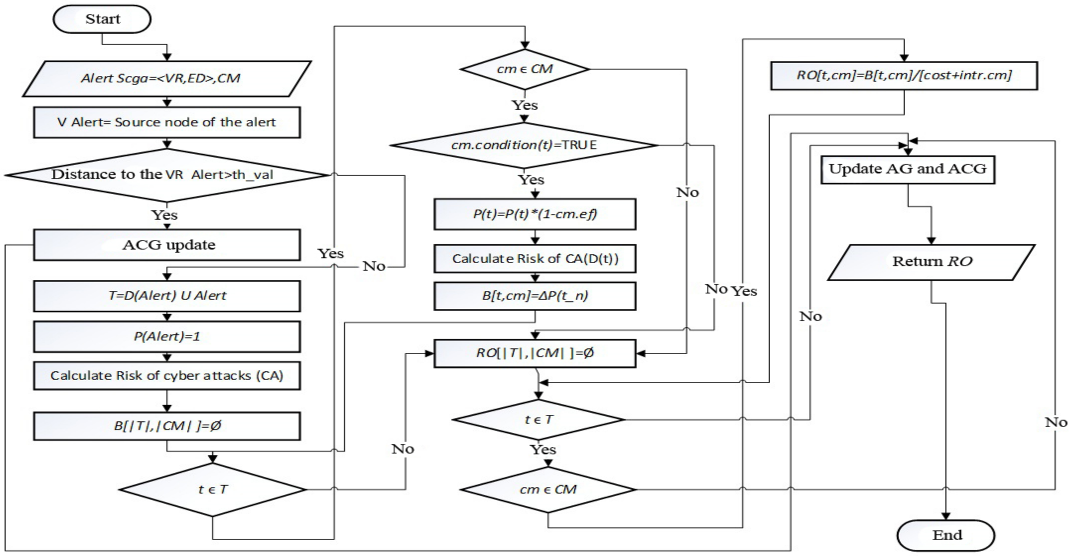

Figure 2: Algorithm for selecting countermeasures to minimize the influence of Probe cyberattack on VCE

To achieve the goal of choosing a countermeasure, a comprehensive indicator of the choice of countermeasure $CO.$ is used.

$$CO = \left(\left(h_1 \cdot JA \right) + \left(h_2 \cdot VA \right) \right) \Big/ k, \qquad (12)$$

where $h_1, h_2 -$ are characteristics of the influence of countermeasure values on the FS and CS of the VCE, $JA -$ is the value of the negative influence that arises as a result of the application of countermeasures in relation to the SLA $\left(Benefit(or \quad B) \right)$, $VA -$ is the cost, which reflects the expenses necessary to implement countermeasures in terms of resources and operational complexity (the higher the indicator, the greater the cost [cost]), and $k -$ is the coefficient of rationing.

During the process of the research, a methodology was developed for providing FS for a VCE based on SCNs. The methodology was developed on the basis of infrastructure as a service—that is, users of cloud services being free to install any OS or application. This has a limitation; the use of the methodology is not related to host-based IDSs—that is, exactly how to process encrypted traffic to detect an attack has not been solved. The methodology can be used only in systems based on paravirtualization [18], [19], [20], [21].

The output data from the methodology comprises AGs, alert correlation graphs, alerts from the network analyzer, and profiles of VMs. The functional diagram of the test VCE based on SCNs is presented in Fig. 3. The test VCE includes the following elements: network agents, databases (DB) of VM profiles, a network controller, an attack analyzer, and hardware, such as a switch or router.

A network agent is installed on each cloud server, which is designed to scan traffic that passes through network bridges. Bridges control all traffic between VMs in a physical cloud server. The VM profile database contains information about the state of each machine, and VMs in the cloud are profiled in such a way as to obtain accurate information about the state of the VM, the state of the services, the state of the open ports, etc.

