Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Порівняльний аналіз ризиків безпеки різних IT-інфраструктур для системи платіжних шлюзів

Виконав: студент VI курсу, групи СБм-62
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Козак В.І. (прізвище та ініціали)

Керівник (підпис) Кульчицький Т.Б. (прізвище та ініціали)

Нормоконтроль (підпис) Лечаченко Т.А. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Козаку Володимиру Івановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Порівняльний аналіз ризиків безпеки різних IT-інфраструктур для системи платіжних шлюзів

Керівник роботи Кульчицький Тарас Русланович, д-р філософії, ст. викл. кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «16» листопада 2023 року № 4/7-1061

2. Термін подання студентом завершеної роботи 26 грудня 2023р.

3. Вихідні дані до роботи Наукові публікації про хмарні сервіси платіжних шлюзів

4. Зміст роботи (перелік питань, які потрібно розробити)
1 Аналіз предметної області безпеки іт-інсраструктури платіжних шлюзів
2 Аналіз ідентифікація активів системи платіжних шлюзів
3 Аналіз ризиків системи платіжних шлюзів
4 Охорона праці та безпека в надзвичайних ситуаціях
Висновки
Перелік використаних джерел
Додатки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Титульний слайд
Актуальність роботи
Цілі та завдання
ISSRM Управління ризиками безпеки інформаційних систем
Модель домену ISSRM
Модель внутрішньої інфраструктури ArchiMate
Модель хмарної інфраструктури ArchiMate
Процес перевірки замовлення
Процес перевірки шахрайства та приняття транзакції
Системні активи системи платіжного шлюзу
Висновки. Додаток А

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., кандидат технічних наук, зав. кафедри КС		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 16 листопада 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	25.11.2023	*Виконано*
2.	Підбір наукових джерел про хмарні сервіси платіжних	26.11.2023-28.11.2023	*Виконано*
	шлюзів		
3.	Опрацювання наукових публікацій та збір даних по	29.11.2023-1.12.2023	*Виконано*
	темі роботи		
4.	Виконання дослідження згідно мети кваліфікаційної	2.12.2023-4.12.2023	*Виконано*
	роботи		
5.	Оформлення розділу «Аналіз предметної області	5.12.2023-7.12.2023	*Виконано*
	безпеки іт-інсраструктури платіжних шлюзів»		
6.	Оформлення розділу «Аналіз ідентифікація активів	8.12.2023-10.12.2023	*Виконано*
	системи платіжних шлюзів»		
7.	Оформлення розділу «Аналіз ризиків системи	11.12.2023-13.12.2023	*Виконано*
	платіжних шлюзів»		
8.	Виконання завдання до підрозділу «Охорона праці»	14.12.2023-15.12.2023	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	16.12.2023-17.12.2023	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	18.12.2023-19.12.2023	*Виконано*
11.	Нормоконтроль	19.12.2023-20.12.2023	*Виконано*
12.	Перевірка на плагіат	21.12.2023	*Виконано*
13.	Попередній захист кваліфікаційної роботи	22.12.2023	*Виконано*
14.	Захист кваліфікаційної роботи	26.12.2023	

Студент _____ Козак В.І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Кульчицький Т.Р.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Порівняльний аналіз ризиків безпеки різних ІТ-інфраструктур для системи платіжних шлюзів // Кваліфікаційна робота освітнього рівня «Магістр» // Козак Володимир Іванович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-62 // Тернопіль, 2023 // С. 82, рис. – 16, табл. – 26, додат. 1 , бібліогр. – 58.

Ключові слова*:* ПЛАТІЖНА СИСТЕМА, ХАКЕР, АТАКА, ПЛАТІЖНИЙ ШЛЮЗ, ВНУТРІШНЯ ІНФРАСТРУКТУРА, ЗОВНІШНЯ ІНФРАСТРУКТУРА.

Кваліфікаційна робота присв'ячена розробці методів вибору процедур, які можна використати для виявлення відмінностей ризиків безпеки у внутрішній інфраструктурі та хмарній інфраструктурі.

В роботі описано з методи і мови моделювання, використаних у дослідженні, представляючи обґрунтування обраного методу. Розглянуто типи платіжних шлюзів і огляд інфраструктур, використаних у дослідженні. Крім того, тут представлено корпоративну архітектуру внутрішньої та хмарної інфраструктури для визначення контексту та зв'язку бізнес-активів і допоміжних активів за допомогою моделювання корпоративної архітектури. Описано процес виявлення активів і представлено цілі безпеки бізнес-активів. У роботі увагу було зосереджено на пошуку загроз для активів інформаційної системи у внутрішній інфраструктурі та хмарній інфраструктурі за допомогою методу моделювання загроз STRIDE. Крім того, буде обговорено, як ризики будуть диференціюватись на основі міграції інфраструктури.

ANNOTATION

Comparative Analysis of Security Risks in Different IT Infrastructures for a Payment Gateway System // The educational level "Master" qualification work // Volodymyr Kozak // Ternopil Ivan Pulyuy National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, SBm-62 group // Ternopil, 2023 // P. 82, fig. - 16, tables - 26, annexes -1, ref. - 58.

Key words: PAYMENT SYSTEM, HACKER, ATTACK, PAYMENT GATEWAY, INTERNAL INFRASTRUCTURE, EXTERNAL INFRASTRUCTURE.

The qualification work is devoted to the development of procedures selection methods that can be used to identify the differences in security risks in on-premise infrastructure and cloud infrastructure.

The paper describes the methods and modeling language used in the research, presenting the justification of the chosen method. The types of payment gateways and an overview of the infrastructures used in the study are considered. In addition, it presents the enterprise architecture of on-premises and cloud infrastructure to define the context and relationship of business assets and supporting assets using enterprise architecture modeling. The asset discovery process is described and the security objectives of business assets are presented. The work focused on finding threats to information system assets in internal infrastructure and cloud infrastructure using the STRIDE threat modeling method. In addition, it will be discussed how risks will be differentiated based on infrastructure migration.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ISSRM (англ. Information System Security Risk Management) – Управління ризиками безпеки інформаційних систем.

OCTAVE (англ. Operationally Critical Threat, Asset, and Vulnerability Evaluation) – Операційно критична оцінка загроз, активів і вразливостей.

STRIDE (англ. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service) – Підробка, підробка, відмова, розкриття інформації, заперечення служби, підвищення пільг.

PCI DSS (англ. Payment Card Industry Data Security Standard) – Індустріальний стандарт безпеки даних платіжних карток.

NIST (англ. National Institute of Standards and Technology) – Національний інститут стандартів і технологій.

MEHARI (англ. Method for Harmonized Analysis of Risk) – Метод для гармонізованого аналізу ризиків.

IS (англ. Information Systems) – Інформаційні системи.

EA (англ. Enterprise Architecture) -– Архітектура підприємства.

RM (англ. Risk Management) – Управління ризиками.

RA (англ. Risk Analysis) – Аналіз ризику.

CIA (англ. Confidentiality, Integrity, Availability) – Конфіденційність, цілісність, доступність.

PSP (англ. Payment Service Provider) – Постачальник платіжних послуг

ISO/IEC (англ. International Organisation for Standardisation and the International Electrotechnical Commission) – Міжнародна організація зі стандартизації та Міжнародна електротехнічна комісія.

BPMN (англ. Business Process Model and Notation) – Модель і нотація бізнес-процесу.

SP (англ. Spoofing) – Спуфінг.

TA (англ. Tampering) – Тамперінг.

RE (англ. Repudiation) – Відмова.

IND (англ. Information Disclosure) – Розкриття інформації.

DS (англ. Denial of Service) – Відмова в обслуговуванні.

EP (англ. Elevation of Privilege) – Підвищення привілеїв.

WAF (англ. Web Application Firewall) – Брандмауер веб-додатків.

IaaS (англ. Infrastructure as a Service) – Інфраструтура як сервіс.

SaaS (англ. Software as a Service) – Програмне забезпечення як сервіс.

PaaS (англ. Platform as a Service) – Платформа як сервіс.

ЗМІСТ

ВСТУП

Актуальність теми. Хмарні технології стали вибором, ніж тенденцією керівників найвищого рівня для нових і існуючих IT-інфраструктур. Перехід внутрішньої інфраструктури до хмарної інфраструктури має такі переваги, як використання найсучасніших технологій, гнучкість, засоби управління та конкурентоспроможність у динамічному світі [1].

З розвитком хмарних технологій безпека стала проблемою [2]. Можливість отримання третіми особами неавторизованого доступу до конфіденційних ресурсів, викрадення облікового запису, відмова в обслуговуванні та зловмисних інсайдерських атак є ризиками для хмарних середовищ.

Згідно з прогнозами Gartner [3], до 2025 року через хмару закриється 80% внутрішніх корпоративних центрів обробки даних. Чотирнадцятий щорічний звіт про безпеку інфраструктури в усьому світі Netscout [4] показує, що 49% корпоративних програм вже знаходяться в хмарі. Ризики безпеки, пов’язані з хмарною інфраструктурою, можуть відрізнятися від ризиків внутрішнього центру обробки даних через корпоративну хмарну архітектуру. Таким чином, аналіз ризиків (RA), проведений для бізнес-процесу у внутрішній інфраструктурі, не застосовуватиметься до хмари, навіть якщо бізнес-процес залишається незмінним.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є модельний підхід, який може ідентифікувати зміни в системних активах, коли змінюється інфраструктура, і взаємозалежність бізнес-процесів на прикладі платіжних шлюзів.

