DOI: 10.20535/2411-1031.2018.6.1.153207
УДК 004.75

ІГОР БОНДАРЕНКО,
ЯРОСЛАВ ДОРОГИЙ,
СЕРГІЙ СТІРЕНКО,
ТИМУР ШЕМСЕДИНОВ

АНАЛІЗ ПРОБЛЕМ ПОБУДОВИ КРИТИЧНОЇ ІТ-ІНФРАСТРУКТУРИ МІНІСТЕРСТВА

Проаналізовано проблеми створення критичної ІТ-інфраструктури міністерства. Розглянуто класичну модель хмарних сервісів, яка складається з трьох шарів. Показано, що специфіка задач, що виконуються міністерствами (відомствами), ставить перед розробником підвищені вимоги щодо надійності, безпеки, доступності при автоматизації їх процесів. Як наслідок, показано, що використання тільки цих трьох шарів для створення критичної ІТ-інфраструктури міністерств (відомств), навіть у вигляді приватної хмари, вже не є достатнім. Запропоновано ще декілька додаткових шарів для класичної моделі хмарних сервісів, таких як BaaS та XaaS. Перший шар – бізнес як сервіс (BaaS), включає автоматизацію керування процесами на організаційному рівні, включно з моніторингом показників ефективності, аналітичними звітами, консолідацією даних та централізованою інтеграцією рівня підприємства. Другий шар – все як сервіс (XaaS), передбачає тотальну автоматизацію галузевого рівня, включно із введенням галузевих стандартів, автоматизації наскрізної інтеграції багатьох підприємств. Проведено подальший аналіз утвореної моделі та визначено, що для створення єдиного інформаційного простору міністерства (відомства) як об'єкта інформатизації з критичною ІТ-інфраструктурою потрібно закласти в її реалізацію цілий ряд нових можливостей. Вони обумовлюють необхідність модернізувати як апаратну інфраструктуру, так системну і прикладну частини програмного забезпечення. Тому для створення критичної ІТ-інфраструктури з цими можливостями необхідна реалізація нових спеціалізованих засобів передачі та зберігання інформації. Ці засоби характеризуються рядом ключових характеристик таких як, інтерактивність, багатоверсійність, гетерогенність, розподіленість і динамічна модифікація структур даних під час життєвого циклу інформаційних систем критичної ІТ-інфраструктури відповідно до метамоделей предметної області на базі інтерпретації метаданих. Все вищезазначене вказує на необхідність закладення в модель ще одного останнього шару GaaS (переходу до глобальної інтеграції у вигляді сервісу). В останній частині статті наведено аналіз вимог до побудови критичної ІТ-інфраструктури.

Ключові слова: архітектура, хмарні послуги, хмарні сервіси, глобальна інтеграція як сервіс, центр обробки даних, критична ІТ-інфраструктура.

Постановка проблеми. В умовах глобальної інформатизації суспільства перед кожною організацією виникає дилема – створювати, розвивати і підтримувати власні ІТ-інфраструктури або звертатися до організацій, які надають необхідні послуги з інформаційного та програмно-апаратного забезпечення реалізації автоматизованих ділових процесів організації. Якщо мова йде про велику кількість користувачів і потужні розподілені ІТ-інфраструктури, дилема переформулюється таким чином – створювати, розвивати і підтримувати власні центри обробки даних (ЦОД) чи користуватися послугами хостингових компаній, які надають хостинг-послуги користувачам системи створених і підтримуваних ними ЦОД [1].

Якщо організація зупиняється на першій альтернативі, то цілком природно, що їй необхідно забезпечити ефективне функціонування своїх ЦОД. Важливо, що результатом

цього, звичайно, є зменшення витрат на експлуатацію ЦОД, яке супроводжується зниженням цін для користувачів і дозволить, зрештою, закласти основу для ефективної діяльності організацій, які пішли іншим шляхом [2].

Нині склалося загальне уявлення про ЦОД як комплексного організаційно-технічного рішення, призначеного для створення високопродуктивної, відмовостійкої критичної IT-інфраструктури. Сучасні ЦОД орієнтовані на вирішення завдань шляхом надання послуг у вигляді інформаційних сервісів. До основних завдань ЦОД, в першу чергу, відносяться ефективне консолідоване зберігання і оброблення даних користувачів, надання їм прикладних сервісів, а також підтримка функціонування корпоративних застосувань.

Комплексний аналіз і синтез критичної IT-інфраструктури та її базових компонентів, управління її функціонуванням вимагають розроблення нових підходів.

Аналіз останніх досліджень і публікацій. Для фахівців в сфері побудови критичних IT-інфраструктур відомі погляди вітчизняних та закордонних вчених Бірюкова Д.С., Ворона Т.О. та ін. [3-7].

Аналіз робіт демонструє підвищену роль та місце інформаційної складової діяльності, набуття нею ще більшої ваги. Інформаційна складова стає однією з найважливіших елементів забезпечення національної безпеки, інформаційної безпеки тощо.

Приклади країн світу (Південна Корея, країни ЄС, США тощо) з розвиненою критичною IT-інфраструктурою свідчать про значне збільшення залежності національної безпеки, соціально-економічної стабільності, кібербезпеки загалом від рівня захищеності самої IT-інфраструктури. Достатньо вивести з ладу не самі командні центри, а критичну IT-інфраструктуру держави для того, аби розпочався некерований процес, тобто хаос.

Саме тому, одними із найважливіших завдань є проектування, розроблення і реалізація безпечної критичної IT-інфраструктури, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян у сфері інформаційної безпеки.

