УДК 330.341.1:004.75]:330.46]](043.3) DOI: 10.33111/mise.98.5

Галіцин В. К., д.е.н.,
професор кафедри інформаційного менеджменту
Галіцина О. В., к.е.н.,
доцент кафедри статистики
Камінський О. Є., к.е.н.,
доцент кафедри інформаційного менеджменту Київський національний економічний університет імені Вадима Гетьмана

Galitsin V. K., Doctor of Economic Sciences,
Professor of the Information Management Department,
Galitsina O. V., Candidate of Economic Sciences,
Associate Professor of the Statistic Department,
Kaminsky O. E., Candidate of Economic Sciences,
Associate Professor of the Information Management Department,
Kyiv National Economic University named after Vadym Hetman

СИСТЕМНИЙ АНАЛІЗ ОРГАНІЗАЦІЇ МОНІТОРИНГУ ХМАРНИХ ПЛАТФОРМ

SYSTEM ANALYSIS OF THE MONITORING ORGANIZATION CLOUD PLATFORM

Анотація. *У статті досліджено теоретичні засади та інструментарій організації систем моніторингу хмарних платформ у сучасних умовах, із застосуванням системного підходу в якості методологічної бази дослідження моніторингу хмарних технологій. Запропоновано узагальнену модель поведінки користувачів та взаємодії суб'єктів у системі хмари в якості нечіткого недетермінованого цифрового автомата. Проаналізовано архітектуру хмарних платформ. Розроблено структурну схема взаємодії хмарної платформи і підсистеми моніторингу поведінки користувачів і взаємодії суб'єктів, яка контролює всі вхідні і вихідні значення користувачів, суб'єктів і систем як ціле, веде звіт про свою роботу та реалізує дозволені переходи відповідно до правил моніторингу. Дана модель аналізу дій користувачів і акторів хмарних платформ є елементом системи моніторингу хмарної платформи і буде сприяти підвищенню рівня захищеності систем хмарних обчислень. Модель для моніторингу поведінки користувачів та взаємодії суб'єктів у системі хмари являє собою сигнатурну модель для пошуку заборонених дій у системі хмарної платформи. Запропоновано алгоритм аналізу поведінки користувача в системі хмарної платформи призначений для розробки системи моніторингу. Запропонований підхід дозволить підвищити безпеку платформи за рахунок підвищення надійності виявлення несанкціонованих запитів і дій користувачів, а також учасників взаємодії в системі хмари. Експертно-аналітичні методи дозволять визначати загальний рівень критичності системи захисту хмарної платформи, її слабкі місця, для того, щоб отримати загальну суму оцінок по всіх інформаційних ресурсах. Зазначені методи допомагають виявити елементи, що потребують максимального захисту. Подальші дослідження мають концентруватися на доповненні даної моделі розрахунком факторів ризику при моніторингу хмарних сервісів, розгорнутих в хмарі.*

Ключові слова: *системи моніторингу, хмарні платформи, цифрові автомати, потоки даних, хмарні обчислення, інформаційні технології.*

Abstract. *The theoretical bases and tools of the organization of cloud platform monitoring systems in modern conditions are investigated in the article, using the system approach as a methodological basis for the study of cloud technology monitoring. A generalized model of user behavior and interaction of entities in the cloud system is proposed as a fuzzy undetermined digital automaton The architecture of cloud platforms is analyzed. A block diagram of the cloud platform and subsystem monitoring of user behavior and entity interaction has been developed, which monitors all inputs, outputs of users, entities and systems as a whole, keeps track of its operations, and implements permitted transitions in accordance with monitoring rules. This model of analysis of actions of users and actors of cloud platforms is an element of the monitoring system of the cloud platform and will help to increase the level of security of cloud computing systems. A model for monitoring user behavior and the interaction of entities in the cloud system is a signature model for looking for prohibited activities in the cloud platform system. The proposed algorithm for analyzing user behavior in the cloud platform system is designed to develop a monitoring system. The proposed approach will improve the security of the platform by increasing the reliability of detection of unauthorized requests and actions of users, as well as participants of interaction in the cloud system. Expert-analytical methods will allow to determine the general level of criticality of the system of protection of the cloud platform, its weaknesses, in order to obtain the total sum of estimates for all information resources. These methods help identify items that need maximum protection. Further studies should focus on complementing this model with the calculation of risk factors in monitoring cloud-deployed cloud services.*
Keywords: *monitoring systems, cloud platforms, digital vending machines, data flows, cloud computing, information technology.*

Постановка проблеми. Незважаючи на зростаючу кількість досліджень у даному напрямку, питання міграції IT-інфраструктур підприємств до хмарних середовищ в IT-сфері України та економічні наслідки такого впровадження у вітчизняній економічній науці поки недостатньо вивчені.

