DOI: 10.15587/2312-8372.2017.118388

РОЗРОБКА МОДЕЛІ ВИБОРУ ОПТИМАЛЬНОЇ КОНФІГУРАЦІЇ КОМПОНЕНТІВ АРХІТЕКТУРИ КРИТИЧНОЇ ІТ-ІНФРАСТРУКТУРИ ПРИ ЇЇ ПРОЕКТУВАННІ

Дорогий Я. Ю.

1. Вступ

Щоб конкурувати на глобальному ринку, підприємства все більше взаємодіють з партнерами та замовниками за межами своєї країни походження. Мета глобалізації операцій – скорочення витрат, отримання робочої сили та досвіду, а також доступу на нові ринки.

У рамках своєї глобальної стратегії та структури багато підприємств створюють дочірні підприємства в інших країнах. Підприємство повинно визначити, в якій мірі кожна філія є самодостатньою та незалежною від штаб-квартири при прийнятті рішень. Покращення фінансової ефективності відбувається при активній реакції філії на зміни локального ринку, і навпаки, у випадку слідування стандартизованим глобальним бізнес-процесам таке покращення є малоймовірним [1]. У той же час, надання дозволу філії приймати рішення без втручання штаб-квартири може створити напругу у відносинах, особливо щодо рішень, що пов'язані з проектуванням та управлінням ІТ-інфраструктури. Підприємства формують свою бізнес-стратегію через свої механізми управління, а потім узгоджують свої інформаційні ресурси для підтримки бізнес-стратегії. Перехід до децентралізованого підходу дає можливість компаніям використовувати свої ІТ-ресурси для реагування на умови, що виникають на місцевому ринку, в той же час, є ризик в тому, що інвестиції в ІТ можуть не співпадати з загальною бізнес-стратегією підприємства. Такий недолік може збільшити ймовірність витрат фінансових ресурсів, незадоволеність користувачами, невдачі управління безпекою, створення менеджерів, які не хочуть інвестувати в майбутні ІТ-ініціативи і, зрештою, підірвати кінцевий фінансовий результат. Саме тому, багато підприємств мають глобально-централізовані процеси прийняття рішень щодо ІТ-інфраструктури, особливо підприємства критичної інфраструктури. Основна мета – зменшення ризиків, оптимізація розподілу ресурсів, задоволення користувачів, посилення контролю та підтримки стратегії компанії [2].

Основним аргументом в підтримку централізованого проектування та управління ІТ-інфраструктурою є можливість участі у прийнятті ІТ-рішень для впливових та досвідчених професіоналів та менеджерів. Ці спеціалісти надають перевагу ІТ-проектам на основі їх актуальності, і як наслідок, ці проекти отримують адекватне фінансування. У випадку, коли орган управління є децентралізованим, спеціалісти з інформаційних технологій не можуть зрозуміти негативні наслідки їх ідеального «місцевого» рішення для всієї компанії. Протилежний аргумент – централізований підхід прийняття рішень щодо ІТ може обмежувати вплив місцевих професіоналів та менеджерів в процесі прийняття рішень, в той час, як саме вони можуть мати краще розуміння самої проблеми та відповідних ринків. ІТ-фахівці, що знаходяться у епіцентрі проблем, зумовлених умовами місцевого ринку, можуть мати

кращі можливості щодо визначення вимог до рішень та пріоритетності проектів. Тому актуальним є дослідження проектування та управління ІТ-інфраструктурою.

2. Об`єкт дослідження та його технологічний аудит

Об'єктом дослідження є критична ІТ-інфраструктура.

Критична ІТ-інфраструктура повинна:

– забезпечувати функціонування екологічно небезпечних та соціально значимих виробництв та технологічних процесів, порушення штатного режиму яких може призвести до надзвичайної ситуації техногенного характеру;

– виконувати функції інформаційної системи, порушення (зупинення) функціонування якої може призвести до негативних наслідків в політичній, економічній, соціальній, інформаційній, екологічній та інших галузях;

– забезпечувати надання значного об'єму інформаційних послуг, часткове або повне зупинення яких може призвести до значних негативних наслідків для національної безпеки в багатьох галузях.

Основна проблема в даній галузі – повна відсутність готових рішень, методологій, інструментарію, які б підійшли для моделювання, проектування та дослідження критичних ІТ-інфраструктур.

3. Мета та задачі дослідження

Метою даної роботи є розробка моделі вибору оптимальної конфігурації компонентів архітектури критичної ІТ-інфраструктури на стадії її проектування.

Для досягнення поставленої мети необхідно виконати такі задачі:

1. Удосконалити існуючий математичний апарат прийняття рішень за допомогою Марковських процесів прийняття рішень для дослідження критичних ІТ-інфраструктур.
2. Дослідити за допомогою побудованої моделі вибір конфігурації центру обробки даних (ЦОД) для архітектури критичної ІТ-інфраструктури.

4. Дослідження існуючих рішень проблеми

Попередні дослідження визначили п'ять напрямів проектування та управління ІТ – стратегічне узгодження, управління ризиками, управління ресурсами, доставка вартості та оцінка ефективності [3]. Робота присвячена напряму стратегічного узгодження в області проектування критичних ІТ-інфраструктур та визначає недоліки та переваги рішень, що пов'язані з централізованими/децентралізованими проектними рішеннями щодо архітектури ІТ-інфраструктури. Стратегічне узгодження вимагає від керівників узгодити ІТ-стратегію з загальною бізнес-стратегією як основну точку фокусу їх ІТ-інфраструктури. Запропоновано модель підтримки прийняття рішень для забезпечення прийняття відповідних проектних рішень, що співпадають з стратегією підприємства з точки зору централізації/децентралізації, в яку включено знання про майбутні недоліки/переваги кожного проектного рішення на базі запропонованих критеріїв при проектуванні ІТ-інфраструктури.