Метою роботи є встановлення особливостей критичної IT-інфраструктури міністерства з точки зору аналізування, синтезування та керування функціонуванням її базових компонентів і подоланням проблем, які при цьому виникають.

Виклад основного матеріалу досліджень. Критична IT-інфраструктура: планування, розвиток та експлуатація. Започаткована порівняно недавно концепція ЦОД уже втілена багатьма великими корпораціями переважно для забезпечення доступу великої кількості користувачів до певних ресурсів (сервісів, застосувань, обчислювальних потужностей, даних) [1]. В Україні концепція ЦОД перспективна, в першу чергу, для міністерств і відомств, яким притаманна наявність розподіленої системи підпорядкованих підприємств, організацій, установ і окремих підрозділів. Якщо врахувати, що центральні органи міністерства (відомства), як і підпорядковані підприємства, організації, установи і окремі підрозділи, мають необхідність підтримувати певні інформаційно-обчислювальні потужності, то виникає проблема пошуку різноманітних форм збільшення ефективності їх використання.

Останнім часом дуже часто можна зустріти надання сервісів кінцевим користувачам через так званні хмари або хмарні сервіси. Існує декілька моделей надання хмарних послуг. NIST (National institute of Standards and Technology, U.S. Department of Commerce) в своїй спеціальній публікації 800-146 [8] виділив три моделі хмарних сервісів (див. рис. Рисунок):

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

Перший шар «Infrastructure as a Service» або IaaS. Іноді його ще називають «Hardware as a Service», або HaaS. Ще кілька років тому, якщо потрібно було запустити бізнес-застосування у своєму офісі та керувати веб-сайтом організації, необхідно було придбати сервери та інше обладнання з метою управління локальними програмами та забезпечення безперебійного ведення бізнесу. Але тепер з IaaS є можливість орендувати апаратні ресурси

у компанії, які надають такі послуги. На відміну від оренди звичайних виділених серверів або оренди віртуальних приватних серверів, коли замовник сплачує орендну платню навіть у випадку простоїв обладнання і лише звільняється від витрат на обслуговування техніки і виділення офісних приміщень під сервери, надання сервісів IaaS у хмарах може оплачуватись по факту використання обчислювальних потужностей. Найбільшими гравцями в цьому секторі є Amazon, Microsoft, VMWare, Rackspace, Red Hat.

Другий шар хмарних сервісів відомий як «Platform as a Service» або PaaS. Основна ідея сервісів такого типу полягає в тому, що розробка власного програмного забезпечення (ПЗ) компанії може здійснюватись в самому шарі, заощаджуючи час і ресурси за рахунок відсутності у необхідності підтримки проміжного програмного забезпечення за власний кошт.

