УДК 004. 891 + 330.46 **doi: 10.26906/SUNZ.2024.1.146**

Л. О. Нікітіна[1], Н. В. Дженюк[1], Л. В. Борисова[2]

[1] Національний технічний університет «Харківський політехнічний інститут», Харків, Україна
[2] Національний університет цивільного захисту України, Харків

ЕКСПЕРТНА СИСТЕМА ДЛЯ ОЦІНКИ РИЗИКІВ ХМАРНИХ СЕРВІСІВ

Анотація. Реалії сучасності вимагають від суспільства впровадження цифрових технологій, які набувають все більшої складності та інтелектуальності. Цифровізація (digitalization) стає невід'ємним компонентом усіх сфер діяльності людини. Тенденцією розвитку та економічного зростання фірм і організацій стають хмарні технології, які дозволяють організаціям мати гнучкі витрати в IT-секторі і регулювати їх шляхом купівлі доступу до ресурсів та сервісів у провайдерів замість купівлі самих ресурсів та сервісів. Для організацій, які приймають рішення, пов'язані з використанням хмарних сервісів, виникають труднощі з оцінкою та оптимальним вибором сервісів та провайдерів, оскільки для цього поки що не існує загальноприйнятих вказівок або процедур. З іншого боку, перед провайдерами постає проблема забезпечення належної якості хмарних сервісів, що надаються користувачам. Як провайдерам, так і користувачам необхідно мати інструменти, які дають змогу визначити та оцінити можливі ризики хмарних сервісів. Одним з таких інструментів може бути експертна система з оцінки хмарних сервісів, концепція якої розглядається у даній статті.

Ключові слова: хмарні обчислення; хмарні послуги; експертна система; система нечіткого логічного висновку; база знань; оцінка ризиків; вразливість.

Вступ

Хмарні технології в наш час набувають все більшої популярності. В області інформаційних технологій термін "хмара" використовується для позначення хмарних обчислень або хмарних сервісів. У «хмарі» поєднуються комунікації, ресурси апаратного та програмного забезпечення, сховища даних. Доступ до ресурсів забезпечується через мережу Інтернет. Користувачі «хмари» не повинні прямо володіти фізичним обладнанням або управляти ним, вони можуть віддалено використовувати ресурси за потребою та платити лише за фактичне використання. Крім того, коли не вистачає потужності власних ресурсів, користувачі можуть розгортати свої застосунки у «хмарі», і використовувати їх у зручний спосіб.

Будемо використовувати такі означення [1, 2]:

– хмарні технології – концепція надання послуг зі зберігання та обробки даних, згідно з якою обчислювальні ресурси надаються користувачеві через Інтернет як онлайн сервіси;

– хмарний сервіс – послуга з надання хмарних ресурсів за допомогою технологій «хмарних обчислень»;

– хмарні обчислення – використання обчислювальних служб (серверів, сховищ, баз даних, комунікаційних мереж, програмного забезпечення, аналітики та інтелектуального аналізу) через мережу Інтернет в режимі «на вимогу» згідно з угодою з провайдером, який надає ці послуги;

– сервіси – служби, які забезпечують хмарні обчислення; вони дозволяють прискорити впровадження інновацій, підвищити гнучкість використання ресурсів, отримати економію завдяки високій масштабованості; користувач зазвичай платить лише за хмарні сервіси у міру зміни потреб бізнесу;

– постачальник хмарних послуг (CSP, сервіс-провайдер) – це IT-компанія, яка надає масштабовані обчислювальні ресурси на вимогу, наприклад обчислювальну потужність, сховище даних або програми через Інтернет.

