РОЗПОДІЛ ВІДПОВІДАЛЬНОСТІ В СУІБ ПРИ ВИКОРИСТАННІ ХМАРНИХ СЕРВІСІВ (IaaS, PaaS, SaaS)

Рой Є.О., Доленко О.Д., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Стрімка цифровізація бізнес-процесів та масштабний перехід організацій до використання хмарних обчислень суттєво трансформують сучасні підходи до побудови систем управління інформаційною безпекою (СУІБ) [1, 2]. Перенесення інформаційних ресурсів до хмарного середовища усуває необхідність утримання власної фізичної інфраструктури, проте створює нові виклики, пов'язані з втратою безпосереднього контролю за обчислюваним середовищем та збереженням даних [2]. Згідно з вимогами стандарту ДСТУ ISO/IEC 27001:2023, організація повинна гарантувати забезпечення засадничих засад безпеки – конфіденційності, цілісності та доступності даних незалежно від того, де розташовані обчислювальні потужності [3]. Головною суперечністю під час міграції у хмару є помилкове уявлення про те, що хмарний провайдер (CSP) бере на себе повну відповідальність за безпеку інформаційних активів клієнта [1, 4]. Невизначеність меж операційної відповідальності призводить до виникнення критичних прогалин у системі захисту, витоку конфіденційної інформації та невиконання регуляторних вимог [2, 4].

Метою доповіді є аналіз та систематизація моделей розподілу відповідальності між хмарним провайдером та замовником у сервісних архітектурах IaaS, PaaS, SaaS, а також обґрунтування практичних кроків щодо інтеграції хмарних контролів стандарту ISO/IEC 27017 у СУІБ за ДСТУ ISO/IEC 27001:2023 для мінімізації ризиків міграції [1, 5].

Фундаментом безпечного функціонування хмарних систем є концептуальне розмежування двох принципів: безпека хмари та безпека у хмарі [4, 5]. Постачальник хмарних послуг безпосередньо відповідає за фізичну охорону дата–центрів, відмовостійкість апаратного забезпечення, мережеву інфраструктуру та гіпервізори. Натомість замовник (клієнт) залишається відповідальним за захист власних даних, конфігурацію програмного забезпечення, керування ідентифікацією та доступом (IAM), а також дотримання корпоративних політик безпеки [4, 5]. Ступінь контролю та обсяг операційних обов'язків замовника суттєво варіюються залежно від використовуваної моделі хмарного обслуговування: Infrastructure as a Service (IaaS) надає замовнику найвищий рівень контролю та відповідальності за ОС, middleware, додатки та налаштування мережевих екранів; Platform as a Service (PaaS) перекладає управління ОС та runtime на провайдера, залишаючи за клієнтом розроблені додатки та дані; Software as a Service (SaaS) забезпечує найменший рівень контролю, де провайдер обслуговує весь програмно–апаратний стек, а клієнт відповідає виключно за дані та керування доступом користувачів [4, 5].

Впровадження хмарних послуг вимагає адаптації наявної СУІБ шляхом додавання спеціалізованих контролів стандарту ISO/IEC 27017, який розширює каталог ДСТУ ISO/IEC 27001:2023 (зокрема контролі Додатку А 5.23 «Захист

інформації при використанні хмарних сервісів» та 5.19 «Безпека у відносинах із постачальниками») [3, 5]. Процес інтеграції передбачає [3, 5]:

1) визначення ролей організації, де вона виступає клієнтом або постачальником хмарних сервісів;

2) формування Матриці спільної відповідальності із закріпленням обов'язків щодо резервного копіювання, шифрування і реагування на інциденти;

3) оновлення оцінки ризиків і Положення про застосовність;

4) впровадження технічних заходів, таких як багатофакторна автентифікація, розділення середовищ розробки й продакшну, централізоване логування та процедури безпечного видалення даних;

5) збір доказів виконання контролів для включення ISO/IEC 27017 до наглядового або сертифікаційного аудиту СУІБ.

Аналіз ризиків СУІБ під час переходу до хмари повинен базуватися на комплексних фреймворках підтримки прийняття рішень, які враховують бізнес–цілі організації [1]. Застосування методу аналізу ієрархій дозволяє розрахувати вагові коефіцієнти цілей та визначити чисельний рівень чистих ризиків. Систематизація загроз охоплює бізнесові, організаційні та технічні ризики, серед яких найбільш критичними є витік даних, переривання функціональності організації та залежність від постачальника. Для мінімізації ризиків вимагається перевірка аудиторських звітів провайдера та впровадження власних планів безперервності бізнесу [1]. Отже, використання хмарних технологій (IaaS, PaaS, SaaS) не звільняє організацію від кінцевої відповідальності за забезпечення інформаційної безпеки та збереження конфіденційних даних. Чітка формалізація Моделі спільної відповідальності та її інтеграція у СУІБ за стандартами ДСТУ ISO/IEC 27001:2023 та ISO/IEC 27017 дозволяє усунути прогалини у захисті, гарантувати комплаєнс та забезпечити стійкість бізнес–процесів.

Список літератури

1. A Risk Management Framework for Cloud Migration Decision Support / S. Islam et al. *Journal of Risk and Financial Management*. 2017. Vol. 10, no. 2. P. 10. URL: https://doi.org/10.3390/jrfm10020010 (date of access: 23.10.2026).

2. Kacha L., Zitouni A. An Overview on Data Security in Cloud Computing. *arXiv preprint*. P. 1–14. URL: https://doi.org/10.48550/arXiv.1812.09053 (date of access: 23.10.2026).

3. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. Київ: ДП «УкрНДНЦ», 2023. 19 с.

4. Рудий С. В., Сєвєрінов О. В. Дослідження моделі безпеки при використанні хмарних сервісів // Проблеми інформатизації : матеріали десятої міжнародної науково-технічної конференції, 24–25 листопада 2022 р. 2022. Т. 1. С. 61. URL: https://openarchive.nure.ua/bitstreams/38baabd3-1255-4337-b8dd-3074b51aca13/download.

5. Мартиненко Я. А. Хмарні обчислення як рішення для захисту інформації в ІКС / наук. керівник О. В. Сєвєрінов // Радіоелектроніка та молодь у XXI столітті : матеріали 28-го Міжнародного молодіжного форуму, 16–18 квітня 2024 р. Харків : ХНУРЕ, 2024. Т. 5. С. 122–124. DOI: https://doi.org/10.30837/IYF.PCEIP.2024.122.