Зарубіжні та вітчизняні дослідники вважають, що проблеми з безпекою є однією з найбільших перешкод на шляху до повного переходу на використання хмарних сервісів [1, 2]. У дослідженні Т. Акермана та інших [3] зазначено, що хмарні обчислення, як найпоширеніша парадигма IT-аутсорсингу, все ще має серйозні ризики щодо IT-безпеки, а також стверджується, що дослідники все ще не в змозі повною мірою відобразити складний характер ризиків IT-безпеки та методи їх вимірювання. Аналітики дослідницької та консультаційної компанії в сфері промисловості IDC повідомляють, що 87,5 % їх клієнтів вважають, що безпека хмари є головною проблемою [4]. Розвиток парадигми хмарних обчислень в Україні приведе до того, що всі апаратно-програмні компоненти IT-інфраструктури підприємств мігруватимуть до хмар зовнішніх провайдерів, які й виконуватимуть функції сторони,

що відповідає за забезпечення моніторингу інформаційних ресурсів, необхідних для її роботи, що і визначає актуальність даного дослідження.

Аналіз останніх досліджень і публікацій. Безпека великих хмарних платформ охоплює кілька категорій. У роботі Д. Фернандеса та Л. Соареса [5] були проаналізовані наукові публікації з проблем хмарної безпеки, що стосуються вразливостей, загроз і нападів. Автори визначають основні поняття, що лежать в основі безпеки хмар, та класифікують їх таким чином: елементи віртуалізації, мульті-оренда, хмарна платформа та програмне забезпечення, аутсорсинг даних, безпека зберігання даних і стандартизація та довіра до провайдера. Також автори розглядають управління ризиками для кожної категорії. У дослідженні [6] проголошено, що поява хмарних вірусів пов'язана зі складною віртуалізованою інфраструктурою хмари та її динамічним характером, і вразливості можна поділити на три складові: По-перше, багаторазовий доступ до хмари різних користувачів з усього світу несе відповідальність за виток інформації. По-друге, користувачі хмар не знають розташування їх віртуальних машин, а провайдер не знає вміст віртуальних машин і програм, що дає шлях до загроз безпеки. По-третє, всі віртуалізовані сервери підключені до обмеженої кількості мережевих карт, що призводить до більшої вразливості в віртуальному середовищі.

На нашу думку, існуючі моделі моніторингу інформаційних систем не повністю можуть бути застосовані для випадку впровадження парадигми хмарних обчислень, оскільки жодна з них не враховує особливостей внутрішньої взаємодії базових рівнів хмари, що є характерною ознакою хмарного середовища, та не враховує можливість віддаленого доступу до хмарних сервісів.

Формулювання цілей статті. У статті досліджено теоретичні засади та інструментарій організації систем моніторингу хмарних платформ у сучасних умовах, із застосуванням системного підходу в якості методологічної бази дослідження моніторингу хмарних технологій.

Основний матеріал дослідження. Використовуючи положення теорії систем і системного аналізу, представимо хмару у вигляді кортежу:

$$DP = \langle R, D, W, L, \rangle \,, \tag{1}$$

де R — інформаційні ресурси, представлені у вигляді множини елементів $r_i, i = \overline{1,k}$. Ресурси характеризуються нечіткістю вла-

стивостей інформації, в числі яких назвемо конфіденційність, цілісність і доступність. Склад інформаційних ресурсів, відповідних хмарі, визначається спільно технічним і керуючим персоналом ЦОД; D — характерні для хмарної платформи загрози, представлені у вигляді множини об'єктів $d_j, j = \overline{1,m}$. Усі виявлені загрози групуються по виду впливу на властивості ресурсу, який має бути захищеним; W — характерні для хмарної технології вразливості, представлені у вигляді множини об'єктів $w_n, n = \overline{1,l}$; L — характерні для хмарної технології інформаційні зв'язки між її елементами, які ми можемо представити у вигляді $L_{r,d,w,m}(l_1, l_2)$, де $l_1, l_2 \in R \cup D \cup W$.