В роботі [4] зроблено висновок, що стратегічне узгодження, в залежності від контексту, може бути децентралізованим, централізованим або змішаним. У дослідженні [5] опитано 500 менеджерів, відповідальних за управління ІТ-інфраструктурою та проведено подальше опитування 30 ІТ-директорів. Як результат, визначено, що стратегічне

узгодження ІТ-рішень забезпечує зростання доходів у випадку узгодження з бізнес-стратегією підприємства, а в іншому випадку, може призвести до контрпродуктивних інвестицій в ІТ-інфраструктуру.

Узгодження інвестицій в ІТ-інфраструктуру, виходячи з потреб бізнесу, впливає на результат ІТ-ініціатив, таких як впровадження системи ERP. Відповідно до аргументів, описаних вище, деякі дослідження підтримують централізацію, а деякі дослідження підтримують децентралізацію. Наприклад, дослідження [6] показало, що продуктивність зростає, а втрати зменшуються при використанні підприємством централізованого планування та контролю за ІТ-інфраструктурою. Ще одне дослідження [7] виявило, що відмінні характеристики обробки даних CRM та локалізований характер зусиль CRM найкраще підтримуються при використанні технологій CRM у тісній зв'язці з більш широкою інфраструктурою та локальному управлінні.

В роботах [8–11] автори також вказують на необхідність дослідження ІТ-інфраструктури у зв'язці з забезпечуючими системами. Проектування архітектури у відриві від них може вплинути на оптимальність отриманої ІТ-інфраструктури.

5. Методи досліджень

5.1. Опис математичної моделі вибору оптимальної конфігурації компонентів архітектури критичної ІТ-інфраструктури

Пропонована модель має наступні *параметри*:

F – скінченна множина філій підприємства ($F = \{1,..,f\}$);

P – скінченна множина платформ ІТ ($P = \{1,..,p\}$);

T – скінченна множина відліків часу ($T = \{1,..,t\}$);

I – скінченна множина критеріїв проектування;

Z – множина категорій запитів на зміну архітектури ($Z = \{1,..,z\}$);

$f \in F$ – значення індексу філії підприємства;

$p \in P$ – значення індексу платформи ІТ;

$z \in Z$ – значення індексу запиту на зміну архітектури;

$i \in I$ – значення індексу критерію проектування;

$b_t \in I$ – бюджет нового проекту в момент часу t;

c_{fp} – вартість проектування/переходу на нову платформу p для філії f з врахуванням всіх витрат на ПЗ, апаратні засоби, інтеграцію та впровадження;

a_{fpz} – вартість виконання запиту на зміну архітектури z на платформу p для філії f;

b_{fpzi} – виграш від виконання запиту на зміну архітектури z на платформу p для філії f за критерієм i.

Простір станів моделі описується наступними змінними:

x_{zf} – кількість запитів на зміну архітектури z, що ще не виконані для філії f;

cur_{fp} – поточна платформа філії f;

X – матриця значень x_{zf};

CUR – матриця значень cur_{zf};

S – стан процесу ($S = [X, CUR, t]$).

Випадкові величини, що використовуються в моделі:

pr_{zft} – кількість запитів на зміну архітектури z для філії f в момент часу t;

PR – матриця значень pr_{zft}.

Простір рішень моделі описується наступними змінними:

y_{zft} – кількість запитів на зміну архітектури z для філії f в момент часу t, що потрібно виконати;

l_{fpt} – флаг переходу на платформу p для філії f в момент часу t, що потрібно виконати;

Y – масив змінних простору рішень;

$\Re(S)$ – множина можливих рішень для стану S;

$C^i(Y)$ – виграш за критерієм i, пов'язаний з рішенням Y;

$C(Y)$ – виграш за всіма критеріями, пов'язаний з рішенням Y;

$RWD_n^i(S)$ – максимальне очікуване значення виграшу на *n-му* етапі в стані S за критерієм i;

$RWD(S)$ – максимальне очікуване значення виграшу на *n-му* етапі в стані S за критерієм i.

Модель має певний ряд обмежень. Для стану $S = [X, CUR, t]$ змінні простору станів в Y повинні задовольняти наступні обмеження:

– обмеження бюджету проекту:

$$\sum_f \sum_p c_{fp} l_{fpt} + \sum_z \sum_f a_{zpf} y_{zft} \le b_t; \quad (1)$$

– обмеження об'єму проекту:

$$y_{zft} \le x_{zf}; \quad (2)$$

– вимоги щодо платформ:

$$\sum_p l_{fpt} = 1, \forall f, \quad (3)$$

$$y_{zft} \ge 0. \quad (4)$$

Всі рішення Y, що задовольняють вимогам (1)–(4), для стану S формують множину можливих рішень $\Re(S)$. Модель є гнучкою. Можна додати додаткові обмеження. Наприклад, можна врахувати виконання проектних рішень, що забезпечують цілісність системи та її безпеку.

Кожне можливе прийняте рішення має певну кількість безпосередньо очікуваних витрат та виграшів. По-перше, очікуваний виграш b_{fzi} за критерієм i при виконанні запиту на зміну архітектури z для філії f. Також підприємство бере на себе

витрати a_{fz} на виконання запиту на зміну архітектури z для філії f. Додатково, можуть також бути витрати c_{fp}, пов'язані з міграцією філії f на платформу p.

Враховуючи наведене вище, виграш на черговому етапі проектування за критерієм i, пов'язаний з рішенням Y, можна розрахувати за формулою:

$$C^i(Y) = \sum_z \sum_f \sum_i b_{zfi} y_{zft} - \sum_f \sum_p c_{fp} l_{fpt} - \sum_z \sum_f a_{fz} y_{fzt}. \quad (5)$$

Значення $C^i(Y)$ може бути як позитивним, так і негативним. Якщо $\sum_z \sum_f \sum_i b_{zfi} y_{zft} > \sum_f \sum_p c_{fp} l_{fpt} + \sum_z \sum_f a_{fz} y_{fzt}$, то виграш, пов'язаний з вибраними проектними рішеннями, представлений першим термом функції виграшу на черговому етапі проектування, переважує витрати, які потрібно зробити.