Для досягнення поставленої мети потрібно виконати ряд завдань, зокрема:

– Проаналізувати стан досліджень в області хмарних технологій платіжних шлюзів

– Дослідити існуючі на даний час методи аналізу загроз для платіжних шлюзів

– Проаналізувати методи заплбігання кібератакам на платіжні шлюзи

– Виконати порівняня існуючих методів

– Розробити змодельовану структуру для аналізу загроз при переході на хмарні технології

Об’єкт дослідження платіжні шлюзи з хмарною та внутрішньою інфраструктурою.

Предмет дослідження. загрози при переході на хмарну інфраструктуру.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що було вивчено та змодельовано загрози кібератак при переході підприємства на хмарні платіжні шлюзи.

Практичне значення одержаних результатів. Виконано аналіз та моделювання загроз при переході на хмарні технології при проведенні платежів.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на XI міжнародній науково-технічній конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2023 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції (Див. додатки А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 58 найменувань та 1 додатку. Загальний обсяг кваліфікаційної роботи складає 82 сторінки, з них __ сторінок основного тексту, який містить __ рисунків та __ таблиць.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ БЕЗПЕКИ ІТ-ІНСРАСТРУКТУРИ ПЛАТІЖНИХ ШЛЮЗІВ

1.1 Постановка задач дослідження

Ризики безпеки, пов’язані з хмарною інфраструктурою, можуть відрізнятися від ризиків внутрішнього центру обробки даних через корпоративну хмарну архітектуру. Таким чином, аналіз ризиків (RA), проведений для бізнес-процесу у внутрішній інфраструктурі, не застосовуватиметься до хмари, навіть якщо бізнес-процес залишається незмінним.

Ці зміни в системних активах створюють загрози, тому ризики безпеки можуть залишатися, усунути або ініціювати під час хмарної міграції. Ідентифікація активів інформаційної системи, заснована лише на моделюванні бізнес-процесів, не в змозі зафіксувати зміни корпоративної архітектури системи до та після міграції. Перед проведенням RA у будь-якому контексті необхідно визначити активи. Активи інформаційної системи – це активи, які підтримують бізнес-активи та потребують захисту від загроз [5].

В організаціях аналіз бізнес-процесів проводить нетехнічна особа. Тому в аналізі, орієнтованому на бізнес-процес, бракує відображення всіх активів інформаційної системи, які підтримують бізнес-активи. Крім того, відображення між бізнес-процесом і відповідною інфраструктурою відсутнє та ізольоване. Ця робота зосереджена на пропонуванні процедури фіксації та порівняння відмінностей у ризиках безпеки через зміни інфраструктури, які відбуваються під час міграції системи платіжного шлюзу.

Дослідження пропонує модельний підхід, який може ідентифікувати зміни в системних активах, коли змінюється інфраструктура, і взаємозалежність бізнес-процесів. Моделювання архітектури підприємства використовується для визначення архітектурних відмінностей між внутрішньою та хмарною інфраструктурами.

Цей підхід відображає взаємозв’язки та взаємозалежність активів бізнесу та системи, що допомагає визначити, які активи матимуть вплив через ризик

безпеки. Управління ризиками безпеки інформаційних систем (ISSRM) використовується як метод RA для виявлення ризиків безпеки внутрішньої та хмарної інфраструктури [5]. Відмінності ризиків безпеки, виявлені в дослідженні, розглядаються як прогалини ризиків безпеки в роботі.

Ця робота є тематичним дослідженням на основі системи платіжного шлюзу. Організація системи платіжного шлюзу вимагає знати, які ризики безпеки зміняться через хмарну міграцію. Невідомі активи інформаційної системи створюють загрози для організації та роблять аналіз ризиків безпеки неповним. Бізнес-процес у дослідженні залишатиметься постійним, і тому зміни в інфраструктурі мають бути зосереджені на отриманні ресурсів інформаційної системи з внутрішньої та хмарної архітектури.

Система платіжного шлюзу у внутрішній інфраструктурі розміщена у невіртуалізованому середовищі, тоді як хмарна модель базується на технології віртуалізації. Через проблеми конфіденційності розголошувати назву платіжного шлюзу заборонено. Тому подальша назва платіжного шлюзу називається «PayGate».

1.2 Стандарти управління ризиками безпеки

Стандарти управління ризиками безпеки були впроваджені як керівництво для управління ризиками безпеки в інформаційних системах. Існує різна кількість стандартів, які були нещодавно створені та об’єднані з існуючих стандартів.

Оскільки це дослідження ґрунтується на проведенні аналізу ризиків для платіжного шлюзу IT-Grundschutz, PCI DSS і вимоги до конкретних компаній обговорюються окремо від провідних галузевих стандартів, таких як ISO/IEC 27xx і NIST, як показано на рис. 1.1.

Національний інститут стандартів і технологій (NIST) у США опублікував кілька стандартів, пов’язаних з управлінням ризиками безпеки та оцінкою в системах інформаційних технологій. Спеціальна публікація NIST 800-30 є посібником для проведення аналізу ризиків, який пояснює, від підготовки

призначення до підтримки оцінки, а також як оцінка ризику та управління ризиками різних організацій будуть співвідноситись одне з одним [6].

NIST SP 800-39 — це публікація, яка представляє аспекти організації, бізнес-процесу та системного рівня при управлінні ризиком інформаційної безпеки та підтримує кроки, описані в структурі управління ризиками. Крім того, NIST SP 800-53 і NIST SP 800-37 також описують процес управління ризиками та конфіденційність, пов'язану з хмарою [7].

Згідно з Радою стандартів безпеки PCI, стандарт безпеки даних індустрії платіжних карток (PCI DSS) є всесвітнім стандартом для будь-якої організації, яка зберігає, обробляє та передає дані власників карток [8]. Стандарт PCI DSS визначає та розглядає технічні та експлуатаційні аспекти. Система платіжного шлюзу, на основі якої базується дослідження, має бути сумісною з PCI, оскільки вона керує даними кредитної картки.

Стандарт складається з дванадцяти вимог, і важливо мати постійну оцінку для технічного обслуговування. Невідповідність вимогам може призвести до грошових втрат і витоку конфіденційних даних, що залишить організації погану репутацію.

Сімейство ISO/IEC 2700x складається з кількох стандартів, що стосуються систем управління інформаційною безпекою (ISMS) [9]. Стандарт ISO/IEC 27005 спеціально розроблений для підтримки підходів до управління ризиками інформаційної безпеки та узгоджений із основними концепціями, визначеними в ISO/IEC 27001 [10]. Компанія системи платіжного шлюзу в прикладі підтримує стандарт ISO/IEC 27005: 2011. IT-Grundschutz — це стандарт, розроблений у Німеччині, який забезпечує передовий підхід, сумісний зі стандартами ISO 27001, для вдосконалення системи управління інформаційною безпекою (ISMS).

IT-Grundschutz розвинувся з ISO27001 через його технічну адаптацію, тоді як стандарти ISO адаптовані до бізнес-процесів [11].

Стандарт безпеки ISO 27005 має системний підхід до розробки та підтримки процесу управління ризиками інформаційної безпеки. Третя версія, ISO/IEC 27005: 2018, забезпечує основу для ефективного управління ризиками кібербезпеки [12]. Стандарт безпеки має три основні фази в процесі управління

ризиками: ідентифікація ризику, оцінка ризику та оцінка ризику [10]. Стандарт безпеки, який хоче підтримувати організація, залежить від необхідності та вимог організації. Організація, яка розглядатиме процес платіжного шлюзу, має ліцензію на сертифікацію ISO27005. Тому при виборі методу управління ризиками безпеки враховується сумісність з ISO27005.

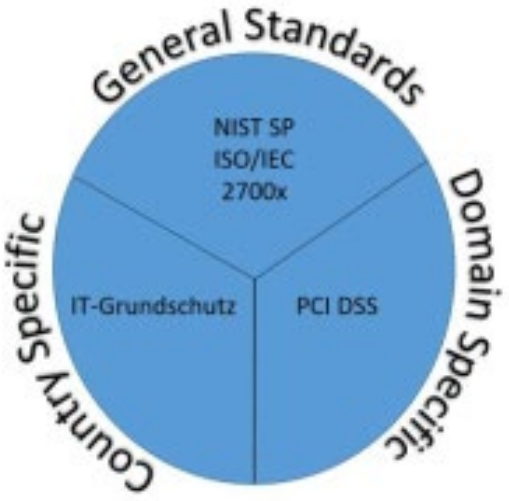

Рисунок 1.1 – Стандарти управління ризиками безпеки [11, 8, 7, 10]

1.3 Методи управління ризиками безпеки

На даний момент існує багато методів управління ризиками безпеки, і абсурдно шукати найкращі, як завжди метод унікальний і має плюси і мінуси. Представлено порівняння методів CORAS [13], MEHARI [5], OCTAVE [18] та ISSRM [5], щоб визначити, що найбільше підходить для цієї конкретної роботи. CORAS є одним із перших методів ризиків безпеки, який має підхід аналізу ризиків, керований моделлю [13].

