УДК 004.042

В.П. Пасько, В.А. Гасанов, А.С. Гришко, А.В. Максимюк

ІНТЕРОПЕРАБЕЛЬНІСТЬ МАТРИЦІ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація: досліджено вплив міжнародних стандартів у сфері інформаційної безпеки на розвиток ключових підходів до прийняття управлінських рішень на основі розроблених критеріїв з урахування ймовірних ризиків. Пропонується модель та загальний механізм оцінювання інформаційних ризиків корпорації в хмарі з використанням вагових коефіцієнтів. Результати дослідження можуть бути використані при проведення експертної оцінки інформаційної безпеки та ризиків хмарних технологій.

Ключові слова: ризик, оцінка ризиків, управління ризиками, хмарні технології, прийняття управлінських рішень.

Вступ

Глобалізаційні процеси, що активно продукують нові підходи до організації взаємодії елементів в межах системи та між системами загалом на світових ринках, особливо важливо акцентують увагу на сучасних способах організації ефективної діяльності самих суб’єктів взаємодії. Актуальні розробки у ІТ-сфері призвели до необхідності використання хмарних обчислень світовими корпораціями з метою оптимізації та обґрунтування доцільності застосування хмарних технологій, адже змінюваність системи дозволяє швидко адаптуватися до вимог оточуючого середовища. Все більше корпорацій розглядають можливість переходу до хмарних технологій, які мають величезний потенціал.

Однак для того, щоб реалізувати переваги і отримати максимальну віддачу від своїх інвестицій, корпорації повинні брати до уваги різні проблеми і особливості впровадження хмарних ІТ-сервісів, їх унікальність для кожного конкретного випадку [1]. Ефективне впровадження сучасних інформаційних технологій передбачає імплементацію відповідних нормативно-правових документів, що регулюють правові норми, проблеми, ризики і способи їх мінімізації. Розробка та впровадження міжнародних стандартів в сфері безпеки інформаційних технологій необхідні для підвищення довіри до он-лайн операцій, фінансових транзакцій, оцінка ймовірності та визначення розмірів наслідків кібер-інцидентів та забезпечення програмної та технологічної сумісності серед торгових партнерів. Такі стандарти особливо важливі в сучасному інформаційному просторі, де продукти програмного забезпечення, процеси їх інтеграції та послуги із забезпечення функціонування цих продуктів, розробляються та поширюються у глобальному масштабі за допомогою поетапно спланованих послідовних операцій, які

приховують від споживача особливості хмарної інфраструктури провайдера. Для сфери хмарних обчислень особливу роль мають міжнародні стандарти, оскільки взаємодія споживачів та провайдерів хмарних послуг часто регулюється саме цими стандартами через географічну особливість розміщення суб’єктів системи находяться в різних країнах.

Постановка проблеми та актуальні розробки

Потенційні порушення в сфері інформаційної безпеки є базовою основною перешкодою на шляху впровадження хмарних технологій на практиці управління адміністративними процесами. Проблема розробки IT-стратегії впровадження полягає в тому, що ще на стадії її формування важливо визначити, які моделі підтримки прийняття рішень при виборі хмарних IT-сервісів для впровадження в корпорації найбільше будуть задовольняти бізнес-стратегії корпорації, сумісність діючого способу організації взаємодії серед суб’єктів системи в корпорації, оцінити провайдерів хмарних послуг з точки зору надійності, достовірності, оперативності та безпеки інформаційних потоків.

Метою пропонованої статті є екстраполяція наявних аналітичних інтерпретацій управління ризиками хмарних технологій, зважаючи на міжнародні стандарти з ризиків інформаційної безпеки, та забезпечення інтертекстуальності моделей підвищення ефективності.

Аналіз стандартів в галузі хмарних технологій

Для об’єктивного оцінювання інформаційних ризиків використовують підходи, в основі яких закладені міжнародні стандарти з ризиків інформаційної безпеки. Враховуючи динаміку глобального інформаційного простору та частоту загроз, що виникають у ньому, з'являються нові дослідження оцінювання ефективності та поточного стану стандартів в сфері хмарних обчислень [7, 8].