Хмара може бути організована як сукупність великої кількості фізичних хостів, які об'єднані телекомунікаційною мережею. Прикладами постачальників хмарних послуг є Microsoft Azure (120 зон доступу, 62 регіони), Google Cloud Platform (GCP, 118 зон, 39 регіонів), Amazon Web Services (AWS, 102 зони, 32 регіони), Alibaba Cloud (89 зон, 30 регіонів), Oracle Cloud (46 зон, 38 регіонів), IBM Cloud (30 зон, 10 регіонів) та ін. [2–9]. Комерційні хмари можуть працювати на мільйонах фізичних хостів. Кожен із цих хостів може розміщувати багато віртуальних машин (VM), за допомогою яких їх можна викликати або видаляти динамічно. Крім того, хмарні гіпервізори використовуються для керування наданням ресурсів, що передбачає відображення та планування створених віртуальних машин, що знаходяться на фізичних серверах хмари. Ці технічні та економічні переваги хмарних обчислень на вимогу зробили можливим переміщення традиційних корпоративних обчислень до хмар. Хмарні технології мають ряд переваг: зручність, доступність, економія коштів за рахунок зниження вартості інфраструктури, масштабованість, певний рівень безпеки даних. Однак, окрім явних переваг, вони мають і недоліки: обмежена пропускна здатність, залежність від провайдера, проблеми з приватністю, привабливість для зловмисників. Зазначені недоліки роблять актуальною проблему визначення та оцінки ризиків у організації та використанні хмарних обчислень. Такі ризики мають враховувати як провайдери хмарних сервісів, так і користувачі (організації і приватні особи) при виборі сервісів та провайдерів.

1 Хмарні обчислення

Хмарні обчислення будуються на основі клієнт-серверної моделі, метою якої є підвищення доступності обчислювальних ресурсів. Національний інститут стандартів і технологій (National Institute of Standards and Technology, NIST) визначає, що хмарні обчислення мають ряд характеристик і будуються на основі моделі сервісів і моделі розгортання [10–12]. Головними характеристиками хмарних обчислень є:

1) об'єднання ресурсів – постачальник хмарних послуг може розподіляти ресурси між кількома клієнтами, кожен з яких використовує свій набір послуг;

2) самообслуговування на вимогу – клієнт за необхідності без взаємодій з персоналом постачальника послуг може задіяти обчислювальні можливості (серверний час, мережеве сховище даних та ін.), безперервно відстежувати та контролювати обчислювальні можливості відповідно до своїх потреб;

3) легкість обслуговування – оновлення та оптимізація ресурсів хмари (серверів) відбувається за мінімальний або навіть нульовий час;

4) масштабованість і гнучкість – можливість швидко та ефективно балансувати поточні навантаження, які потребують великої кількості серверів;

5) економність – зменшення витрат на організацію та використання простору для зберігання даних, бо найчастіше він виділяється безкоштовно;

6) служби вимірюваності послуг та звітності – дозволяють провайдерам і клієнтам відстежувати, які послуги та з якою метою використовувалися, та формувати відповідні звіти; це допомагає контролювати виставлення рахунків і забезпечувати оптимальне використання ресурсів;

7) безпека – хмарні служби створюють резервні копії даних, щоб запобігти будь-якій втраті даних;

8) автоматизація – здатність автоматично встановлювати, налаштовувати та підтримувати хмарні сервіси відома як автоматизація в хмарних обчисленнях; це вимагає встановлення та розгортання віртуальних машин, серверів і великих сховищ;

9) стійкість – здатність сервісу швидко відновлюватися після будь-яких збоїв, час перезапуску та відновлення серверів, баз даних і мережевих систем після будь-яких втрат або пошкоджень;

10) доступність – доступ до хмарних сервісів можна отримати віддалено, без географічних обмежень або обмежень на використання хмарних ресурсів;

11) широкий доступ до мережі – клієнти можуть отримати доступ до хмарних даних або перенести дані в хмару з будь-якого місця за допомогою пристрою та підключення до Інтернету.

Хмарні сервіси управляють доступом до ресурсів хмари відповідно до вимог клієнта.

Хмарні обчислення пропонують такі три види сервісів:

1) програмне забезпечення як сервіс (SaaS, сервіси хмарних додатків) – здебільшого додатки SaaS запускаються безпосередньо через веб-браузер, і користувачеві не потрібно завантажувати та встановлювати ці програми; за допомогою SaaS користувач може отримати доступ до програмного забезпечення через Інтернет без потреби в будь-якій платформі; приклади: Google Apps, Salesforce Dropbox, Slack, Hubspot, Cisco WebEx;

2) платформа як сервіс (PaaS) – надає платформу для створення програмного забезпечення; приклади: Windows Azure, Force.com, Magento Commerce Cloud, OpenShift;

3) інфраструктура як послуга (IaaS) – відповідає за керування даними, які використовуються програмними додатками, проміжним програмним забезпеченням (middleware) і середовищами виконання; приклади: Amazon Web Services (AWS) EC2, Google Compute Engine (GCE), Cisco Metapod.