Невизначеність поставленої задачі полягає у частоті запитів на зміну від кожної філії. В даній роботі вважається, що значення PR є статично незалежними. Нехай $S = [X], [CUR]$ – поточний стан, $Y \in \Re(S)$ – вибраний масив рішень і $S' = [X'], [CUR']$ – стан після виконання запиту на зміну. Тоді значення стану S' змінюється відповідно до (6)–(8):

$$x'_{zf} = x_{zf} - y_{zft} + pr_{zft}, \quad (6)$$

$$cur'_{fp} = l_{fpt}, \quad (7)$$

$$t' = t + 1. \quad (8)$$

Ймовірність переходу з стану S в стан S' для рішення Y визначається як (9):

$$P_{SS'(Y)} = \prod_{f \in F} \prod_{z \in Z} \wp\left\{ pr_{zft} \mid cur_{fp} = x'_{zf} - x_{zf} + y_{zft} \right\}. \quad (9)$$

Функції пошуку моделі наступні:

$$RWD^i_1(S) = \max_{Y \in \Re(S)} C^i(Y), \quad (10)$$

$$RWD^i_n(S) = \max_{Y \in \Re(S)} \left\{ C^i(Y) + \sum_{S'} P_{SS'}(Y) RWD^i_{n-1}(S') \right\}, \; n > 1, \quad (11)$$

$$RWD(S) = \max_{Y \in \Re(S)} \sum_i \sum_j^n RWD^i_j(S). \quad (12)$$

5.2. Опис варіантів побудови платформ на базі хмарних IT-інфраструктур

Для хмарних обчислень необхідно забезпечити керування застосуваннями, реалізувати взаємодію з платформами віртуалізації і мережною інфраструктурою під загальним сценарієм для всієї системи. Система в цілому має підтримувати велику кількість компонентів і надавати загальні інструменти керуван-

ня, які можуть гарантувати надійне, безпечне і якісне надання послуг клієнтам. Мережна, апаратна і програмна інфраструктури хмарної системи мають відповідати існуючим і новим мережним стандартам:

- ISO/IEC 17789 (ITU-T Y.3502) – Інформаційні технології. Хмарні обчислення. Еталонна архітектура [12];
- NIST SP 500-291 – Стандарти хмарних обчислень [13];
- NIST SP 500-292 – Базова архітектура хмарних обчислень [14];
- ISO/IEC Committee Draft 27017 – Основи управління інформаційною безпекою для хмарних обчислень на базі ISO/IEC 27002 [15];
- ISO/IEC Draft International Standard 27018 – Основи захисту даних для публічних хмарних сервісів [16];
- ISO/IEC Working Draft 27036-4 – Інформаційна безпека відносин з постачальниками – Частина 4: Керівні принципи для забезпечення безпеки хмарних сервісів [17];
- ISO/IEC Draft International Standard 27040. Безпека систем зберігання даних IEEE P2301 – Профілі сумісності і переносимості (CPIP) [18];
- IEEE P2302 – Взаємодія хмарних систем (SIIF) [19];
- ANSI/TIA-942 [20], EN 50173-5 [21], ISO/IEC 24764 [22] – стандарти проектування хмарних дата-центрів.

Національний інститут стандартів і технологій США (National Institute of Standards and Technology – NIST) у документі [12] подав огляд еталонної архітектури хмарних обчислень, який ідентифікує основних суб'єктів, їх діяльність і функції у хмарних обчисленнях (рис. 1).

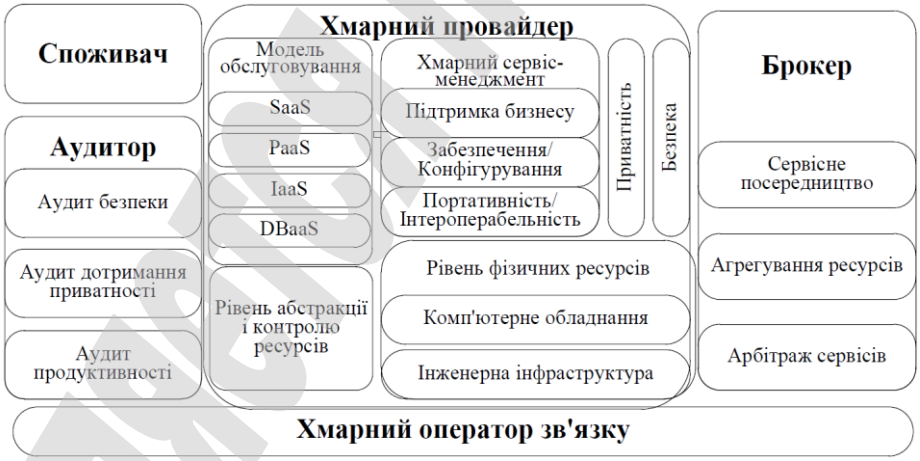

Рис. 1. Еталонна архітектура хмарних обчислень Національного інституту стандартів і технологій США

Основними суб'єктами еталонної архітектури є:

- споживачі – особи, як фізичні, так і юридичні, які користуються послугами провайдерів хмарних обчислень;
- провайдери – особи, як фізичні, так і юридичні, які відповідають за надання хмарних обчислень;
- аудитори – фізичні або юридичні особи або організація, які виконують незалежне оцінювання хмарних обчислень;

– брокери – особи, як фізичні, так і юридичні, які є ланкою між провайдером і споживачем хмарних обчислень (можливі варіанти без участі брокера, тобто хмарні послуги поставляються від провайдера до споживача безпосередньо);

– оператори зв'язку – особи, як фізичні, так і юридичні, або компанія, яка надала послуги підключення та доставки хмарних послуг від провайдера до споживача.

Основними моделями обслуговування є:

– IaaS – інфраструктура як послуга.
– PaaS – платформа як послуга.
– SaaS – програмне забезпечення як послуга.