Відповідно до існуючої класифікації стандартоутворюючих корпорацій та органи мають наступну ієрархію рівнів:

– Міжнародний (ISO / IEC [7], ITU [10]);

– Міждержавний (форуми і консорціумами [4]);

– Регіональний (європейські CEN / CENELEC [6]);

– Національний (державні закони та стандарти, відомчі нормативні документи, керівництва, інструкції та ін. [5, 9]).

З причин відсутності міжнародних стандартів по сертифікації елементів хмарної інфраструктури та актуальності інформаційної безпеки елементи (дата-центри, канали і мережі комунікацій та інші) використовують сертифікати безпеки стандартів, як між-

народних, так і інших країн, суміжних напрямків.

Міжнародні корпорації, які займаються стандартами в сфері інформаційної безпеки [9], представлені на рис. 1. В кожній країні також існують регіональні корпорації і відомства, що займаються розробкою нормативних документів у сфері інформаційної безпеки. На рис. 2 представлена схема взаємодії міжнародних і регіональних стандартоутворюючих корпорацій в сфері хмарних технологій [6].

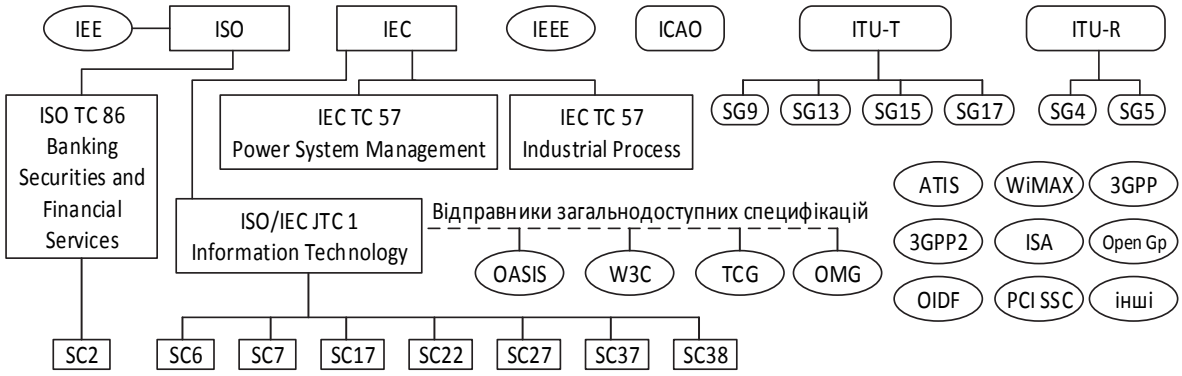

Рис. 1. Міжнародні корпорації, приймаючі участь
в розробці міжнародних стандартів
в галузі інформаційної безпеки хмарних технологій

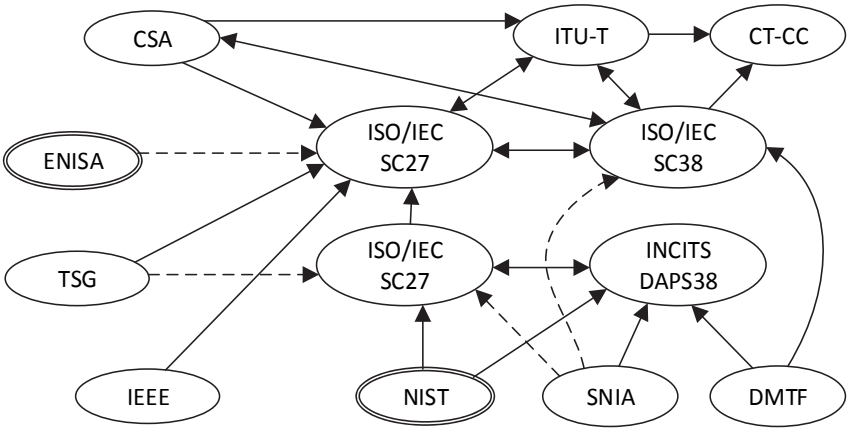

Рис. 2. Схема взаємодії між регіональними
та міжнародними стандартоутворюючими корпораціями

Аналіз структури ризиків втрати інформації

При визначенні ризику ключовими поняттями є «ступінь невизначеності», «характеристика майбутнього», «наявність можливості», «величина ймовірності», «розмір збитків», «вид діяльності», «доцільність вибору» і є спільними характеристиками для продукування належного рівня інформаційної безпеки, незалежно від сфери застосування. Існування ризику пов’язано з неможливістю гарантувати з високою ймовірністю відсутності витоку інформації або порушення інформаційної безпеки.