Під терміном "модель розгортання хмарного обчислення" розуміють архітектуру розгортання віртуального обчислювального середовища, що змінюється залежно від обсягу даних, які ви треба зберегти, і того, хто має доступ до інфраструктури. Модель розгортання хмари визначає конкретний тип хмарного середовища, на основі характеристик типу власності, масштабу, типу доступу, характеру, призначення хмари, розташування серверів і функцій керування ними.

При виборі провайдера та сервісів користувачеві необхідно зрозуміти, яка модель найкраще йому підходить в конкретних умовах для вирішення конкретних задач.

Існують такі основні моделі розгортання хмарних обчислень:

– публічна хмара (Public Cloud) – є доступною для всіх, і будь-яка організація може мати доступ до систем і сервісів;

– приватна хмара (Private Cloud) – послуги побудовані відповідно до принципів хмарних обчислень, але доступні лише в приватній мережі;

– хмара спільноти (Community or Partner Cloud) – хмарні послуги провайдер пропонує обмеженій і чітко визначеній кількості сторін.

Крім того, існують моделі гібридної хмари (Hybrid Cloud, об’єднання приватних та публічних хмар), багатопровайдерної хмари (Multi-Cloud, комбінація приватних хмар, публічних хмар або приватних і публічних хмар).

Кожну з основних моделей можна оцінити за чотирибальною шкалою за такими параметрами як "товарність" (commodity), вартість (cost), відповідальність (liability) і гарантованість (assurance) у порівнянні з "не-хмарою" (табл. 1, [13]).

На даний момент не існує загального підходу для вибору моделі розгортання хмари. Вибір моделі необхідно робити відповідно до поточних вимог. При виборі найкращої моделі розгортання можна враховувати, крім зазначених вище, такі фактори як масштабованість (Scalability), легкість використання (Easy to use), конфіденційність (Privacy), відповідність (Compliance) та ін.

Таблиця 1 – **Параметри для оцінки моделей**

	"товарність" (commodity)	Вартість (cost)	відповідальність (liability)	гарантованість (assurance)
Public Cloud	4	1	1	1
Private Cloud	3	2	2	2
Partner Cloud	2	3	3	3
Non-Cloud	1	4	4	4

Ризики та вигоди, пов’язані з кожною моделлю хмарних обчислень, відрізняються і користувачеві це треба усвідомлювати і враховувати при виборі провайдера та сервісів.

2 Загрози, вразливості та ризики у хмарних обчисленнях

Безпека використання хмарних обчислень полягає у забезпеченні доступності, цілісності, конфіденційності та підтримці інформаційних ресурсів інфраструктури. Будь-яка фірма, яка використовує хмару, прагне захистити свої активи, найціннішим з яких є інформація. Хмарні сервіси надають можливість отримати швидкий та зручний доступ до інформаційних ресурсів та сервісів, але, водночас, такі ресурси і сервіси можуть бути вразливими до різноманітних небезпек і загроз. Вразливості хмари стають причинами широкого спектру ризиків, які впливають на активи як користувачів, так і провайдерів хмарних сервісів (рис. 1).

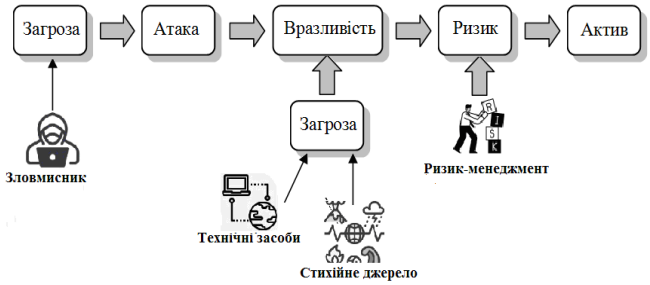

Рис. 1. Зв'язок між загрозами, вразливостями, ризиками

Загроза (threat) у контексті хмарних обчислень – це атака на хмарні ресурси, яка намагається порушити їхню роботу та доступ до них. Загрози мають широкий спектр дії – від втрати та витоку даних, випадкового розкриття облікових даних до складних кібератак. Загрози спрямовані на найбільш слабкі ланки системи захисту хмари – на вразливості і призводять до порушення інформаційної безпеки, режиму функціонування і доступності конкретних компонентів системи.

