Системы телекоммуникации, связи и защиты информации

УДК 621.391

Я.Ю. Дорогий, канд. техн. наук

Національний технічний університет України «Київський політехнічний інститут»,

вул. Політехнічна, 42, корпус 18, м. Київ, 03056, Україна.

Розподіл ресурсів критичної IT-інфраструктури з використанням хмарних технологій

В статті розглянуті питання щодо розподілу ресурсів критичної IT-інфраструктури з використанням хмарних технологій, визначення параметрів для формування критерію оптимальності управління критичною IT-інфраструктурою. Запропонований критерій оптимальності управління чітко визначає умови функціонування критичної IT-інфраструктури. В роботі запропонована нечітка багатокритеріальна модель управління ресурсами критичної IT-інфраструктури на базі оптимізації за параметрами забезпеченості та надійності ресурсів, побудованої з використанням технології побудови хмар IAAS. Наведений її детальний опис, умови функціонування та приклад її використання в реальному середовищі на прикладі використання технології реплікації для віртуальних машин, на яких розгорнуті критичні сервіси та процеси. Бібл. 12.

Ключові слова: *критична IT-інфраструктура; життєвий цикл; управління інфраструктурою; хмарні обчислення; хмарні технології; розподіл ресурсів.*

Введення в проблему

Критична IT-інфраструктура – це сукупність IT-інфраструктур державного та приватного сектору, які забезпечують функціонування та безпеку стратегічних інститутів, систем і об'єктів держави (органів центрального та місцевого управління, систем управління енергетикою, транспортом, зв'язком, банківським сектором, підприємств, під час діяльності яких використовуються та/або виробляються небезпечні речовини тощо) і безпеку громадян (системи управління правоохоронних структур і оборонного сектору тощо), несанкціоноване втручання в роботу яких може загрожувати економічній, екологічній, соціальній та іншим видам безпеки або завдати шкоди міжнародному іміджу держави [1, 2].

Критична IT-інфраструктура також повинна відповідати наведеним вище критеріям, а також має деякі інші критерії та обмеження, що є специфічними для галузі її використання та цілей, які перед нею ставляться, і які будуть розглянуті в цій статті.

При розгляді питань віртуалізації ресурсів критичної IT-інфраструктури виникає ряд додаткових обмежень, які і будуть розглянуті в даній роботі.

Швидкий розвиток інформаційних технологій, їх активне впровадження в процеси управління створили ситуацію, коли сам процес надання інформаційних послуг став об'єктом управління.

Основні постачальники комп'ютерного та телекомунікаційного обладнання й інформаційних технологій представили для широкого загалу велику кількість рішень, призначених для розв'язання проблеми створення IT-інфраструктур. Методологічні засади її розв'язання викладені в рішеннях ITIL, на основі якої отримала розвиток ITSM. Остання розробка, яка досить детально описує проблематику та майже повністю перекриває попередні розробки – COBIT [3]. Всі вказані розробки є методологічним апаратом, який потрібно використовувати для створення конкретної критичної IT-інфраструктури. Специфіка життя в окремо взятій країні також накладає свої обмеження на створення тієї чи іншої критичної IT-інфраструктури.

На даний момент в Україні вже почалася робота в напрямку розвитку проблематики критичних IT-інфраструктур, хоча ракурс розгляду в основному стосується безпеки функціонування. Теж саме можна сказати і про міжнародних дослідників, хоча деякі роботи [4-6] і розглядають частково інші питання, крім безпеки. Остання розробка [7] дещо покращує

розуміння поставленої проблематики, але не надає конкретних алгоритмів щодо планування, створення, управління та інших задач, що виникають при розробці IT-інфраструктур, і тим більше, не відповідають на ці ж самі питання стосовно критичних IT-інфраструктур. Питання віртуалізації підняті в деяких роботах [8-10], але розглянуті з точки зору звичайних IT-інфраструктур, де немає жорстких обмежень та вимог стосовно виділення ресурсів для деяких процесів та сервісів.

