# Не поспішайте на захід:

## чи все так однозначно з міграцією у закордонні хмари

Буквально з перших днів війни українські компанії відчутно активізували дії щодо міграції IT-інфраструктур на захід. Чи є це єдиним правильним варіантом, або як краще захиститись від викликів, які стоять перед нами сьогодні? Про це та багато іншого ми поспілкувались з Геннадієм Карповим – директором з технологій компанії De Novo.

**— Для більшості компаній у нашій країні початок масштабних бойових дій став справжнім шоком. Багато хто в терміновому порядку почав рятувати IT-інфраструктури та дані. Як це вплинуло на ландшафт українського хмарного ринку?**

– Схоже, що до 24 лютого мало хто насправді вірив, що війна розпочнеться. Тому лише досить незначна частка компаній заздалегідь переймалася розробкою детальних інструкцій на випадок початку бойових дій. Коли ж війна стала реальністю, діяти почали буквально «рефлекторно», орієнтуючись не стільки на розрахунки та заздалегідь узгоджений план дій, скільки на інтуїцію. Цілком природною реакцією в умовах невизначеності та страху, які панували в перші дні російського вторгнення, було бажання максимально швидкого «відходу на безпечну відстань». Треба було терміново рятувати найцінніше – у тому числі й IT-активи – шляхом перенесення їх у максимально безпечне, як тоді здавалося, місце. Тому чимало компаній розпочали міграцію (найчастіше – стихійну) до дата-центрів та хмар на території ЄС або, як мінімум, намагалися перенести свої інфраструктури на захід України (передусім у Львів). Водночас далеко не завжди інтуїтивне рішення є найвірнішим та найефективнішим (тут можна згадати, як у перші ж дні війни кияни масово намагалися виїхати до передмість).

**— Львів виглядає як безпечне місце, він набагато далі від активних бойових дій, ніж був Київ у перші місяці війни.**

– Я б сказав, виглядав на той момент. Але за теперішньої ситуації, далі зовсім не означає безпечніше. Можна сказати, що всі регіони України, які віддалені від зони бойових дій хоча б на кількасот кілометрів, однаково безпечні (умовно безпечні, звісно). Вони всі недосяжні для зброї малого радіуса дії, але, як показало життя, однаково вразливі для далекобійних систем.

Водночас, у Києві набагато більше підготовлених та надійних майданчиків, ніж на заході України, де, фактично, лише Львів може надати відносно сучасну інженерну інфраструктуру для розміщення IT-обладнання. При цьому обсяг пропозиції там у рази менший, ніж у Києві, а поява нових майданчиків, з урахуванням нинішніх реалій, особливо в розрізі термінів постачання інженерного обладнання, малоймовірна навіть у середньостроковій перспективі. Отже, хоч би як це дивно не звучало, при раціональному підході Київ зараз, як і раніше, виглядає більш привабливим місцем для розміщення IT-активів.

**— Але «закордон» тоді виглядає ще безпечнішим, адже туди точно не «прилетить»?**

– Безперечно, туди не «прилетить». Але ЦОД там може спалахнути, відключитися через аномальну спеку або людський фактор. За останні кілька років можна навести далеко не один приклад подій такого роду, у тому числі й у глобальних операторів хмар.

Як війна вплинула на ймовірність подібних «локальних катастроф» для вітчизняних ЦОД та хмарних операторів? Сказати важко, але, схоже, не дуже сильно – особисто мені невідомі випадки впливу цих нових загроз для хоч якихось великих ЦОД, хоча війна триває вже більше півроку. Звісно, я говорю про регіони, досить віддалені від зони активних бойових дій.

Тому, якщо бізнес у мирний час був толерантним до тимчасової недоступності IT-компонентів через локальну катастрофу, – нічого особливо не змінилось. Так само, як і в протилежній ситуації – коли компанія дуже чутлива до відмов IT. В останньому випадку необхідність наявності DR інструментів (DR – Disaster Recovery, відновлення

після катастроф) як була, так і залишилася. І це не залежить від розташування ЦОД – в Україні чи за її межами.

**— Про які DR інструменти йде мова?**

– Класичний підхід – це два майданчики, основний та резервний (або два рівноцінні сайти, що в штатному режимі розподіляють навантаження), між якими в тій чи іншій формі виконується безперервна реплікація даних.

До речі, для захисту саме від локальних катастроф дуже бажано, щоб майданчики були синхронними, тобто втрата одного з них не повинна призводити до втрати підтверджених бізнес-транзакцій. Якщо ця умова виконується, то активація резервного майданчика – це суто IT-завдання. В іншому випадку потрібне залучення бізнес-підрозділів для ідентифікації та повторного проведення втрачених транзакцій (яскравий приклад втраченої транзакції – банкомат гроші видав, але з рахунку вони не списалися, або навпаки).

За сучасного рівня розвитку технологій, синхронна відстань не перевищує 100–150 км, а це означає, що синхронна пара, як правило, знаходиться в межах одного міста. Тому створити її, наприклад, між Києвом та Львовом неможливо суто технологічно, і розмістити таку пару майданчиків найкраще або у Києві, або у Львові, але не одна тут, інша там. Цей висновок може здатися контрінтуїтивним, але якщо ми вирішуємо конкретне завдання – забезпечуємо захист від локальних катастроф – то все виглядає саме так.