Хмарні вразливості (vulnerabilities) – це слабкі місця або прогалини в середовищі хмарних обчислень, якими зловмисники можуть скористатися, щоб отримати несанкціонований доступ, викрасти дані або порушити роботу сервісів.

Ризики у хмарних обчисленнях є результатом вразливостей хмарних ресурсів та сервісів під дією атак. Відповідальність за пом'якшення ризиків розподіляється між провайдером і хмарним споживачем.

Ризик – це можливість втрати, пошкодження або знищення активів або даних особи або організації через загрозу подій або дій. Ризики виникають як результат вразливостей.

Організація може бути вразливою до різноманітних загроз, які можуть впливати на ефективність роботи та дотримання нормативних вимог. Щоб запобігти впливу ризиків простого усвідомлення недостатньо. Необхідно використовувати управління ризиками у хмарі (CRM) для їхньої мінімізації, а в деяких випадках і усунення [13-18].

Найважливіші класи ризиків, пов'язаних із хмарою (не у порядку критичності) [13]:

1) втрата керування: при використанні хмарних інфраструктур клієнт обов'язково передає контроль постачальнику хмарних технологій (СР) щодо низки питань, які можуть вплинути на безпеку; при цьому згідно з угодою про рівень обслуговування провайдер хмарних послуг може бути не зобов'язаним надавати такі послуги, а це є прогалиною в безпеці;

2) блокування: відсутність доступних інструментів, процедур або стандартних форматів даних чи інтерфейсів послуг, які могли б гарантувати переносимість даних, програм і послуг; це може ускладнити або заблокувати для клієнта перехід від одного постачальника до іншого або перенесення даних і послуг назад у власне IT-середовище;

3) помилки ізоляції: ця категорія ризику охоплює збій механізмів, що розділяють сховище, пам'ять, маршрутизацію та навіть репутацію між різними орендарями (наприклад, так звані атаки з переходом на гостьову систему);

4) ризики відповідності: інвестиції в отримання сертифікації (наприклад, галузевого стандарту чи нормативних вимог) можуть бути піддані ризику через міграцію до хмари, якщо СР не може надати докази власної відповідності відповідним вимогам або якщо СР не дозволяє аудит клієнтом хмари (СС);

5) компроміс інтерфейсу керування: інтерфейси керування клієнтами постачальника загальнодоступної хмари доступні через Інтернет і забезпечують доступ до більших наборів ресурсів (ніж у традиційних хостинг-провайдерів), тому становлять підвищений ризик, особливо в поєднанні з віддаленим доступом і вразливістю веб-браузера;

6) захист даних: у деяких випадках замовнику хмари (у ролі контролера даних) може бути важко ефективно перевірити практику обробки даних постачальником хмари і переконатися, що дані обробляються належним чином, особливо у випадках багаторазової передачі даних, наприклад, між об'єднаними хмарами;

7) небезпечне або неповне видалення даних: запит на видалення хмарного ресурсу не завжди виконується як справжнє видалення даних, додаткові копії даних зберігаються, але вони недоступні, або тому, що диск, який потрібно знищити, також зберігає дані з інших клієнтів;

8) зловмисний інсайдер: хмарні архітектури вимагають певних ролей, які є надзвичайно ризикованими, наприклад, ролі системних адміністраторів СР і постачальників послуг керованої безпеки;

Стандарт ISO/IEC 27001:2022 регламентує стратегію інформаційної безпеки, орієнтовану на захист конфіденційності, забезпечення автентичності і доступності даних [28]. Аналіз та інтерпретація ризику виконуються за допомогою оцінки ризику. Цей процес базується на виявленні та оцінці вразливостей, які існують в організації [14]. В стандарті ISO 31000:2018 акцент концепції ризику робиться не тільки на визначенні його ймовірності та наслідків, а й на процесі управління ризиками. Управління ризиками в хмарі – це процес оцінки, захисту та керування ризиками, пов'язаними із хмарними обчисленнями. Управління ризиками визначає, які проблеми мають пріоритет і як реагувати на можливі ризики. Процес управління ризиками орієнтований

на врахування потенційних небезпек, які стосуються як провайдерів, так і користувачів [29].