Аналіз існуючих рішень

Різні постачальники хмарних сервісів мають дещо різні визначення понять «Хмарні обчислення». Це пов'язано з тим, що вони намагаються підкреслити унікальність власної розробки і надають їм назви, які іноді зовсім не відображають реальну суть сервісів, що пропонуються.

Загалом можна виділити три головні напрямки хмарних обчислень:

- IaaS (Infrastructure as a Service);
- PaaS (Platform as a Service);
- SaaS (Software as Service).

IaaS зазвичай надає уніфіковані апаратні і програмні ресурси, але в деяких випадках і на інфраструктурному рівні для установки ПО з оплатою pay as you go (по мірі використання). Замовлена інфраструктура може динамічно масштабуватися. На базі такого підходу побудовані Amazon EC2 (Elastic Cloud Computing) Service і Amazon S3 (Simple Storage Service).

PaaS надає більш високий рівень сервісу, що дозволяє розробляти, тестувати і впроваджувати власні програми. Вбудована масштабованість накладає обмеження на тип розробляються. Яскравим прикладом реалізації такого підходу є сервіс Google App Engine, що дозволяє впроваджувати Web-додатки на тій же системі, на якій працюють власні додатки Google.

SaaS пропонує готове спеціалізоване ПО, що веде до спрощення використання додатків і до зменшення витрат на розробку. Одним з чудових прикладів реалізації за таким підходом є Salesforce та її онлайнова система управління відносинами з клієнтами. Дослідження компанії Forrester показують, що серед різних варіантів хмарних середовищ переважає SaaS [11].

Оскільки в критичних IT-інфраструктурах зосереджені потужні і досить дорогі ресурси, виникає проблема їх ефективного використання. Це стає можливим за рахунок розподілу, управління і диспетчерування ресурсів і навантаженням на основі комплексу відповідних математичних моделей і методів. Формалізація проблеми ефективного використання ресурсів привела до задач нечіткого програмування з широким вибором критеріїв оптимізації і врахуванням критичності, ресурсних, часових, технологічних та інших обмежень.

Для формування критерію оптимальності створення і подальшого функціонування критичної IT-інфраструктури пропонується використати наступну множину параметрів:

- надійність – показник надійності критичної IT-інфраструктури в період експлуатації;
- живучість – можливість виконувати свої функції при втраті ресурсів, підсистем і т. ін.;
- забезпеченість – показник максимальної кількості процесів та сервісів, що обслуговуються;
- відновлюваність – тривалість відновлення готовності до експлуатації;
- економічність – витрати різноманітних ресурсів на забезпечення функціонування критичної IT-інфраструктури;
- безпечність – показник неможливості виконання несанкціонованих дій, спрямованих на порушення роботи критичної IT-інфраструктури чи її частин;
- строк життя;
- ефективність – поєднання вище згаданих параметрів в кожному окремому випадку під визначену задачу.

При формуванні вимог критерію управління критичною IT-інфраструктурою необхідно також враховувати особливості розв'язання задачі. Слід зазначити, що визначення всієї множини параметрів не можна повністю звести до системи формалізованих процедур, бо деякі з них вимагають якісного аналізу. Для такого аналізу слід використати метод структуризації, який дозволяє поділити задачу на підзадачі, визначитись за допомогою експертів або без низ з методами розв'язання цих підзадач, обмеженнями використання цих розв'язків та методами поєднання розв'язків.

Постановка проблеми розподілу ресурсів

Розглянемо приклад, коли при наданні сервісу IaaS ресурси віртуального серверу розподіляються нодами, а облік їх використання здійснюється в нодо-годинах. Критичний сервіс вимагає фіксовану мінімальну кількість нод, яка гарантовано буде знаходитись у його розпорядженні в будь який момент часу, і яка буде зарезервована за ним навіть під час

простою. Крім того, критичний процес/сервіс має можливість зарезервувати кількість нод, що будуть надані йому додатково, у випадку потреби з його сторони та наявності відповідних ресурсів у хмарі.

Необхідно розробити моделі і методи розподілу ресурсів і навантаження хмарних ЦОД, що відповідають наведеним вище особливостям хмарних IT-інфраструктур. базуються на прийнятних для провайдерів критеріях і враховують ресурсні, технологічні та інші обмеження.