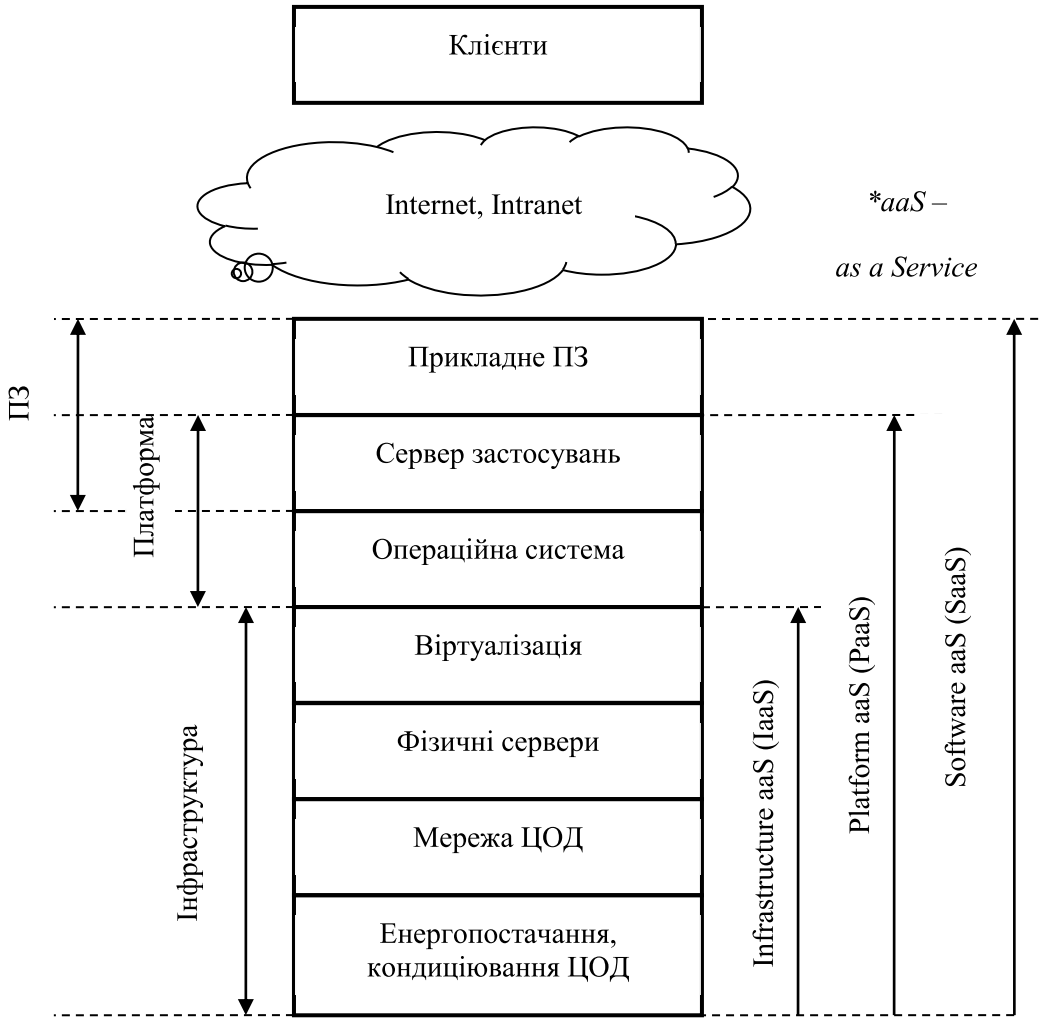

Рисунок 1 – Модель надання хмарних сервісів

PaaS-компанії пропонують широкий спектр рішень для розробки і розгортання застосувань через Інтернет. Це дозволяє заощадити гроші на обладнанні, а також спрощує спільну роботу для географічно-розподіленої команди розробників ПЗ. Найбільш відомими сервісами такого типу є Google App Engine, Microsoft Azure, Saleforce's Force.com, the Salesforce-owned Heroku, Engine Yard.

Третій і останній шар хмар – «Software as a Service» або SaaS. Саме з цим шаром частіше всього працюють кінцеві користувачі IT-послуг у повсякденному житті. Будь-яке застосування, розміщене на віддаленому сервері, яке може бути доступне через Інтернет, вважається SaaS. Послуги, які кінцевий користувач споживає повністю з Інтернету, такі як Netflix, MOG, Google Apps, Box.net, Dropbox, iCloud від Apple, належать до цієї категорії. Однак, враховуючи те, що специфіка виконуваних міністерствами (відомствами) задач

ставить перед розробником підвищені вимоги щодо надійності, безпеки, доступності при автоматизації її процесів. Тому використання тільки трьох шарів для створення її критичної IT-інфраструктури, навіть у вигляді приватної хмари, вже не є достатнім.

Зважаючи на вищезазначене, наступні кроки передбачають автоматизацію процесів BaaS та поступовий перехід до XaaS [9]:

– BaaS (Business as a Service) – бізнес як сервіс, включає автоматизацію керування процесами на організаційному рівні, включно з моніторингом показників ефективності, аналітичними звітами, консолідацією даних та централізованою інтеграцією рівня підприємства;

– XaaS (Anything as a Service) – все як сервіс, тотальна автоматизація галузевого рівня, включно із введенням галузевих стандартів, автоматизації наскрізної інтеграції багатьох підприємств.

Однак, і цього буде не достатньо. Для створення єдиного інформаційного простору міністерства (відомства) як об'єкта інформатизації з критичною IT-інфраструктурою потрібно закласти в її реалізацію наступні можливості, що обумовлюють необхідність модернізувати як апаратну інфраструктуру, так системну і прикладну частини програмного забезпечення:

– низька затримка / доступність (low latency / availability), тобто рішення з малим часом відповіді (чи малий "таймаут");

– велике навантаження (highload) – значна кількість одночасних (конкурентних) запитів до обмеженого ресурсу сервісу;

– велика кількість з'єднань (high connectivity) – одночасні довготривалі відкриті з'єднання клієнтів з сервером;

– велика зв'язність (high interconnection) – перехресний обмін повідомленнями, запитами та подіями між клієнтськими з'єднаннями;

– масштабованість (scalability) – можливість необмежено горизонтально нарощувати кількість серверів, що забезпечують роботу одного сервісу;

– інтерактивність (interactivity) – двосторонній обмін даними між клієнтом та сервером у режимі часу, наближеному до реального;

– робота з великими даними (big data) – даними, обсяг яких передбачає використання спеціальних засобів кластеризації для масштабування та розподіленого виконання запитів;

– робота з пам'яттю для великих даних (big memory & in-memory) – розгортання великих даних у пам'яті, що робить можливим дуже швидке виконання запитів;

– гнучкість інтеграції (integration flexibility) – цілий ряд заходів, що дають можливість швидко поєднувати компоненти інформаційних систем;

– синхронізація даних (data Synchronization);

– офлайн (off-line) – при відключенні клієнтів від мережі можливо забезпечити функціонування ПЗ із подальшою синхронізацією.

Тому для створення критичної IT-інфраструктури з вищевказаними можливостями необхідна реалізація спеціалізованих засобів передачі та зберігання інформації, що характеризуються рядом ключових характеристик таких як, інтерактивність, багатоверсійність, гетерогенність, розподіленість і динамічна модифікація структур даних під час життєвого циклу інформаційних систем критичної IT-інфраструктури відповідно до метамоделей предметної області на базі інтерпретації метаданих.

Ключовими вимогами до новостворюваної критичної IT-інфраструктури стають:

– формат представлення структур даних у різних компонентах системи;

– мінімізація перетворення даних і міжпроцесного обміну;

– безсхемне зберігання;

– скафолдінг і застосування метаданих;

– реалізація принципу бездискових СКБД для роботи з даними в оперативній пам'яті;

– доповнене відкладене збереження даних для постійного зберігання.

Постійне зберігання можливе як на базі файлових систем, так і в реляційних, об'єктних, безсхемних і документних СКБД. Синхронізація даних між клієнтом і сервером має проводитися як в реальному режимі часі, так і у відкладеному режимі, тобто має бути можливість працювати як в онлайн (інтерактивно разом з іншими користувачами), так і в офлайн, з даними, збереженими в локальному сховищі, і мати двонаправлену синхронізацію даних з версійним розгалуженням. Для реалізації наведених принципів має бути побудовано абстрактний шар доступу до даних з уніфікованим API.

