Хмара для фінансових установ. Чекліст для бізнесу:

що перевірити після Постанови НБУ №99



«Перш ніж переносити дані в хмару, розберіться, чи відповідає провайдер вимогам щодо безпеки, надійності і безперервності бізнесу», — власною експертизою ділиться Сергій БОБКО, керівник відділу продажів хмарних сервісів «Датагруп».

Хмарні технології давно стали частиною IT-інфраструктури бізнесу. Але що більше критичних процесів компанія переносить у хмару, то гостріше постають питання: наскільки захищені дані, що станеться у разі збою провайдера і чи зможе компанія швидко забрати свої дані, якщо вирішить змінити постачальника.

Для фінансового сектору відповіді на ці питання зафіксовані на рівні регулятора — Національного Банку України. Постанова НБУ №99, що набула чинності 1 листопада 2025 року, визначає правила застосування хмарних технологій банками, надавачами фінансових послуг, операторами та учасниками платіжних систем, а також технологічними операторами платіжних послуг. Документ встановлює вимоги до договорів із хмарними провайдерами, управління ризиками, інформаційної безпеки, безперервності роботи та контролю за ланцюгом постачання.

Для компаній поза фінансовим сектором Постанова №99 не є обов'язковою вимогою. Але закладені в ній принципи — хто відповідає за дані, наскільки захищений сервіс, що робити у разі збою провайдера — актуальні для будь-якого бізнесу, який працює з хмарою.

Про те, що змінила Постанова №99 і що варто перевірити користувачам хмарних сервісів, ми поговорили з **Сергієм БОБКОМ**, експертом у сфері хмарних технологій та інформаційної безпеки, керівником відділу продажів хмарних сервісів «Датагруп».

Що конкретно змінює Постанова №99 для фінансового бізнесу?

Постанова визначає, як фінансові установи мають застосовувати хмарні технології, і встановлює вимоги до хмарних послуг. Головне тут — документ стосується саме установи-користувача, а не провайдера. Тобто відповідальність за дотримання вимог не можна просто перекласти на хмарну компанію.

На практиці це означає, що бізнесу недостатньо обрати надійного провайдера. Потрібно ще вибудувати власний процес управління ризиками, призначити відповідальних людей і контролювати, чи відповідають отримувані послуги вимогам регулятора.

Чи означає це, що чинний договір із провайдером доведеться переглядати?

Так, якщо діяльність компанії відповідає критеріям регулювання Постанови, доволі детальним. Постанова прописує, що саме має бути в договорі про хмарні послуги: перелік і опис послуг, вимоги до інформаційної безпеки, порядок звітування провайдера, умови доступу до ресурсів, правила роботи з даними, відповідальність сторін і умови щодо партнерів провайдера.

Окремо йдеться про розподіл відповідальності між установою та провайдером — наприклад, хто керує криптографічними ключами, хто моніторить безпеку, хто відповідає за резервне копіювання чи реагування на кіберінциденти.

Тож перше, що варто зробити, — дістати договір і перечитати його не тільки з юридичного боку, а й з IT– та кібербезпекового.

А сертифікат від провайдера — цього достатньо?

Самого по собі сертифіката — ні. Договір має передбачати, що провайдер періодично, не рідше разу на рік, надає або оприлюднює сертифікати відповідності міжнародним стандартам інформаційної безпеки. Тому варто перевіряти не саму наявність сертифіката, а те, які сервіси й процеси у надавача фінансових послуг він реально охоплює.

Хто в результаті відповідає за дані в хмарі — бізнес чи провайдер?

Постанова прямо вимагає зафіксувати цей розподіл у договорі. Сторони мають визначити, хто відповідає за налаштування доступів, моніторинг безпеки, управління ключами шифрування, резервне копіювання, реагування на інциденти, підтримку сервісів та їхню доступність.

Формулювання на кшталт «за безпеку відповідає провайдер» тут не працює. Потрібно чітко прописати, хто, за що і в яких межах відповідає.

Що варто знати про партнерів хмарного провайдера?

Постанова окремо звертає увагу на так звані ланцюгові хмарні послуги — коли провайдер залучає

інших партнерів для надання сервісу. Установа може користуватися такими послугами, але провайдер має підтвердити, що партнер виконує відповідні зобов'язання. Про заплановані зміни партнерів чи послуг, які можуть вплинути на договір або підвищити ризики, провайдер зобов'язаний повідомляти.