CORAS узгоджується з ISO 31000 і має мову та метод, які містять практичне та систематичне керівництво. Цей метод в основному складається з 8 кроків: «Початкова підготовка до аналізу, представлення цілі клієнту, уточнення опису цілі за допомогою діаграм активів, затвердження опису цілі, ідентифікація ризиків за допомогою діаграм загроз, оцінка ризиків за допомогою діаграм ризиків і ризиків. лікування за допомогою діаграм лікування», як зазначено в [14]. Він має графічну мову для моделювання ризиків і загроз. Підхід зосереджений на захисті

поточних активів [15], але прямі, непрямі та людські активи також будуть розглянуті під час визначення цілі [16].

Метод узгодженого аналізу ризиків (MEHARI) — це метод управління та оцінки ризиків, розроблений більше двох десятиліть тому. MEHARI — це гнучкий метод визначення контекстних закладів, оскільки його можна застосувати до всієї організації або звузити до бізнес-діяльності. Організації можуть використовувати MEHARI для аудиту, якщо конкретний контекст відповідає процесу СУІS, а також сама конструкція підтримує ISO/IEC 27005. Послуги, інформаційні дані та відповідність нормам є типами активів, які розглядаються в класифікації активів на етапі ідентифікації ризику, крім аналіз ставок [5, 17].

Оперативно критична оцінка загроз, активів і вразливостей (OCTAVE) — це самостійне стратегічне оцінювання на основі ризиків, метою якого є визначення поточного стану практики безпеки в організації. Цей метод ґрунтується на аспектах операційних ризиків і практики безпеки. Він перевіряє стратегічні питання, зосереджується на практиці безпеки та оцінює організацію. Трифазний підхід OCTAVE визначає те, що є важливим для організації за допомогою поточних методів пом’якшення, перевірки рівня інфраструктури для виявлення вразливостей і визначення ризиків для критичних активів.

Малі/середні та великі організації можуть використовувати OCTAVE, оскільки він має два варіанти під назвами OCTAVE -S та OCTAVE-Allegro, які сумісні з великими та малими організаціями [18]. Метод OCTAVE враховує участь співробітників у процесі управління ризиками. Цей підхід використовує критичні активи для визначення та визначення пріоритетів для покращення.

Однак OCTAVE має організаційні та технічні відмінності, які не відповідають стандартам ISO27005, такі як залежність від майстерень, людей і етапів у процесі управління ризиками згідно з [19]. Крім того, він не відображає співвідношення різних ризиків [20].

Управління ризиками безпеки інформаційної системи (ISSRM) складається з моделі предметної області, яка була розроблена шляхом об’єднання стандартів управління ризиками безпеки, управління ризиками безпеки та огляду пов’язаних із безпекою стандартів [5]. ISSRM узгоджується зі стандартами ISO 2700k, а також

враховує системні та бізнес-активи під час управління ризиками безпеки. Метод ISSRM є гнучким, оскільки він не має спеціального інструменту або вбудованої мови моделювання. Порівняння методів управління ризиками, як показано в таблиці 1, показує, який метод є найбільш придатним для порівняння ризиків безпеки у внутрішній і хмарній інфраструктурі.

Таблиця 1.1 – Порівняння методів управління ризиками

Ім’я	Підтримка ISO/IEC 27005?	Моделювання загроз включено?	Розглядаються інфра-структурні компоненти?	Інстру-менти включено?	Мова моде-лювання незалежна?
CORAS	НІ	ТАК	ТАК	ТАК	НІ
MEHARI	ТАК	НІ	ТАК	ТАК	НІ
OCTAVE	НІ	ТАК	ТАК	НІ	
ISSRM	ТАК	ТАК	ТАК	НІ	ТАК

ISO 27005 не містить конкретного методу управління ризиками, і організації можуть вільно обирати власний метод, який підтримує ISO 27005 у щоб відповідати стандарту. Підходи CORAS і OCTAVE мають схожість, але обидва не підтримують стандарти ISO 27005. Одним із основних фактів, які слід враховувати при виборі підходу управління ризиками, є те, чи враховуються бізнес-активи та допоміжні активи. OCTAVE розглядає як організаційні, так і технічні активи, але основна увага приділяється критичним активам. Тому обидва підходи усуваються як відповідний метод RM. MEHARI відповідає стандартам ISO, але має інструмент на основі Excel. Оскільки дисертація присвячена пошуку прогалин у ризиках безпеки різних інфраструктур, візуалізована діаграма та гнучкість вибору мови моделювання вважаються перевагою. Таким чином, ISSRM обрано як кращий метод управління ризиками для проведення аналізу ризику.

1.4 ISSRM і модель предметної області

Ідентифікація активів є першим кроком, якого слід дотримуватися в більшості методів аналізу ризиків. Однак ідентифікація активів може мати обмеження на основі визначення методу RM. ISO 27005 визначає актив як будь-що, що має цінність для організації, тому допоміжні активи розглядаються.

Ідентифікація та класифікація активів є важливою для розробки безпечної системи та зменшення ризиків безпеки. Як показано на рис. 1.2, першим кроком процесу ISSRM є визначення контексту та активів. Після цього необхідно визначити ціль безпеки бізнес-активу на основі тріади конфіденційності, цілісності та доступності (CIA). Аналіз і оцінка ризиків проводяться, щоб визначити, що може завдати шкоди активам і загрожувати цілям безпеки. Перші три кроки будуть повторюватися, доки не буде зроблено задовільний розподіл перед обробкою ризику, оскільки вирішальним є ретельне визначення ризиків для того, щоб провести ефективне їх лікування/усунення.

На рис. 1.2 показано, як ISSRM відповідає структурі ISO27005, що підтверджує придатність для проведення RA для цієї роботи.

Відповідно до ISO 27005 завершення ідентифікації та оцінки ризику вважається аналізом ризику, а оцінка ризиків робить оцінку ризику повною. Визначення цілі безпеки можна розглядати в ISSRM як окремий крок на додаток до кроків, представлених у структурі ISO 27005.

ISSRM має модель предметної області, яка містить три концепції, пов’язані з активами, ризиками та обробкою ризиків, як показано на рис. 1.3 [5]. Наступні параграфи, які пояснюють концепції ISSRM, базуються на [5]. У концепції, пов’язаній з активами, активом вважається все, що є корисним для організації для досягнення цілей. В ISSRM активи поділяються на бізнес-активи та активи інформаційної системи. Цілі безпеки будуть визначені відповідно до конфіденційності, цілісності та доступності бізнес-активу з використанням показників вартості, тоді як інформаційні активи є допоміжним активом для бізнесу.

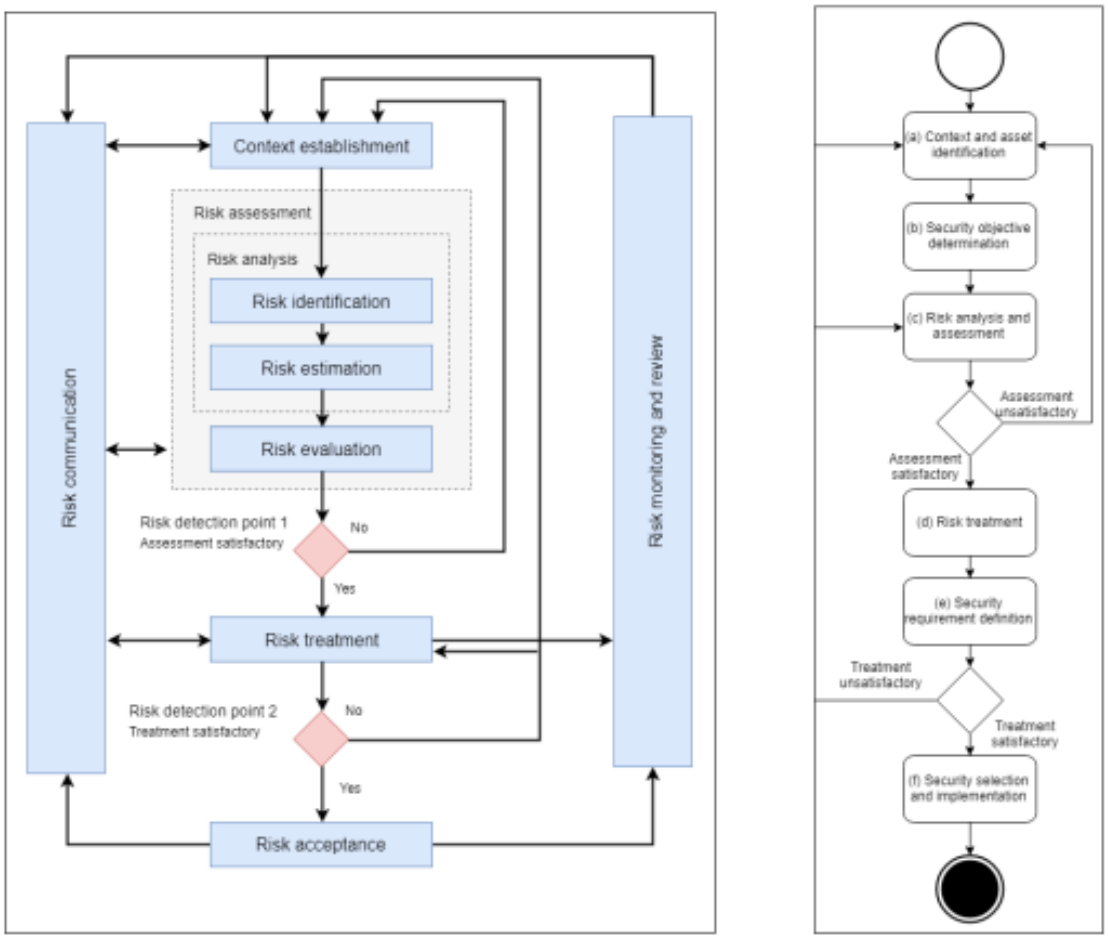

Рисунок 1.2 – Структура ISO27005 [21] ліворуч і ISSRM [5] праворуч

Якщо будь-яка інформація, процес, можливості чи навички потрібні для бізнесу, їх можна класифікувати як бізнес-актив. Інфраструктура, програмне забезпечення разом із людьми, задіяними в системі, вважаються активом IS. Концепції, пов’язані з ризиком, ілюструють, як один або більше активів в організації можуть мати несприятливі наслідки ризику через комбінацію загроз, застосованих агентом загроз щодо однієї чи кількох вразливостей в інформаційній системі.

