Revista Cubana de Ciencias Informáticas
ISSN: 1994-1536
ISSN: 2227-1899
Editorial Ediciones Futuro

Valerievich Tsaregorodtsev, Anatoliy; Dmitrievich Volkov, Sergey
Improving information exchange processes when implementing the State's information function on the internal level
Revista Cubana de Ciencias Informáticas, vol. 15, Esp., 2021, October-December, pp. 181-198
Editorial Ediciones Futuro

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

Tipo de artículo: Artículo original
Temática: Seguridad informática
Recibido: 30/06/2021| Aceptado: 01/10/2021

# Improving information exchange processes when implementing the State's information function on the internal level

## Mejorar los procesos de intercambio de información al implementar la función de información del Estado a nivel interno

Anatoliy Valerievich Tsaregorodtsev [1*] https://orcid.org/0000-0002-8447-3352
Sergey Dmitrievich Volkov [1] https://orcid.org/0000-0003-2809-5913

[1] Moscow State Linguistic University, 38, Ostozhenka str., Moscow, 119034, Russia, avtsaregorodtsev@linguanet.ru, volkov1234@gmail.com

*Autor para la correspondencia. (volkov1234@gmail.com)

---

**RESUMEN**

La función de información es uno de los componentes clave de todo el mecanismo del Estado, todo el sistema de órganos estatales. La computación en la nube se está convirtiendo en una de las tecnologías de TI más comunes para implementar aplicaciones debido a sus características clave: soluciones flexibles, disponibilidad bajo demanda y buena relación precio / calidad. Debido a que la computación en la nube trae consigo nuevos desafíos en el campo de la seguridad de la información, es imperativo que las organizaciones controlen el proceso de gestión de riesgos de la información en la nube. Este documento propone un enfoque de evaluación de riesgos para evaluar el daño potencial del ataque a la implementación de componentes de datos confidenciales y justifica la necesidad de incluir nubes privadas con un alto grado de protección en un entorno de computación en nube híbrida. El enfoque sugerido para la estimación de riesgos de seguridad de la información permite la conducción del funcionamiento de la seguridad del entorno de nube en condiciones de influencia de clase de vulnerabilidad considerada y también una eficacia de medida y complejo de instalaciones para resistir estas vulnerabilidades. Sobre la base de la estimación recibida, surge la oportunidad de elegir entre diferentes variantes de configuración del entorno de computación en la nube y elegir la forma más adecuada de acuerdo con los requisitos de seguridad.

**Palabras clave**: esfera de información; función de información; computación en la nube; amenazas a la seguridad de la información; análisis de riesgo de información; requisitos de seguridad de la información.

## ABSTRACT

The information function is one of the key components of the State's entire mechanism, the entire system of state bodies. Cloud computing is now becoming one of the most common IT technologies for deploying applications due to its key features: flexible solutions, on-demand availability and good price/quality ratio. Due to the fact that cloud computing bring with them new challenges in the field of information security, it is imperative for organizations to control the process of information risk management in the cloud. This paper proposes a risk assessment approach for assessing the potential damage from the attack on the implementation of components of confidential data and justifies the need for the inclusion of private clouds with a high degree of protection in a hybrid cloud computing environment. Suggested approach to information security risk estimation allows conduction of cloud environment security functioning in conditions of considered vulnerability class influence and also an effectiveness of measure and facility complex to withstand these vulnerabilities. On the basis of received estimation an opportunity to choose between different variants of cloud computing environment configuration and choose more appropriate way according to security requirements arises.

**Keywords**: information sphere; information function; cloud computing; information security threats; information risk analysis; information security requirements.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

# Introducción

The current stage of social development can be characterized by the increasing influence of information sphere, which includes not only the information itself, but also information infrastructure and entities that collect, store, distribute and use information. Therefore, one of the spheres of social life, in which the role of the State has not been sufficiently studied, is the information sphere.

The need to regulate the information sphere determines the need for an appropriate direction of the State's activity — the State’s information function.

The implementation of the State's information function on the internal level is aimed at optimizing and improving the efficiency of public authorities work. Most often it includes optimization of processes that contain information with limited access or information that cannot be disclosed due to the internal belief of public authorities that there is no need to make it public, and there is no direct regulatory requirement for its disclosure.

At the same time, the creation of a full-fledged state information system is impossible without creation of a unified architecture of state structures, which simplifies the process of interdepartmental cooperation. The informatization in this sphere is aimed at improving the mechanism of information exchange between various parts of the State’s management system, developing measures to optimize internal information systems, and eliminating intra- and interdepartmental barriers.