Ризик виникає як наслідок прийняття рішень відносно стану ситуації та прагматично є фундаментом для появи причинно-наслідкового зв’язку «рішення-результат». Існує два підходи до оцінки величини ризику: *об’єктивний* та *суб’єктивний*.

В основі встановлення об’єктивної міри ризику покладено дані про попередні втрати, гіпотези про тенденції, стани та можливі сценарії розвитку, імовірності втрат сьогодні і прогнозування їх в майбутньому. Оскільки невизначеність є джерелом ризику, то для його зменшення необхідно нівелювати рівень невизначеності, тобто перевести невизначеність у повну визначеність шляхом отримання достовірної, надійної та комплексної інформації у даний момент часу.

Згідно чинного законодавством України, інформація є об’єктом права власності, а також об’єктом володіння, використання та розпорядження. Інформаційні ризики слід розглядати і враховувати на рівні з економічними [3]. Детальну класифікацію інформаційних ризиків наведено на рис. 3.

Керувати ризиком означає застосовувати дії, направлені на підтримання такого його рівня, що відповідає меті управління корпорацією.

Процес аналізу ризиків складається з етапів:

– визначення видів ризиків, існуючих або тих що можуть виникнути та впливати на діяльність корпорації;

– оцінки впливу на діяльність корпорації та оцінки ймовірної шкоди, що може бути заподіяна внаслідок реалізації того або іншого ризику.

Основні задачі управління ризиком:

– підтримка ризику заданому рівні, що не перевищує допустимий;

– нівелювання ризику при заданих умовах.

Серед методів оцінки ризику варто розглянути наступні:

– кількісні – використовуються об'єктивні дані, що дозволяють визначити вартість активів, рівень ймовірних втрат тощо;

– якісні – використовується відносний показник ризику або вартості активу;

– змішані – комбінація кількісного і якісного методу, сукупність переваг і недоліків вище згаданих методів.

Для управління інформаційними ризиками потрібно ідентифікувати і оцінити всі можливі загрози інформаційній системі. Найчастіше для розрахунку ризиків використовується формула [2]:

$$AV * EF * ARO = ALE, \quad (1)$$

де *AV* (*Asset Value*) – вартість ресурсу; *EF* (*Exposure Factor*) – міра уразливості ресурсу до загрози; *ARO* (*Annual Rate of Occurrence*) – оцінка ймовірності реалізації загрози; *ALE* (*Annual Lost Exposure*) – підсумкові очікувані втрати від конкретної загрози за певний період часу.