Потенційні негативні наслідки можуть вплинути як на бізнес-активи, так і на інформаційні активи прямо чи опосередковано, оскільки витік даних агентом загрози може вплинути на конфіденційність інформації про клієнта в системі. Для оцінки ризику використовується метрика рівня ризику, яка залежить від рівня впливу та потенціалу події.

Третя концепція доменної моделі ISSRM, «пов’язана з обробкою ризиків», описує лікування ідентифікованих ризиків безпеки. Рішення може бути

уникнення ризику, зменшення ризику, передача ризику або утримання ризику, і це рішення буде прийнято на основі вимог безпеки організації.

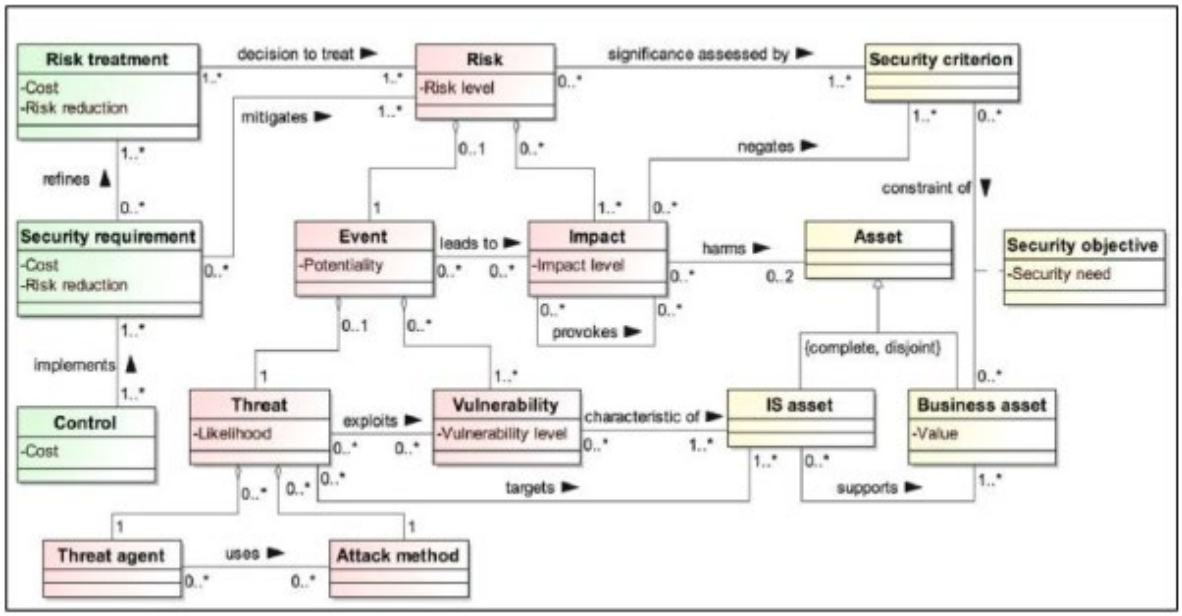

Рисунок 1.3 – Модель домену ISSRM [5]

1.5 Мови моделювання

Моделювання системи допомагає організаціям самостійно оцінити вимоги та повноту складної системи, маючи при цьому чітке розуміння проблем, які були неясними на початкових етапах. Крім того, він підтримує порівняння вимог і візуалізацію зв’язків окремих об’єктів на різних рівнях, таких як бізнес, рівень інформаційних технологій [5]. Модель та нотація бізнес-процесів (BPMN) — це мова моделювання бізнес-процесів, яка має набір правил, визначених для зв’язування об’єктів з різними значеннями.

Сам BPMN не створений для моделювання ризиків безпеки. Однак дослідження [22] показує, що BPMN може бути сумісним з моделлю домену ISSRM для визначення контексту та активів в управлінні ризиками безпеки. У цій дипломній роботі йдеться про порівняння змін ризиків безпеки, які можуть виникнути внаслідок міграції. Діаграма бізнес-процесу, заснована на BPMN, матиме лише обмежену кількість активів IS, оскільки метою BPMN є моделювання бізнес-потоку. Тому візуалізація бізнес-процесу, зіставленого з базовою інфраструктурою, є важливою для ідентифікації активів IS та зв’язку з

бізнес-процесами для проведення аналізу ризиків. Архітектура підприємства (EA), концепція, яка демонструє IT-інфраструктуру та її узгодження з бізнесом [23].

TOGAF — це фреймворк EA для розробки корпоративних архітектур [14]. У статті [24] автори описали концептуальне узгодження TOGAF і доменної моделі ISSRM. Однак TOGAF є незалежною структурою, яка не додається до жодної мови моделювання архітектури підприємства [14].

Але ArchiMate — це мова моделювання EA, яка може візуалізувати різні домени, і вона добре узгоджена зі структурою TOGAF [15]. Як показано на рис. 1.4, ArchiMate 2.1 має трирівневе представлення, яке складається з бізнес-рівня, прикладного рівня та технологічного рівня. Трирівневий вигляд ArchiMate 2.1 використовується, щоб показати відображення рівня бізнесу та IT через прикладний рівень.

На рис. 1.4 представлено три аспекти, які можна моделювати за допомогою ArchiMate. Активна структура представляє компоненти рівня, а аспект поведінки представляє послуги, які пропонує кожен рівень. Такі об’єкти, як бізнес-об’єкти, технологічні артефакти та об’єкти даних у програмі, представлені за допомогою активної структури. Здатність моделювати бізнес і технології ArchiMate використовується в дослідженні для виявлення архітектурних відмінностей між внутрішньою та хмарною технологією та для проведення моделювання загроз для активів IS.

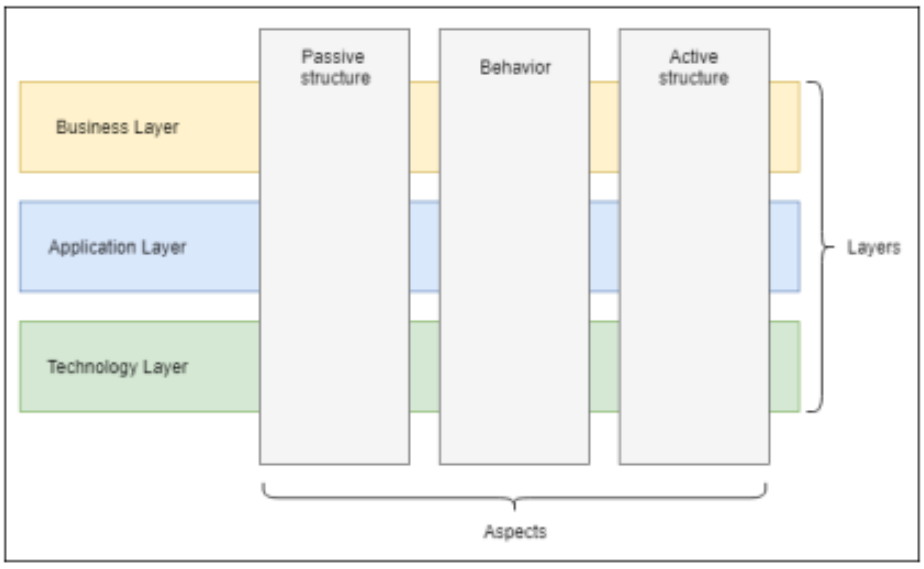

Рисунок 1.4 – ArchiMate Core Framework, адаптовано з [25]

Існує обмежена кількість мереж моделювання мови, доступні для моделювання інфраструктури, такі як CySeMol [26], UML Class diagrams і SecuriLang. Програмні системи, доступні для CySeMol, застаріли, і SecuriLang створено шляхом вдосконалення мови CySeMol [27]. Інструмент SecuriCAD, розроблений Foreseeti [23], використовує мову моделювання інфраструктури SecuriLang і може бути використаний для ілюстрації низькорівневого перегляду компонентів інфраструктури та взаємозв'язків об'єктів [28]. Однак у інструменті SecuriCAD є помилки розробки, про які повідомлялося під час дослідження. Підсумовуючи, під час дослідження використовується лише моделювання BPMN та ArchiMate.