Все вищезазначене приводить нас до імплементації останнього кроку автоматизації – переходу до глобальної інтеграції у вигляді сервісу (GaaS – global integration as a service, глобальна інтеграція як сервіс).

Це максимальний рівень автоматизації міжсистемної інтеграції, який передбачає відкриті стандарти та можливість двостороннього обміну між інформаційними системами багатьох галузей, державних систем, різних держав, державних та комерційних структур, завдяки наявності відкритих протоколів та форматів даних, інтроспективних API, скафолдінгу інтерфейсів користувача, можливістю вбудовувати одну систему у іншу, не поступаючись при цьому безпекою, можливість інтерактивного міжсистемного обміну повідомленнями, викликами та синхронізації даних, в тому числі на різних технологічних базах, але на єдиних відкритих стандартах.

Проблеми створення критичної IT-інфраструктурою міністерства. В умовах глобальної інформатизації функціональні процеси міністерства все тісніше переплітаються з IT: створюються складні розподілені бази даних (БД), найважливіша частина логіки ділових процесів переноситься на сервери. Це вимагає високого рівня сервісу, безперебійності роботи сервісів і високої відмовостійкості. Більше того, в багатьох випадках дані для роботи міністерства настільки критичні, що вони вимагають доступності до них навіть в разі аварій з катастрофічними наслідками. Це додало складності проблемам створення критичної IT-інфраструктури, оскільки окрім основного ЦОД, необхідно мати ще як мінімум один зеркальний. Тому організація свого ЦОД вимагає від державної установи значних капіталовкладень, ефективної організації роботи з підтримки критичної IT-інфраструктури, наявності у штаті висококваліфікованих фахівців. Отже, міністерству необхідно переходити на вищий рівень фінансування і управління його критичною IT-інфраструктурою.

Таким чином, розвиток ділових процесів міністерства породжує інтенсивні інформаційні потоки і обумовив появу цілісних ЦОД, часто децентралізованих, з метою забезпечення резервування даних, які надають послуги відразу сотням і тисячам користувачів за рахунок тих же апаратно-програмних ресурсів. Серверні приміщення поступово перетворюються в ЦОД. Це спровокувало зростання щільності і потужності устаткування. Поступово інтегратори, постачальники, виробники устаткування накопичили досвід впровадження і проектування ЦОД під певні завдання, виробляючи типові рішення, які дозволяють реалізовувати проекти з меншими витратами. Цей досвід став фундаментом для розроблення стандартів, нових науково обґрунтованих підходів до організації ЦОД. Однак, залишаються проблеми, які ще потребують вирішення, чи краще сказати існують постійні проблеми, що виникають в організаціях, які вирішили створювати власні ЦОД. Мова йде про низку серйозних і складних проблем, які підлягають вирішенню, як під час створення ЦОД, так і під час його експлуатації. Розглянемо ці проблеми.

По-перше, проблема створення умов для функціонування інформаційно-обчислювальних потужностей ЦОД. Необхідне приміщення або окрема будівля, в якій розташовується ЦОД міністерства, спроектовані так, щоб відповідати сучасним стандартам. Тобто необхідно вирішити безліч не надто складних, але досить важливих проблем на кшталт кондиціювання повітря, ліквідації пожеж, безпеки обладнання ЦОД. Для міністерства дуже важливо надавати послуги в безперебійному режимі, оскільки вимоги користувачів-держслужбовців постійно зростають.

По-друге, проблема ресурсів. Головні апаратні ресурси, якими оперує будь-який ЦОД – це канали зв'язку з Інтернет або конкретними установами, процесорний час (обчислювальна потужність серверів), оперативна пам'ять серверів і дисковий простір. Відсутність засобів обліку і аналізу відповідності наявних ресурсів встановленим до критичних IT-інфраструктур вимогам призводить до ситуацій з фінансовими втратами, втратою критично важливих даних для міністерства та втратами престижу для всієї держави. Так, ЦОД може не впоратися з великою кількістю запитів від надмірної кількості користувачів, тобто не може підтримувати необхідну працездатність всіх послуг, що надаються. Може закінчитися вільний дисковий простір і більшість сервісів не зможе функціонувати, бракуватиме оперативної пам'яті, обчислювальних потужностей або каналів зв'язку і сервіси почнуть працювати з помітними затримками.

Необхідно також враховувати пікові навантаження, коли велика кількість користувачів одночасно вирішили скористатися послугами певного виду. Наприклад, одночасний їх доступ до сайту, який розташований на обладнанні ЦОД, вичерпує можливості каналів зв'язку і тому інші сервіси цього ЦОД у цей момент будуть недоступними для використання або час відгуку буде занадто великим. У таких випадках сервери ЦОД можуть призупиняти свою роботу, перезавантажуватися, що перетворить ситуацію у ще більш критичну. Найпростіше вирішення цієї проблеми за рахунок вкладення додаткових коштів (придбання додаткових серверів, збільшення потужності каналів зв'язку тощо) не є оптимальним. Більш перспективними видаються складніші і гнучкіші рішення, які полягають в правильному балансуванні навантаження і розподілі ресурсів. Наприклад, кластерне рішення дозволить більш рівномірно використовувати всі ресурси системи, ніж низка звичайних серверів з тією ж сумарною потужністю.