Any VM that is connected to a large number of other machines is a priority. This is due to the fact that compromising a VM with a large number of links can cause a greater decrease in the FS and CS of a VCE in general. In addition, it is necessary to store information about the services operating on a VM to verify the reliability of the alerts that apply to it. An attacker can use a port scan program to scan the network and search for open ports on any VM. Therefore, information about any open port on the VM and the history of open ports plays a significant role in determining how vulnerable the VM is. All of these factors together create a VM profile. VM profiles are stored in the database and contain information about vulnerabilities, alerts from the network analyzer, open ports, services, etc.

A network controller is a key component in maintaining software reconfiguration capabilities. It implements a virtual network reconfiguration function based on the openflow protocol. The proposed methodology uses integrated management functions for the Open vSwitch and openflow switch protocols in the network controller. This allows setting of security rules for filtering traffic on an integrated basis for the cloud system.

The network controller collects information about the network and the current openflow network and provides input to the attack analyzer to create AGs. Information about a topology change is automatically sent to the controller and then processed to restore the AG. The network controller is also responsible for applying the appropriate countermeasures from the attack analyzer.

The attack analyzer implements the main functions of the FS and CS of the VCE based on SCNs, which include procedures such as creating and updating the scenarios of the AG and the ACG.

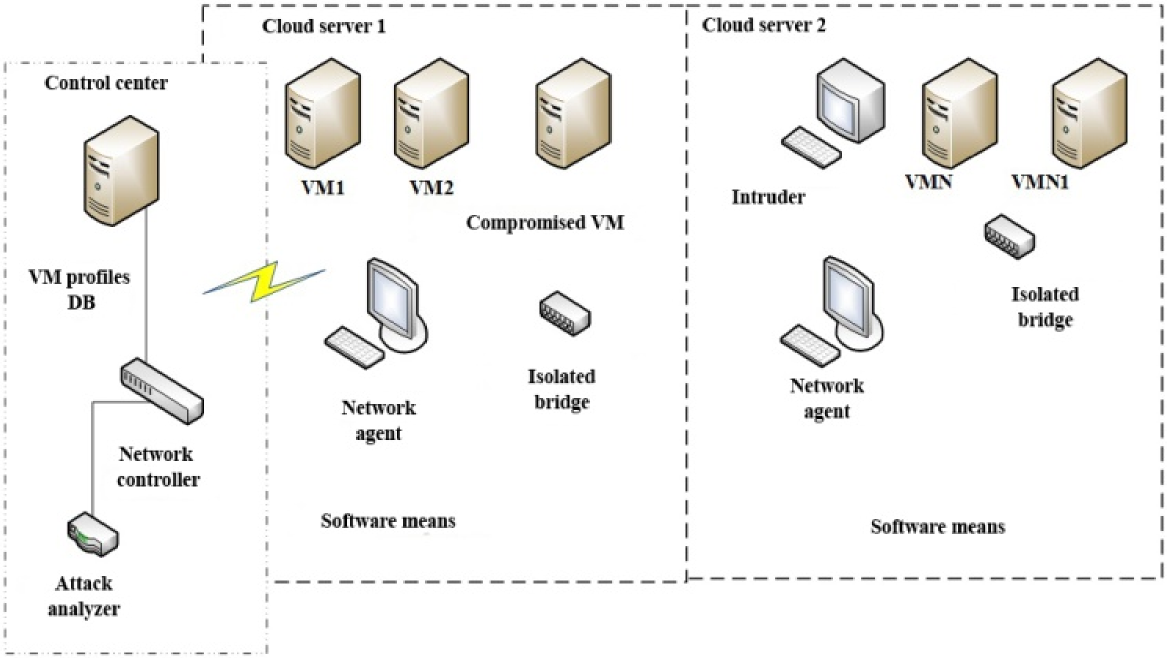

Figure 3: Functional diagram of VCE based on SCN

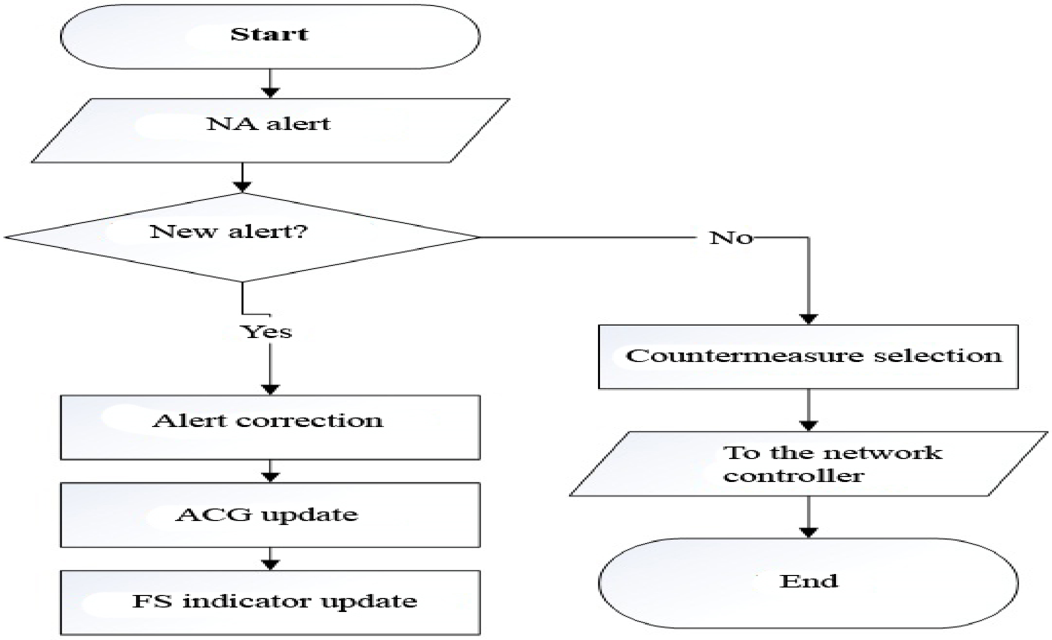

Figure 4: Algorithm for providing FS and CS of VCE based on SCN. Accepted abbreviations: NA - network analyzer; ACG – alert correlation graph

5. THE RESULTS OF EXPERIMENTAL STUDIES

To verify the obtained methods and models, experimental studies were conducted to ensure the FS of VCEs based on software-configured networks. To assess the effectiveness of the obtained scientific results, a test VCE was developed that included 24 VMs. Fig. 5 shows a structural diagram of a test stand.