Cloud computing is now becoming one of the most common IT technologies for deploying applications due to its key features: flexible solutions, on-demand availability and good price/quality ratio (Werner, 2012).

At the same time, the most critical issues in building a cloud-based infrastructure involve information security aspects. Achieving an organization's information security objectives is a key factor in decision-making on IT outsourcing services and, in particular, state administration bodies’ data asset migration to different models of cloud services providers. Therefore, when moving to a new model of IT services provision, special attention should be paid to the issues of ensuring data processing security (Berdnik, 2013).

The analysis of possible threats and risk analysis are the basis for the choice of measures to provide information security of cloud computing systems, which must be executed to decrease risk to accessible level (Werner, 2013, Radin, Zubarev, 2014).

While a quantitative risk assessment is widespread in some spheres such as finances and credit, a quantitative risk assessment in information security is usually accompanied by a row of restrictions where the absence of data for verification of these methods takes a special part (Kachko, Lavrynenko, Tsaregorodtsev, 2014).

Suggested approach for risk analysis and management will allow to make reasonable decisions when choosing information security systems, software for components of information systems (IS), functioning on a basis of cloud computing technologies.

# Métodos o Metodología Computacional

## The method of building an information security system on cloud architecture

Today, a number of open information security issues do not allow building secure cloud services for critical assets processing. It is only by including demilitarized zones (DMZ) as a private cloud into the architecture that we can provide the required level of security for processed data.

The private cloud environment (PCE) is characterized by the advantages of a traditional (internal) IT infrastructure, namely: the ability to apply best practices, methods and metrics for risk analysis and assessment, full control of every central IS management process and the ability to conduct internal audits. The main issues are serious financial costs of PCE creation and operation, limited scalability and fault tolerance. In addition to all the threats specific to the public environment they may also include errors in the strategic planning of the use of a computing capacity, which can reduce the availability, integrity and security of the data being processed.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

The DMZ inclusion in cloud architecture is necessary to ensure an organization's full control over its critical assets even in the face of high financial costs of PCE operation. Public cloud is needed to provide the required level of scalability and flexibility in allocating on-demand resources at peak system loads.
Use of components with different security levels leads to a new, hybrid type of cloud deployment.

To solve the problem of building a secure cloud infrastructure, we propose to consider the method of building a secure hybrid cloud environment (SHCE). The method will ensure compliance with security requirements, determine the sequence of critical data processing and ensure the location of this data between protected components of the cloud environment. Based on the above key stages of information security analysis of cloud infrastructure, we will describe the method in the Event-Driven Process Chain (EPC) notation.

## Stage 1 "Identifying and Assessing an Organization's Critical Assets"

An employee of a business unit identifies information assets involved in the business processes to be automated within the cloud environment.

The employee of the business unit analyzes and describes in detail the organization's business process by mandatorily indicating the functions responsible for critical data processing. In building and selecting a cloud architecture one should take into account information related to possible financial losses that the organization may incur in case of an unauthorized access to its confidential information.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

