УДК 004.56.5(043.2)

МОДЕЛЬ МЕТОДИКИ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНИХ СИСТЕМ, ПОБУДОВАНИХ НА SaaS ПЛАТФОРМАХ

Гаранюк П.І., Пантелюк Д.М., Ромака В.А., Стецяк Т.Б.

Національний університет "Львівська політехніка",
УКРАЇНА, м.Львів, вул.С.Бандери, 12

У статті розроблена методика оцінювання ризиків безпеки інформації, що зберігається в хмарному середовищі. Запропоновано новий підхід в аналізі та якісному оцінюванні ризиків в хмарних системах.

Ключові слова: *ризик, інформаційна безпека, хмарні обчислення, оцінювання загроз*

Постановка проблеми. Проблема забезпечення інформаційної безпеки (ІБ) є першочерговим завданням при проектуванні інформаційно-телекомунікаційних систем. Практика показує, що в наш час ядро мережної архітектури змінилося з локалізованих автономних обчислень на середовище розподілених обчислень, що багаторазово збільшило її складність. Широке розповсюдження отримали хмарні обчислення - модель забезпечення мережевого доступу до обчислювальних ресурсів, які можуть бути оперативно звільнені з мінімальними експлуатаційними витратами [1].

Поява хмарних сервісів стала актуальною причиною масштабної міграції більшості систем на них, однак рішення задач забезпечення безпеки, пов'язаних з експлуатацією додатків в новому середовищі, вимагає особливого підходу. Багато типів загроз достатньо вивчені і для них розроблені засоби захисту, проте їх ще потрібно адаптувати для використання в хмарі.

Одним із першочергових завдань, що вирішуються для забезпечення ІБ організації є проведення аудиту автоматизованих систем (АС) та оцінювання рівня загроз ІБ.

Аналіз останніх досліджень та публікацій. З літератури відомі різні методики для оцінювання загроз інформації і вразливостей АС, використовувані для локальних обчислювальних мереж (ЛОМ) [2-4]. До найбільш відомих з них належать: методика експертного оцінювання системи безпеки інформації, методика багатокритеріального оцінювання, модель СЗІ з повним перекриттям, методика на основі базового показника уразливості.

Недоліком існуючих методик є складність застосування до сучасних каналів несанкціонованої передачі інформації для розподілених систем. Так, методика багатокритеріального оцінювання, описана в [4] призначена швидше для оцінювання локальної інфраструктури, оскільки вона розглядає проблеми фізичного збереження даних. Для хмарних обчислень доцільно сконцентруватися на безпеці інформації в процесі її обробки та захисті мережі, в якій ця інформація циркулює.

Метою статті є дослідження проблеми оцінювання ризику ІС та розробка методики оцінювання ризиків для ІС, побудованих на SaaS платформах.

Виклад основного матеріалу дослідження. Основне завдання даної методики полягає в тому, щоб визначити чисельний показник ризику ІБ з метою прийняття ефективних заходів щодо захисту інформації. Пропонована методика оцінювання ризиків дозволяє виконати повноцінний аналіз та оцінювання ризиків без залучення висококваліфікованих фахівців. Узагальнений алгоритм проведення оцінювання ризиків ІБ на підприємствах наведено на рис. 1.