**— Припустимо, але, крім пошкодження конкретного ЦОД, існує ймовірність тривалого знеструмлення міста чи району внаслідок атак на критичну інфраструктуру регіону, це цілком реальна загроза.**

– Так, не виключено, що «регіональна катастрофа» як результат військових дій цілком можлива. Але, якщо розглядати такий варіант, то кожен керівник/власник компанії, перш за все, повинен поставити собі запитання: «А чи зможе мій бізнес продовжуватись у таких умовах, навіть якщо IT-компонента не постраждає? Адже, швидше за все, будуть проблеми зі зв'язком, не буде палива, може не працювати банківська система, виникне правовий вакуум, можуть кардинально змінитися потреби і мої товари/послуги будуть просто непотрібні...»

Думаю, що здебільшого відповідь буде: «Ні, не зможе. Доведеться взяти паузу до прояснення/нормалізації ситуації. Але всю інформацію в IT-системах потрібно надійно зберегти – вона точно знадобиться під час перезапуску».

До речі, якщо говорити виключно про тривале знеструмлення (без урахування всіх пов'язаних з цим «вторинних» наслідків), то тут однозначну перевагу матимуть ЦОД рівня не нижче за Tier III (згідно з класифікацією Uptime Institute) – для них первинним джерелом енергії є дизель-генераторна станція, спроможна до безперервної роботи протягом необмеженого часу. У цьому сенсі Київ виглядає привабливіше – більшість (якщо не всі) ЦОД країни, які відповідають рівню Tier III, знаходяться саме тут.

**— Але виходить, якщо перемістити IT-системи за кордон, то ризик «регіональної катастрофи» внаслідок війни зникає?**

– Так, саме так. Але цей крок має свою ціну, і чималу ціну. По-перше, суто економічний аспект – вартість закордонних хмарних ресурсів може бути у півтора-два рази вищою. До речі, домовитися з гіперскейлером (глобальним хмарним провайдером) про «тимчасові труднощі з оплатою» буде непросто. Все ж таки вони «там» знаходяться поза контекстом війни, на відміну від вітчизняних операторів.

По-друге, є й технологічні аспекти, хоча б відсутність «мережевої близькості», що може призвести до помітного уповільнення роботи IT-сервісів.

Ну і, по-третє, наявність працездатної IT-компоненти ніяк не допомагає у разі настання регіональної катастрофи на території ведення бізнесу – як я вже згадував, у цьому випадку бізнесу швидше за все доведеться «стати на паузу». Таким чином, більша вартість та технологічні незручності міграції в закордонний ЦОД або хмару виявляються невиправданими.

**— Ви говорили, що у разі постановки бізнесу «на паузу» всю інформацію в IT-системах потрібно надійно зберегти. Але як це зробити?**

– Ось для цього завдання «закордон» – це практично безальтернативний варіант, як надійне місце зберігання «холодної» репліки даних. «Холодна» означає, що це повністю актуальна копія всієї інформації, але без обчислювальних ресурсів, необхідних для підтримання її постійної доступності (це, умовно, як «флешка», до якої не додається ноутбук). Економічно це дуже ефективно – основну частину вартості хмари становлять саме обчислювальні ресурси, але для «холодної» репліки (до моменту її активації) вони саме і не потрібні.

Таким чином, оптимальна схема розміщення IT-систем практично будь-якого вітчизняного бізнесу зараз виглядає так: працююча IT-інфраструктура в Україні (Київ чи Львів – технологічно принципової різниці немає, але пропозиція та якість у Києві вища) плюс «холодна» репліка за кордоном, переважно у гіперскейлера.

**— А чи є у De Novo сервіси, які дозволяють реалізувати цю концепцію?**

– Так, звичайно. Протягом буквально кількох тижнів після початку війни ми розробили цілу низку сервісів сімейства Geo XR. Це модифікація наших стандартних послуг резервного копіювання (у нас їх багато, практично на всі випадки життя). Основна відмінність – на додаток до локальної резервної копії (вона використовується для швидкого відновлення у звичайних ситуаціях, коли потрібно відновити одну віртуальну машину, диск або окремий файл) створюється віддалена резервна копія («геокопія») в об'єктному сховищі одного з глобальних хмарних провайдерів (вже згаданий «закордон»). В порівнянні з повним переміщенням IT-сервісів у закордонну хмару вартість цієї послуги – тобто, «холодної» репліки в надійному сховищі – більш ніж привабливa.

Вкрай важливою особливістю сімейства Geo XR є функція автономного (без будь-якої участі De Novo) відновлення самим клієнтом у будь-яку віртуальну інфраструктуру корпоративного класу (VMware vSphere, Microsoft Hyper-V – різниці немає), або ж у хмару самого гіперскейлера.

**— Отже, де краще зберігати дані — в українській чи закордонній хмарі?**

– Вочевидь, більшості компаній варто розглянути комбінацію обох підходів. Настав час раціональних рішень. «Найсерйозніша втрата в битві – це втрата голови» («Аліса в Задзеркаллі»). На мій погляд, розміщення IT-сервісів в Україні у поєднанні з «холодною» реплікою в надійному закордонному ЦОД із можливістю автономного відновлення – це найбільш збалансований підхід як з економічної, так і з технологічної точок зору.

**Ігор КИРИЛОВ**, МтБ