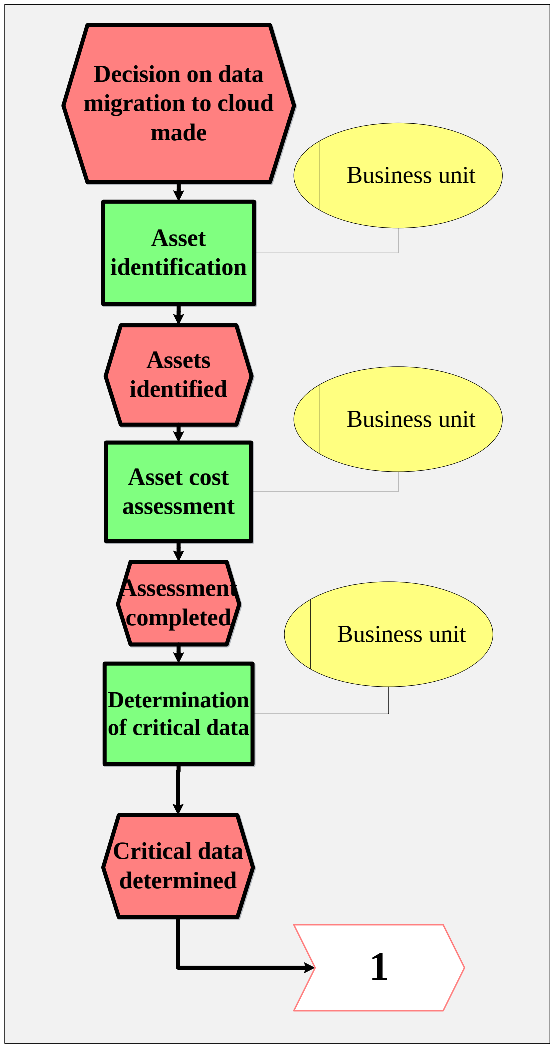


**Fig. 1 -** Stage 1 “Identifying and Assessing an Organization’s Critical Assets”.

## Stage 2 “Identification of Security Requirements and Determination of Data Processing Sequence in SHCE”

The IS service officer identifies information security requirements of the IT system based on cloud computing technology. One of the approaches to building an organization’s IS objective trees of the cloud infrastructure is considered in the paper (Tsaregorodtsev, Kachko, 2011) . The criteria and mathematical apparatus for "measuring" the system properties on objective trees based on such algebraic objects as semi-groups with a unit - monoids, is discussed in detail in (Kachko, Lavrynenko, Tsaregorodtsev, 2014).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

The sequence of critical data processing based on the formalized security model of data processing in the cloud-computing environment is described in detail in (Tsaregorodtsev, Zelenina, Ruzicky, 2017).

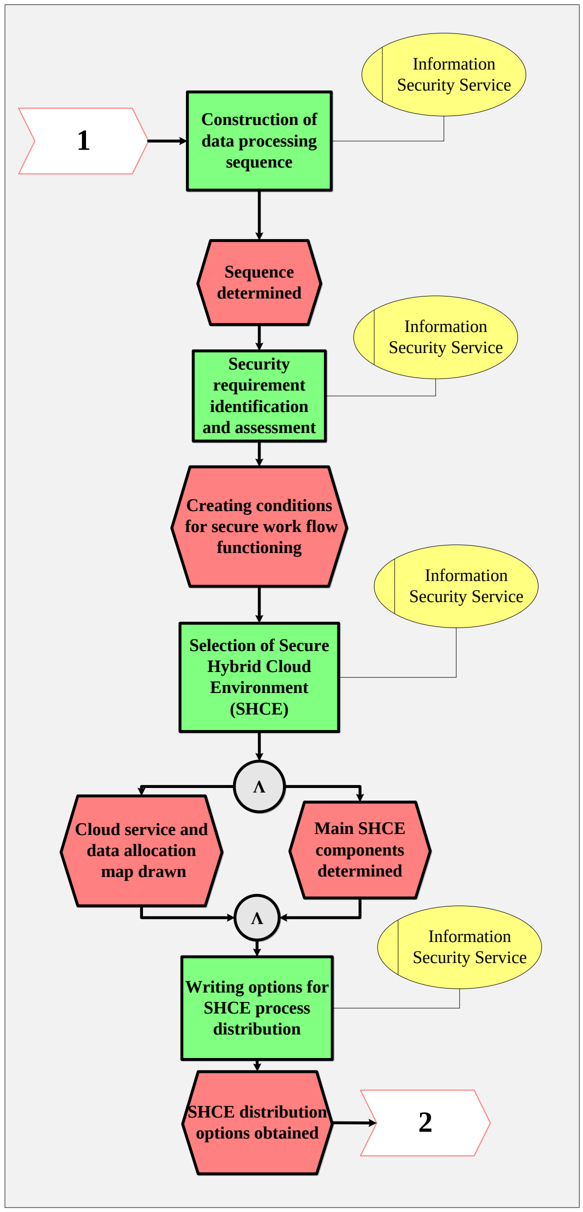


**Fig. 2 –** Stage 2 “Identifying Security Requirements and Determining Data Processing Sequence in SHCE”.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

## Stage 3 "Threat Identification and SHCE Risk Model Construction"

Information risk management is a key process of measuring various information security indicators. On this stage for each information asset, it is necessary to determine the level of its vulnerability, presence of potential threats capable of exploiting these vulnerabilities and to assess the impact of security incidents on the organization's business processes in its daily operation. To succeed in implementing all actions of the risk analysis process, it is required to introduce control and countermeasure processes into the organization.