Модель розподілу ресурсів хмарної критичної IT-інфраструктури

Розглянемо одну з основних задач функціонування критичної IT-інфраструктури – задачу управління ресурсами. Для цієї задачі можна побудувати багато різних моделей з різними вихідними умовами та обмеженнями.

Нехай є декілька фізичних серверів $S_i, i = 1...n$, на яких під управлінням гіпервізорів працюють віртуальні машини (ВМ) $V_i, i = 1...\text{m}$.

Введемо необхідні для формування моделі розподілу ресурсів критичної IT-інфраструктури позначення:

$Z_1,...,Z_n$ – комплекс бізнес-процесів, підтримка яких забезпечує ефективне функціонування об'єкта управління;

$S_1,...,S_m$ – комплекс універсальних сервісів, підтримка яких забезпечує ефективне функціонування об'єкта управління;

$w_i^z,...,w_n^z$ – коефіцієнти критичності бізнес-процесів $Z_1,...,Z_n$ відповідно за нечіткою шкалою:

- критичний - $\alpha_1 \le w_i^z \le 1$;
- дуже важливий - $\alpha_2 \le w_i^z < \alpha_1$;
- важливий - $\alpha_3 \le w_i^z < \alpha_2$;
- не важливий - $w_i^z < \alpha_3$.

$w_i^s,...,w_m^s$ – коефіцієнти критичності універсальних сервісів $S_1,...,S_m$ відповідно за нечіткою шкалою:

- критичний - $\gamma_1 \le w_i^s \le 1$;
- дуже важливий - $\gamma_2 \le w_i^s < \gamma_1$;
- важливий - $\gamma_3 \le w_i^s < \gamma_2$;
- не важливий - $w_i^s < \gamma_3$.

$R_1,...,R_m$ – ресурси сервера S_i критичної IT-інфраструктури у нодах, що необхідні для підтримки бізнес-процесів;

$T_1,...,T_m$ - надійність ресурсів сервера S_i критичної IT-інфраструктури;

$p_0 = \left\| \tilde{p}_{0ij}^k \right\|$ – матриця потреб бізнес-процесів у ресурсах критичної IT-інфраструктури на віртуальній машині V_k, яка гарантовано задовольняється, де $\tilde{p}_{0ij}^k$ дорівнює кількості потрібного для бізнес-процесу Z_i ресурсу R_j у вигляді трикутного нечіткого числа $\tilde{p}_{0ij}^k = (p_{0ij}^{k\text{г}}, p_{0ij}^{k\text{с}}, p_{0ij}^{k\text{к}})$ чи 0, якщо ресурс не потрібен, де $p_{0ij}^{k\text{г}}$ - найгірший (максимальний) варіант потреби у ресурсі, $p_{0ij}^{k\text{с}}$ - середня потреба у ресурсі, $p_{0ij}^{k\text{к}}$ - найкращий (мінімальний) варіант потреби у ресурсі.

$s_0 = \left\| \tilde{s}_{0ij}^k \right\|$ – матриця потреб універсальних сервісів у ресурсах критичної IT-інфраструктури на віртуальній машині V_k, яка гарантовано задовольняється, де $\tilde{s}_{0ij}^k$ дорівнює кількості потрібного для універсального сервісу S_i ресурсу R_j у вигляді трикутного нечіткого числа $\tilde{s}_{0ij}^k = (\tilde{s}_{0ij}^{k\text{г}}, \tilde{s}_{0ij}^{k\text{с}}, \tilde{s}_{0ij}^{k\text{к}})$ чи 0, якщо ресурс не потрібен, де $s_{0ij}^{k\text{г}}$ - найгірший (максимальний) варіант потреби у ресурсі, $s_{0ij}^{k\text{с}}$ - середня потреба у ресурсі, $s_{0ij}^{k\text{к}}$ - найкращий (мінімальний) варіант потреби у ресурсі.