В деяких випадках клієнту хмари доцільно і можливо передавати ризик постачальнику хмари; однак не всі ризики можна передати: якщо ризик призводить до краху бізнесу, серйозної шкоди репутації або юридичних наслідків, будь-якій іншій стороні важко або неможливо компенсувати цю шкоду.

3 Експертна система для оцінки ризиків хмарних сервісів

Для організацій, які приймають рішення, пов'язані з використанням хмарних сервісів, виникають труднощі з оцінкою та оптимальним вибором сервісів та провайдерів, оскільки для цього поки що не існує загальноприйнятих вказівок або процедур. З іншого боку, перед провайдерами постає проблема забезпечення належної якості хмарних сервісів, що надаються користувачам. Як провайдерам, так і користувачам необхідно мати інструменти, які дають змогу визначити та оцінити можливі ризики хмарних сервісів. Одним з таких інструментів може бути експертна система (ЕС) для оцінки хмарних сервісів, концепція якої розглядається у даній статті.

Експертна система дозволяє:

– сформувати базу даних:

o реєстр можливих вразливостей хмарних сервісів;

o реєстр ризиків;

o реєстр активів користувача;

o таблиці оцінок рівнів ризиків та їхнього впливу на активи;

o таблиці ймовірностей ризиків;

o сценарії реагування на ризики;

– сформувати базу знань на основі продукційної моделі;

– виконати оцінку та аналіз ризиків;

– провайдеру – отримати рекомендації з формування реакції на ризики;

– користувачеві – визначити та порівняти вплив ризиків, притаманних різним провайдерам, на активи користувача;

– зберігати у базі даних звіти, сформовані у ході сеансів роботи системи.

Така система може бути побудована за архітектурою експертних систем (рис. 2).

Користувачами ЕС є привілейовані користувачі з боку провайдера – експерт і ризик-менеджер та кінцевий користувач хмарних сервісів. Привілейовані користувачі мають доступ до формування бази даних та знань через підсистему управління знаннями та до підсистеми управління ризиками. Кінцевий користувач може формувати вхідні дані для виконання оцінки ризиків та їхнього впливу на важливі для нього активи.

Експертна система, запропонована в цьому документі, містить інтерфейси, з якими взаємодіють користувачі, машину виведення, яка виконує обґрунтування знань/даних, базу даних і базу знань, яка зберігає загальні та абстрактні знання про оцінку комерційних хмарних сервісів. База знань формується на основі знань експертів та знань про хмарні обчислення, опубліковані в джерелах інформації.

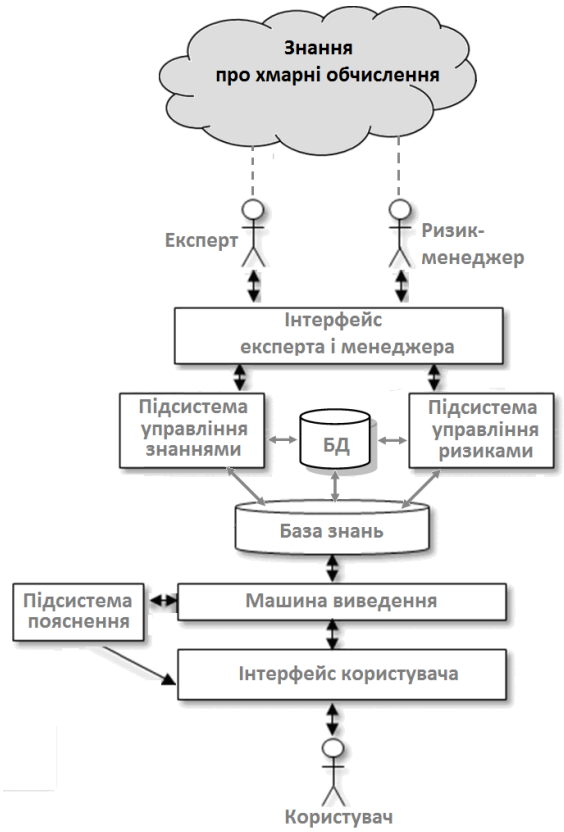

Рисунок 2 – Архітектура експертної системи

Наразі ми зробили акцент на формуванні бази знань та роботі машини виведення для оцінки ризиків. Програмна реалізація системи у даному документі не розглядається.