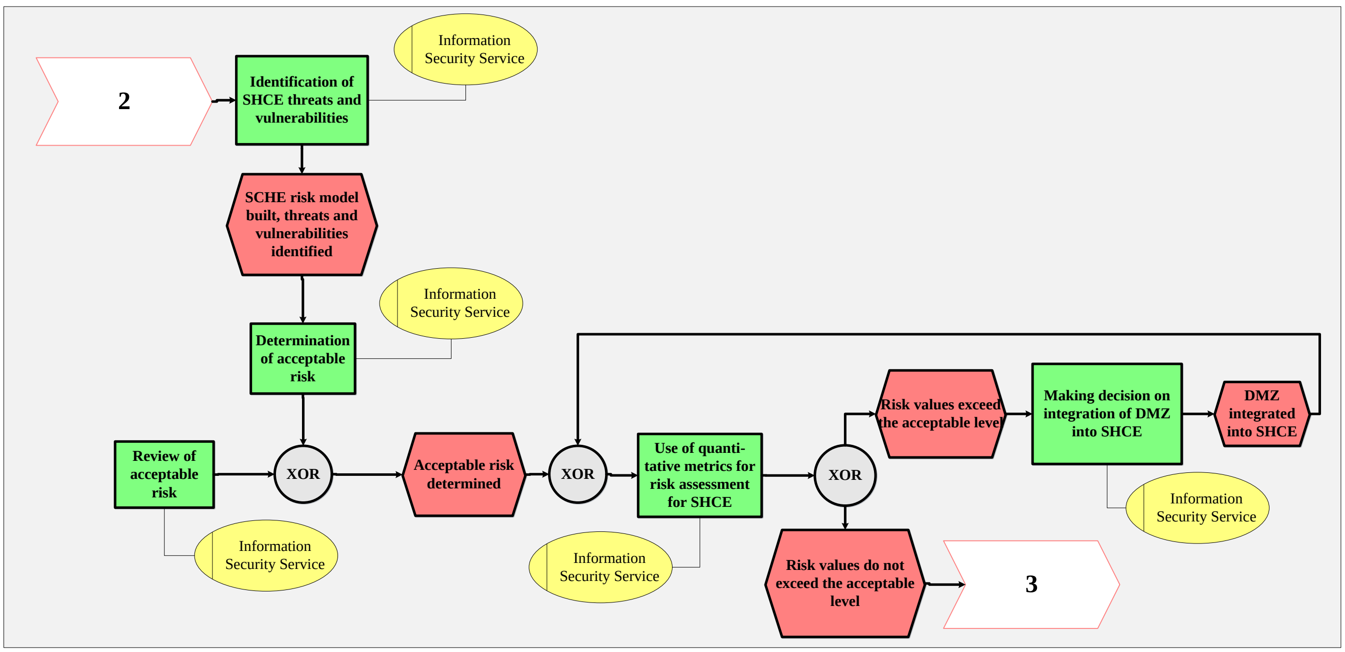


**Fig. 3 –** Stage 3 "Threat Identification and SHCE Risk Model Construction".

## Stage 4 "Application of Cost Methodology and Construction of SHCE Architecture"

Using the cost methodology, the IS service officer obtains the costs of various options for SHCE deployment and, based on practical recommendations, selects various options for building SHCE architecture.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