Виділимо три типи інформаційних зв'язків для хмарної платформи:

1. Взаємодія інформаційних ресурсів хмари:

$$L_{r_1 r_2} = \begin{cases} 1, \text{якщо ресурси пов}'\text{язані;} \\ 0, \text{взаємодії немає} \end{cases}$$

2. Взаємодія інформаційних ресурсів і загроз:

$$L_{r_1 d_1} = \begin{cases} 1, \text{якщо взаємодія є;} \\ 0, \text{взаємодії немає} \end{cases}$$

3. Взаємодія загроз і відповідних вразливостей:

$$L_{d_1 w_1} = \begin{cases} 1, \text{якщо взаємодія є;} \\ 0, \text{взаємодії немає} \end{cases}$$

Відзначимо, що адекватну модель хмари і DP_i можна отримати тільки після визначення множин об'єктів і інформаційних зв'язків між її елементами.

У зв'язку з цим виникає потреба, оцінюючи хмарні ризики, визначати інформаційні ресурси, які потребують моніторингу. Ресурси можна розділити на дані, програми та процеси. Вплив на систему безпеки процесу міграції IT-інфраструктури до хмарного середовища залежить від моделі хмарних послуг і моделі розгортання хмари. Поєднання моделі обслуговування та моделі розгортання може допомогти визначити відповідний баланс системи безпеки для інформаційних ресурсів.

Архітектура хмарної платформи включає використання 7 головних дійових акторів (табл. 1).

Таблиця 1

ОСНОВНІ АКТОРИ ХМАРНОЇ ПЛАТФОРМИ

Назва актора	Функції
Ресурс	Сутність, що відповідає за доступність хмарного сервіса або послуги для кінцевих користувачів
Користувач хмарної платформи	Особа або організація, яка використовує, або створює ресурси хмарної платформи
Адміністратор хмарної платформи	Особа або організація, що виконує оцінку наданих ресурсів, послуг, обслуговує інформаційні системи, контролює продуктивність і безпеку реалізації хмари
Агрегатор хмарної платформи	Сутність, яка керує використанням і наданням ресурсів і послуг кінцевим користувачам. Інтегрує хмарні сервіси
Оператор зв'язку	Посередник, який надає послуги підключення між ресурсом і користувачем (мережа Інтернет)
Програмний агент системи безпеки	Сутність, що контролює запити від користувачів до ресурсів, яка визначає процеси необхідні для надання послуги або ресурсу користувачам
Програмний агент системи моніторингу	Сутність, що контролює всю платформу в цілому та визначає індикатори роботи хмарної платформи

Джерело: розробка авторів

У даному випадку модель акторів нами використовується в якості основи для моделювання системи моніторингу хмарної платформи. Ідея композиції систем акторів є важливим аспектом модульності. Програмний агент системи безпеки та моніторингу хмарної платформи є суб'єктом, відповідальним за моніторинг та адекватність запитів користувачів, за правильність відправлення запиту іншим суб'єктам системи та за взаємодію суб'єктів.

Щоб зрозуміти роботу цього актора, необхідно проаналізувати поведінку користувача в системі хмарних обчислень. Модель для моніторингу поведінки користувачів і взаємодії суб'єктів у системі хмари являє собою сигнатурну модель для пошуку заборонених дій у системі хмарної платформи. Запропонований алгоритм аналізу поведінки користувача в системі хмарної платформи призначений для розробки системи моніторингу. Запропонований підхід дозволить підвищити безпеку платформи за рахунок підвищення надійності виявлення несанкціонованих запитів і дій користувачів, а також учасників взаємодії у системі хмари.