1.6 Моделювання загроз

Інформаційні системи взаємодіють з іншими системами і можуть працювати в кількох інфраструктурах різними групами користувачів. Усі активи IS не мають однакового рівня важливості, оскільки системні вимоги та цілі можуть відрізнятися. Не можна розглядати однакове ставлення до всіх активів системи як хороший підхід до управління ризиками безпеки. Процесам, які зберігають важливу інформацію, потрібно приділяти більше уваги. Таким чином, компанія повинна визначити пріоритетність активів на основі вимог компанії.

Техніка безпеки зосереджена на зменшенні несанкціонованої шкоди, яка спрямована на актив. Переважно увагу до безпеки та ризиків не враховували на ранніх стадіях розробки системи [22]. Відповідно до [5] ризик визначається як «Поєднання загрози з однією або декількома вразливими місцями, що призводить до негативного впливу на два або більше активів шляхом їх пошкодження».

Тому визначення можливих загроз для активів є необхідністю. Було проведено опитування [29] щодо різних підходів до моделювання загроз, де деякі присвячені методам управління ризиками, а деякі не пов'язані з конкретним методом управління ризиками. Дерева атак, CORAS, STRIDE – це деякі з методів моделювання загроз, які розглядалися в опитуванні. Методологія моделювання загроз STRIDE була винайдена Л. Конфельдером і П. Гаргом [30] і існує в галузі з

1999 року. Попереднє дослідження [31] про управління ризиками в системі електронної комерції застосовувало STRIDE як модель загроз для виявлення загроз дотримуючись ISSRM, і він продемонстрував сумісність використання STRIDE разом з ISSRM.

Тому ідентифікація загроз у цьому дослідженні базуватиметься на STRIDE. STRIDE можна використовувати, щоб зосередитися на процесорах, даних і сутностях. Таксономія STRIDE дає змогу ідентифікувати загрози в системах, класифікуючи їх на шість типів загроз. У таблиці 1.2 наведено категорії STRIDE та їхні описи.

Таблиця 1.2 – Категорії загроз STRIDE [30]

Категорія загрози	Порушення властивості безпеки	Опис
Spoofing	Authentication	Видавати себе за щось або когось, чого не призначено
Tampering	Integrity	Зміна чогось в інфраструктурі або процесі
Repudiation	Non-repudiation	Стверджувати, що хтось або щось не несе відповідальності за дію, яка сталася.
Information disclosure	Confidentiality	Розкриття інформації особам, які не мають права
Denial of service	Availability	Зробіть послуги недоступними, заборонивши, погіршивши або використовуючи ресурси, щоб зробити послугу недоступною
Elevation of privilege	Authorization	Виконання конкретної справи, яку сторона не має на меті робити

Дослідження [32] пропонує новий підхід до оцінки ризику за допомогою ЕО. Метою роботи є подолання розриву між технічними та бізнес-поглядами систематичної оцінки ризиків безпеки. За допомогою запропонованого підходу автор спробував зменшити складність бізнес-процесу підтримки активів, проілюструвавши абстракцію, яка показує взаємозалежність кожного рівня. Це дослідження описує узгодження ЕА від ідентифікації активів до обробки ризиків.

Проте дослідницька робота не була реалізована в кейс-стаді. Аналіз загроз хмарних обчислень описано в кількох статтях, у тому числі в тих, які проводять кількісний і якісний аналіз. У статті [33] автори представляють моделювання загроз для хмарної інфраструктури. Намір дослідження полягає в тому, щоб надати потенційні загрози та методи пом'якшення для хмарної інфраструктури, оскільки не було проведено багато досліджень щодо моделювання інфраструктурних загроз, хоча хмарні обчислення є тенденцією.

Дослідження зосереджено на кількох методах моделювання та вимірювання загроз, застосованих до реальної хмарної інфраструктури. Дерева атак, графіки атак і аналіз поверхні атак — це методи моделювання загроз, які використовували автори. Цей документ допомагає постачальникам хмарних технологій визначити та посилити безпеку хмари. Однак моделювання бізнес-рівня і взаємозалежність бізнесу та інфраструктури не представлена в цьому дослідженні. У дослідженні [34] було проведено ідентифікацію загроз на основі STRIDE у хмарі. Мотивація авторів для написання цієї статті полягає в тому, щоб представити загрози та ризики на основі хмари.

Але автор не враховує вплив на активи. Крім того, цей документ базується на узагальнених загрозах у хмарному середовищі. Дослідницька робота [35] «Управління ризиками безпеки в авіаційному транспортному секторі» — це дослідження, яке використовувало ISSRM для аналізу співпраці між організаціями. Автор змоделював бізнес-рівень і дотримувався моделі домену ISSRM, але в цій роботі неможливо побачити видимість інфраструктури, пов'язаної з бізнес-рівнем. Автор зазначив, що аналіз загроз безпеці в корпоративній співпраці, що підтримується хмарою, є майбутньою роботою.

У роботі [36] запропоновано метод аналізу ризиків віртуалізованих систем. Автор продемонстрував, наскільки корисно проводити оцінку ризиків не лише для інфраструктури, але й для процесу. Однією з наукових новизни дисертації є введення числової процедури поєднання оцінок експлойтів та їх ймовірностей. Поглиблений аналіз загроз у системах віртуалізації з різних точок зору мав додаткову цінність на етапі оцінювання. Хмарні обчислення є однією з основних форм віртуалізації, і для клієнта, якому потрібно порівняти, як може змінитися ризик у віртуалізованому середовищі та внутрішній інфраструктурі. Детальний опис представлення зв'язків компонентів і завдань різних рівнів не висвітлювався.

Автор статті [37] використовував ArchiMate для моделювання архітектури підприємства для управління ризиками безпеки. Метою автора було представити узгодження EA з SRM. Автор лише показав відображення високого рівня, але низькорівневе моделювання кожного рівня та зв’язку між бізнес-активами та пов’язаними з ним інформаційними активами не було центром уваги. Попередні дослідження [14] описують складність інформаційної безпеки RM та необхідність інтеграції моделювання EA з ISSRM. Мета статті полягає в тому, щоб розширити модель домену ISSRM як структуру, яка складається з методу, мови та інструменту.

TOGAF використовувався як структура EA, і узгодження ISSRM разом із TOGAF чітко описано шляхом підкреслення взаємозв’язків обох концепцій. Основна увага була зосереджена на інтеграції двох моделей, і це не застосовувалося до реального сценарію. Автори не представили можливості використання EA та ISSRM для оцінки ризику. У цьому дослідженні використовується інтеграція концепцій, пов’язаних з активами. Дослідницька робота [38] демонструє моделювання концепцій безпеки та відповідних зв’язків з архітектурою підприємства.

Також було описано сумісність ArchiMate з фреймворками EA. У дослідженні не представлено підхід до управління ризиками, розглянутий у роботі, навіть якщо моделі проектування, пов’язані з концепціями ризиків, представлені належним чином. Дослідження, пов’язані з хмарною інфраструктурою, аналізом ризиків і моделюванням загроз, проводилися в

минулому. Але під час огляду літератури було виявлено відсутність підходу до аналізу ризиків на основі EA для порівняння інфраструктур.

Тому дослідження буде зосереджено на тому, як можна використовувати аналіз ризиків безпеки на основі EA для порівняння змін ризиків безпеки між різними інфраструктурами. Крім того, це дослідження базується на реальній реалізації.

Таблиця 1.3 – Обрані категорії для аналізу

Категорія	Назва вибраного методу / мова / тип / діаграма
Метод управління ризиками	ISSRM
Тип активів	Бізнес та IC активи
Типи інфраструктур	Внутрішня інфраструктура та хмарна інфраструктура
Мова моделювання бізнес-процесів	BPMN
Бізнес-актив і картографування інфраструктури структура	TOGAF
Мова відображення бізнес-активів та інфраструктури	ArchiMate з використанням програмного забезпечення Archi
Метод моделювання загроз	STRIDE

В загальному розділі представлені теоретичні основи методологій і стандартів управління ризиками безпеки. Було проведено порівняння, щоб визначити найбільш прийнятну методологію управління ризиками, і ISSRM було обрано завдяки системному підходу та категоризації різних концепцій у моделі домену. Ця теза проілюструє, як зміни в інфраструктурі вплинуть на процес аналізу ризиків. Оскільки ISSRM не залежить від мови моделювання, для моделювання бізнес-процесу було обрано BPMN. ArchiMate буде використовуватися для моделювання архітектури підприємства, а взаємозв’язок між рівнями буде представлено через модель ArchiMate EA. Методологія

моделювання загроз STRIDE використовується для аналізу загроз традиційної внутрішньої інфраструктури та хмарної інфраструктури. У таблиці 3 узагальнено обрані підходи для порівняння ризиків безпеки у внутрішній інфраструктурі та хмарній інфраструктурі.

1.7 Висновок до першого розділу

В першому розділі кваліфікаційної роботи освітнього рівня «Магістр» описано описано вступ до проблеми, мотивацію дослідження та обсяг дослідження. Звіти були проаналізовані, щоб дізнатися статистику та минулі тенденції, щоб підтвердити важливість досліджень.

2 АНАЛІЗ ІДЕНТИФІКАЦІЯ АКТИВІВ СИСТЕМИ ПЛАТІЖНИХ ШЛЮЗІВ

2.1 Система платіжних шлюзів

Підрозділ зосереджений на наданні відповідей на питання: «Які архітектурні відмінності між внутрішньою інфраструктурою та хмарною інфраструктурою?». Воно підтримується трьома підпитаннями, і в розділі описуються архітектурні відмінності між домашньою і хмарною інфраструктурою.