Крім основних моделей обслуговування існують такі моделі:

– HaaS – апаратне забезпечення як послуга.
– SecaaS – безпека як послуга.
– BPaaS – бізнес-процес як послуга.
– DBaaS – база даних як послуга.
– TaaS – довіра як послуга.
– SDPaaS – хмарне середовище розроблення як послуга та інші [23].

Крім того, розрізняють чотири основні моделі розгортання:

– Приватна (Private cloud).
– Модель спільноти (Community cloud).
– Публічна (Public cloud).
– Гібридна (Hybrid cloud).

На основі аналізу розглянутих вище стандартів установлено, що типова хмарна архітектура є клієнт-серверною з підтримкою технології віртуалізації, побудованою на базі ЦОД, і має ієрархічну структуру. На рис. 2 зображено типову мережну архітектуру хмарної системи.

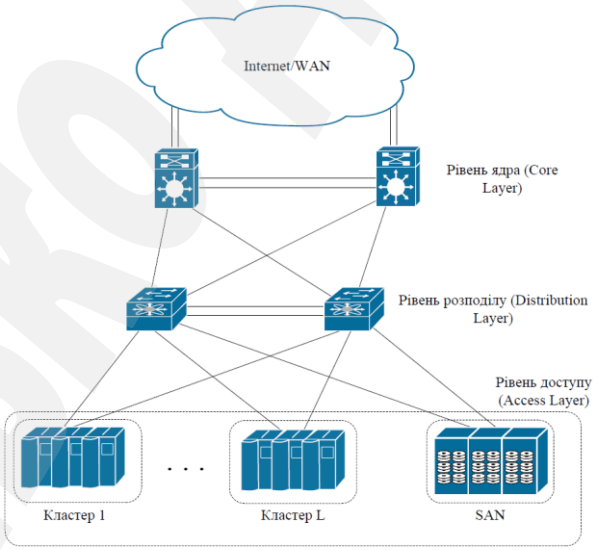

Рис. 2. Типова мережева архітектура хмарних систем

Мережева структура складається з трьох основних рівнів:

– Рівень ядра (Core layer). На цьому рівні функціонують маршрутизатори або комутатори третього рівня моделі OSI, які складають основу всієї мережі

дата-центру з високошвидкісним и портами (10/40/100 GbE) для маршрутизації потоків між WAN і мережею дата-центру.

− Рівень агрегації або розподілу (Aggregation/Distribution layer). На цьому рівні також працюють комутатори третього рівня моделі OSI, основне призначення яких полягає у розподілі навантаження між локальними мережами дата-центру.

− Рівень доступу (Access layer). На даному рівні розташовуються кінцеві точки (сервера) та мережеве обладнання, що пов'язує кінцеві точки з рівнем агрегації. На рівні доступу функціонують кластери дата-центрів, що складаються з великої кількості фізичних серверів і віртуальних машин, які функціонують на кожному з них. На цьому ж рівні розташовується загальна мережа зберігання даних SAN (Storage Area Network). Група, що складається зі взаємозв'язаних компонентів зберігання даних, обчислювальних і мережних ресурсів, які працюють спільно на рівні доступу з метою надання доступу до сервісів або застосувань клієнтам, називається точкою доставки або POD (Point of delivery).

На сьогодні поширені дві основні топології з’єднання серверів у кластерах: Top of Rack (ToR) і End of Row (EoR) [24]. ToR топологія передбачає розміщення окремого комутатора (або двох для забезпечення надлишковості) на вершині кожної стійки серверів. Комутатори рівня доступу з’єднуються з комутаторами верхнього рівня (рівня агрегації) волоконно-оптичними кабелями (рис. 3).

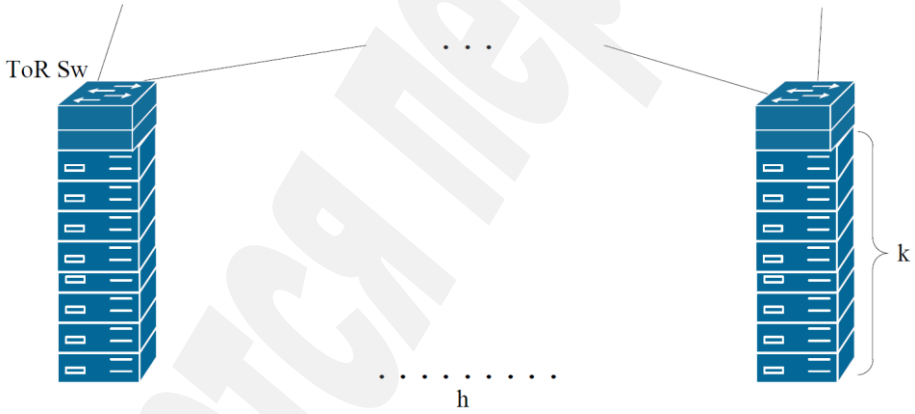

Рис. 3. Топологія ToR (Top of Rack)

Позначення на рис. 3: m – загальна кількість серверів у кластері і k – кількість серверів у кожній стійці, з’єднаних з комутаторами рівня доступу двома патчкордами для забезпечення надлишковості. Інша топологія (рис. 4) передбачає використання одного (двох для надлишковості) комутатора в кінці (EoR) або в середині (MoR – Middle of Row) масиву стійок з серверами [25].

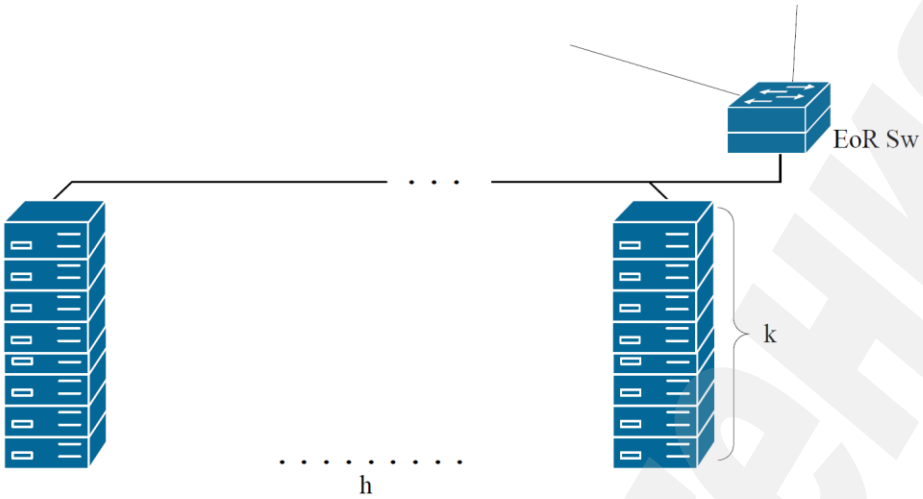

Рис. 4. Топологія кластера EoR/MoR (End of Row/Middle of Row)

У такому виконанні мережеве навантаження повністю доводиться на EoR-комутатор.