Узагальнена модель поведінки користувача та взаємодії суб'єктів у хмарній системі в якості нечіткого недетермінованого цифрового автомата M представлена у виразі функцією:

$$M = \{T, T_0, P_1, P_2, f, \beta\}, \quad (2)$$

де M — модель поведінки користувачів хмарної платформи у вигляді цифрового автомата, T — поточний стан хмарної платформи внаслідок дій користувачів, T_0 — початковий стан хмарної платформи, P_1 — вхідний набір правил для опису дій користувачів, P_2 — вихідний набір реакцій хмарної платформи на дії користувачів, $f(t, p_1)$ — функція переходу для системи моніторингу хмарної платформи, $\beta(t, p_1)$ — функція виходів для системи моніторингу хмарної платформи.

У відповідності з (2) функція f породжує множину нечітких матриць переходу, а функція β породжує множину нечітких матриць виходу. Серед множини станів автомата виділяється множина фінальних (заключних) станів. При традиційному використанні автоматної моделі, стани, управляючі рішення, функції переходів і виходів відомі або з даних моніторингу, або експертним шляхом. Для виконання певної операції у системі користувач виконує певну послідовність дій (виконання операцій, введення даних, виконання умов, виведення даних, запит ресурсів і послуг). Представлена математична модель системи моніторингу хмарної платформи описує всі вхідні та вихідні значення та стани системи та поведінку користувача в системі. При використанні автоматного підходу функція переходів може задаватися експертним шляхом і відображати вже наявний досвід фахівців.

Таким чином, на рис. 1 відображено структурну схему взаємодії хмарної платформи і підсистеми моніторингу поведінки користувачів і взаємодії суб'єктів, згідно з якими вона контролює всі вхідні і вихідні значення користувачів, суб'єктів і систем як ціле, веде звіт про свою роботу, впливає на комп'ютерну підсистему для реалізації дозволених переходів відповідно до таблиці виходів і переходів. Користувач виконує дію над хмарним сервісом платформи, під впливом попередніх дій, виконаних над цим сервісом. Платформа виконує дії користувача тільки у випадку, якщо підсистема моніторингу дозволить цю дію. Контроль здійснюється згідно з попередньо скомпільованою таблицею виходів, переходів і правил моніторингу. Для визначення можливих каналів витоку інформації у хмарній платформі необхідно визначити інформаційні потоки в системі хмарних обчислень.

У результаті аналізу системи хмарних обчислень були визначені такі інформаційні потоки:

- протокол дій хмарного агрегатора;
- протокол дій адміністратора;
- протокол дій користувачів хмарної платформи;
- відомості про стан ресурсів хмарної платформи;
- дані про запити, дії та час роботи користувачів хмарної платформи (всіх груп).

Для даної моделі основною функцією буде аналіз аномальної поведінки користувачів хмарної платформи на основі автоматної черги. Далі потрібно визначити вхідні та вихідні потоки.

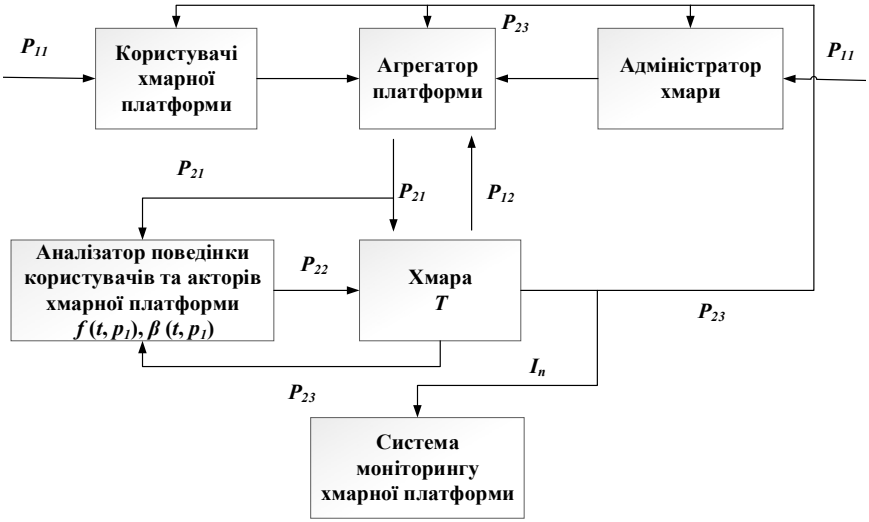

Рис. 1. Структурна схема взаємодії
хмарної платформи та користувачів

Джерело: розробка авторів

де P_{11} — керуючий вплив на користувачів або акторів платформи, P_{12} — вплив платформи на користувача або актор (правила), P_{21} — протокол дій користувачів, P_{22} — реакція підсистеми моніторингу безпеки на дії користувачів, P_{23} — реакція платформи на дії користувачів або акторів (результат роботи платформи), I_n — індикатори ризику впровадження та стану системи безпеки платформи.