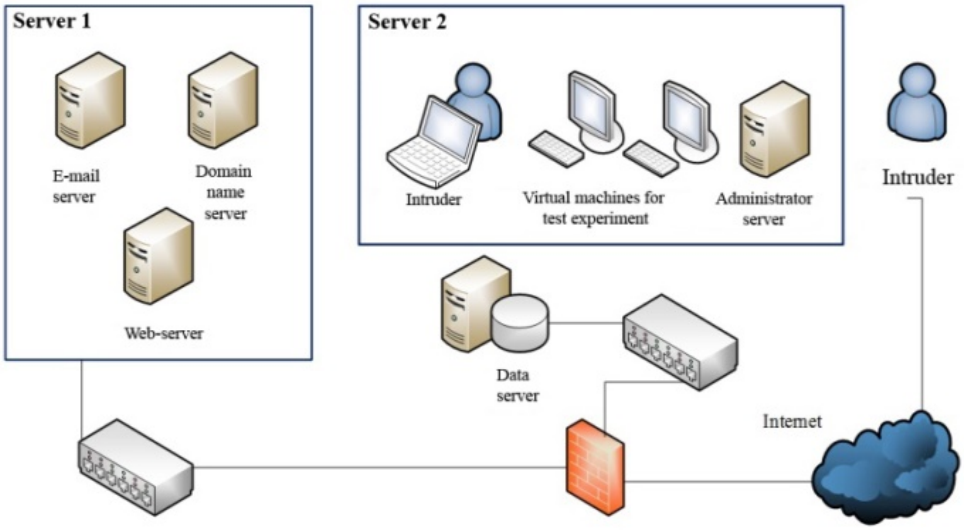

Figure 5: The scheme of the stand for experimental research

For example, Open vSwitch needs to be tested during the process of configuration of a physical or virtual switch by sending packets in different ways, such as the ping and tcpdump utilities. For a virtual switch, this is difficult to accomplish as the virtual switch is not visible to the OS, although it has a set of special testing tools.

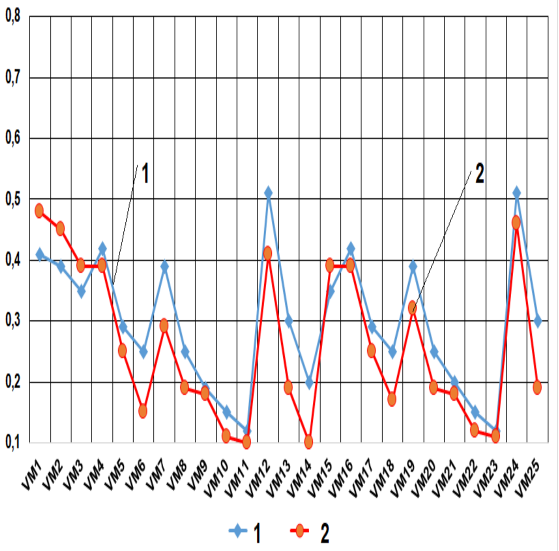

Figure 6: VM assessment graphs in terms of indicators $A_{U_{VM}}$ (Line 1) and A_{VM} (Line 2)

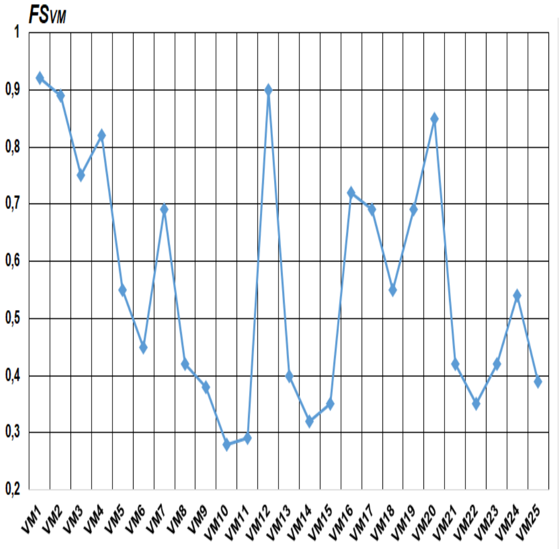

Figure 7: VM assessment graph depending on the indicator FS_{VM}

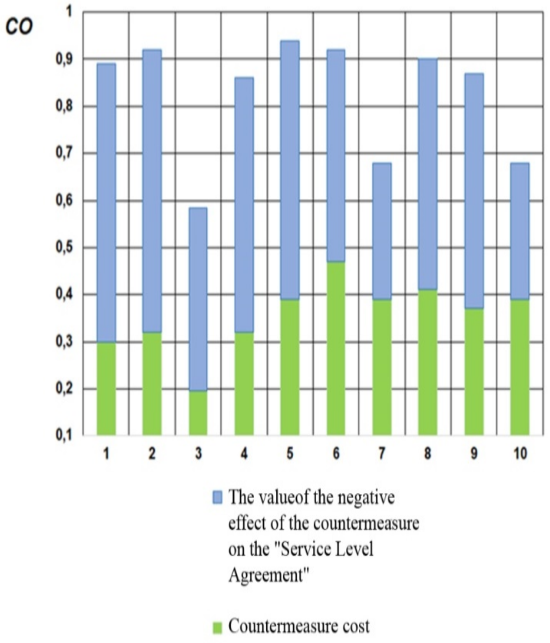

Figure 8: Diagram of a comprehensive indicator of CO countermeasure selection for VCE