З точки зору зв'язності мережі архітектури ToR і EoR/MoR являють собою протилежні рішення. В першому випадку зв'язаність мережі максимальна. Але потрібні великі витрати на обладнання і більшу кількість портів на комутаторі рівня агрегації, до якого безпосередньо підключені ToR-комутатори рівня доступу. В другому випадку потрібна менша кількість портів на комутаторі рівня агрегації і менші витрати на комутатор рівня доступу, але зв'язність мережі при цьому буде мінімальною.

При виборі топології необхідно враховувати накладні витрати на розгортання, кількість обладнання та інші критерії. Тому третій варіант – гібридна архітектура мережі рівня доступу кластера ЦОД між топологіями ToR і EoR. Даний варіант формується на базі комбінації двох концепцій з урахуванням накладних витрат та економії портів. Як результат, варіант забезпечує мінімально прийнятний рівень критичності відмов комутаторів рівня доступу, не знижуючи при цьому показники надійності, порівняно з топологією ToR. Модель такої архітектури показано на рис. 5.

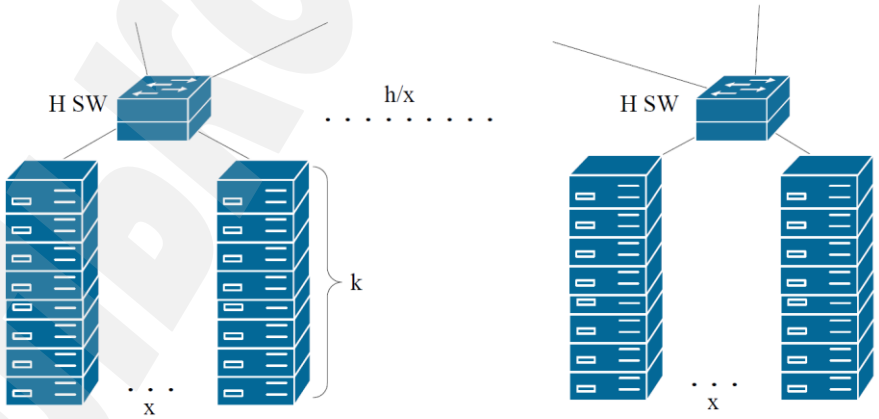

Рис. 5. Гібридна топологія кластеру

Гібридна топологія передбачає підключення декількох стійок серверів до окремих комутаторів рівня доступу, які можуть бути розташовані в середині ряду.

На базі представлених топологій кластерів формується архітектура мережі ЦОД. Є два основних варіанти реалізації мережі ЦОД. Перший варіант побудови – архітектуру мережі ЦОД з одним POD [26] подано на рис. 6.

Система є працездатною, якщо складається з мережі зберігання даних SAN, хоча б одного з мережевих маршрутів до кластерів рівня доступу і хоча б одного кластера з серверами.

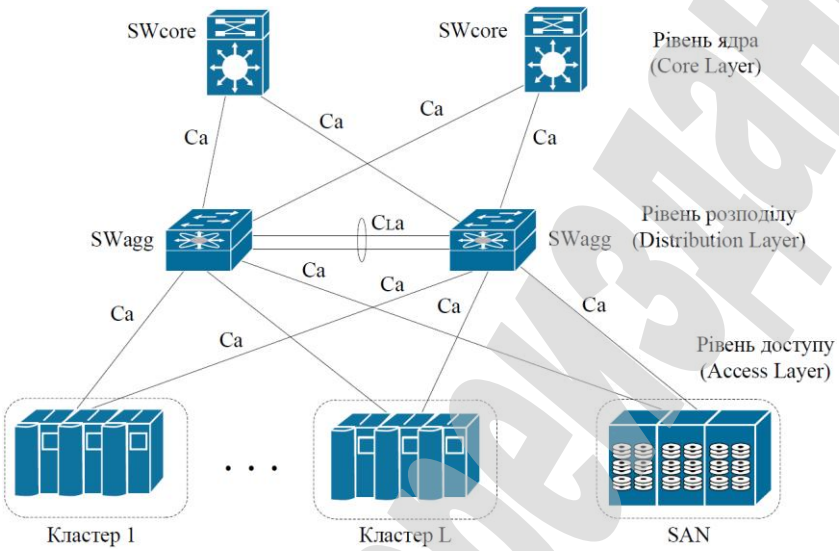

Рис. 6. Архітектура мережі центру обробки даних (ЦОД) з одною точкою доставки (POD)

Другий варіант побудови – архітектура мережі віртуального ЦОД з декількома POD, показаний на рис. 7.