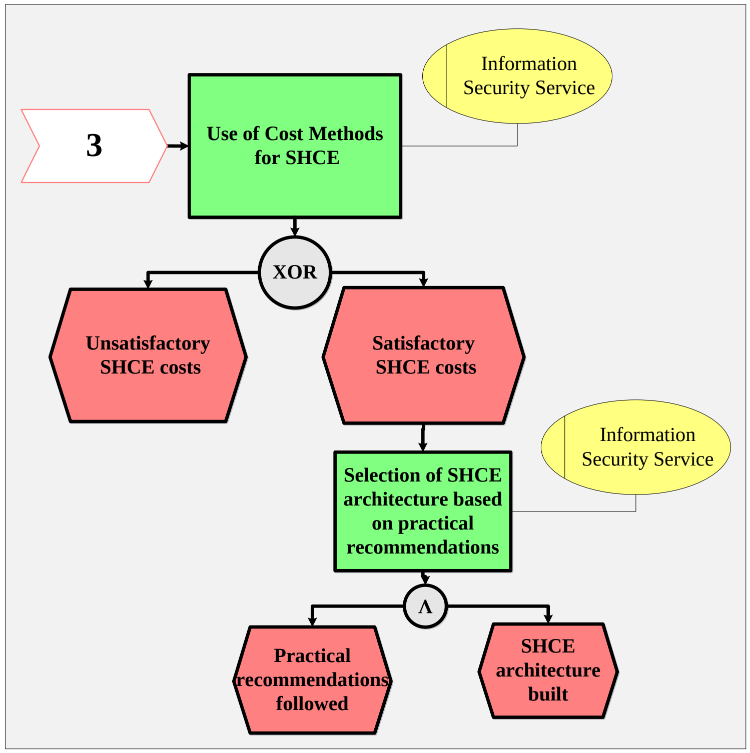


**Fig. 4 -** Stage 4 "Use of Cost Method and SHCE architecture construction".

## Fundamentals of quantitative risk assessment method

Let us define key concepts, which will be used in the suggested approach. The vulnerability is a software defect or a weakness in the security system, which can be exploited by third parties to cause damage or harm to an organization (Mell, Tim, 2011). Known vulnerabilities are vulnerabilities, which either have no bug fixes or have bug fixes, applied with a time delay. The security threat is a potential objectionable event in the object of assessment, which can lead to a successful use of exploit with unwanted influence on confidentiality, integrity and availability of assessment object assets. The result of vulnerability exploitation by any threat can be appearance of an unwanted event, which is called the malicious use (Accorsi, Wonnemann, 2010). It is worth to be noticed that malicious uses can appear only with the existence of threat as well as of vulnerability and concerned vulnerability can be exploited by a certain threat. It means that a multiplicity of all potential malicious uses is the subset of both vulnerability list and potential threats list. Consequently, where M - malicious events list, ST - threats multiplicity, SV - vulnerability multiplicity.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

Let us present the qualitative risk assessment method in the form of the following steps (table 1).

**Table 1 –** Qualitative information security risk assessment method.

| № | Step description | |
|---|---|---|
| 1 | Risk identification | |
| | 1.1 | Identification of information security risks and influence on assets |
| | 1.2 | Identification of assessment object vulnerabilities, provision principles, processes, procedures and security environment |
| 2 | Risk analysis | |
| | 2.1 | Influence level estimation of malicious use |
| | 2.2 | Frequency estimation of malicious use |
| 3 | Risk assessment | |
| | 3.1 | Risk level definition for each list of frequency and influence |
| | 3.2 | Risk assessment and comparison with criterions of risk acceptance |
| | 3.3 | Risk categorization for processing into lists of risks |
| | 3.4 | Internal relations definition between risk lists |
| | 3.5 | Identification of conflicts between risk lists |
| | 3.6 | Appointment of priority list and risks |
| | 3.7 | Solution of found conflicts |
| 4 | Risk processing | |
| | 4.1 | Identification of alternative decisions for security provision and their grouping into lists |
| | 4.2 | Effect identification and targets of alternative systems of information security (ISS) |
| | 4.3 | Estimation and search of optimal ISS or decision list for security ensuring |

On the top level suggested approach to risk estimation includes two general steps. First step describes an analysis managed by risk which includes malicious use list and connected with it risk levels estimation, which are the result of steps 2, 3 of suggested method with the following comparison of received data with criteria of risk acceptance which are defined at the first step. The result of this phase is a list of risks requiring processing (Tsaregorodtsev, Kachko, 2012).

Processing risk list, alternative decision list and other compromise parameters appropriate to the development, project or financial condition are the input data for the second step of the method, in frames of which information security risks are problems and challenges requiring decision in the form of available alternative security mechanisms (Tsaregorodtsev, 2013).

Described under the first step actions include key analysis elements: threat list, vulnerabilities, malicious use, its frequency and influence, information security risk, risk acceptance criterion (Winkler, 2016). Figure 5 describes key essences and their relations of the first step of risk assessment approach. All these

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

constituents are necessary for evaluation of estimation object risk level and its assessment focusing on comprehension of what risk requires processing (Tsaregorodtsev, 2017).