По-третє, проблеми резервування. Це важлива проблема для ЦОД, оскільки однією з основних вимог до критичної IT-інфраструктури є висока відмовостійкість систем, які вона використовує. Найчастіше розглядають такі три складових резервування:

– каналів зв'язку: наявність лише одного ланцюжка мережевих пристроїв для доступу може спричинити повну зупинку системи в разі виходу з ладу одного із послідовно з'єднаних елементів, наприклад, маршрутизатора. Тому необхідні надлишкові канали зв'язку, які дозволяють продовжити роботу системи в разі втрати основного каналу. Використання у якості надлишкових резервних каналів зв'язку меншої пропускної здатності дозволить досягти лише показної економії коштів, оскільки система залишиться працездатною, але значно знизиться якість сервісів, які надаються, оскільки при цьому зросте час відгуку на запити користувачів. З тих же міркувань важливо мати декілька провайдерів Інтернету. В будь-якому випадку необхідно мати засоби аналізу і вибору оптимального рівня резервування;

– БД: відсутність резервування може призвести до втрати даних ЦОД. Застосування сучасних сховищ даних із збереженням декількох копій кожного сегменту БД на різних фізичних дисках різних стійок у динамічному режимі забезпечить високий рівень збереження. Крім того, можна застосовувати дублювання БД на різних майданчиках, технології періодичного зняття резервних копій усіх даних на магнітні стрічки, які зберігаються в спеціальних умовах і можуть бути використані для відновлення даних у будь-який момент часу;

– серверів з логікою ділових процесів: застосування кластерних рішень при побудові критичної IT-інфраструктури міністерства навіть при виході з ладу декількох серверів забезпечує функціонування системи і кінцеві користувачі навіть не помітять проблем, які виникли в ЦОД міністерства.

У будь-якому випадку необхідні дані вибору і обґрунтування найбільш прийнятних технологій і параметрів резервування.

По-четверте, проблеми безпеки. З точки зору безпеки розглядають можливість злому зсередини і ззовні. Вирішенням даної проблеми може бути придбання і впровадження

спеціалізованого ПЗ або ж розроблення власних рішень, імплементація системи управління інформаційною безпекою (СУІБ). Окрім можливості злому зсередини, є чимала імовірність злому ззовні. Зловмисник може оволодіти конфіденційними даними міністерства, скориставшись слабким зовнішнім захистом. Вирішенням даної проблеми може бути придбання спеціалізованого програмного забезпечення, такого як брандмауери, фільтри протоколів. У обох випадках ЦОД міністерства повинен мати засоби аналізу проблем безпеки, розроблення і обґрунтування комплексної системи захисту інформації з використанням сучасних засобів, наприклад різних патчів, сервісних пакетів для ПЗ.

По-п'яте, проблеми функціонування ПЗ. Як свідчить практика, будь-якому створеному людиною ПЗ притаманні помилки. При певних вхідних даних програми можуть видавати неправильні дані або навіть перестати функціонувати. Неправильні налаштування щодо безпеки можуть надавати можливість зловмисникам проводити різноманітні атаки, наприклад DoS (Denial of Service). Оскільки помилки ПЗ можуть призвести до непередбачуваних наслідків, міністерство повинно використовувати сучасні засоби розроблення надійного ПЗ, засоби аналізу та моніторингу ПЗ зовнішніх інтегрованих систем. Крім того потрібна розвинена технологія установлення патчів і контролю версій.

По-шосте, проблеми технічної підтримки. Оскільки критична ІТ-інфраструктура міністерства становить складний програмно-апаратний комплекс і покликана обслуговувати значну кількість користувачів різного рівня розуміння основ ІТ, технічна підтримка діяльності можлива лише за наявності відповідної організаційної структури, оснащеної сучасним інструментарієм та комплексом методик збирання, аналізування інформації, прийняття рішень та управління їх відпрацюванням. За складністю завдання технічної підтримки звичайно поділяють на такі чотири рівні [10]:

– завдання першого рівня включають перезавантаження виділених серверів, відповіді на запитання користувачів. У ЦОД технічна підтримка першого рівня будується на основі ескалації запиту (передавання запиту ієрархією нагору до фахівців відповідної компетенції), час якої не може перевищувати 24 години;

– завдання другого рівня включають типові процедури з підготовки апаратно-програмних засобів до роботи, наприклад, установлення і налаштування штатного ПЗ, а також поповнення бази знань для технічної підтримки першого рівня;

– завдання третього рівня спрямовані на вирішення глобальних проблем, пов'язаних із системним зниженням якості обслуговування. Наприклад, якщо сервер оброблює запити клієнтів із затримками, які перевищують домовлений рівень, часто виникають пікові навантаження, ПЗ не встановлюється або не працює взагалі чи в деяких режимах, апаратні проблеми;

– завдання четвертого рівня охоплюють усе коло завдань технічної підтримки, вимагають повної компетентності фахівців у всіх проблемах технічної підтримки ЦОД, у тому числі вміння працювати з незнайомим ПЗ, відновлювати системи після спроб зламу, пошук облікових записів, що стосуються спаму, установлення системних обмежень.

Створення зазначених інструментарію та комплексу методик для вирішення завдань технічної підтримки критичної ІТ-інфраструктури становить важливу науково-практичну проблему. Розв'язання цієї проблеми вимагає глибокого розуміння процесів, які відбуваються в критичних ІТ-інфраструктурах, чіткої постановки конкретних завдань дослідження, розроблення математичних моделей і відповідних методів вирішення задач та, насамкінець, реалізації згаданих інструментарію та методик.