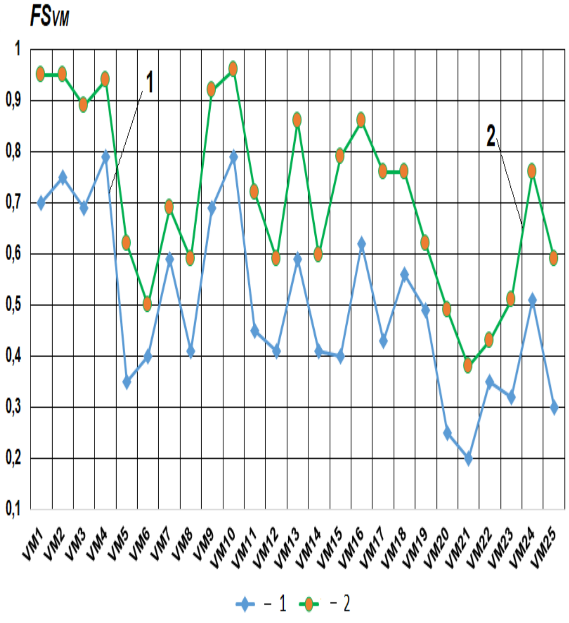

Figure 9: The change of the value FS_{VM} for VM. (Line 1 – after taking countermeasures, Line 2 - before taking countermeasures

6. DISCUSSION OF THE EXPERIMENTAL RESULTS

Fig. 6 shows the graphs $A_{U_{VM}}$—assessments of the vulnerability exploits of a VM in a VCE (Line 1)—and A_{VM}—assessments of the vulnerability of a VM (Line 2). These indicators were obtained by processing the experimental data using formulas (11) and (10).

The graphs in Fig. 6 show how many vulnerabilities in the VMs can be used by an attacker to compromise them. We should note that the lower these indicators are, the lower the risk that an attacker could achieve this goal. If one of the indicators exceeds a value of 0.5, then, with a high degree of probability, it can be considered that the overall FS indicator of the VCE will also be high. This, in turn, means that there is a high probability of the VM being compromised and appropriate countermeasures being taken against it.

Assessment of a VM depends on the FS index (FS_{VM}), shown in Fig. 7, which displays the general state of the FS of the test VCE or for a specific IO. The lower the value, the higher the state of the FS of the VM in a private cloud environment.

Fig. 8 shows the graphs for a comprehensive indicator CO of countermeasure selection, reflecting the value of the negative influence of the countermeasure on the SLA. The obtained graph also reflects the costs required to implement countermeasures in terms of resources and operational complexity (the higher the indicator, the greater the cost [cost]). These indicators together reflect a comprehensive indicator CO of countermeasure selection. It should be noted that countermeasures with a high CO correspond to more serious and rarely used countermeasures that can significantly change almost the entire infrastructure of the VCE.

Fig. 9 shows the values of the indicator FS_{VM} of a test VM before and after the appropriate countermeasure. Graph analysis of Fig. 9 shows that the average reduction of VM vulnerability is approximately 12–17%. This makes it possible to increase the efficiency of a VCE based on software-configured networks.

The novelty of this research is that the following models have been improved:

1) Model of influence of attacks on VCRs. The proposed model differs from the existing ones in that, for the creation of edges in the ACG, a function is used that takes into account the time difference between alerts received from neighboring nodes in the system.

2) Model of assessment of the VCR state. The model differs from the existing ones in that, in order to select countermeasures, indicators are used of the influence of a countermeasure on the SLA of the VCR and of the costs required for the use of countermeasures in terms of resources and operational complexity.