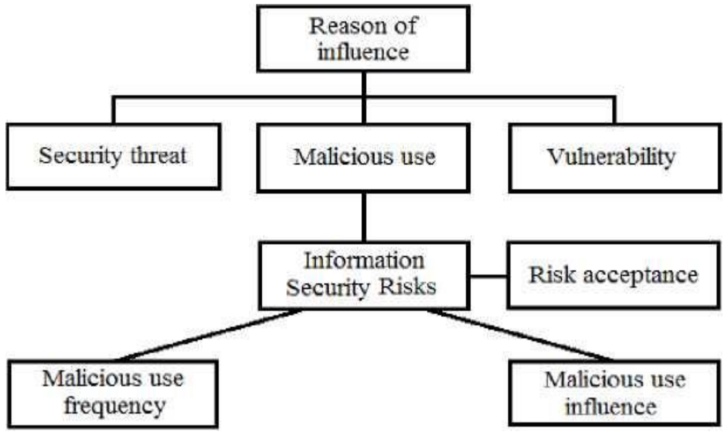


**Fig. 5 -** Indexes for risk level calculation in frames of the first step.

Herewith a risk is calculated for every malicious use by means of combination of its frequency with one of influences. It means that malicious use leads to appearance of one or many information security risks depending on amount of interconnected factors (frequency and influence). Both indexes (frequency and influence) can be defined with quantitative estimation metric basing on data from public sources, one of which is NVD Common Vulnerability Scoring System Support (CVSS).

The frequency of malicious use and its influence can be presented in the form of quantitative indexes: certain number of appearances during time interval or possibility of malicious use appearance in certain time period. The influence can be presented in the form of financial reputation losses (Tsaregorodtsev, Kachko, 2011, Tsaregorodtsev, Kachko, 2012).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

# Resultados y discusión

## Definition of malicious use frequency and corresponding influence on the basis of CVSS

We use general prepositions of CVSS method for definition of two key variables influencing on risk estimation. For this purpose let's combine indexes of basic, temporary and infrastructural metrics in a special way. The higher level of vulnerability to exploit use the more chances an attacker has to provide a successful attack and the higher is the index of malicious use frequency (F). Let us calculate this index for every vulnerability presented in the risk model of a cloud environment with assumption that fundamental vulnerability characteristics are described by the basic metric, and an index accounting of temporary metric will allow to decrease the probability of successful exploit use. The same principle is referred to the damage (influence): potential damage depends on confidentiality, availability and integrity requirements defined in infrastructural metric.

Tables 2 and 3 describe indexes chosen for analysis with corresponding CVSS weights.

Using of three basic metric indexes and three temporary metric indexes allows evaluating malicious use frequency (how often vulnerability is the subject to exploit influence). Basic metric describes vulnerability characteristics and its liability to exploit influence because these indexes are chosen for determination of primary frequency.

It is considered that the primary frequency can be updated. Temporary metric indexes include indirect factors of vulnerability in question.

**Table 2 -** CVSS indexes for malicious use frequency calculation.

| Metric group | Index | Index meaning | Weight |
|---|---|---|---|
| Basic | Access vector (AV) | Local access (L) | 0,395 |
| | | Adjoin network (A) | 0,646 |
| | | Network (N) | 1 |
| | Complexity vector (AC) | High (H) | 0,35 |
| | | Medium (M) | 0,61 |
| | | Low (L) | 0,71 |

| | | | |
|---|---|---|---|
| | Authentication (Au) | Reusable | 0,45 |
| | | Disposable | 0,56 |
| | | Absent | 0,704 |
| Temporary | Indexes of code and exploit techniques availability (Au) | Theory (no proof) (U) | 0,85 |
| | | Experiment (POC) | 0,9 |
| | | Functional (F) | 0,95 |
| | | High (H) | 1 |
| | Indexes of solution readiness level (RL) | Official patch (OF) | 0,87 |
| | | Temporary decision (TF) | 0,9 |
| | | Decision based on advice or recommendations (W) | 0,95 |
| | | Absent (U) | 1 |
| | Indexes of information reliability level (RC) | Conjectural character (UC) | 0,9 |
| | | Unregulated (UR) | 0,95 |
| | | Accepted (C) | 1 |

**Table 3 -** CVSS indexes for malicious use influence calculation.

| Metric group | Index | Index meaning | Weight |
|---|---|---|---|
| Basic | Influence on confidentiality (C) | No (N) | 0 |
| | | Partial (P) | 0,275 |
| | | Complete (C) | 0,66 |
| | Influence on integrity (I) | No (N) | 0 |
| | | Partial (P) | 0,275 |
| | | Complete (C) | 0,66 |
| | Influence on availability (A) | No (N) | 0 |
| | | Partial (P) | 0,275 |
| | | Complete (C) | 0,66 |
| Infrastructural | Confidentiality requirements (CR) | Low (L) | 0,5 |
| | | Medium (M) | 1,0 |
| | | High (H) | 1,51 |
| | Integrity requirements (IR) | Low (L) | 0,5 |
| | | Medium (M) | 1,0 |
| | | High (H) | 1,51 |
| | Availability requirements (AR) | Low (L) | 0,5 |
| | | Medium (M) | 1,0 |
| | | High (H) | 1,51 |
| | Concomitant potential damage (CDP) | Low (L) | 0,1 |
| | | Low-Medium (LM) | 0,3 |
| | | Medium-High (MH) | 0,4 |
| | | High (H) | 0,5 |

Then received estimation must be normalized to receive values within interval [0; 1], what allow interpretation of received values as it is presented in table 4.