Вимоги до побудови критичної ІТ-інфраструктури. Виходячи з результатів виконаного аналізу проблематики, сформулюємо вимоги до побудови критичної ІТ-інфраструктури, які і будуть визначати масштаби робіт, пов'язаних із її створенням.

У загальному випадку критична ІТ-інфраструктура та її інформаційно-телекомунікаційна система (ІТС), одночасно з головним завданням – забезпечення сумісної ефективної роботи функціональних і забезпечуючих підсистем, а також телекомунікаційної мережі у відповідності з визначеним регламентом вирішує багато інших задач:

– підвищення ефективності управління ІТ;
– підвищення продуктивності роботи ІТ-систем;
– підвищення якості ІТ-сервісів і задоволеності користувачів;
– забезпечення оптимального використання ресурсів ІТС;
– підвищення надійності і доступності критично важливих ІТ-сервісів.

Принципи управління ІТС багато в чому визначаються і закладаються ще на етапі проектування, коли виявляються наступні аспекти створюваної критичної ІТ-інфраструктури та її ІТС:

– призначення і цілі ІТС, тобто, характер і вимоги, що визначаються діловими процесами;
– постановка завдань для системи управління критичною ІТ-інфраструктурою;
– дослідження і аналіз вихідних даних;
– плани розвитку і модернізації ІТС та критичної ІТ-інфраструктури в цілому;
– етапність реалізації критичної ІТ-інфраструктури;
– можливе фінансування.

При модернізації і удосконаленні критичної ІТ-інфраструктури на етапі експлуатації враховуються такі аспекти:

– аналіз змін характеристик системи і властивостей ділових процесів;
– динаміка параметрів ІТС;
– можливість використання перспективних ІТ.

Процес проектування і впровадження критичної ІТ-інфраструктури повинен відрізнятися гнучкістю, неперервністю і поетапністю. Основна складність проектування критичної ІТ-інфраструктури обумовлена великою кількістю і різноманіттям взаємопов'язаних завдань, які вирішуються в її ІТС, необхідністю ефективного управління її ІТ-сервісами і функціонуванням її ІТС в умовах динаміки доступності і продуктивності ресурсів, зміни властивостей телекомунікаційної мережі (ТМ).

Для підвищення загальної ефективності управління підсистемами і ТМ, відповідальності адміністраторів усіх рівнів за прийняття і здійснення рішень щодо управління критичною ІТ-інфраструктурою створюється система управління критичною ІТ-інфраструктурою, яка повинна задовольняти такі вимоги:

– централізацію управління з можливістю децентралізації функцій управління;
– оптимізацію кількості рівнів ієрархії управління критичною ІТ-інфраструктурою;
– мінімальну кількість адміністраторів;
– орієнтацію адміністраторів на виконання обмеженої множини функцій;
– використання універсальних механізмів дій адміністраторів різних рівнів і сервісів із втіленням загальної інформатизації і автоматизації управління;
– використання єдиної системи вітчизняних і міжнародних стандартів та рекомендацій.

Організаційно система управління критичною ІТ-інфраструктурою становить собою територіально-розподілену ієрархічну структуру. Структура системи управління критичною ІТ-інфраструктурою на апаратному і програмному рівнях повинна бути модульною і ієрархічною. Це дає можливість гнучко комплектувати, розгортати і налаштовувати конкретні вузли критичної ІТ-інфраструктури в залежності від їх рівня і вимог, які вони повинні задовольняти, а також легко нарощувати функціональність. Топологія системи управління критичною ІТ-інфраструктурою в межах зони відповідальності окремого адміністратора, розміщення вузлів управління, число рівнів ієрархії визначаються з урахуванням організаційної структури міністерства (відомства).

Створення системи управління критичною ІТ-інфраструктурою повинне відбуватися в рамках створення єдиної платформи розробки, реалізації і експлуатації критичної ІТ-інфраструктури. При цьому повинен забезпечений пріоритет створення системи управління

критичною ІТ-інфраструктурою в інтересах основної діяльності підприємства на єдиній нормативній базі і єдиній системі нормування витрат щодо розроблення. Технології, які забезпечують роботу апарату управління, що бере участь в адміністративній та допоміжній діяльності, повинні бути єдиними, але при цьому пріоритетною повинна бути основна діяльність. Технології, які забезпечують роботу апарату управління, що бере участь у різних видах діяльності, можуть бути різними але повинні бути сумісними. Технології, які забезпечують роботу апарату управління, що бере участь в основній діяльності, повинні бути вітчизняної розробки або такими, що допускають можливість сертифікації.

Створена система управління критичною ІТ-інфраструктурою повинна комплексно враховувати:

- потреби користувачів;
- проектні рішення щодо складових систем;
- оперативні вимоги, у першу чергу відносно основної діяльності, як найбільш жорсткі за показниками оперативності, доступності, надійності;
- вимоги до захисту інформації, ступінь залежності від виробників;
- використання власної бази для підготовки кадрів;
- вартісні показники розробки;
- відповідність організаційній, функціональній структурі міністерства (відомства).

Висновки. Виконано аналіз підходів до побудови критичної ІТ-інфраструктури міністерства (відомства). Розглянуті проблеми, що виникають при її побудові та подальшому розвитку, а також визначено набір її основних характеристик.