4 База знань та машина виведення

Вивчення джерел інформації [10-27] дало підставу зробити висновок про доцільність побудови бази знань на основі продукційної моделі.

Правило продукції – це вираз виду:

$$(i): Q; P; A; \Rightarrow B; S, F, N, \qquad (1)$$

де (i) – унікальний ідентифікатор продукції; Q – сфера застосування продукції; P – умова застосовності ядра продукції; $A \Rightarrow B$ – ядро продукції, в якому A – умова ядра, B – висновок ядра; "$\Rightarrow$" – знак логічної секвенції (наслідку); S – метод або спосіб визначення кількісного значення ступеню істинності висновку ядра; F – коефіцієнт визначеності або впевненості продукції; N – післяумова продукції.

База знань складається з множини правил виду (1). Кожне правило являє собою незалежну одиницю знань. Передумови можуть розглядатися як модель (образ), а наслідок – як висновки або дії, які необхідно виконати. Для отримання експертизи хмарних сервісів користувач ЕС налаштовує базу знань, вводить вхідні дані (наявні або гіпотетичні значення ступеню вразливостей хмари, важливість своїх активів, ризики, що перебувають у сфері його інтересів та ін.) та запускає машину виведення.

На основі рекомендацій ЕС користувач може прийняти рішення про перехід до хмарного середо-

вища певного провайдера або порівняти ризики різних провайдерів (рис. 3).

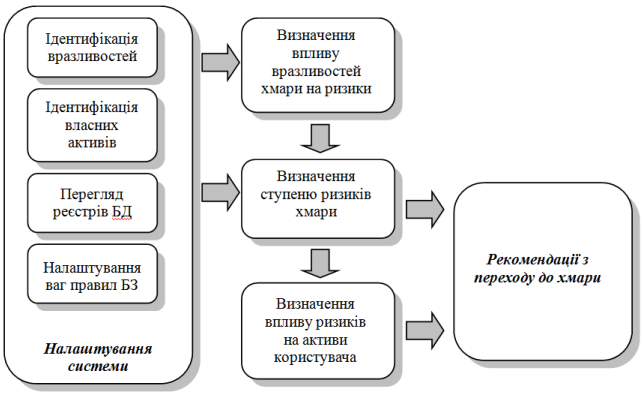

Рис. 3. Рекомендації користувачеві хмари

У циклі виведення виконуються такі операції:

1) співставлення – зразок правила співставляється з фактами, наявними у базі фактів;

2) вибір – якщо знайдено декілька підходящих правил, то вони створюють конфліктний набір; з конфліктного набору вибирається одне правило, яке найбільше підходить за заданим критерієм – тобто виконується рішення конфлікту;

3) спрацьовування – якщо співставлення антецедента правила з фактами робочої пам'яті виконано успішно, то правило спрацьовує;

4) дія – до робочої пам'яті додається новий істинний факт, що є консеквентом правила, яке спрацювало.

Результатом є визначення впливу вразливостей на ризики і ризиків – на активи.

Через інтерфейс користувачеві ЕС доступні функції виконання запитів до БД та БЗ: перегляд наявних реєстрів вразливостей, ризиків, активів, перегляд наявних правил та їхньої ваги, виконання різноманітних вибірок. Для визначення готовності до хмарного середовища користувачеві потрібно зібрати необхідну інформацію про:

– провайдера хмарних сервісів;
– сторонніх постачальників;
– поточні рішення та конфігурацію безпеки.

Для повного контрольного списку оцінки ризиків хмари користувачеві необхідно виконати:

1) визначення всіх активів, які зберігатимуться у хмарному середовищі – дані клієнтів, фінансових записів, облікові дані співробітників, відомості про комерційну діяльність;

2) класифікацію своїх даних відповідно до їх чутливості; це допоможе визначити активи, які піддаються найбільшому ризику та потребують кращого захисту;

3) визначення потенційних загроз; тестування хмарних загроз і проникнення найкраще доручити експертам, які знайомі з векторами атак і мають інструменти, необхідні для моделювання атак;

4) оцінювання ризиків, пов'язаних з кожною загрозою та впливу на активи.