A methodology is proposed for providing FS for VCEs based on SCNs. The methodology, unlike the well-known ones, is based on a mechanism for detecting attacks and reconfiguring virtual networks, which makes it possible to increase the FS of VMs against being compromised; for this, a complex indicator FS_{VM} is used.

The disadvantages include the fact that a small-scale virtual network consisting of only 25 VMs was used to test the proposed methodology. In the future, it is planned to increase the number of VMs in the test network by 100–150.

Compared to similar studies [4, 7], we primarily focused on the complex formulation of the problem of protecting the cloud environment and on the development of an algorithm for selecting countermeasures that can guarantee the protection of cloud resources in conditions of increasing complexity of cyberattacks on them.

7. CONCLUSIONS AND SUGGESTIONS

The main research results presented in this article are as follows:

1) The tasks of ensuring the FS and CS of VCRs for various IOs were investigated. It was shown that FS and CS are achieved on the basis of a systematic approach to solving the problem of increasing the reliability and security of complex control objects.

2) The mathematical model for providing the FS and CS of VCRs for software-configured networks of IOs was improved by taking into account the influence on VCRs of cyberattack parameters. The model also takes into account the state of the VCR and the selection of possible countermeasures based on a comprehensive indicator for software-configured networks. A graph of attacks on a VCE was developed, which allows receiving of information about all known vulnerabilities of the system and shows, in real

time, the state of the FS and CS of a VCR. As a result of the comprehensive application of the proposed models, the IO information security administrator can predict possible cyberthreats and attacks, particularly by correlating the detected events in a virtual cloud network.

3) Algorithms were developed for the analysis of threats in the cloud, the results of which are to identify one or more attack routes on a VCE and to select countermeasures for specific scenarios of attacks on the IO and its VCR.

4) A methodology was proposed for providing the FS and CS of a VCE based on the use of software-configured networks. This methodology aims to increase the resistance to compromise of VMs based on the detection of cyberattacks and the reconfiguration of virtual networks.

5) An experimental test was performed on the developed methodology and models. To confirm the adequacy of the results, a test VCE was implemented. It was experimentally shown that the proposed solutions can increase the FS and CS of VCEs by 12–17% compared with the known solutions.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through Research Group no. (RG-1438-070).

REFERENCES:

[1] G. Jakobson. “Mission-centricity in cyber security: Architecting cyber attack resilient missions,” *IEEE, In 2013 5th International Conference on Cyber Conflict (CYCON 2013),* pp. 1–18, 2013.

[2] A. AlDairi. “Cyber security attacks on smart cities and associated mobile technologies,” *Procedia Computer Science*, 109, pp.1086–1091, 2017.

[3] E. Sherzer, G. Gilboa-Freedman, H. Levy. “Resource allocation in a cloud under virus attacks,” *In VALUETOOLS*, pp. 223–224, 2017.

[4] M. Nguyen, P. Samanta, S. Debroy. “Analyzing Moving Target Defense for Resilient Campus Private Cloud,” *In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp. 114–121, 2018.

[5] J. Qi, A. Hahn, X. Lu, J. Wang, C. Liu. “Cybersecurity for distributed energy resources and smart inverters,” *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28–39, 2016.

[6] C.J. Brown, S.E. Dog, S.P. Edwards, N.C. McNab, M. Steele, J.M. Franklin. “Mobile Device Security: Cloud and Hybrid Builds,” *No. Special Publication (NIST SP)*-1800-4, 2019.

[7] M. Adelmeyer, F. Teuteberg. “Cloud Computing Adoption in Critical Infrastructures-Status Quo and Elements of a Research Agenda.," *MKWI 2018 Proceedings*, pp.1345–1356, 2018.

[8] P. Amann, A. Klayn, G. Mounier. “Changing the rules of the game: How can law enforcement deter criminals by increasing the risks of conducting cybercrime?,” *Cyber Security: A Peer-Reviewed Journal*, vol. 1, no. 1, pp. 16–27, 2017.