 ISSN 1560-8956

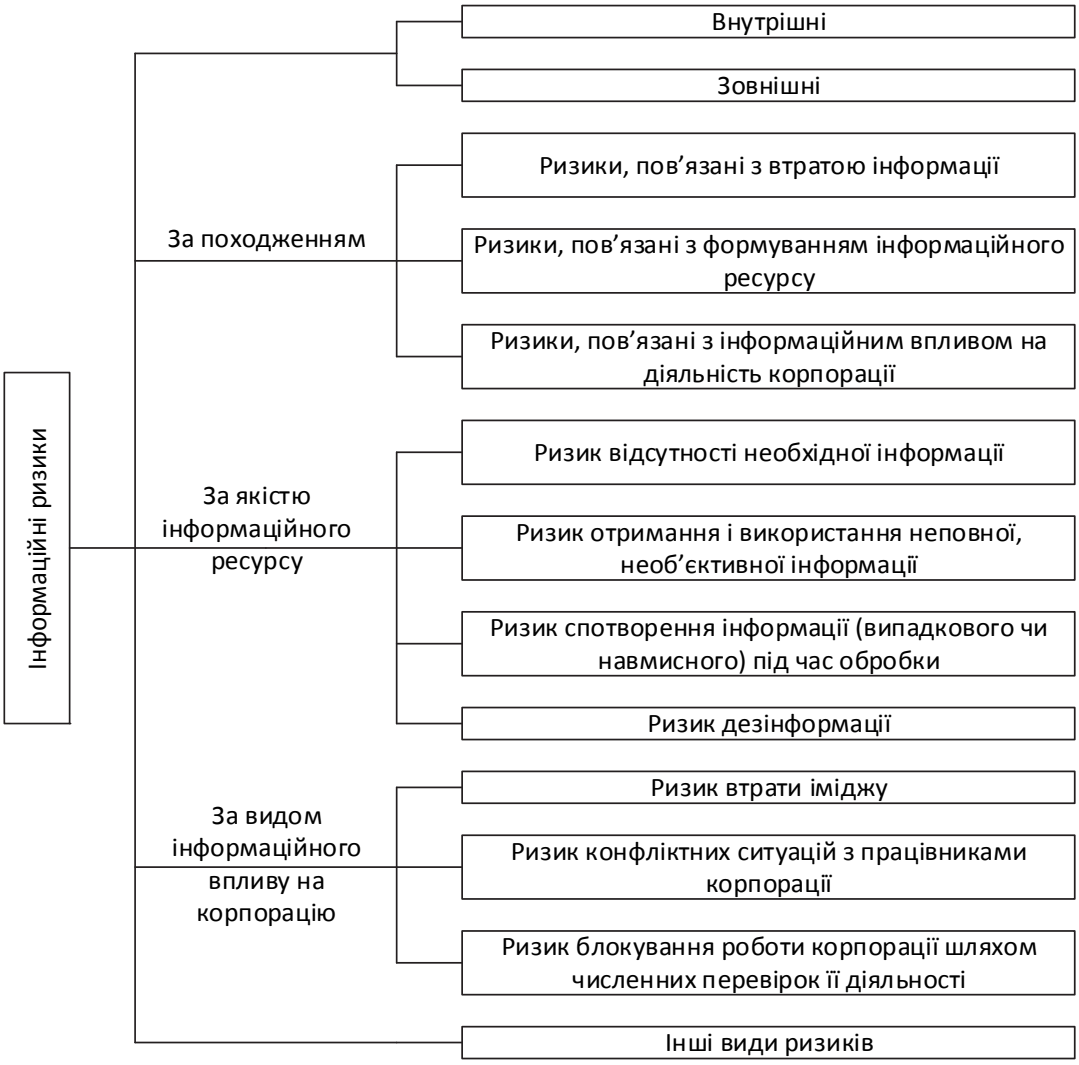

Рис. 3. Класифікація інформаційних ризиків

Припустимо, що для n активів задана відносна вартість кожного – a_j (j = 1, n). Крім того, задано c_{ij} – вплив вразливості v_i на актив a_j. Тоді сукупний вплив вразливості v_i на активи корпорації обчислюється за формулою:

$$V_i = \sum_{(i-1)}^{n} v_{ij} * C_j . \quad (2)$$

Нехай є p загроз, які впливають на V вразливостей, а d_{ki} – це потенціал впливу загрози t_k уразливості v_i. Тоді відносний сукупний вплив загрози T_k визначається як:

$$T_k = \sum_{(i-1)}^{m} d_{ki} * V_i . \quad (3)$$

Для усунення впливу загроз є q засобів управління, які можуть пом'якшити p їх загроз, а e_{lk} – вплив засобів контролю Z_0 на загрозу t_k. Тоді відносний сукупний вплив засобів контролю Z_0 визначається за формулою:

$$Z_0 = \sum_{(i-1)}^{p} e_{0l} * T_l . \quad (4)$$

Модель формування ризиків втрати інформації повинна:

– враховувати найбільшу кількість впливових факторів;

– дозволяти розраховувати ймовірність виникнення вразливостей та реалізації загрози;

– вирахувати часові межі для реалізації загроз і наслідки у вигляді збитків;

– визначати доцільність застосування запропонованих засобів захисту з оцінкою ступеня захищеності системи.