ЗП 1. 1: Яка внутрішня інфраструктура системи платіжних шлюзів?

ЗП 1. 2: Що таке хмарна інфраструктура системи платіжного шлюзу?

ЗП 1. 3: Що можна використовувати для моделювання внутрішньої та хмарної інфраструктури?

Інформаційно-комунікаційні технології (ІСТ) сягають корінням у різноманітні галузі, одним із прикладів яких є електронна комерція. Електронна комерція відкрила ворота для торговців і покупців, надаючи можливість купувати і продавати без будь-яких географічних кордонів. Коли кількість пристроїв для електронної комерції зросла, була створена програма для обробки платежів, яка виступає посередником для фінансових установ і продавців. Аналіз ризиків безпеки дослідження базується на цьому посереднику, яким є платіжний шлюз. Система – це група компонентів, які взаємодіють і з'єднуються для досягнення спільної мети [5]. У таблиці 2.1 представлені приклади компонентів системи в системі платіжного шлюзу.

Дослідження базується на системі платіжного шлюзу PayGate. PayGate надає послуги більш ніж у 21 країні ЄС, і 110 продавців використовують багатоканальне платіжне рішення. Наявність процесу платіжного шлюзу важлива для безперебійного обслуговування клієнтів, крім захисту конфіденційності та цілісності інформації та процесів. Платіжні шлюзи класифікуються на основі методу інтеграції, який вони використовують для зв'язку з продавцем. Хостинг і саморозміщення є методами інтеграції платіжних шлюзів [39].

Таблиця 2.1 – Платіжна шлюзова система.

Системні компоненти	Приклади вивчення проблеми
Продукт/Компоненти	База даних, інтерфейс PayGate, система обробки платежів
Інфраструктура	Сервери веб-додатків, балансувальники навантаження, брандмауери, мережа та пристрої
Застосування	Додаток PayGate і додаток для шахрайства
Персонал інформаційних технологій	Підтримка додатків, підтримка БД, розробник
Користувачі - внутрішні	Продавець інтернет-магазину
Користувачі - Зовнішні	Клієнт інтернет-магазину
Навколишнє середовище	Європа

Хостинговий платіжний шлюз.

Хостинговий платіжний шлюз перенаправляє клієнта до системи постачальників платіжних послуг для введення платіжних відомостей під час оформлення замовлення. Платіжні дані не фіксуються веб-магазином через це перенаправлення. Розміщення iframe платіжного шлюзу в торговельному магазині є альтернативою для переспрямування на сторінку постачальника платіжних послуг (PSP) під час оформлення замовлення. Оскільки клієнт надає інформацію про кредитну картку безпосередньо системі платіжного шлюзу, сайт електронної комерції не вимагає відповідності PCI. Приклади: PayPal, 2Checkput і Payza.

Самостійний платіжний шлюз.

У самостійних платіжних шлюзах веб-магазин збирає платіжні дані клієнта під час оформлення замовлення. Інтеграція API використовується для надсилання веб-магазином отриманого запиту платіжної інформації до платіжного шлюзу. Тому клієнт не вводитиме платіжні дані безпосередньо в платіжному шлюзі.

Технічна інфраструктура.

Технічна інфраструктура існує на основі поєднання таких компонентів, як програмне забезпечення, мережа, апаратне забезпечення та люди. Організація PayGate планує перенести систему платіжного шлюзу в хмарну інфраструктуру. Тому проводиться детальний аналіз поточної інфраструктури, щоб знайти зміни в архітектурі перед міграцією в хмару.

Інфраструктура внутрішнього платіжного шлюзу.

Дослідження інфраструктури PayGate базується на тих самих передумовах, що й організація. Інфраструктура є невіртуалізованою і складається з маршрутизаторів, брандмауера веб-додатків, апаратного модуля безпеки, сховищ даних і балансувальника навантаження. Середовище даних власників карток було відокремлено від систем керування замовленнями, перевірки на шахрайство та підтримки продавців. Інфраструктура, яка розглядатиметься в цій дисертації, складається з фізичних і логічних відділів, розміщених у приміщеннях підприємства.

Співробітники організації платіжного шлюзу здійснюють обслуговування та управління серверами. Поточна інфраструктура зберігає інформацію про кредитні картки понад сотні торгових служб, а платіжний шлюз існує на ринку близько п’яти років. Деталі інфраструктури системи PayGate були зібрані шляхом опитування експертів домену.

Крім того, були проаналізовані карти мереж, деталі апаратного забезпечення, брандмауер веб-додатків (WAF) і попередні звіти про вразливості. Внутрішній інфраструктурний брандмауер веб-додатків — це програмний брандмауер, налаштований за допомогою Apache ModSecurity.

Апаратний модуль безпеки на схемі і фізичний пристрій, що використовується для криптообробки [40]. Цей модуль підключено до сховища даних, де зберігаються платіжні реквізити. У системі платіжного шлюзу внутрішні додатки розробляються співробітниками PayGate, а сторонні додатки стосуються таких додатків, як додаток для шахрайства, який використовується в середовищі для перевірки легітимності клієнта.

Правилами шахрайства керує PayGate. У середовищі є два типи брандмауерів, одна категорія базується на програмному забезпеченні, а друга – на

апаратному забезпеченні. Оскільки це середовище PCI, щокварталу проводиться сканування вразливостей. Однак не існує автоматизованого механізму авторизації доступу людей до серверної кімнати, і цей доступ контролюється охоронцем. Відеоспостереження доступне як частина вимоги PCI, і це ще система виявлення вторгнень.

Хмарна інфраструктура.

Прийняття та використання хмарних обчислювальних технологій значно зросло з кінця 2000-х років із великим заохоченням таких компаній, як Google, Amazon, Microsoft, IBM і Rack space, як видно з їхніх хмарних рішень [41]. Підприємствам, які переходять до хмарних центрів обробки даних, не потрібно купувати й підтримувати великі IT-технології на місці, а замість цього отримувати доступ до цих IT-ресурсів із віддаленого місця, яким часто керує постачальник хмарних послуг.

Хмара поділяється на три основні моделі, такі як інфраструктура як послуга (IaaS), програмне забезпечення як послуга (SaaS) і платформа як послуга (PaaS). У IaaS постачальник послуг надасть доступ до обчислювальних ресурсів у віртуальному середовищі, дозволяючи клієнту отримати доступ до обчислювальних ресурсів із пулу апаратних ресурсів. Ці ресурси можна розподілити, щоб забезпечити надійність і уникнути єдиної точки збою. Замовник несе відповідальність за встановлення необхідного програмного забезпечення, додатків і внутрішніх роздільників брандмауера [42].

Більшість хмарних рішень базуються на гіпервізорах типу 1, а віртуальні машини побудовані на цих гіпервізорах. Такі ресурси, як центральний процесор, пам'ять і мережа, використовуються різними клієнтами. Політики та процедури щодо обслуговування обладнання є важливими, а чіткий розподіл обов’язків дозволить уникнути загроз для систем. Приклад: загроза через невиправлений гіпервізор може створити загрозу безпеці для всіх віртуальних машин на хості. У PaaS клієнти отримують можливість самостійно розробляти, розгортати та керувати додатками на попередньо встановленій платформі або за допомогою необхідних інструментів. Оскільки платформа залежить від сервісно-орієнтованої

архітектури, проблеми, пов’язані з цією архітектурою, такі як DOS, XML-атаки, ін’єкції, будуть автоматично успадковані.

У SaaS клієнт отримає вбудовані програми, розміщені в інфраструктурі постачальника послуг. Ця послуга доступна через Інтернет і розміщена на платформі. Основні контрзаходи безпеки, за які повинні відповідати постачальники послуг, це те, що вони повинні підтримувати відповідні виправлення програм і правильно налаштувати веб-конфігурації. Однією з ключових відмінностей між IaaS, PaaS і SaaS є рівень контролю, який клієнт має в хмарному стеку, на відміну від рівня контролю хмарного постачальника.

Спільне використання ресурсів і межі розгортання базуватимуться на моделі хмарного розгортання. Публічна хмара є економічно ефективним рішенням порівняно з приватними, спільнотними та гібридними моделями розгортання. Звіти показують, що міграція підприємства в хмару зростатиме протягом наступних двох років [3].

Тому в роботі розглядається модель публічного розгортання. Відповідно до NIST SP 800-145 [58], «клієнт хмари не керує базовою хмарною інфраструктурою та не контролює її, але має контроль над операційними системами, сховищем і розгорнутими програмами; і, можливо, обмежений контроль вибраних мережевих компонентів (наприклад, брандмауери хоста)».

На рис. 2.1 показано, які типи систем повинні бути забезпечені постачальником хмарних послуг з точки зору безпеки. Крім того, динамічний характер середовища IaaS (наприклад, зі створенням, видаленням і міграцією віртуальних машин) створює більше проблем для захисту від кібератак на систему. Концепція хмари та її використання в галузі не нова, але обов’язки повинні бути чітко визначені постачальником хмарних послуг і клієнтом, щоб визначити, хто повинен захистити систему IS від загрози. Однак обов’язки можуть залежати від моделі розгортання або архітектурної моделі [43]. На малюнку 5 показано резюме спільної відповідальності замовника та постачальника хмарних технологій.

