УДК 004.052.2-004.052.3
А.Є. Климчук, А.М. Луцків канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ШЛЯХИ ПІДВИЩЕННЯ ГАРАНТОЗДАТНОСТІ ХМАРНИХ СЕРВІСІВ IAAS

A.Y. Klymchuk, A.M. Lutskiv Ph.D., Assoc. Prof.
ANALYSIS OF APPROACHES USED TO RAISE DEPENDABILITY OF IAAS

Актуальність створення гарантоздатних хмарних сервісів зумовлена потребами користувачів у хмарних службах з гарантованим рівним обслуговування (SLA, service level agreement). SLA є набором вимог, які висуваються до сучасних інформаційних систем, а саме час безвідмовної роботи, стабільність, гарантоздатність тощо.

Під гарантоздатністю (dependability), розуміють комплексну властивість інформаційних та керуючих систем забезпечувати безперервність функціонування техногенних і природних об'єктів у діапазоні безпечних параметрів їх експлуатації з метою мінімізації ризиків аварій та збитків.

Серед характеристик гарантоздатності:

- доступність – готовність до використання;
- надійність – здатність забезпечити неперервність обслуговування під час використання;
- безпечність – відсутність небезпечного впливу на оточення;
- захищеність – здатність зберегти конфіденційність;
- ремонтопридатність.

Безвідмовність (reliability) - властивість безперервно надавати коректні (необхідні) послуги впродовж заданого часу (напрацювання).

Стабільність (stability) - здатність системи функціювати, не змінюючи структуру та знаходитись у рівновазі, підтримувати сталість у часі.

Однією із ключових проблем створення сучасних хмарних сервісів у рамках технології IaaS є уніфікація вимог, якими мають керуватись розробники цих систем. На сьогодні існує ціла низка стандартів та рекомендацій (best practices) по створенню відповідних систем, зокрема:

- ANSI / TIA-942 [1] - описує побудову дата центрів;
- ISO / IEC 17788 [2] (NIST SP 500-291 [3]) - основні визначення та поняття;
- ISO / IEC 17789 [4] (NIST SP 500-292 [5]) - архітектура і практика використання;
- ISO / IEC TS 27017 [6] (NIST SP 500-299 [7]) – інформаційна безпека;
- ISO / IEC 27018 [8] (NIST SP 800-144 [9]) - захист персональних даних при наданні публічних хмарних послуг;
- ETSI TR 103 125 [10] - огляд існуючих стандартів ETSI, пов'язаних з якістю хмарних послуг.

Загалом, наведені стандарти регламентують наступні параметри: енергоощадність, безпека будівель, енергозабезпечення, пожежний захист, кліматичні умови. Питання гарантоздатності відображене в рівнях (tiers) стандарту ANSI / TIA-942, а саме доступність IaaS-сервісу у співвідношенні до його зального часу використання гарантується: рівень 1 (99,671%), рівень 2 (99,749%), рівень 3 (99,982%), рівень 4 (99,995%). Оптимальними температурними режимами є температура в межах 18–27 °C, максимальна відносна вологість повітря 60%. Для визначення енергоефективності застосовують метрику ефективності енергоспоживання:

$$\text{ефективність енергоспоживання} = \frac{\text{сумарна потужність ЦОД}}{\text{потужність IT} - \text{обладнання}}$$

Нормальним значенням ефективності енергоспоживання для звичайного ЦОД у США є значення 2.0. Це означає, що об'єкт використовує 2Вт загальної потужності на кожен 1Вт доставленої до IT-обладнання енергії.

Фізична безпека у дата центрах є багаторівневою. На об'єкті, використовуються огорожі, пости охорони і камери відеоспостереження. Якщо це великий ЦОД, або якщо він містить будь-яку конфіденційну інформацію, тоді, окрім стандартних методів захисту, використовують ще й шлюзи та біометричні методи аутентифікації.

Варто зазначити, що частина з наведених стандартів створена для країн ЄС, інша орієнтована на США, тому існує проблема їх уніфікації. Спостерігається неузгодженість між цими стандартами, а також відсутність вітчизняної нормативної бази в галузі розроблення відповідних хмарних сервісів. Так на сьогодні наявна лише нормативна база по створенню гарантоздатих систем у аерокосмічній галузі, зокрема настанова СОУ-Н НКАУ 0060:2010 [11]. Нормативна база гарантоздатності базується на наукових працях вітчизняних вчених, а саме, на працях Харченка В.С., Скляра В.В., Конорева Б.М., Алексеєва Ю.С., Одарущенка О.Н., Черткова Г.Н. Основною метою стандартизації є створення власних гарантоздатних систем в Україні, зокрема приватних хмарних IaaS-сервісів (дата-центрів, спеціалізованих високопродуктивних обчислювальних систем тощо).

На думку авторів при створенні систем такого класу необхідно взяти за основу стандарт NIST SP 500-291, який акумулює наявну інформацію про хмарні обчисленнях з точки зору безпеки, портованості, сумісності. Містить введення в хмарні технології, термінологію, бізнес-моделі, прогнозує їх розвиток на найближчі роки. Доцільно також створити робочі групи по узгодженню та формуванню вітчизняних відповідників з метою забезпечення вітчизняної нормативної бази, оскільки, саме нею послуговуються державні підприємства та організації при створенні IaaS-систем.

Література

1. ANSI / TIA-942 Telecommunications 942 Telecommunications Infrastructure Standard for Data Centers.
2. ISO / IEC 17788 Information technology - Distributed application platforms and services - Cloud computing - Overview and vocabulary.
3. NIST SP 500-291 NIST Cloud Computing Standards Roadmap.
4. ISO / IEC 17789 Information technology - Cloud computing - Reference architecture.
5. NIST SP 500-292 Cloud Computing Reference Architecture.
6. ISO / IEC TS 27017 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (FDIS).
7. NIST SP 500-299 Cloud Computing Security Reference Architecture.
8. ISO / IEC 27018 Code of practice for data protection controls for public cloud computing services.
9. NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
10. ETSI TR 103 125 Technical Report Cloud; SLAs for Cloud services.
11. СОУ-Н НКАУ 0060:2010 Галузева система управління якістю. Гарантоздатність програмно-технічних комплексів критичного призначення.