[9] A.A. Tamimi, R. Dawood, L. Sadaqa. “Disaster Recovery Techniques in Cloud Computing,” *In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT),* pp. 845-850, 2019.

[10] B. Duncan, A. Happe, A. Bratterud, J. Sen. “Cloud Cyber Security: Finding an Effective Approach with Unikernels,” Security in Computing and Communications; IntechOpen: London, UK, 2017.

[11] O. O. Akinsanya, M. Papadaki, L. Sun. “Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?,” *In CERC,* pp. 211–222, 2019.

[12] M. Jouini, L.B.A. Rabai. “A security framework for secure cloud computing environments,” *In Cloud security: Concepts, methodologies, tools, and applications, IGI Global*, pp. 249–263, 2019.

[13] N. Khan, A. Al-Yasiri. ”Cloud security threats and techniques to strengthen cloud computing adoption framework,” *In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, IGI Global,* pp. 268–285, 2018.

[14] D. R. Bharadwaj, A. Bhattacharya, M. Chakkaravarthy. “Cloud Threat Defense–A Threat Protection and Security Compliance Solution,” *In 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM),*pp. 95–99, 2018.

[15] E. O. Yeboah-Boateng. “Cyber-Security Concerns With Cloud Computing: Business Value Creation and Performance Perspectives,” *In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, IGI Global,* pp. 995–1026, 2018.

[16] S. Srinivasan, K. Raja. “An Advanced Dynamic Authentic Security Method for Cloud Computing,” *In Cyber Security,* Springer, Singapore, pp. 143–152, 2018.

[17] X. Masip-Bruin, E. Marin-Tordera, A. Jukan, G. J. Ren. “Managing resources continuity from the edge to the cloud: Architecture and performance,” *Future Generation Computer Systems*, vol. 79, pp. 777-785, 2018.

[18] L. Wang, A. Liu, S. Jajodia. "Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts," *Computer communications*, vol. 29, no.15, pp. 2917–2933, 2006.

[19] F. Amato, F. Moscato, V. Moscato, F. Colace. "Improving security in cloud by formal modeling of IaaS resources," *Future Generation Computer Systems,* vol. 87, pp. 754–764, 2018.

[20] V.A. Lakhno. "Algorithms for Forming a Knowledge Base for Decision Support Systems in Cybersecurity Tasks," *Advances in Intelligent Systems and Computing*, vol. 938, pp. 268–278, 2020.

[21] B. Akhmetov, V. Lakhno, Y. Tkach, A. Adranova, G. Zhilkishbayeva. "Problems of Development of a Cloud-Oriented Educational Environment of the University", *International Journal of Advanced Trends in Computer Science and Engineering*, vol.9, No.2, 2020, pp. 2196-2203.

[22] B.S. Akhmetov, B.B. Akhmetov, V. Lakhno, V. Malyukov. "Adaptive model of mutual financial investment procedure control in cybersecurity systems of situational transport centers," *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences*, vol. 3, no. 435, pp. 159–172, 2019.

[23] A. Adranova, V. Lakhno, B. Akhmetov, A. Kystaubayeva, G. Mussagulova. "Modeling of cyber threats in information networks of distance education systems", *Journal of Theoretical and Applied Information Technology*, vol.97. No 18, 2019, pp.4921-4933.

[24] L.A. Gordon, M.P. Loeb, L. Zhou. "Investing in cybersecurity: Insights from the Gordon-Loeb model," *Journal of Information Security*, vol. 7, no.2, pp. 49-60, 2016, Doi:10.4236/jis.2016.72004

[25] L.A. Gordon, M.P. Loeb, W. Lucyshyn, L. Zhou. "The impact of information sharing on cybersecurity underinvestment: A real options perspective," *Journal of Accounting and Public Policy*, vol. 34, no.5, pp. 509–519, 2015, doi: 10.1016/j.jaccpubpol.2015.05.001