$p = \left\| \tilde{p}_{ij}^l \right\|$ – матриця потреб бізнес-процесів у ресурсах критичної IT-інфраструктури на віртуальній машині $V_l (l \ne k)$, які додатково бажано зарезервувати, де $\tilde{p}_{ij}^l$ дорівнює кількості потрібного для бізнес-процесу Z_i ресурсу R_j у вигляді трикутного нечіткого числа $\tilde{p}_{ij}^l = (p_{ij}^{l\text{г}}, p_{ij}^{l\text{с}}, p_{ij}^{l\text{к}})$ чи 0, якщо ресурс не потрібен, де $p_{ij}^{l\text{г}}$ - найгірший (максимальний) варіант потреби у ресурсі, $p_{ij}^{l\text{с}}$ - середня потреба у ресурсі, $p_{ij}^{l\text{к}}$ - найкращий (мінімальний) варіант потреби у ресурсі.

$s = \left\| \tilde{s}_{ij}^{l} \right\|$ – матриця потреб універсальних сервісів у ресурсах критичної ІТ-інфраструктури на віртуальній машині $V_l (l \neq k)$, які додатково бажано зарезервувати, де $\tilde{s}_{ij}^{l}$ дорівнює кількості потрібного для універсального сервісу S_i ресурсу R_j у вигляді трикутного нечіткого числа $\tilde{s}_{ij}^{l} = (\tilde{s}_{ij}^{l\text{г}}, \tilde{s}_{ij}^{lc}, \tilde{s}_{ij}^{l\text{к}})$ чи 0, якщо ресурс не потрібен, де $s_{ij}^{l\text{г}}$ - найгірший (максимальний) варіант потреби у ресурсі, s_{ij}^{lc} - середня потреба у ресурсі, $s_{ij}^{l\text{к}}$ - найкращий (мінімальний) варіант потреби у ресурсі.

$t = \left\| \tilde{t}_{j}^{i} \right\|$ – матриця надійності ресурсів критичної ІТ-інфраструктури на віртуальній машині V_i, де $\tilde{t}_j$ дорівнює надійності ресурсу R_j у вигляді трикутного нечіткого числа $\tilde{t}_j^i = (t_j^{i\text{г}}, t_j^{ic}, t_j^{i\text{к}})$ чи 0, якщо надійність ресурсу не важлива, де $t_j^{i\text{г}}$ - найгірший (мінімальний) варіант надійності ресурсу, t_j^{ic} - середня надійність ресурсу, $t_j^{i\text{к}}$ - найкращий (максимальний) варіант надійності ресурсу.

Середня потреба у ресурсі та надійність визначається за формулами (1):

$$p_{0ij}^{kc} = \frac{p_{0ij}^{k\text{г}} + \beta p_{0ij}^{k\text{нв}} + p_{0ij}^{k\text{к}}}{2 + \beta_0}, p_{ij}^{lc} = \frac{p_{ij}^{l\text{г}} + \beta p_{ij}^{l\text{нв}} + p_{ij}^{l\text{к}}}{2 + \beta},$$

$$s_{0ij}^{lc} = \frac{s_{0ij}^{l\text{г}} + \chi s_{0ij}^{l\text{нв}} + s_{0ij}^{l\text{к}}}{2 + \chi_0}, s_{ij}^{lc} = \frac{s_{ij}^{l\text{г}} + \chi s_{ij}^{l\text{нв}} + s_{ij}^{l\text{к}}}{2 + \chi}, \quad (1)$$

$$t_j^{ic} = \frac{t_j^{i\text{г}} + \tau t_j^{i\text{нв}} + t_j^{i\text{к}}}{2 + \tau}$$

де $p_{0ij}^{k\text{нв}}, s_{0ij}^{k\text{нв}}, p_{ij}^{l\text{нв}}, s_{ij}^{l\text{нв}}$ - найімовірніші варіанти потреб у ресурсі для бізнес-процесу та універсального сервісу; $t_j^{i\text{нв}}$ - найімовірніше значення надійності ресурсу, $\beta, \chi, \beta_0, \chi_0, \tau$ - зважені параметри усереднення, які визначаються експериментально.