Моделювання та отримання цих показників дозволяє корпорації прийняти рішення щодо безпеки інформації в інформаційно-обчислювальній системі корпорації, а саме управляти ризиками інформаційної безпеки.

Майже в усіх методиках базою для визначення рівня ризику є допустимість появи тієї чи іншої події, яка визначає рівень ймовірності реалізації загрози. В основу методик визначення ймовірності найчастіше закладається експертний метод або використовується дані статистики попередніх періодів.

Для розробки моделі управління ризиками інформаційної безпеки корпорації необхідно вибрати таку модель або комбінацію моделей, яка б включала в себе визначення, збір та обробку даних про результуючі фактори, які притаманні системі, та дозволяє з високим рівнем ймовірності визначити найгірший сценарій для реалізації загрози. Дана модель має бути адаптивною та оперативно змінюватись з урахуванням вихідних результатів (кількості користувачів, кількості обладнання, швидкості каналу передачі даних тощо).

Етапи роботи розробленої інформаційно-аналітичної системи

Процес вибору хмарних IT-сервісів складний, погано формалізований і слабо структурований. Для прийняття обґрунтованого рішення для впровадження хмарних IT-сервісів в корпорації необхідно зібрати дані та провести їх аналіз для визначення витрат і вигод, результативності та ризиків від їх застосування. Результатом буде отримано набір даних для попереднього аналізу та оцінки інформаційних ризиків. За результатами оцінки отримуємо ваговий коефіцієнт для кожного провайдера, на основі якого приймається рішення про впровадження.

Етап 1. Збір даних

Матрична методологія базується на трьох матрицях: *загроз*, *вразливостей* і *контролю*, за допомогою яких збираються дані для аналізу ризиків [11]. Матриця вразливостей (табл. 2) показує кореляційний зв'язок між активами і вразливостями, матриця загроз (табл. 3) відображає причинно-наслідковий зв’язок вразливостей та загроз, а матриця контролю (табл. 4) демонструє співвідношення між загрозами і засобами управління. Значення, отримане в результаті аналізу, в кожній відповідній комірці матриці

характеризує цінність відношення між елементом рядка і стовпця. Використовується така система оцінок: *низька*, *середня*, *висока,* тощо (табл. 1).

Таблиця 1. Шкала оцінок

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
немає впливу	слабкий вплив	…	помірний вплив	…	…	…	…	…	сильний вплив

В процесі первинного аналізу формуються списки активів, вразливостей, загроз і засобів управління. Матриці заповнюються даними про взаєзв'язок елемента стовпця матриці з елементом рядка. Дані з матриці вразливостей переносяться в матрицю загроз, а потім дані з матриці загроз заносяться в матрицю контролю.

Таблиця 2. Матриця вразливостей

Вразливості	Активи і витрати	Публічна інформація	Конфіденційна інформація	Фінансова інформація	Службова інформація	Репутація	Витрати на відновлення	Апаратні засоби	Програмне забезпечення	Обслуговування
Веб-сервер										
Обчислювальний сервер										
Брандмауер										
Маршрутизатор										
…										

Таблиця 3. Матриця загроз

Вразливості	Загроза	Відмова в обслуговуванні	Шкідливий код	Помилки користувача	Внутрішні атаки	Спам	фізичне пошкодження апаратних засобів	Апаратні засоби
Веб-сервер								
Обчислювальний сервер								
Брандмауер								
Маршрутизатор								
…								

Перший етап передбачає аналіз наявної вхідної інформації: визначення високорівневих вимог бізнесу; визначення моделі хмарного сервісу та моделі розгортання; дані про провайдерів і додатках.

Наприклад, такими вихідними даними можуть бути: кількість трафіка, що буде витрачено; тип шифрування, який використовується; фінансові витрати; необхідна вимога щодо потужності (можливості) сервера; та інші додаткові сервіси.