Вхідними інформаційними потоками є:

– протокол дій хмарного агрегатора;

– протокол дій адміністратора;
– протокол дій користувачів хмарної платформи;
– алгоритм аналізу запитів і дій акторів хмарної платформи;
– шаблони нормальних і аномальних запитів і поведінки користувачів.

Вихідним інформаційними потоками будуть:
- звіти щодо запитів і поведінки акторів платформи;
- формування шаблонів запитів і поведінки акторів платформи;
- індикатори роботи хмарної платформи (технічні та фінансові).

Висновки. Дана модель аналізу дій користувачів і акторів хмарних платформ на базі нечіткого недетермінованого цифрового автомата є елементом системи моніторингу хмарної платформи і буде сприяти підвищенню рівня захищеності систем хмарних обчислень. Експертно-аналітичні методи дозволять нам визначати загальний рівень критичності системи захисту хмарної платформи, її слабкі місця. Для цього необхідно отримати загальну суму оцінок по всіх інформаційних ресурсах. Зазначені методи допомагають виявити елементи, що потребують максимального захисту. Подальші дослідження мають концентруватися на доповненні даної моделі розрахунком факторів ризику при моніторингу хмарних сервісів, розгорнутих у хмарі.

Список літератури

1. Bohli J., Gruschka N., Jensen M., Iacono L.L., Marnau N. Security and Privacy-Enhancing Multi cloud Architectures. *IEEE Transactions on Dependable and Secure Computing,* Vol. 10. №4, 2013. URL: https://www.semanticscholar.org/paper/Security-and-Privacy-Enhancing-Multicloud-Bohli-Gruschka/0e841 8f57749f77718f05f3db39b32353e8d1931 (дата звернення: 22.10.2018).

2. Gill A., Banker D., Seltsika P. Moving Forward: Emerging Themes in Financial Services Technologies Adoption. *Communications of the Association for Information Systems:* Vol. 36, Article 12, 2015. URL: https://www.semanticscholar.org/paper/Moving-Forward%3A-Emerging-Themes-in-Financial-Gill-Bunker/99b1e6c3770de1067ace1d575e0727a87b8d58da (дата звернення: 22.10.2018).

3. Ackermann T., Widjaja T., Benlian A., Percieved IT Security Risks of Cloud Computing: Conceptualization and Scale Development. *Thirty Third International Conference on Information Systems*, 2012. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.665.7295&rep=rep1&type=pdf (дата звернення: 22.10.2018).

4. Christiansen C. A., Kolodgy C. J., Hudson S., Pintal G. Identity and Access Management for Approaching Clouds. *White paper*, 2010. URL:

https://ru.scribd.com/document/82546531/Cloud-Security-Wp-236234-PDF (дата звернення: 22.10.2018).

5. Fernandes D., Soares L. F. B., Gomes J. V. Security issues in cloud environments: a survey. Int. J. Inf. Secur. 13:113–170, 2014. URL: http://www.di.ubi.pt/~mario/artigos/2013-IJIS.pdf (дата звернення: 22.10.2018).

6. Mansukhani B., Zia T. A. The Security Challemges and Countermeasures of Virtual Cloud. *Australian Information Security Management Confference*, 2012. URL: https://researchoutput.csu.edu.au/en/publications/the-security-challenges-and-countermeasures-of-virtual-cloud (дата звернення: 22.11.2018)

7. Галіцин В.К., Камінський О.Є. Моніторинг хмарних сервісів, розгорнутих в багато хмарному середовищі. *Моделювання та інформаційні системи в економіці*. 2017. Вип. 94. С. 160–169.

References

1. Bohli J., Gruschka N., Jensen M., Iacono L.L., Marnau N. Security and Privacy-Enhancing Multi cloud Architectures. IEEE Transactions on Dependable and Secure Computing, Vol. 10. #4, 2013. URL: https://www.semanticscholar.org/paper/Security-and-Privacy-Enhancing-Multicloud-Bohli-Gruschka/0e8418f57749f77718f05f3db39b32353e8d1931 (data zvernennja: 22.10.2018).