$\tilde{r}_1^k, ..., \tilde{r}_m^k$ – трикутні нечіткі числа вигляду $(r_j^{k\text{г}}, r_j^{kc}, r_j^{k\text{к}})$, що визначають кількість ресурсів $R_1, ..., R_m$ відповідно на віртуальній машині V_k.

a_{ij} - булева змінна, яка визначає, чи встановлена ВМ V_j на сервері S_i.

Очевидно, що для вказаної моделі розподілу ресурсів має виконуватись вимога (2):

$$p_{ij}^{l} + p_{oij}^{k} \geq p_{oij}^{k}, \quad (2)$$

У випадку, коли немає можливості для виділення додаткових ресурсів, нерівність (2) перетворюється у рівність (3):

$$p_{ij}^{l} + p_{oij}^{k} = p_{oij}^{k}, \quad (3)$$

Критичний процес або сервіс завжди обслуговується. Інші процеси або сервіси обслуговуються згідно коефіцієнтів критичності.

Введемо коефіцієнти при трикутних нечітких змінних наступним чином:

$$x_i = \begin{cases} 1, \text{ якщо бізнес-процес } Z_i \text{ є критичним} \\ \text{і обслуговується в першу чергу} \\ \alpha_2, \text{ процес є дуже важливим і обслуговується} \\ \alpha_3, \text{ процес є важливим і обслуговується} \\ 0, \text{ процес не важливий і не обслуговується} \end{cases}$$

$$y_i = \begin{cases} 1, \text{ якщо універсальний процес } S_i \text{ є критичним} \\ \text{і обслуговується в першу чергу} \\ \gamma_2, \text{ сервіс є дуже важливим і обслуговується} \\ \gamma_3, \text{ сервіс є важливим і обслуговується} \\ 0, \text{ сервіс не важливий і не обслуговується} \end{cases}$$

Оскільки кожна ВМ розташована тільки на одному сервері, то має виконуватись наступна умова (4):

$$\sum_{i}^{n} a_{ij} = 1, j = 1...m, \quad (4)$$

Умова критичності сервісів і процесів накладає наступне обмеження (5):

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} p_{0ij}^{kc} \leq r_j^{k\text{г}}, k = 1...\text{n}, \quad (5)$$

Таким чином, управління розподілом ресурсами критичної ІТ-інфраструктури зводиться до пошуку максимуму наступної цільової функції (6):

$$\tilde{U} = \sum_{i}^{n} \tilde{x}_i \tilde{w}_i^z + \sum_{j}^{m} \tilde{y}_j \tilde{w}_j^S \to \max,$$

$$T = \sum_{j} \tilde{t}_j^i r_j^k \to \max, \quad (6)$$

за наявності обмежень (7) і (8):

$$\sum_{i=1}^{n} \tilde{x}_i \cdot (\tilde{p}_{0ij}^k + \tilde{p}_{ij}^l) + \sum_{i=1}^{m} \tilde{y}_i \cdot (\tilde{s}_{0ij}^k + \tilde{s}_{ij}^l) \le \tilde{r}_j^k, , \quad (7)$$

$$N_{кр} \to \max , \quad (8)$$

для $j = 1...m$ и $k,l = 1...n$, та врахуванням умов (4) і (5).

Умова (8) визначає той факт, що кількість критичних процесів та універсальних сервісів, які потрібно обслужити є максимальною, тобто всі критичні процеси та сервіси повинні бути забезпечені ресурсами. В противному випадку управління розподілом ресурсів є неможливим і потрібно вводити додаткові ресурси.

Коефіцієнти $\tilde{w}_i^z, \tilde{w}_k^s$ цільової функції становлять собою нечіткі числа - $\tilde{w}_i^z \in \left[w_i^{zL}; w_i^{zR} \right]$, $\tilde{w}_k^s \in \left[w_k^{sL}; w_k^{sR} \right]$, L і R - ліві та праві границі носія нечіткого числа.

Задача (4) – (8) становить собою задачу нечіткого лінійного програмування, яку можна розв'язати за допомогою методів, які описані в [12].