Таблиця 4. Матриця контролю

Засоби контролю	Загроза	Відмова в обслуговуванні	Шкідливий код	Помилки користувача	Внутрішні атаки	Спам	Фізичне пошкодження апаратних засобів	Апаратні засоби
Брандмауер								
Система виявлення вторгнення								
Навчання персоналу								
Політика безпеки								
…								

Етап 2. Оцінка

На наступному етапі визначається відповідність обраним критеріям, використовуючи формули (2), (3) та (4), і тим самим визначається доцільність вибору корпорацією того чи іншого провайдера. Таким чином, проводиться аналіз можливості переходу до хмарних технологій на основі визначених вагових коефіцієнтів для порівняння з іншими наявними альтернативами.

Етап 3. Перевірка параметрів

Аналіз можливих загроз і аналіз ризиків є основою для обґрунтування вибору заходів щодо забезпечення інформаційної безпеки інформаційних систем хмарних обчислень, які необхідні для зниження ризику до прийнятого рівня.

На базі загальної системи оцінки вразливостей CVSS (*Common Vulnerability Scoring System*), що дозволяє визначити якісний показник схильності вразливостям з урахуванням факторів навколишнього середовища, розроблена методика кількісної оцінки потенційних вразливостей для різних типів розгортання хмарних середовищ.

Запропонований підхід до аналізу та управління ризиками дозволяє оцінити захищеності хмарного середовища, що функціонує в умовах впливу заданого класу загроз, а також ефективності комплексу заходів і засобів протидії цим загрозам. На осно-

ві такої оцінки з'являється можливість вибору варіанту конфігурації середовища хмарних обчислень і найбільш прийнятного варіанту з точки зору безпеки. Загальна система оцінювання вразливостей CVSS в даний час досить широко застосовується і все більше набуває вигляду стандарту для визначення оцінки вразливостей [12].

Основне завдання системи полягає в оцінці рівня вразливостей і надання рекомендацій щодо зменшення впливу наслідків прояви пов'язаних загроз. Слід зазначити, що загальна система обліку вразливостей є інструментом для аналізу характеристик і впливу вразливостей, незалежно від вендора (постачальника) програмного забезпечення, тому може бути використана для класифікації вразливостей хмарних середовищ.

На цьому етапі, на основі проаналізованих даних, експерт вибирає хмару (сервер), яка є найбільш оптимальним варіантом та відповідає встановленим критеріям. У випадку ймовірної часткової або повної невідповідності вибраного варіанту, експерт повертається на етап «Збір даних» та вносить зміни відповідно до критеріїв.

Етап 4. Оголошення

На четвертому етапі на основі графіку кореляції величини збитку та ймовірності події (та запропонованого експертом оптимального варіанту) команда починає обговорення обґрунтованої пропозиції щодо розробки стратегії рішень відповідно до цього варіанту.

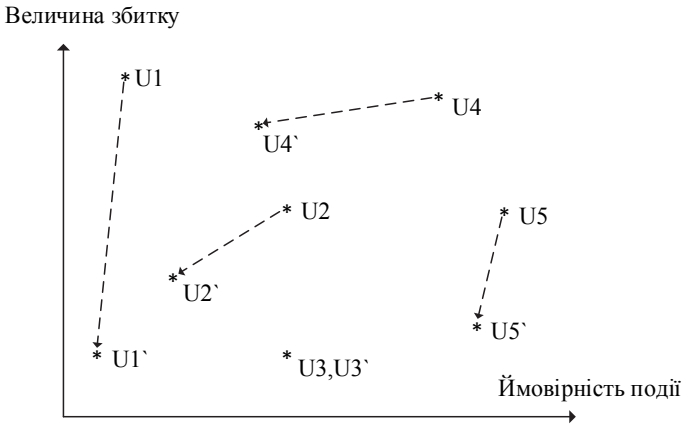

Рис. 4. Регресійна модель оцінки ризику

Регресійна модель такого типу дозволяє оптимально відстежити наявний та прогнозований рівень ризику переходу до хмарного середовища, оскільки відображає зміну діючої моделі на пропоновану.