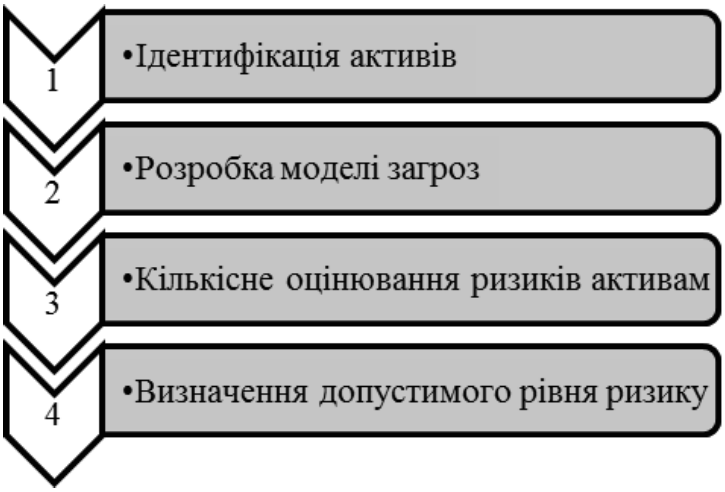

Рис. 1. Алгоритм оцінювання ризиків ІБ

На першому етапі необхідно провести аналіз інфраструктури підприємства з метою ідентифікації важливих інформаційних ресурсів підприємства, які називають інформаційними активами. Специфіка SaaS-платформ полягає у передачі управління апаратними та програмними ресурсами компанії-провайдеру. Іншими словами, саме провайдер дбає про працездатність системи, здійснює технічну підтримку системи та самостійно встановлює оновлення. Тому при оцінюванні ризиків основну увагу слід приділяти безпеці оброблюваної інформації, а не підтримуючій інфраструктурі.

На другому етапі з метою максимально точного визначення ризиків ІБ необхідно розробити конкретну модель загроз для даного підприємства. Широке поширення отримала формалізована модель інформаційної атаки на основі дерев атак, розроблена Б. Шнайером. Дерева атаки представляють собою концептуальні діаграми, які описують загрози системі і можливі атаки, спрямовані на їх реалізацію. В якості основної конструкції тут виступає ієрархічне дерево[6]. Приклад такої моделі представлено на рис.2.

Для її розробки необхідно зрозуміти, з яких елементів складається система. У типовій системі хмарних обчислень можна виділити наступні рівні: клієнтське програмне забезпечення, віртуалізована інфраструктура, середовище виконання хмарних додатків і система зберігання даних [5].

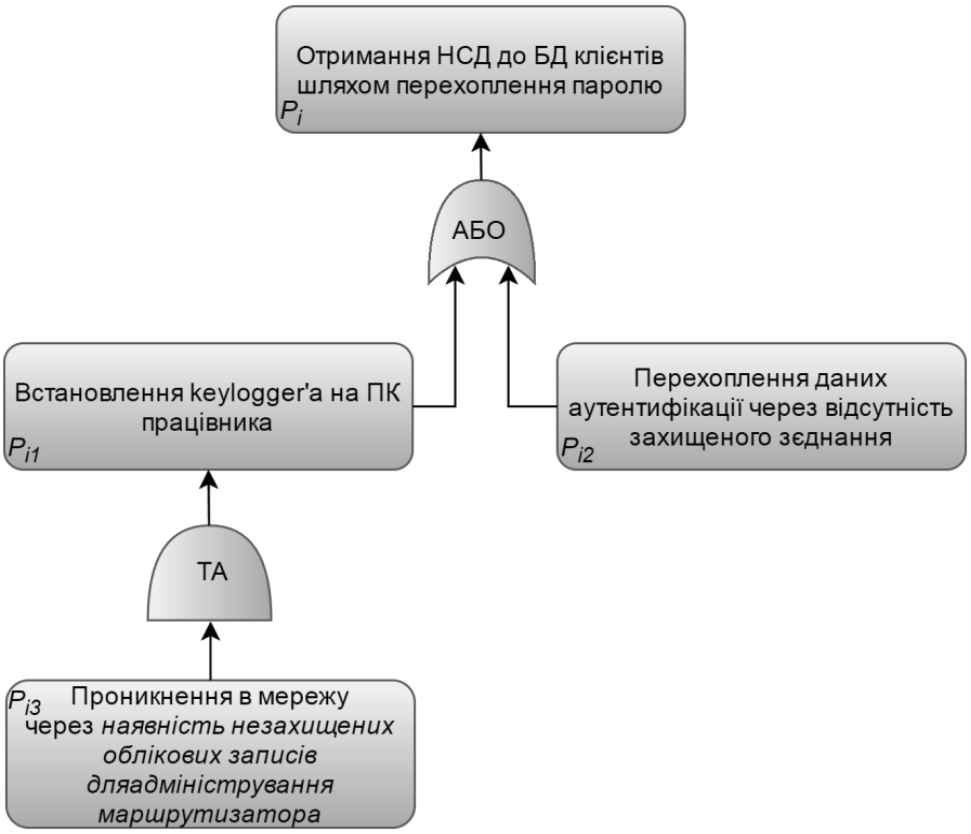

Рис. 2. Приклад дерева загроз

На третьому етапі необхідно оцінити значення ризиків для інформаційних активів. Оцінювання проводиться шляхом отримання добутку ймовірності реалізації загрози на значення збитку. Для *i*-го ресурсу формула матиме вигляд:

$$R_i = P_i * C_i. \quad (1)$$

Ймовірність реалізації загрози P_i визначається добутком ймовірностей реалізації сценаріїв кожного вузла.