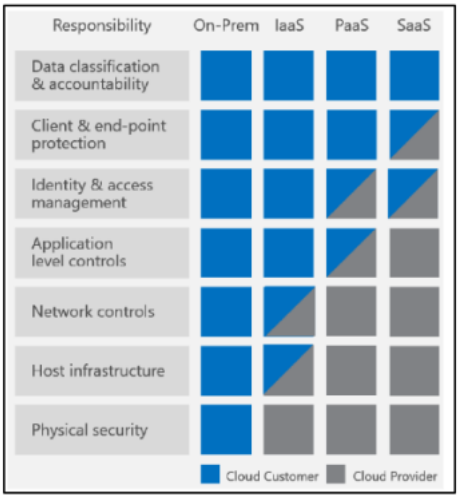

Рисунок 2.1 – Спільна відповідальність замовника хмари та постачальника хмари [44]

Корпоративна архітектура системи платіжного шлюзу.

Архітектура організацій є складною через розподілену природу та інтеграцію сучасних технологій. Архітектура в основному є структурою з чітким сприйняттям, яка представляє взаємозалежності та взаємозв'язки бізнес-процесів та інформаційних систем [45]. Можливість систематичного моделювання EA допомагає фіксувати динамічні зміни інфраструктури та залежностей. Таким чином, інфраструктура системи платіжного шлюзу перед міграцією та після міграції моделюється за допомогою мови моделювання EA під назвою ArchiMate 2.1.

Як показано на рис. 2.2, модель ArchiMate EA містить три рівні: бізнес-рівень, прикладний рівень і технологічний рівень. Бізнес-рівень містить бізнес-послуги та бізнес-процеси. Програма є проміжним рівнем, оскільки вона підтримує бізнес-процеси та послуги, надаючи програмні послуги, і ці послуги розміщені на технологічному рівні. Технологічний рівень містить апаратне забезпечення, мережеві компоненти та засоби, а також пропонує послуги, необхідні для запуску програм. Внутрішній EA та хмарний EA моделюється для визначення змін архітектурних компонентів а знайти зв'язки між бізнес-процесом та інфраструктурою. Було зроблено припущення, що завдання бізнес-процесу залишилися незмінними, а інфраструктура буде змінена.

В обох стандартах ISSRM і ISO 27005 «люди» вважаються активом IS, і їх можна розділити на внутрішні та зовнішні сторони.

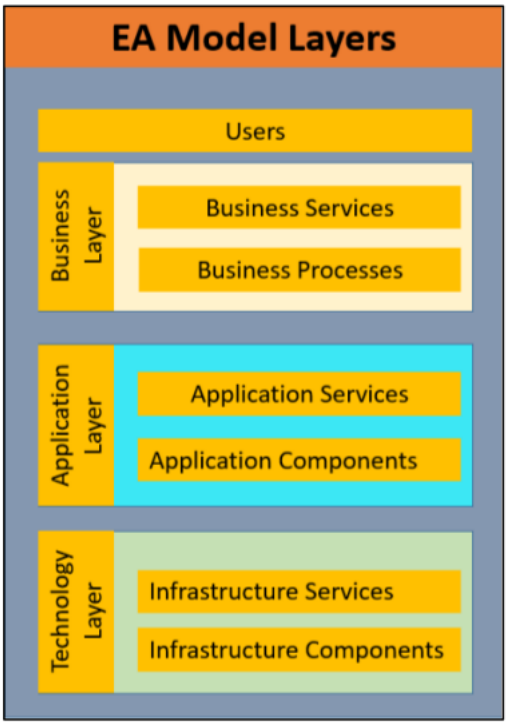

Рисунок 2.2 – Рівні моделі EA [38]

Внутрішня корпоративна архітектура системи PayGate.

Аналіз середовища даних власника картки в PayGate допоміг ідентифікувати основні процеси та їх підпроцеси. Відповідно до вимог та зібраної інформації було змодельовано три шари. Бізнес-рівень дає огляд з точки зору бізнесу, а технологічний рівень на рис 2.3 представляє інфраструктурні компоненти внутрішньої системи платіжного шлюзу. Абстракція першого рівня технологічного рівня, як показано на рис. 2.3, була змодельована за допомогою мережевої карти середовища. Взаємозалежності між бізнес-рівнем і технологічним рівнем були змодельовані після ретельного аналізу. Нижче наведено приклад того, як моделювання EA полегшить пошук базової технології бізнес-процесу та, отже, визначення відповідних активів IC.

Приклад: Клієнт (група користувачів) отримує «Прийняти платежі за замовлення» (бізнес-сервіс) від процесу платіжної операції (процесу на бізнес-рівні), а додаток платіжного шлюзу та програми керування замовленнями

використовуються для надання даних кредитної картки процесу, підключення PSP і «процесу». інформація про замовлення» додатки для процесу платіжної операції.

Ці програми безпосередньо пов’язані зі службами технологічного рівня, такими як платіжний шлюз, генерація журналів, служби баз даних і служби розміщення програм. Інфраструктурою, яка надає ці послуги, є зона підтримки, ферма серверів додатків і веб-магазин.

Діаграми на рис. 2.3 ілюструють абстракцію високого рівня внутрішнього EA системи платіжного шлюзу.

На рис. 2.3 модель внутрішньої інфраструктури EA представляє п’ятьох учасників. Бізнес-рівень складається з бізнес-сервісів і бізнес-процесів. У системі платіжного шлюзу на бізнес-рівні представлено чотири бізнес-процеси. Це процес платіжних операцій, повторюваний процес, процес відшкодування та процес підтримки продавця. Ці чотири бізнес-процеси не мають доступу до одного технологічного компонента чи програм. У анотації показано, як ці процеси пов’язані з технологічним рівнем. Є чотири програми, розміщені на прикладному рівні. Керування замовленнями має власну програму, але в основному пов’язану з програмою PayGate. Додатки для боротьби з шахрайством і програми підтримки продавців не розробляються компанією PayGate, але вони повністю контролюють конфігурацію програми.

Устаткування, мережа та засоби представлені, але не відображають усі компоненти чи зв’язки, оскільки це діаграма високого рівня. Інженер із підтримки інфраструктури та охоронець зіставляються лише з процесом транзакцій paymenet. Ці два актори також мають бути пов’язані з іншими процесами. Однак посилання не були представлені, щоб зменшити надмірну складність діаграми. Резервне сховище не підключено до внутрішнього зв’язку, оскільки воно зберігається окремо.

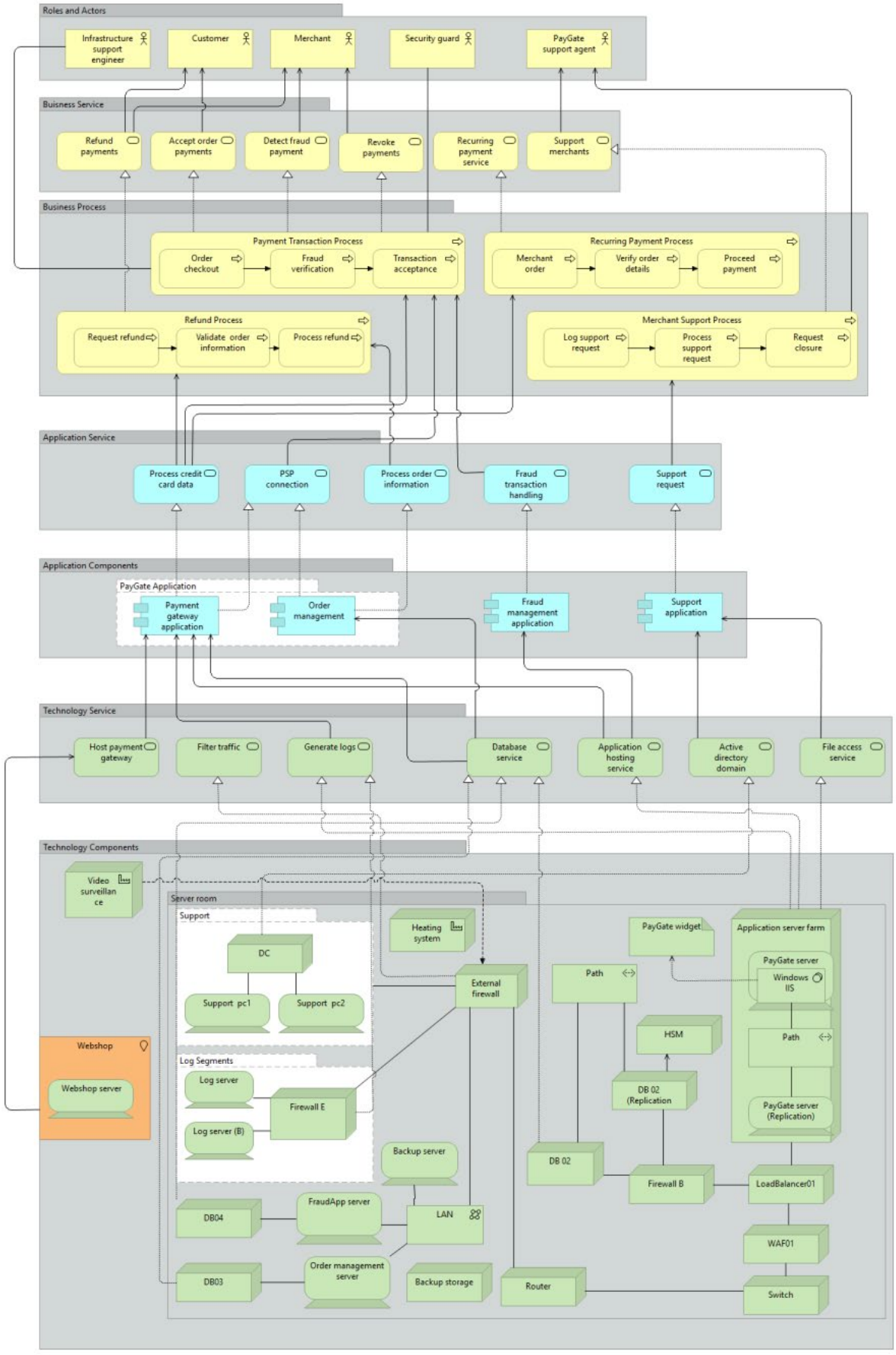

Рисунок 2.3 – Модель внутрішньої інфраструктури ArchiMate.