Приклад використання запропонованої моделі

Розглянемо розподілену та багаторівневу хмару. Зазвичай, така хмара має сотні серверів, розташованих на різних стійках, в різних географічних точках. З'єднання між двома машинами з різних стійок може проходити через один або кілька комутаторів. Багаторівневий розподіл представляє дуже складне завдання надійного, масштабованого, доступного поширення даних.

Для такої хмари потрібно розробити політику розташування реплік, яка повинна задовольнити наступним властивостям:

- максимізація надійності;
- максимізація забезпеченості.

Репліки повинні бути розташовані не тільки на різних дисках або різних машинах, але і в різних стійках. Це гарантує, що процес або сервіс буде доступним, навіть якщо ціла стійка пошкоджена або відключена від мережі. При такому розташуванні читання займає час, який приблизно дорівнює пропускній здатності мережі, хоча потік даних при записі повинен пройти через різні стійки.

Одночасно, при створенні нового критичного процесу або сервісу, визначається, де розмістити репліку. При цьому потрібно враховувати наступне:

1. Нова репліка критичного процесу або універсального сервісу розміщується на віртуальну машину сервера з найменшою середньою завантаженістю дисків. У такий спосіб вирівнюється завантаженість дисків на різних серверах та досягається найбільша надійність операції.

2. Число нових створюваних критичних процесів або універсальних сервісів на кожній віртуальній машині серверів є обмеженим. Незважаючи на те, що створення нового процесу є швидкою операцією, вона передбачає подальший запис даних на цю віртуальну машину, що вже є важкою операцією, і яка може привести до розбалансування обсягу трафіку даних на різні частини системи.

3. Як сказано вище, потрібно розподілити віртуальні машини між серверами в різних стійках. Це також дозволяє досягти найбільшої надійності операції.

4. Як тільки число реплік падає нижче встановлюваної користувачем величини, потрібно знову виконати репліку критичного процесу або сервісу. Ця ситуація може статися з декількох причин:

- віртуальна машина стала недоступною;
- сервер став недоступним;
- один з дисків вийшов з ладу;
- збільшене число реплік.

Кожному критичному процесу або універсальному сервісу, для якого потрібно зробити репліку, встановлюється відповідний пріоритет, який теж залежить від декількох факторів. По-перше, пріоритет вище у того критичного процесу або універсального сервісу, який має найменше число реплік. По-друге, щоб збільшити надійність виконання застосувань, збільшується пріоритет у процесів або у сервісів, які блокують прогрес у роботі клієнта. В першу чергу, обслуговуються критичні процеси.

5. Вибирається процес або сервіс з найбільшим пріоритетом і копіюється з однієї з реплік серверу, який є найбільш забезпеченим. Нова репліка розташовується, виходячи з тих же причин, що і при створенні.

6. Створення реплік постійно балансується. Залежно від розподілу реплік в системі, репліки переміщуються для вирівнювання завантаженості дисків і балансування навантаження. Також потрібно постійно вирішувати, яку з реплік має сенс видалити в даний момент. Як правило, видаляється репліка, яка знаходиться на віртуальній машині серверу з найменшим вільним місцем на

жорстких дисках і яка належить найбільш забезпеченому і надійному критичному процесу.

Розглянута модель управління ресурсами (відповідно, ресурсами є кількість необхідних серверів, віртуальних машин та жорстких дисків, кількість вільних ресурсів для створення нових процесів та сервісів, реплік для розміщення кожного з наших критичних процесів та універсальних сервісів з метою їх надійного функціонування) в рамках існуючих обмежень (наявність серверів та місця для розміщення реплік на окремих серверах та віртуальних машинах, кількість наявних ресурсів для створення нових процесів та сервісів) дозволяє розподілити максимальну кількість критичних бізнес-процесів та універсальних сервісів таким чином, щоб не порушувались принципи функціонування розглянутої хмари, гарантувалась максимальна забезпеченість та надійність функціонування такої критичної ІТ-інфраструктури.

Висновки

В ході роботи запропонована модель розподілу ресурсів критичної ІТ-інфраструктури з використанням хмарних технологій, наведено її детальний опис та приклад використання.