Також проведено детальний аналіз існуючих проблем в управлінні критичною ІТ-інфраструктурою, встановлено можливі способи їх вирішення. Зазначено важливість проблеми створення інструментарію для технічної підтримки життєвого циклу функціонування критичної ІТ-інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] М. Горин, “Корпоративный ЦОД: за рамками технологий”, *Connect! Мир Связи*, № 8, С. 19-20, 2007.

[2] И. Кирилл, “Коммерческие ЦОД в Украине: новый этап развития”, Сети и бизнес, № 3 (52), 2010 [Электронный ресурс]. Доступно: http://www.sib.com.ua/arhiv_2010/2010_3/statia_3_1_2010/ statia_3_1_2010.htm.

[3] Д. С. Бірюков, та С. І. Кондратов, *Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні*. Київ, Україна: НІСД, 2012.

[4] Д. С. Бірюков, С. І. Кондратов, Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні, на *Міжнародній науково-практичній конференції*, Київ, 2014.

[5] П. Д. Рогов, Б. О. Ворович, та Т. О. Ворона, “Війна в кіберпросторі”, *Оборонний вісник*, № 1, С. 16-21, 2017.

[6] С. О. Гнатюк, В. М. Сидоренко, та О. П. Дуксенко, “Сучасні підходи до виявлення та ідентифікації найбільщ важливих об’єктів критичної інфраструктури”, *Безпека інформації*, т. 21, № 3, С. 269-275, 2015.

[7] С. О. Гнатюк, Р. С. Одарченко, та В. М. Сидоренко, “Аналіз методів розрахунку критичності інформаційних систем”, на *Дев’ятій міжнародній науково-практичній конференції “Інтегровані інтелектуальні роботехнічні комплекси”*, Київ, 2016, С. 279-281.

[8] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, *Cloud Computing Synopsis and Recommendations. Recommendations of the National Institute of Standards and Technology* (Special Publication 800-146, NIST), 2012.

[9] Y. Duan, G. Fu, N. Zhou, X. Sun, N. Narendra, and B. Hu, “Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends”, in *Proc. IEEE 8th International Conference on Cloud Computing*, New York, 2015, pp. 621-628. doi: 10.1109/CLOUD.2015.88.
[10] B. Viswanathan, “Understanding The Different Levels of Help Desk Support” [Online]. Available: https://project-management.com/understanding-the-different-levels-of-help-desk-support/.

Стаття надійшла до редакції 25 лютого 2018 року.

REFERENCE

[1] M. Gorin, “Corporate Data Center: Beyond Technology”, *Connect! World of Communication*, no. 8, pp. 19-20, 2007.
[2] I. Kirill, “Commercial data centers in Ukraine: a new stage of development”, Networks and business, no. 3 (52), 2010 [Online]. Available: http://www.sib.com.ua/arhiv_2010/ 2010_3/statia_3_1_2010/ statia_3_1_2010.htm.
[3] D. S. Biriukov, and S. I. Kondratov, *Critical Infrastructure Protection: Problems and Prospects for Implementation in Ukraine*. Kyiv, Ukraine: NISS, 2012.
[4] D. S. Biriukov, and S. I. Kondratov, The concept of critical infrastructure protection: the state, problems and prospects of its implementation in Ukraine, in *Proc. International scientific and practical conference*, Kyiv, 2014.
[5] P. D. Rohov, B. O. Vorovych, and T. O. Vorona, “War in cyberspace”, *Defensive Herald*, no. 1, pp. 16-21, 2017.
[6] S. O. Hnatiuk, V. M. Sydorenko, and O. P. Duksenko, “Modern approaches to critical infrastructure objects detection and identification”, *Bezpeka ìnformacìì*, vol. 21, no. 3, pp. 269-275, 2015.
[7] S. O. Hnatiuk, R. S. Odarchenko, and V. M. Sydorenko, “Analysis of the methods of calculating the criticality of information systems”, in *Proc. 9th International Scientific and Practical Conference "Integrated Intelligent Robot Engineering Complexes”*, Kyiv, 2016, pp. 279-281.
[8] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, *Cloud Computing Synopsis and Recommendations. Recommendations of the National Institute of Standards and Technology* (Special Publication 800-146, NIST), 2012.
[9] Y. Duan, G. Fu, N. Zhou, X. Sun, N. Narendra, and B. Hu, “Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends”, in *Proc. IEEE 8th International Conference on Cloud Computing*, New York, 2015, pp. 621-628. doi: 10.1109/CLOUD.2015.88.
[10] B. Viswanathan, “Understanding The Different Levels of Help Desk Support” [Online]. Available: https://project-management.com/understanding-the-different-levels-of-help-desk-support/.

ИГОРЬ БОНДАРЕНКО,
ЯРОСЛАВ ДОРОГОЙ,
СЕРГЕЙ СТИРЕНКО,
ТИМУР ШЕМСЕДИНОВ

АНАЛИЗ ПРОБЛЕМ ПОСТРОЕНИЯ КРИТИЧЕСКОЙ ИТ-ИНФРАСТРУКТУРЫ МИНИСТЕРСТВА

Проанализированы проблемы создания критической ИТ-инфраструктуры министерства. Рассмотрена классическая модель облачных сервисов, которая состоит из трех слоев. Показано, что специфика задач, выполняемых министерствами (ведомствами), ставит