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

**Table 4 -**Values of exploit use frequency.

| Value | Interpretation |
|---|---|
| 0 | Vulnerability is unavailable for exploit use |
| [0; 0,5] | Opportunity to use exploit is low |
| [0,5; 1] | Opportunity to use exploit is high |
| [1] | Vulnerability will be used accurately |

## Detection of damage under successful use of exploit based on basic and infrastructural metric

Let us introduce new index *I*, which will describe damage to an organization with successful realization of exploit. This index will also be used for vulnerability grouping into a certain transitional model condition in the form of service level. For this purpose it is considered to use three attributes of basic metric (C, I, A) and four attributes of infrastructural metric (CR, IR, AR, CDP), the description is presented in table 3. Infrastructural metric indexes depend on vulnerability use context specific; include possible damage to confidentiality, integrity and availability in a cut of security requirements and potential concomitant damage of certain model condition. Basic metric indexes describe a value of effect on every certain security component, which subsequently is considered in frames of a certain context of infrastructural indexes. Similarly to index of exploit use frequency, basic metric is used for evaluation of primary damage, which represents vector of confidentiality integrity and availability.

## Detection of service levels

Let us represent service levels in the form of condition transition model (Markov process). The first condition represents the absence of damage to confidentiality, integrity and availability and can be described in the form of [0,0; 0,0; 0,0]. The last condition represents maximum damage to confidentiality, integrity and availability taking into account infrastructural metric indexes. Condition [1,0; 1,0; 1,0] is absorbing condition and describes the absence of opportunity to use patch in frames of the model. Thus, the first condition corresponds to complete service level SL0, the last represents the absence of service SLx. All conditions between boundary levels can include complete service list as well as any number of services with lower level or the absence of services depending on the model in question (Trope, Power et al, 2007, Tsaregorodtsev, 2013).

Revista Cubana de Ciencias Informáticas
Vol. 15, No. Especial UCIENCIA I, Septiembre, 2021
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 181-198

## Definition of risk level basing on damage and frequency indexes

For risk level dimension, let us introduce a notion of service level presented in the form of Markov process with continuous time. Service levels depend on project decision and information system' realization variant functioning on the basis of cloud computing technologies, framework of such information system and application list, in other words on the way of information system' using.

Firstly, we define a vulnerability list according to public data, for example to official messages about vulnerabilities, databases (NVD) or by launching special scanner (Nessus).

As it was already mentioned, the damage from successful exploit use describes a seriousness of the vulnerability. However, this does not mean that two vulnerabilities leading to the same damage have the similar seriousness level for described environment and lead to commensurate decrease of service maintenance. In this connection, it is necessary to solve the task of vulnerability seriousness level intervals determination with the following determination of service levels for them. As a result, we obtain service level list beginning with level without service presentation and ending at complete service list, described in the form of condition model. Service level we define as not empty list of vulnerabilities having influence level from the same interval.

Secondly, condition transition model is explored, which was received during the first step and is supplemented by transition intensity. The transition intensity defines the opportunity when a transition from one condition to another is possible and with what probability it is possible to be in this condition at a certain time interval $t$. In the risk level estimation model, every condition refers to the total level of vulnerability list seriousness. Thus, a condition transition model describes different risk levels typical for considered environment at the moment of time $t$. For definition of transition intensity, it is necessary to consider aggregate frequency of exploit use at the certain time interval.

# Conclusiones

To solve the problem of forming an organization's secure cloud infrastructure, it is proposed to use the method of building a protected hybrid cloud environment. The application of this method will significantly increase the efficiency of IT resources, greatly reduce their costs through diversification of the information flows during their migration to hybrid cloud architecture, ensure compliance with security requirements, determine the sequence of critical data processing and ensure the location of this data between protected cloud environment components.

Suggested approach to information security risk estimation allows conduction of cloud environment security functioning in conditions of considered vulnerability class influence and also an effectiveness of measure and facility complex to withstand these vulnerabilities (Tsaregorodtsev, 2017). On the basis of received estimation an opportunity to choose between different variants of cloud computing environment configuration and choose more appropriate way according to security requirements arises.