$$P_i = \prod_{j=1}^{n} P_{ij}\ , \quad (2)$$

де, *n*- мінімальна кількість вузлів, необхідних для досягнення ресурсу *i.*

Ризик P_{ij} визначається експертним методом, за непрямими показниками, а саме:

- можливість виникнення джерела (K_1), що визначає міру доступності порушника до ресурсу (уразливості) (табл.1);
- готовність джерела (K_2), що визначає необхідну кваліфікацію порушника для здійснення атаки (табл. 2);
- здатність виявлення реалізації загрози (K_3), що визначає можливість встановлення факту несанкціонованого доступу (табл. 3).

Таблиця 1

Можливість виникнення джерела загрози

K_1	Характеристика
5	Прямий доступ до ресурсу у зв'язку з виконанням своїх посадових обов'язків.
4	Опосередкований доступ до ресурсу працівниками (отримання привілеїв в системі, помилки розмежування доступу).
3	Несанкціонований доступ до ресурсу сторонніми особами (отримання паролю, вразливість мережі).
2	Доступ до середовища, де знаходиться ресурс іншими клієнтами хмари (уразливість гіпервізора та середовища віртуалізації).
1	Доступ до фізичних ресурсів, де зберігається інформація працівниками провайдера.

Таблиця 2

Готовність джерела загрози

K_2	Характеристика
5	Займається розробкою програмного забезпечення, проектуванням хмарної інфраструктури, володіє глибокими знаннями архітектури мережі, що дозволяє йому включати власні технічні пристрої та програмні засоби в ІС підприємства (рівень провідного розробника)
4	Вміє виконувати завдання з написання та базового тестування окремих компонентів системи, володіє вузькими профільними знаннями середовищ розробки та мов програмування (рівень програміста)
3	Вміння керувати інформаційними процесами в мережі, тобто впливу на конфігурацію та склад наявного програмного забезпечення (рівень системного адміністратора)
2	Створення й запуск в мережі передавання даних сторонніх програм з новими функціями обробки інформації (рівень досвідченого користувача)
1	Запуск лише обмеженого набору фіксованих програм (рівень некваліфікованого користувача).

Таблиця 3

Здатність виявлення реалізації загрози

K_3	Характеристика
5	Не виявлено.
4	Виявлено при настанні незворотних наслідків.
3	Виявлено не одразу, під час перегляду журналів протоколювання подій.
2	Наявність системи виявлення вторгнень (IDS), виявлення одразу після реалізації.
1	Наявність IDS, виявлення до нанесення збитку.

Коефіцієнт $(K_{заг})_i$ для окремого джерела можна визначити як відношення добутку наведених вище показників до максимального значення 125:

$$P_{ij} = (K_{заг})_i = (K_{1i} K_{2i} K_{3i})/125. \quad (3)$$

Наприклад, для моделі загроз на рис.2 ймовірність реалізації загрози за формулою (2) визначається як:

$$P_i = max\ (P_{i1} * P_{i3};\ P_{i2}).$$

Ймовірності P_{ij} шукаємо за показниками K_{1i}, K_{2i}, K_{3i} (табл. 4).

Таблиця 4.

Приклад обчислення P_{ij}

P_{ij}	K_{1j}	K_{2j}	K_{3j}	$(K_{заг})_j$
P_{i1}	3	4	3	0,29
P_{i2}	3	4	4	0,38
P_{i3}	4	5	2	0,24

Розмір збитку C_i відображає в грошовому еквіваленті втрати, які понесе організація внаслідок реалізації загрози. Цим збитком може бути вартість конфіденційної інформації, фінансові витрати на відновлення роботи інформаційної системи, втрата прибутку через порушення технологічного процесу.[7]

4 етап. Виконання оцінювання повторюється для кожного активу. Отримані значення ризиків доцільно подати у відсотковому відношенні до максимально можливого та порівняти їх з допустимим рівнем ризику.