Список використаних джерел

1. Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України: проект Закону / Верховна Рада України [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=44208.
2. *Дорогий Я.Ю.* Критична інфраструктура: вразливості, загрози, ризики / Я.Ю.Дорогий, В.В.Мохор, І.О.Козлюк, В.В.Цуркан // Тези доповідей. ІІ міжнародна науково-практична конференція «Інформаційні технології та взаємодії», 3-5 листопада. – Київ, 2015. – с. 46-47.
   COBIT 5.0. Российское издание. ISACA. — М.: — 2012. — 94 с.
   .
5. *Verissimo P.* The CRUTIAL Architecture for Critical Information Infrastructures / P.Verissimo and etc. // Project: IST-FP6-STREP 027513 (CRUTIAL). – pp. 27.
6. Incident handling during attack on Critical Information Infrastructure // Handbook, Document for teachers. – Enisa, 2014. – pp. 24.
7. *Tsegaye T.* Controls for protecting critical information infrastructure from cyberattacks / T.Tsegaye, S.Flowerday // World Congress on *Internet Security (WorldCIS). – London, 8-10 Dec., 2014.*
8. Implementing NIST Cybersecurity Framework Using COBIT 5.0. – ISACA, 2014.
9. *Теленик С.Ф.* Системи управління хмарними ІТ-структурами / С.Ф. Теленик, О.І. Ролік, М.В. Ясочка, О.С. Квітко // Інтелектуальні системи прийняття рішень і проблеми обчислюваного інтелекту: Матеріали між нар. наук. конф. (16–20 травня) 2011 р. м. Євпаторія. – Том 1. – Херсон: ХНТУ, 2011. – С. 124–127.
10. *Теленик С.Ф.* Моделі і методи розподілу ресурсів в системах з серверною віртуалізацією / С.Ф. Теленик, О.І. Ролік, М.М. Букасов, О.А. Косован, О.І. Кобец // Зб. наук. праць ВІТІ НТУУ «КПІ». – Випуск № 3. – Київ: ВІТІ НТУУ «КПІ», 2009. – С. 100–109.
11. *Кобець О.І.* Моделі і методи розподілу ресурсів в системах, побудованих на хмарних обчисленнях [Електронний ресурс]. – Режим доступу: *http://intkonf.org/kobets-o-i-modeli-i-metodi-rozpodilu-resursiv-v-sistemah-pobudovanih-na-hmarnih-obchislennyah/*.
12. Forrester Research: в 2020 г. рынок публичных облачных вычислений достигнет $241 млрд [Електронний ресурс]. – Режим доступу: http://www.cnews.ru/news/line/forrester_research_v_2020_g.rynok.
13. Liu B. Theory and Practice of Uncertain Programming / B.Liu. – UTLAB. – 2009. - http://orsc.edu.cn/liu/up.pdf.

Поступила в редакцию 08 декабря 2015 г.

УДК 621.391

Я.Ю. Дорогий, канд. техн. наук

Национальный технический университет Украины «Киевский политехнический институт»,

ул. Политехническая, 42, корпус 18, г. Киев, 03056, Украина.

Распределение ресурсов критической IT-инфраструктуры с использованием облачных технологий

В статье рассмотрены вопросы распределения ресурсов критической ИТ-инфраструктуры с использованием облачных технологий, определение параметров для формирования критерия оптимальности управления критической ИТ-инфраструктурой. Предложенный критерий оптимальности управления четко определяет условия функционирования критической ИТ-инфраструктуры. В работе предложена нечеткая многокритериальная модель управления ресурсами критической ИТ-инфраструктуры на базе оптимизации по параметрам обеспеченности и надежности ресурсов, построенной с использованием технологии построения облаков IAAS. Приведено ее детальное описание, условия функционирования и пример ее использования в реальной среде на примере использования технологии репликации для виртуальных машин, на которых развернуты критические сервисы и процессы. Библ. 12.