перед разработчиком повышенные требования по надежности, безопасности, доступности при автоматизации их процессов. Как следствие, показано, что использование только этих трех слоев для создания критической ИТ-инфраструктуры министерств (ведомств), даже в виде частного облака, уже не является достаточным. Предложено еще несколько дополнительных слоев для классической модели облачных сервисов, таких как BaaS и XaaS. Первый слой - бизнес как сервис (BaaS), включает автоматизацию управления процессами на организационном уровне, включая мониторингом показателей эффективности, аналитическими отчетами, консолидацией данных и централизованной интеграцией уровня предприятия. Второй слой – все как сервис (XaaS), предусматривает тотальную автоматизацию отраслевого уровня, включая введение отраслевых стандартов, автоматизацию сквозной интеграции многих предприятий. Проведен дальнейший анализ образованной модели и определено, что для создания единого информационного пространства министерства (ведомства) как объекта информатизации с критической ИТ-инфраструктурой нужно заложить в ее реализацию целый ряд новых возможностей. Они обусловливают необходимость модернизировать как аппаратную инфраструктуру, так системную и прикладную части программного обеспечения. Поэтому для создания критической ИТ-инфраструктуры с этими возможностями необходима реализация новых специализированных средств передачи и хранения информации. Эти средства характеризуются рядом ключевых характеристик таких как, интерактивность, многоверсионность, гетерогенность, распределенность и динамическая модификация структур данных во время жизненного цикла информационных систем критической ИТ-инфраструктуры в соответствии с метамоделей предметной области на базе интерпретации метаданных. Все вышеперечисленное указывает на необходимость закладки в модель еще одного последнего слоя GaaS (перехода к глобальной интеграции в виде сервиса). В последней части статьи приведен анализ требований к построению критической ИТ-инфраструктуры.

Ключевые слова: архитектура, облачные услуги, облачные сервисы, глобальная интеграция как сервис, центр обработки данных, критическая ИТ-инфраструктура.

IHOR BONDARENKO,
YAROSLAV DOROHYI,
SERHII STIRENKO,
TYMUR SHEMSEDYNOV

ANALYSIS OF CRITICAL IT INFRASTRUCTURE DESIGNING PROBLEMS FOR A MINISTRY

The problems of creating a critical IT infrastructure of the ministry are analyzed. The classic model of cloud services, which consists of three layers, is considered. It has been shown that the specificity of the tasks performed by the ministries (departments) puts the developer with increased requirements for reliability, safety, availability in the automation of their processes. As a result, it has been shown that the use of only these three layers to create a critical IT infrastructure of ministries (departments), even as a private cloud, is no longer sufficient. Several additional layers are proposed for the classical cloud service model, such as BaaS and XaaS. The first layer, Business as a Service (BaaS), includes automation of process management at the organizational level, including monitoring of performance indicators, analytical reports, data consolidation and centralized enterprise level integration. The second layer - everything as a service (XaaS), provides total automation of the industry level, including the introduction of industry standards, the automation of cross-integration of many enterprises. A further analysis of the developed model has been carried out and it has been determined that in order to create a single information space of the ministry (agencies) as an object of informatization with a critical IT infrastructure, it is necessary to put in its implementation a number of new possibilities. They stipulate the need to upgrade both the hardware infrastructure, both system and application software. Therefore, the creation of critical IT

infrastructure with these capabilities requires the implementation of new specialized means of data transmission and storage of information. These tools are characterized by a number of key characteristics such as interactivity, multi-tieredness, heterogeneity, distribution, and dynamic modification of data structures during the lifecycle of critical IT infrastructure information systems in accordance with meta-models of the subject area based on metadata interpretation. All of the above points to the need to put into the model another GaaS last layer (the transition to global integration as a service). The last part of the article provides an analysis of the requirements for constructing a critical IT infrastructure.

Keywords: architecture, cloud services, global integration as a service, data center, critical IT-infrastructure.

Ігор Павлович Бондаренко, директор Департаменту інформатизації, Міністерство внутрішніх справ, Київ, Україна.

ORCID: 0000-0003-2946-5146.

E-mail: irgan.daren@gmail.com

Ярослав Юрійович Дорогий, кандидат технічних наук, доцент, доцент кафедри автоматики і управління в технічних системах, Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.

ORCID: 0000-0003-3848-9852.

E-mail: argusyk@gmail.com.

Сергій Григорович Стіренко, доктор технічних наук, доцент, завідувач кафедри обчислювальної техніки, Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.

ORCID: 0000-0001-5478-0450.

E-mail: sergii.stirenko@gmail.com.

Тимур Гафарович Шемседінов, старший викладач кафедри обчислювальної техніки, Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.

E-mail: timur.shemsedinov@gmail.com.

Игорь Павлович Бондаренко, директор Департамента информатизации, Министерство внутренних дел, Киев, Украина.

Ярослав Юрьевич Дорогой, кандидат технических наук, доцент, доцент кафедры автоматики и управления в технических системах, Национальный технический университет Украины “Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.

Сергей Григорьевич Стиренко, доктор технических наук, профессор, заведующий кафедрой вычислительной техники, Национальный технический университет Украины “Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.

Тимур Гафарович Шемсединов, старший преподаватель кафедры вычислительной техники, Национальный технический университет Украины “Киевский политехнический институт имени Игоря Сикорского”, Киев, Украина.

Ihor Bondarenko, Director of the Informatization Department, Ministry of Internal Affairs, Kyiv, Ukraine.

Yaroslav Dorohyi, candidate of technical sciences, associate professor, associate professor in Department of Automation and Control in Technical Systems, National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Sergii Stirenko, doctor of technical sciences, professor, chief of Computing Engineering Department, National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Tymur Shemsedynov, senior teacher in computing engineering academic department, National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.