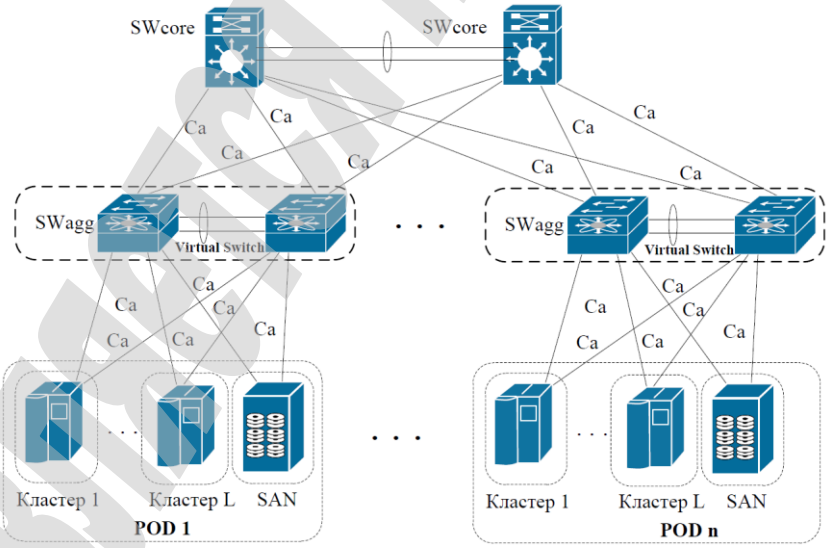

Рис. 7. Архітектура центру обробки даних (ЦОД) з декількома точками доставки (POD)

Таким чином, враховуючи вищенаведене, можна виділити наступні типи платформ, які будуть використані в даній роботі (табл. 1).

Централізоване рішення передбачає, що всі основні компоненти мережі знаходяться в штаб-квартирі підприємства (окрім кластерів).

Таблиця 1

Типи платформ

Платформа	Тип кластеру	Архітектура мережі ЦОД	Централізація/децентралізація	Приблизна вартість, дол.
1	ToR	1 POD	Ц	200000
2	EoR/MoR	1 POD	Ц	300000
3	Hybrid	1 POD	Ц	150000
4	ToR	n POD	Ц	600000
5	EoR/MoR	n POD	Ц	700000
6	Hybrid	n POD	Ц	550000
7	ToR	n POD	ДЦ	900000
8	EoR/MoR	n POD	ДЦ	1000000
9	Hybrid	n POD	ДЦ	800000

Децентралізоване рішення – компоненти розподілені між штаб-квартирою та філіями підприємства.

6. Результати дослідження

Експериментальні дослідження базуються на проблемі вибору архітектури мережі ЦОД для віртуальної критичної IT-інфраструктури підприємства, що складається з штаб-квартири та 2-х філій.

Для дослідження використані наступні варіанти можливих рішень (табл. 2).

Таблиця 2

Варіанти конфігурацій

Конфігурація	Штаб-квартира	Філія 1	Філія 2
1	Платформа 1	Платформа 1	Платформа 1
2	Платформа 1	Платформа 1	Платформа 3
3	Платформа 1	Платформа 2	Платформа 3
…	…	…	…
84	Платформа 9	Платформа 9	Платформа 9

По суті, особи, що приймають рішення щодо вибору архітектури для критичної IT-інфраструктури, мають вирішити, чи потрібно спроектувати всю IT-інфраструктуру на платформі найнижчої вартості (Платформа 3) або знайти варіант, який буде дорожчий, але буде більш надійним, ефективним тощо. Кожний варіант рішення потрібно оцінити з точки зору майбутніх потенційних проектів та внесення змін до IT-інфраструктури, які ці проекти можуть вимагати.

В табл. 3 наведені події, які можуть викликати потребу в змінах для платформ.

Кожний тип події далі поділяється на декілька категорій згідно з їх розміром, поширенням запиту на зміну та супутні витрати/виграши.

В табл. 4 наведена структура даних, що використана для дослідження запропонованої моделі.

У цій роботі порівнюється сукупний виграш, отриманий від рекомендацій, що надає запропонована модель, яка розглядає витрати та виграш за критеріями одночасно.

Таблиця 3

Події, що можуть викликати потребу в змінах для платформ

Тип події	Приклад	Виграш	Витрати
Нове застосування	Встановлення нового застосування через нові бізнес або IT-потреби	Нові фінансові виграши, що надає нове застосування	Витрати на розгортання нового застосування в IT-інфраструктуру
Масштабування	Збільшення числа транзакцій через зростання кількості користувачів тощо	Додаткові фінанси від нових користувачів	Витрати на масштабування інфраструктури
Інтеграція	Інтеграція нових застосувань через зміну виробничих процесів тощо	Додаткові фінансові надходження або економія від використання покращених виробничих процесів	Витрати на інтеграцію
Модифікація системи	Потреба в комбінуванні різних типів даних тощо	Виграш від використання нових підходів щодо прийняття рішень	Витрати на модифікацію компонент з метою підтримки нових типів даних тощо
Безпека	Підвищена увага хакерів вимагає покращення фаєрволів, захисту серверних операційних систем тощо	Зменшення потенційного негативного ефекту від атак та збереження даних	Витрати на проведення заходів, спрямованих на покращення безпеки
Критичність	Перехід сервісу в ранг критичних	Підвищена надійність, безпечність тощо	Витрати на проведення заходів щодо переведення сервісу в ранг критичних

Для моделювання зроблено припущення, що фактична кількість запитів на зміну архітектури для кожної філії за певний період (pr_{zft}) відповідає розподілу Пуасона за параметром λ. Значення λ коливається від 25 % до 200 % базового значення з кроком 5 % (36 точок проектування).

В ході дослідження проаналізовано вплив змін у розподілі запитів на зміну архітектури філій дочірніх компаній на вибір платформи. Базовий розподіл запитів на зміну архітектури встановлений на рівні 30 % для штаб-квартири, 35 % – для філії 1 та 35 % – для філії 2. Для спрощення представлення результатів моделювання фіксує базовий рівень для штаб-квартири на рівні 30 % запитів, а для філій 1 та 2 цей рівень змінюється від 0 % до 70 % з кроком 5 % (14 точок моделювання). Сумарно така схема моделювання дає 504 точки моделювання. Згідно з табл. 4 спочатку визначається загальна кількість запитів на зміну архітектури для кожної філії, а далі, визначається розподіл запитів на зміну архітектури по категоріям, враховуючи їх відносну частоту виникнення. Далі, визначаються відповідні витрати та виграш по філіям.

