

**УДК 004**

**Д.О. Дисевич, В. І. Козак, А. Д. Головко, С. Т. Гаврись**

Тернопільський національний технічний університет імені Івана Пулюя, Україна

## **ХМАРНА ІНФРАСТРУКТУРА ДЛЯ СИСТЕМИ ПЛАТІЖНИХ ШЛЮЗІВ**

**D. O. Dysevuch, V. I. Kozak, A. D. Holovko, S. T. Havrys**

### **CLOUD INFRASTRUCTURE FOR THE SYSTEM OF PAYMENT GATEWAYS**

Внутрішні інфраструктури переносяться в хмару завдяки розширеним можливостям технічного управління, технічному вдосконаленню, а також гнучкості та економічно ефективним варіантам, які пропонує хмара. Крім того, архітектура підприємства змінюється, коли системи переміщуються в іншу інфраструктуру. Завдяки таким інфраструктурним змінам ризики безпеки можуть збільшуватися або зменшуватися, водночас можуть з'являтися нові ризики, а деякі ризики можна усунути. Ідентифікація активів для аналізу ризиків, заснована лише на моделюванні бізнес-процесів, не має інтеграції та представлення взаємозв'язку між ІТ-інфраструктурою та бізнес-процесами.

Отже, певними активами інформаційної системи можна знехтувати в аналізі ризиків. Під час аналізу ризиків безпеки двох інфраструктур необхідно врахувати відмінності в архітектурі підприємства, оскільки неідентифіковані активи інформаційної безпеки можуть бути вразливими та становити ризик для безпеки відповідної організації. У цій роботі активи ідентифікуються за допомогою архітектурного моделювання для виконання аналізу ризиків. Крім того, моделі представляють відмінності, що стосуються активів інформаційної безпеки у внутрішній інфраструктурі та хмарній інфраструктурі, на додаток до відображення відповідних бізнес-процесів. Моделювання загроз на основі STRIDE використовується для визначення ризиків безпеки, що стосуються активів ІБ, отриманих від архітектури підприємства.

Рівень хмарних технологій було змодельовано з використанням інформації, зібраної від популярних хмарних провайдерів, таких як OpenVAS, Amazon і Rack space. Представлена в роботі хмарна модель є узагальненою. Середовище хмарного центру обробки даних не є спеціальним, тому хмарні спільні орендарі можуть перебувати в одному гіпервізорі, навіть якщо мережа розділена. Доступ до послуг зберігання та спільного пулу ресурсів мають усі співкористувачі, підключені до сховища. Користувачі хмарного обслуговування вважаються поза сферою дії через дуже розподілену природу підтримки постачальників, задіяних у хмарних службах. Хмара має розширені функції, а використовувані технології відрізняються. Приклад: хмарна мережа даних. Основна архітектурна відмінність між хмарою та внутрішньою інфраструктурою полягає в тому, що хмара має компоненти, пов'язані з віртуалізацією. Комутатори, мережі в хмарі здебільшого є логічними розділеннями. Хмара має спільний пул ресурсів, щоб сприяти зростанню потреб у ресурсах. Тому доступ до сховища не можна відокремити від інших користувачів загальнодоступної хмари. У хмарній архітектурі також можна ідентифікувати ті самі бізнес-процеси завдяки припущенню, зробленому в рамках дослідження. Серед бізнес-процесів, змодельованих в обох інфраструктурах, буде взято до уваги обробку платіжних транзакцій. Розширення процесу платіжних транзакцій буде обговорено в розділі 4 для виявлення бізнес-активів. На рис. 1 представлено абстракцію хмарного центру обробки даних та інтеграцію з бізнес-процесами PayGate.