2. Gill A., Banker D., Seltsika P. Moving Forward: Emerging Themes in Financial Services Technologies Adoption. Communications of the Association for Information Systems: Vol. 36, Article 12, 2015. URL: https://www.semanticscholar.org/paper/Moving-Forward%3A-Emerging-Themes-in-Financial-Gill-Bunker/99b1e6c3770de1067ace1d575e0727a87b8d58da (data zvernennja: 22.10.2018).

3. Ackermann T., Widjaja T., Benlian A., Percieved IT Security Risks of Cloud Computing: Conceptualization and Scale Development. Thirty Third International Conference on Information Systems, 2012. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.665.7295&rep=rep1&type=pdf (data zvernennja: 22.10.2018).

4. Christiansen C. A., Kolodgy C. J., Hudson S., Pintal G. Identity and Access Management for Approaching Clouds. White paper, 2010. URL: https://ru.scribd.com/document/82546531/Cloud-Security-Wp-236234-PDF (data zvernennja: 22.10.2018).

5. Fernandes D., Soares L. F. B., Gomes J. V. Security issues in cloud environments: a survey. Int. J. Inf. Secur. 13:113–170, 2014. URL: http://www.di.ubi.pt/~mario/artigos/2013-IJIS.pdf (data zvernennja: 22.10.2018).

6. Mansukhani B., Zia T. A. The Security Challemges and Countermeasures of Virtual Cloud. Australian Information Security Management Confference, 2012. URL: https://researchoutput.csu.edu.au/en/publications/

the-security-challenges-and-countermeasures-of-virtual-cloud (data zvernennja: 22.11.2018)
7. Ghalicyn V.K., Kaminsjkyj O.Je. Monitoryngh khmarnykh servisiv, rozghornutykh v baghato khmarnomu seredovyshhi. Modeljuvannja ta informacijni systemy v ekonomici. 2017. Vyp. 94. S. 160–169.

Статтю подано до редакції 05.09.2019 р.

УДК 004.021 DOI: 10.33111/mise.98.6

Галузинський Г.П., к.т.н.,
доцент кафедри інформаційних систем в економіці, ДВНЗ Київський національний економічний університет імені Вадима Гетьмана

Galuzinsky G.P., PhD in Technics,
Associate Professor of the Economics Information Systems Department,
Kyiv National Economic University named after Vadym Hetman

БАГАТОКРИТЕРІАЛЬНА ОПТИМІЗАЦІЯ З ВИКОРИСТАННЯМ ПОКАЗНИКОВИХ ФУНКЦІЙ

MULTIPLE CRITERIAL OPTIMIZATION WITH USE EXPONENTIAL FUNCTIONS

Аннотація. *Розглянуто інтерактивну процедури, яка дозволяє вирішувати безперервні задачі багатокритеріальної оптимізації без необхідності апріорного встановлення серед заданих критеріїв головного, або заміни цих критеріїв деякою скалярною функцією, яка в подальшому використовується як єдина основа для отримання оптимального рішення без урахування суб'єктивних переваг особи, зацікавленої в його ефективності. Аналіз сучасних публікацій показує, що увага авторів переважно зосереджена на способах визначення розрахунковим шляхом вагових коефіцієнтів з метою заміни сукупності критеріїв певною скалярною функцією, яка й використовується як єдина основа для отримання оптимального рішення. Запропоновано пошук компромісного рішення проводити ітеративним шляхом в просторі окремих критеріїв з використанням адитивної функції, що складається з відповідної кількості показникових функцій певного виду. Показано, що запропонований підхід до вироблення інтерактивним шляхом компромісного рішення дозволяє спростити для особи, що приймає рішення, його досягнення. Сутність інтерактивного підходу полягає в тому, щоб дозволити людині втручатись у процес пошуку рішення й розширити можливості його коригування за рахунок зворотного зв'язку між людиною та моделлю. Запропонована процедура при вирішенні безперервних задач оптимізації за наявністю кількох критеріїв (без можливості апріорного встановлення серед них головного) дозволяє реалізувати людино-машинну взаємодію, направлену на вироблення інтерактивним шляхом одного або декількох*