Привілейовані користувачі (експерт та менеджера з ризиків) крім функцій, доступних функції користувачеві, можуть отримати рекомендації з управління ризиками (рис. 4).

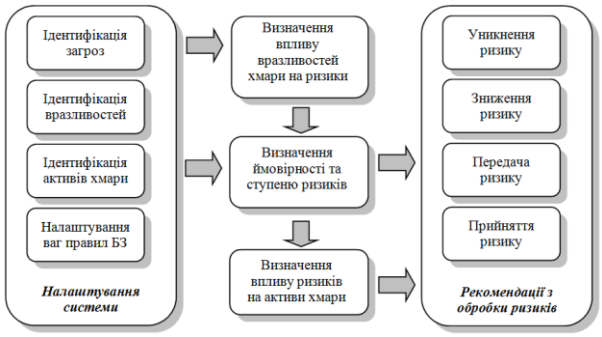

Рис. 4. Рекомендації менеджеру для обробки ризиків

Вважаємо доцільним створення нечіткої бази знань. Одиницями знань у ній будуть нечіткі правила. Приклади таких правил наведені у табл. 2:

Таблиця 2 – **Приклади правил**

Ідентифікатор правила		Антецедент		Консеквент
001	IF	V46=H, V47=M, V31=L	THEN	R05=M
…		…		…
…	IF	R05=H, R09=H, R15=M, R18=M, R32=L	THEN	A10=L

У наведеному прикладі використано позначення: V_n – ідентифікатор вразливості згідно з реєстром вразливостей; R_m – ідентифікатор ризику згідно з реєстром ризиків; A_k – ідентифікатор активу згідно з реєстром активів; H – високий рівень впливу; M – середній рівень впливу; L – низький рівень впливу.

Машина виведення може бути організована як система нечіткого виведення за алгоритмами Мамдані, Сугено та ін. з використанням різних способів дефаззіфікації результатів.

Іншим варіантом може бути багатоступенева нейро-нечітка система виведення. Така система має бути попередньо навчена на відповідних зразках для визначення рівнів ризиків та їхнього впливу на активи.

Висновки

Бурхливий розвиток хмарних обчислень викликав появу комерційних постачальників хмарних сервісів. Умови та спектр пропозицій, характеристики пропонованих сервісів можуть мати суттєві відмінності та особливості. З цієї причини є важливим перед використанням хмарних сервісів певного провайдера проводити оцінювання потенціальних ризиків і їхніх впливів на наявні активи. Крім того, вибираючи з кількох потенційних провайдерів хмарних сервісів, можна порівнювати їх між собою.

Сфера створення та надання хмарних послуг стрімко змінюється, певні аспекти безпеки стають неконтрольованими клієнтами, тому зростають ризики використання сервісів.

Оцінка комерційних хмарних послуг неминуче стає більш складною, ніж оцінка традиційних обчислювальних систем. Для полегшення роботи з оцінювання ризиків у контексті хмарних обчислень та

впливу їх на активи користувача ми запропонували створити експертну систему на основі накопичення та застосування наявних експертних знань у галузі хмарних обчислень. Запропонована експертна система може бути використана як інструмент з надання рекомендацій як провайдерам хмарних послуг в результаті оцінки ризиків, так і користувачам при виборі провайдера.