**Agradecimientos & Financiación**

The reported study was funded by the Ministry of Science and Higher Education of the Russian Federation according to the research project No. FSFU-2020-0020.

# Referencias

Werner, O. Clouds, the virtual infrastructure and information security. Elvis-Plus Publish, 2012.

Kachko, A.K., Lavrynenko, M.M., Tsaregorodtsev, A.V. the approach of secure hybrid cloud construction. safety of information technology, 2014, № 1: 22-27.

Radin, P.K., Zubarev, I.V. The main threats to the security of information in virtual environments and cloud platforms. Cybersecurity. 2014. № 2 (vol. 3).

Sidorova, M. Conflicting Cloud. [22.05.2021]. Disponible en: http://www.itsec.ru/articles2/oborandteh/protivorechivie-oblaka.

Berdnik, A. Threats to Cloud Computing and methods of their protection. [22.05.2021]. Disponible en: http://habrahabr.ru/post/183168.

Winkler, B. Cloud computing: security issues in virtual clouds. Adapted excerpt from the book "Securing the sloud" (Syngress, a division of the publishing house Elsevier). [22.05.2021]. Disponible en: http://technet.microsoft.com/ru-ru/magazine/hh641415.aspx.

Tsaregorodtsev A.V. Security risk analysis of data in corporate networks-bank financial institutions on the basis of cloud computing. National interests: priorities and safety, 2013, № 39 (vol. 228): 35-44.

Tsaregorodtsev, A.V., Kachko, A.K. Ensuring information security in cloud architecture of organization. National Security, 2011, № 5: 25-34.

Tsaregorodtsev, A.V., Kachko, A.K. One of the approaches to the management of information security in the development of information infrastructure. National Security, 2012, № 1 (vol. 18): 46-59.

Accorsi R., Wonnemann C. Auditing Workflow Execution against Dataflow Policies. In Proc. BIS, 2010: 207-217.

Mell P., Tim Grance T. The NIST Definition of Cloud Computing, Version 15, 2011. [08.05.2021]. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

NVD Common Vulnerability Scoring System Support v.2. (National Institute Of Standards and Technology). [08.05.2021]. Disponible en: http://nvd.nist.gov/cvss.cfm?calculator&version=2.

Trope, R.L., Power, E.M., Polley, V.I., Morley, B.C. A Coherent Strategy for Data Security through Data Governance. IEEE Security & Privacy, 2007, № 3 (vol. 5): 32-39.

Tsaregorodtsev, A., Zelenina, A., Ruzicky, E. Methodology of vulnerability assessment for various types of cloud structures. Information Technology Applications, 2017, № 1: 51-59.

Tsaregorodtsev, A.V, Zelenina, A.N., Saveliev, V.A. Classification of vulnerabilities of cloud environments in the problem of quantitative risk assessment. Modeling, optimization and information technology, 2017, № 4 (19). [06.03.2020]. Disponible en: https://moit.vivt.ru/wp-content/uploads/2017/10/ZaregorodzevSoavtori 4 2 17.pdf

Tsaregorodtsev A.V. Two-stage procedure for quantitative assessment of information security risk of cloud computing. Modeling, optimization and information technology, 2017. № 4.

## Conflicto de interés

El autor autoriza la distribución y uso de su artículo.

## Contribuciones de los autores

1. Conceptualización: Anatoliy Valerievich Tsaregorodtsev.
2. Curación de datos: Sergey Dmitrievich Volkov
3. Análisis formal: Sergey Dmitrievich Volkov
4. Adquisición de fondos: Anatoliy Valerievich Tsaregorodtsev
5. Investigación: Sergey Dmitrievich Volkov
6. Metodología: Anatoliy Valerievich Tsaregorodtsev
7. Administración del proyecto: Anatoliy Valerievich Tsaregorodtsev
8. Recursos: Anatoliy Valerievich Tsaregorodtsev
9. Software: Sergey Dmitrievich Volkov
10. Supervisión: Anatoliy Valerievich Tsaregorodtsev
11. Validación: Anatoliy Valerievich Tsaregorodtsev
12. Visualización: Sergey Dmitrievich Volkov
13. Redacción – borrador original: Sergey Dmitrievich Volkov
14. Redacción – revisión y edición: Anatoliy Valerievich Tsaregorodtsev