Таблиця 4

Структура даних

Штаб-квартира/Філія 1/Філія *n*				Платформа 1		…	Платформа 84	
Категорія	Подія	Розмір події	Очікувана частота виникнення події, в місяць	Очікувані витрати, k$	Очікуваний виграш, k$	…	Очікувані витрати, k$	Очікуваний виграш, k$
1	Нове застосування	Незначна	20	10	15	…	12	13
2	Нове застосування	Середня	5	20	30	…	22	44
3	Нове застосування	Велика	1	50	70	…	55	80
4	Масштабування	Незначна	5	5	10	…	3	5
5	Масштабування	Середня	3	15	25	…	10	12
6	Масштабування	Велика	1	30	40	…	40	80
7	Інтеграція	Незначна	15	5	7	…	8	10
8	Інтеграція	Середня	8	10	12	…	15	30
9	Інтеграція	Велика	2	30	45	…	45	70
10	Модифікація системи	Незначна	20	5	6	…	3	5
11	Модифікація системи	Середня	10	10	17	…	12	18
12	Модифікація системи	Велика	1	25	55	…	30	44
13	Безпека	Незначна	100	5	15	…	6	9
14	Безпека	Середня	20	20	100	…	30	70
15	Безпека	Велика	5	50	200	…	60	120
16	Критичність	Незначна	5	5	40	…	2	5
17	Критичність	Середня	2	10	70	…	12	60
18	Критичність	Велика	1	100	800	…	120	700

На рис. 8 показані рекомендації (з 84 можливих конфігурацій, наведених в табл. 2), наданих пропонованою моделлю для різних точок симуляції проектування.

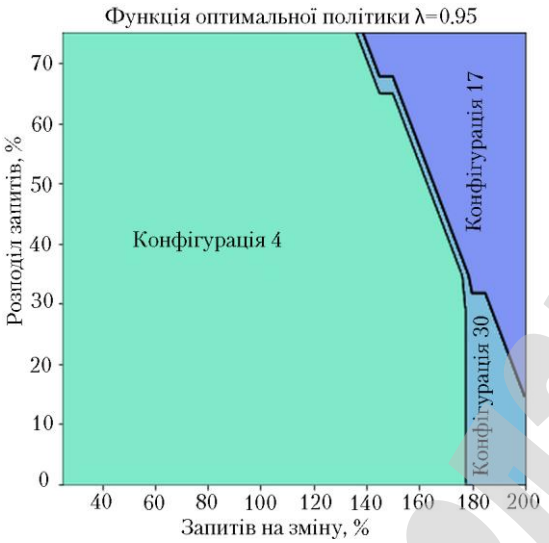

Рис. 8. Результати моделювання

Як видно з рис. 8, оптимальною з точки зору максимізації сукупного виграшу виявилася конфігурація 4.

7. SWOT-аналіз результатів дослідження

Strengths. При роботі з критичними IT-інфраструктурами, оцінка вибору конкретного варіанту реалізації архітектури є однією з проблем, з якою стикаються всі методи, які використовуються для проектування. Запропонована модель є водночас модульною та масштабованою в тому сенсі, що має достатню гнучкість у виборі та використанні як простих, так і складних критеріїв вибору архітектури для критичної IT-інфраструктури. Модульність досягається за рахунок використання різних конфігурацій елементів, тоді як масштабованість представлена у двох формах:

− масштабованість при побудові моделі (топологія і функціональність) критичної IT-інфраструктури;

− масштабованість з точки зору використання різного роду критеріїв, необхідних для порівняння варіантів реалізації. З точки зору моделювання, пропонований підхід дозволяє створювати моделі оцінки варіантів реалізації на базі різних критеріїв, які можна далі використовувати як вхідні моделі для подальшого порівняння за допомогою інших критеріїв, що в свою чергу, дає можливість знайти оптимальну архітектуру критичної IT-інфраструктури. Таким чином, модель дозволяє накопичувати моделі оцінки варіантів реалізації для багаторазового використання.

Модель побудована на використанні Марківського процесу прийняття рішень і надає всі необхідні інструменти для побудови, планування, дослідження, управління, оцінювання варіантів архітектури критичних IT-інфраструктур.

Weaknesses. На даному етапі розробки моделі єдиною вадою є відсутність реальних параметрів роботи щодо компонент критичної IT-інфраструктури.

Opportunities. У майбутньому планується використати запропоновану модель для розробки моделей оцінювання вибору компонент всіх систем та підсистем критичної IT-інфраструктури, з кінцевою метою у вигляді створення бібліотеки моделей, яка дозволить вибирати та легко використовувати їх для різних досліджень. Запропонована модель та бібліотека моделей надасть можливість дослідникам про-

водити попередню оцінку варіантів реалізації архітектури критичної IT-інфраструктури за різними критеріями.

Threats. На даний момент важко передбачити негативні ризики розробленої моделі. Але можна точно сказати, що ніяких додаткових витрат розробник критичної IT-інфраструктури, що буде використовувати пропоновану модель та розроблену в майбутньому бібліотеку моделей, нести не буде.

8. Висновки

1. Удосконалено існуючий математичний апарат Марківських процесів прийняття рішень з метою дослідження критичних IT-інфраструктур. Звичайний Марківський процес прийняття рішень пристосовано для оцінювання вибору оптимальної конфігурації компонентів архітектури критичної IT-інфраструктури за різними критеріями.
2. Досліджено можливість використання моделі. Ця модель дозволяє проводити оцінку варіантів реалізації різних компонент та підсистем критичної IT-інфраструктури. На простій моделі вибору оптимальної архітектури центру обробки даних для критичної IT-інфраструктури перевірена працездатність запропонованої моделі – створена модель в пакеті MatLab, досліджена її робота.
3. В результаті моделювання серед 84 можливих конфігурацій побудови центру обробки даних обрана найкраща за сумарним виграшом (конфігурація 4).