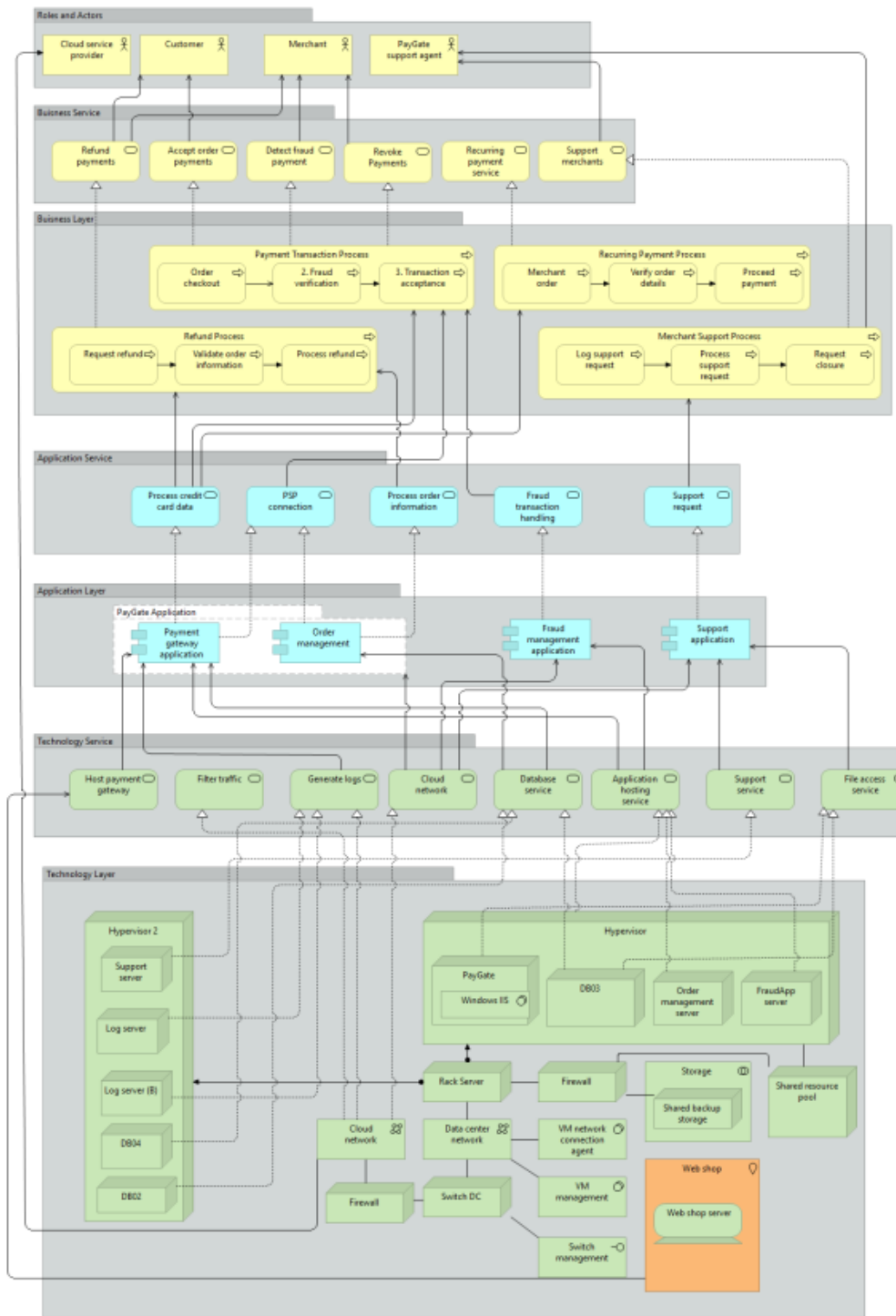


Рисунок 1 - Модель хмарної інфраструктури ArchiMate

## Література

1. "12 Benefits of Cloud Computing and Its Advantages," Salesforce.com. URL : <https://www.salesforce.com/hub/technology/benefits-of-cloud/>.
2. RightScale, "RightScale 2018 State of the Cloud Report," 2018 [Online]. URL : [https://www.suse.com/media/report/rightscale\\_2018\\_state\\_of\\_the\\_cloud\\_report.pdf](https://www.suse.com/media/report/rightscale_2018_state_of_the_cloud_report.pdf).