Для бізнесу висновок простий: під час вибору провайдера варто запитувати не лише «хто ви?», а й «хто ще бере участь у наданні мені цього сервісу?».

Наскільки важливо, де фізично зберігаються дані?

Це один із принципових пунктів. Постанова забороняє установам залучати провайдерів, пов'язаних із державою-агресором, а також користуватися хмарними послугами, якщо обробка чи зберігання даних відбувається на відповідних територіях або в датацентрах, що належать підсанкційним суб'єктам. Обмеження стосуються і ланцюгових партнерів провайдера. Тож перевіряти варто не тільки юридичну особу, з якою підписується договір, а й весь ланцюг постачання послуги.

А якщо компанія захоче змінити провайдера?

Один із головних практичних ризиків хмари — надмірна залежність від одного постачальника. Постанова вимагає, щоб план безперервності передбачав дії на випадок переходу до іншого провайдера або зупинки роботи наявного.

Тому ще на етапі підписання договору варто розуміти, як компанія забере свої дані, у якому форматі, за який час і як забезпечити безперервність бізнес-процесів під час міграції.

Чи доведеться фінансовим установам змінювати внутрішні процеси?

Так. Установа має запровадити процес управління ризиками використання хмари, призначити відповідальних і мати внутрішній документ щодо цих ризиків. Використання хмарних послуг також має бути інтегроване в загальні процеси забезпечення безперервності діяльності.

Тобто відповідність Постанові №99 — не разова перевірка договору, а процес, який стає частиною регулярного управління IT-, операційними та кіберризиками.



Що бізнесу, який підпадає під регулювання Постанови, варто зробити для відповідності отримання хмарних послуг за її вимогами?

Пропонуємо пройтися за таким чеклістом.

1. Перевірити договір із провайдером: чи прописані умови щодо безпеки, відповідальності сторін, доступу до даних, партнерів, сертифікації та припинення співпраці.

2. Перевірити провайдера й інфраструктуру: хто власник компанії, де розташовані датацентри, хто партнери та субпідрядники.

3. Оцінити інформаційну безпеку: які сертифікати є у провайдера, чи поширюються вони саме на потрібні сервіси, як налагоджено моніторинг та реагування на інциденти.

4. Визначити зони відповідальності: хто відповідає за доступи, ключі шифрування, резервне копіювання, відновлення, моніторинг і реагування на кіберінциденти.

5. Перевірити план безперервності: що відбувається у разі недоступності провайдера чи необхідності перейти до іншого.

6. Переглянути внутрішні процеси: чи призначені відповідальні за використання хмари і чи є регулярне оцінювання ризиків.

7. Не забути про НБУ: постанова зобов'язує повідомляти регулятора про укладення договору, зміни в ньому та розірвання у визначені строки.

Хмара, яка відповідає вимогам бізнесу

Постанова №99 переводить використання хмарних технологій у фінансовому секторі з суто технологічного питання в площину керованого бізнес-ризику. Тому вибір провайдера варто починати не з «скільки коштує сервер», а з «чи забезпечить цей провайдер потрібний рівень надійності та відповідності вимогам нашого бізнесу».

У «Датагруп» хмарні рішення будують саме з фокусом на безпеку та відмовостійкість бізнесу. Йдеться про такі IaaS-рішення, як UA-Cloud, EuroCloud, Microsoft Azure та інші сервіси, які дозволяють розміщувати й масштабувати IT-інфраструктуру без потреби утримувати власну. UA-Cloud розміщений в Україні, у датацентровій інфраструктурі з передбаченими заходами фізичного захисту. А EuroCloud із міжнародними ISO-сертифікатами — у датацентрі у Франкфурті-на-Майні.

Водночас відповідність конкретного використання хмарних технологій вимогам Постанови №99 залежить не лише від характеристик хмарного сервісу, а й від способу його використання фінансовою установою, умов договору, розподілу відповідальності та організації внутрішніх процесів управління ризиками.

Залиште заявку на консультацію фахівців «Датагруп», і вони допоможуть вам визначити, яке саме хмарне рішення відповідає вимогам до безпеки та масштабам вашого бізнесу:
https://www.datagroup.ua/smb/hmarni-rishennia

Data group

Щоб дізнатись більше, звертайтесь:
тел.: 0 800 100 008
cloud_sales@datagroup.ua
https://business.datagroup.ua/clouds/