Література

1. Ghemawat, P. Managing Differences: The Central Challenge of Global Strategy [Text] / P. Ghemawat // Harvard Business Review. – 2007. – Vol. 85, No. 3. – P. 58–68.
2. Simonsen, J. Involving Top Management in IT Projects [Text] / J. Simonsen // Communications of the ACM. – 2007. – Vol. 50, No. 8. – P. 52–58. doi:10.1145/1278201.127820
3. Wilkin, C. L. A Review of IT Governance: A Taxonomy to Information Accounting Information Systems [Text] / C. L. Wilkin, R. Chenhall // Journal of Information Systems. – 2010. – Vol. 24, No. 2. – P. 107–146. doi:10.2308/jis.2010.24.2.107
4. Grover, V. Fix IT-Business Relationships Through Better Decision Rights [Text] / V. Grove, R. M. Henry, J. B. Thatcher // Communications of the ACM. – 2007. – Vol. 50, No. 12. – P. 80–86. doi:10.1145/1323688.1323699
5. Shpilberg, D. Avoiding the Alignment Trp in Information Technology [Text] / D. Shpilberg, S. Berez, R. Puryear, S. Shah // MIT Sloan Management Review. – 2007. – Vol. 49, No. 1. – P. 51–58.
6. Neirotti, P. Assessing the strategic value of Information Technology: An analysis on the insurance sector [Text] / P. Neirotti, E. Paolucci // Information & Management. – 2007. – Vol. 44, No. 6. – P. 568–582. doi:10.1016/j.im.2007.05.005
7. Sen, A. IT Alignment Strategies for Customer Relationship Management [Text] / A. Sen, A. P. Sinha // Decision Support Systems. – 2011. – Vol. 51, No. 3. – P. 609–619. doi:10.1016/j.dss.2010.12.014

8. Casalicchio, E. Federated Agent-based Modeling and Simulation Approach to Study Interdependencies in IT Critical Infrastructures [Text] / E. Casalicchio, E. Galli, S. Tucci // Proceedings of the IEEE International Symposium on Distributed Simulation and Real-Time Applications (DS-RT‘07). – Chania, Crete, Greek. – 2007. doi:10.1109/ds-rt.2007.11

9. Pederson, P. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research [Text]: Technical Report No. INL/EXT-06-11464 / P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann. – Idaho: Idaho National Laboratory, 2006. – 116 p. doi:10.2172/911792

10. Panzieri, S. An approach to model complex interdependent infrastructures [Text] / S. Panzieri, R. Setola, G. Ulivi // IFAC Proceedings Volumes. – 2005. – Vol. 38, No. 1. – P. 404–409. doi:10.3182/20050703-6-cz-1902.00068

11. Dorogyy, Y. Development of the approach for designing, modelling and research of critical IT infrastructure [Text] / Y. Dorogyy // Technology audit and production reserves. – 2017. – Vol. 5, No. 2 (37). – P. 34–41. doi:10.15587/2312-8372.2017.112495

12. BS ISO/IEC 17789:2014. Information technology. Cloud computing. Reference architecture [Text]. – The British Standards Institution, 2014. doi:10.3403/30268907

13. NIST SP 500-291. NIST Cloud Computing Standards Roadmap [Text]. – National Institute of Standards and Technology, 2013. doi:10.6028/nist.sp.500-291r2

14. Marcus, B. Interfacing NIST IoT, Big Data, and Cloud Models [Electronic resource] / B. Marcus. – October 5, 2015. – Available at: \www/URL: https://bigdatawg.nist.gov/_uploadfiles/M0450_v1_3857254727.pdf

15. BS ISO/IEC 27017:2015. Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services [Text]. – The British Standards Institution, 2015. doi:10.3403/30259620

16. BS ISO/IEC 27018:2014. Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [Text]. – The British Standards Institution, 2014. doi:10.3403/30266768

17. BS ISO/IEC 27036-4:2016. Information technology. Security techniques. Information security for supplier relationships. Guidelines for security of cloud services [Text]. – The British Standards Institution, 2016. doi:10.3403/30275201

18. BS EN ISO/IEC 27040:2016. Information technology. Security techniques. Storage security [Text]. – The British Standards Institution, 2015. doi:10.3403/30249804

19. IEEE P 2302 ™/D 0.2. Draft Standard for Intercloud Interoperability and Federation (SIIF) [Electronic resource]. – The Institute of Electrical and Electronics Engineers, Inc., January 2012. – Available at: \www/URL: https://www.oasis-open.org/committees/download.php/46205/p2302-12-0002-00-DRFT-intercloud-p2302-draft-0-2.pdf

20. ANSI/TIA-942-2005. Telecommunications Infrastructure Standard for Data Centers [Electronic resource]. – Arlington: Electronic Components Industry

Association (ECIA), 2005. – Available at: \www/URL: http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf

21. BS EN 50173-5:2007+A2:2012 Information technology. Generic cabling systems. Data centres [Text]. – The British Standards Institution, 2007. doi:10.3403/30141480

22. ISO/IEC 24764:2010. Information technology – Generic cabling systems for data centres [Electronic resource]. – International Organization for Standardization, 2010. – Available at: \www/URL: https://www.iso.org/standard/43520.html

23. Shelimanova, Zh. V. Taxonomic scheme of cloud computing [Text] / Zh. V. Shelimanova, O. V. Yanovska, A. A. Furmanov // Radioelektronni i kompiuterni systemy. – 2015. – Vol. 74, No. 4. – P. 51–55.

24. Data Center Networking – Connectivity and Topology Design Guide [Electronic resource]. – Available at: \www/URL: https://www.cdigroup.co.uk/wp-content/pdf-documents/data-centers/Enterasys-Data-Center-Design-Guide.pdf

25. SLA for App Service [Electronic resource] // Microsoft Azure. – July 2016. – Available at: \www/URL: https://azure.microsoft.com/en-us/support/legal/sla/app-service/v1_4/

26. Murray, P. Cloud Networking Architecture Description [Text] / P. Murray, B. Melander, V. Fusenig, M. Meulle, L. Vaquero // Scalable and Adaptable Internet Solutions. – 2011. – P. 14–69.