Допустимим прийнято вважати ризик, який в даній ситуації вважають прийнятним при існуючих суспільних цінностях. Рекомендується вибрати значення, що не перевищує 20%[4].

У разі якщо значення ризику менші допустимого рівня, то робиться висновок про те, що на підприємстві виконані вимоги по забезпеченню ІБ в повній необхідності, а також що ризик ІБ оцінюваного активу допустимий. У разі якщо підсумкове значення ризику більше допустимого то робиться висновок про те, що на підприємстві не виконуються вимоги по ІБ, а також що ризик ІБ оцінюваного типу активу підвищений і вимагає негайного ухвалення рішень.

Висновки. Широке поширення хмарних обчислень на ринку постачальників ІТ-послуг призводить до необхідності вдосконалення науково-методичного апарату для побудови систем захисту інформації. Пропонований підхід дозволяє на основі моделі загроз, вимог замовника до забезпечення захисту інформації здійснювати кількісне ймовірністне оцінювання захищеності ресурсів при використанні хмарних обчислень.

Список використаних джерел

1. mell P. The NIST Definition of Cloud Computing. Retrieved from [Електронний ресурс] / P. Mell, T. Grance // National Institute of Standards and Technology. – 2011. – Режим доступу до ресурсу: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
2. Малюк А.А. Информационная безопасность: Концептуальные и методологические основы защиты информации. – М.: Горячая линия – Телеком, 2004. – 282 с.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – Киев: ТИД «ДС», 2008. – 688 с.
4. Ромака В.А., Корж Р.О., Гарасим Ю.Р. «Менеджмент у сфері захисту інформації» - Львів, 2013
5. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003. — 368 с: ил. — ISBN: 5-318-00193-9

6. Коржов В. Опасны ли облака? [Електронний ресурс] / Валерий Коржов // Сети/network world. – 2010. – Режим доступу до ресурсу: http://www.osp.ru/nets/2010/07/13004633
7. Астахов А.М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с.,

References

1. mell, P., & Grance, T. (2011, September). The NIST Definition of Cloud Computing. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (in English)
2. Maliuk, A. A. (2004). Informatcionnaia bezopasnost: Kontceptualnye i metodologicheskie osnovy zashchity informatcii. Goriachaia liniia – Telekom. doi:ISBN 5-93517-197-X (in Russian)
3. Domarev, V. V. (2008). Bezopasnost informatcionnykh tekhnologii. Metodologiia sozdaniia sistem zashchity. Kiev: TID «DS». (in Russian)
4. Romaka, V.A., Korzh, R.O., & Garasim, Iu.R. (2013). Menedzhment u sferi zakhistu informatciї. Lviv. (in Ukrainian)
5. Schneier, B. (2003). Secrets and Lies: Digital Security in a Networked World. St. Petersburg: Piter. (in Russian)
6. Korzhov, V. (2010). Network world. Retrieved from http://www.osp.ru/nets/2010/07/13004633/ (in Russian)
7. Astakhov, A. M. (2010). Iskusstvo upravleniia informatcionnymi riskami. Moscow: DMK Press. (in Russian)

A MODEL OF TECHNIQUE OF RISK ASSESSMENT OF INFORMATION SYSTEMS DESIGNED ON SAAS PLATFORMS

Haranyuk P.I., Pantelyuk D.M., Romaka V.A., Stetsyak T.B.

Lviv Polytechnic National University
12, S.Bandera St., Ukraine, Lviv
e-mail: garanyuk@gmail.com

The article presents the technique of risk assessment of information security stored in the cloud environment. A new approach to the analysis and qualitative assessment of risks in cloud systems has been suggested.

Key words: *risk, information security, cloud computing, risk assessment.*

Стаття надійшла до редакції 15.03.2016.
Received 15.03.2016.