На четвертому етапі йде компаративний аналіз отриманих результатів, та їх вхідні дані для обговорення рішення експерта разом з членами команди. Якщо пропозиція підтримується більшістю учасників та зацікавлених сторін, то переходять до етапу

впровадження в корпорації.

Висновки

На основі проведеного компаративного аналізу варто зазначити, що переваги використання хмарних технологій превалюють над недоліками. Хоча, особливу увагу варто акцентувати на нівелюванні ризиків, тобто розробці моделі управління ризиками, що демонструє процес становлення ризику на основі сценаріїв розвитку ситуації з урахуванням можливостей внесення коректівів на кожному етапі. Утім, заглиблюючись у вивчення міжнародних стандартів, сучасний стан справ демонструє зацікавленість світовими суб’єктами в уніфікації розроблених міжнародних стандартів, визначенні загальних критеріїв для систематизації та класифікації ризиків, організації ефективної взаємодії членів команди, підбору висококваліфікованих експертів. Запропонований матричний підхід до оцінки ймовірності мінімізації інформаційного ризику переходу до хмарного середовища дозволяє оптимізувати ефективність управління ризиками.

Список використаних джерел

1. Арефьев Н. IaaS, PaaS, SaaS. Раздел территории между провайдерами и клиентами облачных сервисов // Защита виртуальных сред и облачных вычислений Jet Info №5, май 2013 г. – [Электронный ресурс]. Режим доступа: http://www.jetinfo.ru/author/nikolaj-arefev/iaas-paas-saas-razdel-territorii-mezhdu-provajderami-i-klientami-oblachnykh-servisov. Дата обращения: 12.03.2014.

2. Вуколов В. Інформаційні ризики в державному управлінні — http://archive.nbuv.gov.ua/e-journals/Patp/2010_2/10vvvrdu.pdf.

3. Завгородний В.И. Парадигма информационных рисков — http://www.fakit.ru/main_dsp.php?top_id=591.

4. D:A-5.1 Report on A4Cloud contribution to standards. Version 1.1. Deliverable Lead Organisation [Electronic resource] // Cloud Accountability Project (CSA). – Access mode: http://www.a4cloud.eu/sites/default/files/D15.1 Report on A4Cloud contribution to standards.pdf. – 24.11.2015.

5. Department of defense (DoD). Cloud computing security requirements guide (SRG). Version 1, Release 1. – impl. 12.01.2015. – Developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD), 2015. – 152 p.

6. Hibbard, E. A. Latest in Cloud Computing Standards [Electronic resource] // Eric A. Hibbard. – Access mode: http://www.slideshare.net/rnewton. – 24.11.2015.

7. ISO/IEC 17788:2014 Information technology - Cloud computing - Overview and vocabulary [Text]. – impl. 15.10.2014. – Brussels : European Committee for Electrotechnical Standardization, 2014. – 16 p.

8. ITU-T. FG Cloud TR. Version 1.0. (02/2012). Part 6: Overview of SDOs involved

in cloud computing. [Electronic resource] // Switzerland, Geneva. – Access mode: http://www.itu.int/dms_pub/itu-t/opb/fg/T-FGCLOUD-2012-P6-PDF-E.pdf. – 24.11.2015.

9. NISTIR 8074 Volume 2 (Draft) Supplemental Information for the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity [Electronic resource] // National Institute of Standards and Technology. – Access mode: http://csrc.nist.gov/publications/drafts/nistir8074/nistir_8074_ vol1_ draft_report.pdf. – 24.11.2015.

10. Recommendation ITU-T Y.3511. Framework of inter-cloud computing [Text]. – impl. 09.03.2014. – Geneva : International Telecommunication Union, 2014. – 46 p.

11. Юнкерова Ю.И. Экономико-математические методы управления информационными рисками // Петербургский экономический журнал. 2014. № 1. С. 59-64.

12. NVD Common Vulnerability Scoring System Support, vol. 2. Available at: http://nvd.nist.gov/cvss.cfm?calculator&version=2.

УДК 621.398.96