Ключевые слова: *критическая IT-инфраструктура; жизненный цикл; управление инфраструктурой; облачные вычисления; облачные технологии; распределение ресурсов.*

UDC 621.391

Y. Dorogyy, Ph.D.

National Technical University of Ukraine "Kyiv Polytechnic Institute",

st. Polytechnique, 42, b.18, Kiev, 03056, Ukraine.

Resource allocation of critical IT-infrastructure using cloud technologies

The article deals with the issue of resource allocation for critical IT-infrastructure using cloud technology, determine the parameters of creation optimality criterion for managing critical IT-infrastructure. Proposed optimality criterion management clearly defines the conditions for the operation of critical IT-infrastructure. In our work, we proposed the model of fuzzy multicriteria resource management of critical IT-infrastructure based on the optimization of the parameters of security and reliability of resources, built using IAAS cloud technology. In addition, it was considered its details, operating conditions and an example of its use in a production environment on the example of using technology for replication of virtual machines, which are deployed critical services and processes. References 12.

Keywords: *MPLS network; multipath routing; switching on labels; marks the formation of tables; the method of "branch and bound".*

References

1. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zabezpechennia kibernetychnoi bezpeky Ukrainy: proekt Zakonu. Verkhovna Rada Ukrainy [Elektronnyi resurs]. Rezhym dostupu: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=44208. (Ukr).
2. Dorohyi, Ya. Yu., Mokhor, V. V., Kozliuk, I. O., Tsurkan, V. V. (2015). Krytychna infrastruktura: vrazlyvosti, zahrozy, ryzyky. Tezy dopovidei. II mizhnarodna naukovo-praktychna konferentsiia «Informatsiini tekhnolohii ta vzaiemodii», 3-5 lystopada. Pp. 46-47. (Ukr).
3. (2012). COBIT 5.0. Rossyiskoe yzdanye. ISACA. P. 94. (Rus).
4. Verissimo, P. and etc. The CRUTIAL Architecture for Critical Information Infrastructures. Project: IST-FP6-STREP 027513 (CRUTIAL). Pp. 27.
5. (2014). Incident handling during attack on Critical Information Infrastructure. Handbook, Document for teachers. Pp. 24.

6. *Tsegaye, T., Flowerday, S.* (2014). Controls for protecting critical information infrastructure from cyberattacks. World Congress on Internet Security (WorldCIS). London, 8-10 Dec.
7. (2014). Implementing NIST Cybersecurity Framework Using COBIT 5.0. ISACA.
8. *Telenyk, S. F., Rolik, O. I., Yasochka, M. V., Kvitko, O. S.* (2011). Systemy upravlinnia khmarnymy IT-strukturamy. Intelektualni systemy pryiniattia rishen i problemy obchysliuvanoho intelektu: Materialy mizh nar. nauk. konf. (16–20 travnia) 2011 r. m. Yevpatoriia. Vol. 1. Kherson: KhNTU, Pp. 124–127. (Ukr).
9. *Telenyk, S. F., Rolik, O. I., Bukasov, M. M., Kosovan, O. A., Kobets, O. I.* (2009), Modeli i metody rozpodilu resursiv v systemakh z servernoiu virtualizatsiieiu. Zb. nauk. prats VITI NTUU «KPI». Vypusk # 3. Kyiv: VITI NTUU «KPI», Pp. 100–109. (Ukr).
10. *Kobets, O. I.* Modeli i metody rozpodilu resursiv v systemakh, pobudovanykh na khmarnykh obchyslenniakh [Elektronnyi resurs]. Rezhym dostupu: http://intkonf.org/kobets-o-i-modeli-i-metodi-rozpodilu-resursiv-v-sistemah-pobudovanih-na-hmarnih-obchislennyah/. (Ukr).
11. Forrester Research: v 2020 h. гынok publychnыkh oblachnыkh vыchyslenyi dostyhnet $241 mlrd [Elektronnyi resurs]. – Rezhym dostupu: http://www.cnews.ru/news/line/forrester_research_v_2020_g.rynok.
12. *Liu, B.* (2009). Theory and Practice of Uncertain Programming. UTLAB. http://orsc.edu.cn/liu/up.pdf.