СПИСОК ЛІТЕРАТУРИ

1. Peter Mell Timothy Grance. The NIST Definition of Cloud Computing. Recommendations of the. NIST Special Publication 800-145. September 2011. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf
2. Cloud computing. IT Enterprise. https://www.it.ua/knowledge-base/technology-innovation/cloud-solutions
3. What is cloud computing? https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing
4. What is cloud computing? https://www.ibm.com/topics/cloud-computing
5. What is Cloud Computing? https://cloud.google.com/learn/what-is-cloud-computing
6. Top 5 Cloud Services Providers 2023. https://savemyleads.com/blog/useful/top-5-cloud-services-providers-2023
7. Що таке хмарні технології? Переваги та недоліки. https://edin.ua/shho-take-xmarni-texnologi%D1%97-i-navishho-voni-potribni/
8. The top 10 public cloud providers in 2023. https://www.revolgy.com/insights/blog/the-top-10-public-cloud-providers-2023
9. Top 10 Cloud Service Providers Globally in 2023. https://dgtlinfra.com/top-cloud-service-providers/
10. Nayan Ruparelia. Cloud computing. Cambridge, MA : The MIT Press, 2016 – 278 p. https://s3.amazonaws.com/arena-attachments/911381/0ea8a9793158a95d9b91911e49240a43.pdf
11. T.B. Rehman. Cloud Computing Basics. MERCURY LEARNING AND INFORMATION. Mercury Learning and Information LLC, 2019 – 198 p. https://terrorgum.com/tfox/books/cloudcomputingbasics_aselfteachingintroduction.pdf
12. Cloud Computing. https://www.javatpoint.com/cloud-computing
13. ENISA. Cloud computing: benifits, risks and recommendation for information security. Nov 09. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
14. Fotis Kitsios, Elpiniki Chatzidimitriou, Maria Kamariotou. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. https://www.researchgate.net/publication/369606652_The_ISOIEC_27001_Information_Security_Management_Standard_How_to_Extract_Value_from_Data_in_the_IT_Sector
15. INTERNATIONAL STANDARD. ISO/IEC 27017. Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
16. Risk Management in Cloud Computing. https://www.scrut.io/post/risk-management-in-cloud-computing
17. Pedro Costa, João Paulo Santos, Miguel Mira da Silva. Evaluation Criteria for Cloud Services. https://www.researchgate.net/publication/261436007_Evaluation_Criteria_for_Cloud_Services
18. Timothy Morrow. 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud. https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/
19. Shannon Jackson-Barnes. Cloud Computing: Common Vulnerabilities and How to Overcome Them. https://www.orientsoftware.com/blog/vulnerability-in-cloud-computing/
20. Nivedita James Palatty Cloud Vulnerability Management: The Detailed Guide. https://www.getastra.com/blog/security-audit/cloud-vulnerability-management/
21. What Is Cloud Vulnerability Assessment And How To Implement It? https://discovercloud.io/what-is-cloud-vulnerability-assessment-and-how-to-implement-it/
22. Saumick Basu. 5 Top Cloud Vulnerability Scanners for AWS, Google Cloud, and Azure. https://www.getastra.com/blog/security-audit/cloud-vulnerability-scanner/?nowprocket=1
23. A Comprehensive Guide to Cloud Vulnerability Management. https://www.clouddefense.ai/guide-to-cloud-vulnerability-management/
24. Cloud Vulnerability Management Best Practices for 2024. https://www.sentra.io/learn/cloud-vulnerability-management
25. Martin Zboril. RISK ASSESSMENT METHOD OF CLOUD ENVIRONMENT. Computing and Informatics, Vol. 41, 2022, 1186–1206, doi: 10.31577/cai 2022 5 1186.
26. E. Cayirci1, A. Garaga, A. Santana de Oliveira, Y. Roudier. A risk assessment model for selecting cloud service providers. Journal of Cloud Computing: Advances, Systems and Applications (2016), DOI 10.1186/s13677-016-0064-x
27. A Risk Assessment Framework for Cloud Computing. URL: http://eprints.whiterose.ac.uk/95981/
28. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems: https://www.iso.org/standard/27001
29. ISO 31000:2018. Risk management: https://www.iso.org/iso-31000-risk-management.html

Received (Надійшла) 23.12.2023
Accepted for publication (Прийнята до друку) 31.01.2024

An expert system for cloud service risk assessment

L. Nikitina, N. Dzheniuk, L. Borysova

Abstract. Modern realities require society to implement digital technologies that are becoming increasingly complex and intelligent. Digitalization is becoming an integral component of all spheres of human activity. The trend of development and economic growth of companies and organizations is cloud technologies, which allow organizations to have flexible costs in the IT sector and regulate them by purchasing access to resources and services from providers instead of purchasing the resources and services themselves. For organizations that make decisions related to the use of cloud services, there are difficulties in evaluating and optimally choosing services and providers, because there are no generally accepted guidelines or procedures for this yet. On the other hand, providers face the problem of ensuring the proper quality of cloud services provided to users. Both providers and users need to have tools that allow them to identify and assess the possible risks of cloud services. One of such tools can be an expert system for evaluating cloud services, the concept of which is considered in this article.

Keywords: Cloud Computing; Cloud Services; Expert System; Fuzzy Inference System; Knowledge Base; Risk Assessment; Vulnerabilities.