На рис. 2.4 представлено абстракцію хмарного центру обробки даних та інтеграцію з бізнес-процесами PayGate.

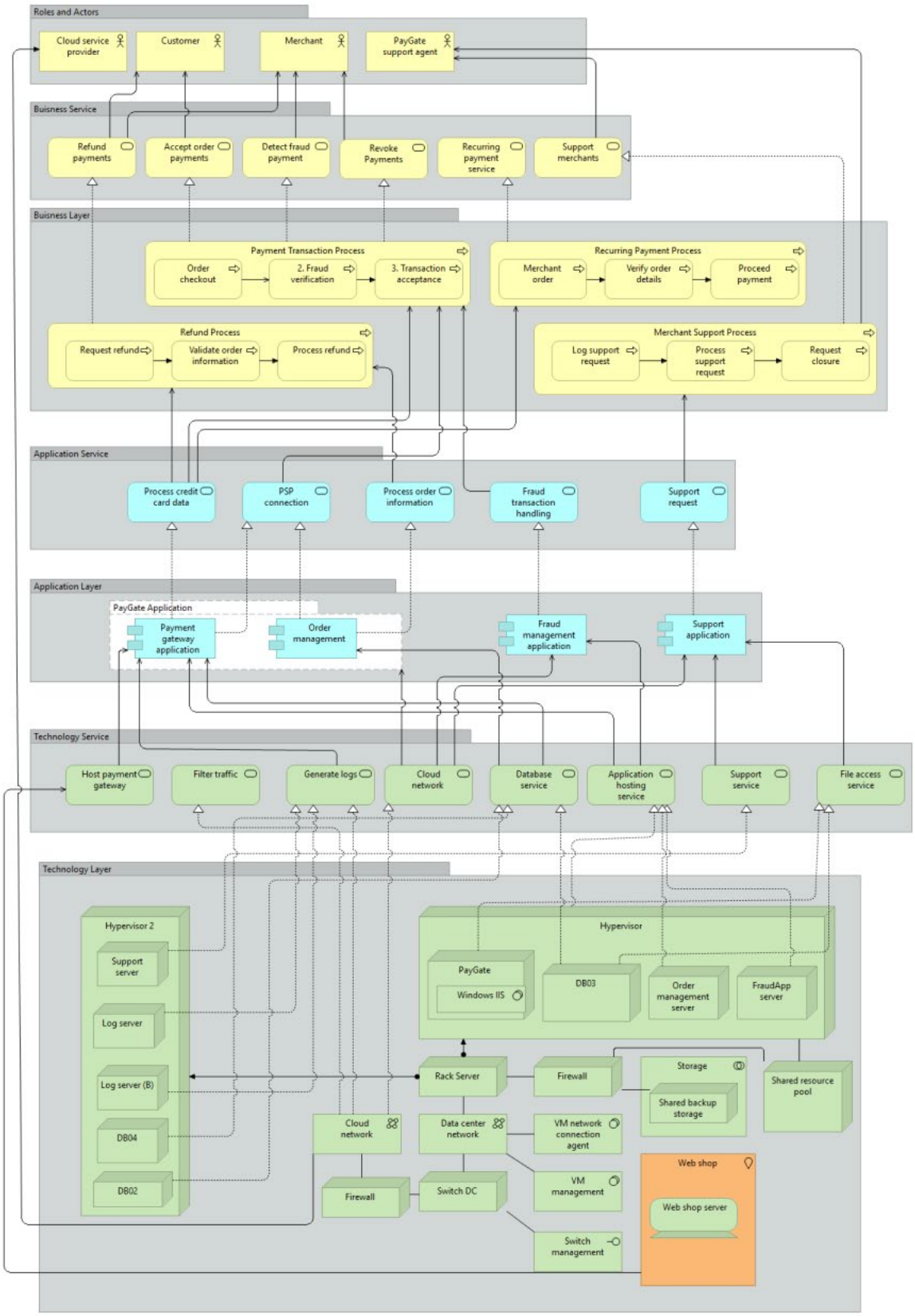

Рисунок 2.4 – Модель хмарної інфраструктури ArchiMate

Хмарна корпоративна архітектура системи.

PayGate Рівень хмарної технології 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 тому самому 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.

2.2 Ідентифікація активів системи платіжних шлюзів

Розділ зосереджено на наданні відповідей на питання: «Що таке бізнес-активи та активи допоміжної інформаційної системи?».

Воно складається з трьох підзапитань, і ця глава допомагає отримати бізнес-активи та активи ІС із внутрішньої та хмарної інфраструктури.

ЗП 2. 1: Що використовувати для ідентифікації та виявлення активів у внутрішній та хмарній інфраструктурі?

ЗП 2. 2: Що таке активи внутрішнього центру обробки даних і хмарної інфраструктури?

ЗП 2. 3: Яка безпека потребує бізнес-активів? Ідентифікація активів у певному контексті потребує належного аналізу, оскільки вона представить організаційні активи, які потрібно захистити, і допоможе визначити ціль безпеки кожного бізнес-активу.

Активи, які розглядатимуться в управлінні ризиками, залежать від методу, обраного як визначення активів, а охоплення активів відрізняється від одного методу управління ризиками до іншого. Погана ідентифікація активів і недостатня увага до узагальнених ризиків можуть призвести до потенційної шкоди. Щоб мати кращу видимість бізнес-активів, які варто захищати, у цьому розділі представлено візуалізацію бізнес-процесу. Зв'язок інформаційної системи з бізнес-активами представлений через ArchiMate через прикладний рівень як перша модель абстрактного рівня.

На рис. 2.5 показано, як активи виявляються за допомогою мов моделювання. Розширення процесу платіжних транзакцій здійснюється за допомогою BPMN. Деталі порядку на рис. 2.5 означають, що буде вибрано та змодельовано лише один ресурс із пов'язаними системними активами.

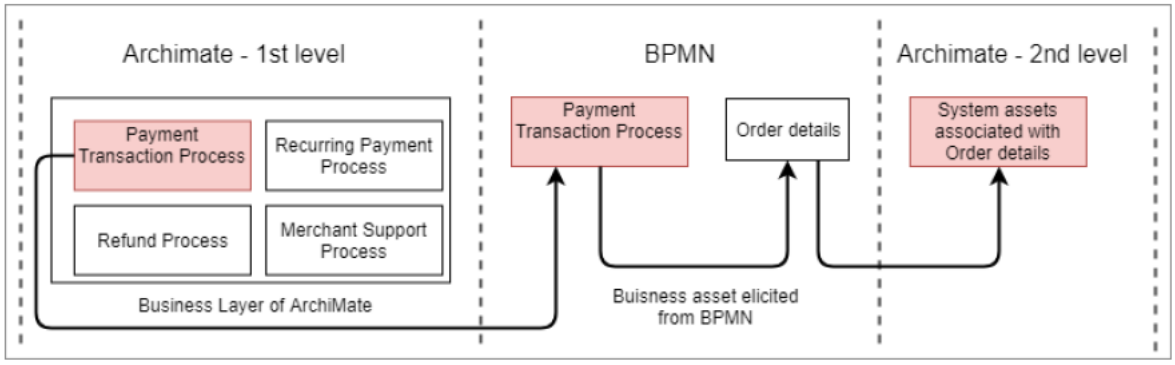

Рисунок 2.5 – Ідентифікація активів на основі моделі

Бізнес-процеси системи платіжних шлюзів.

Процес платіжних шлюзів є сполучною ланкою між клієнтом і фінансовою установою, яка обробляє деталі транзакцій від імені продавця. Продавець надішле запит до компанії платіжного шлюзу з проханням інтегрувати послугу. Приклад заснований на розміщеному платіжному шлюзі, який використовує Widget API.

Система платіжного шлюзу — це комбінація кількох процесів, і недотримання вимог безпеки в одному процесі може призвести до критичної шкоди в інших процесах через взаємозалежності.

На рис. 2.6 показано ланцюжок створення вартості процесу платіжних транзакцій, отриманий від бізнес-рівня архітектури підприємства. Додаток 1 містить діаграму BPMN процесу платіжної транзакції.

Рисунок 2.6 – Ланцюжок створення вартості процесу платіжної транзакції

Процес платіжної транзакції складається з трьох підпроцесів: 1. Оформлення замовлення 2. Перевірка шахрайства 3. Прийняття транзакції.

Процес оформлення замовлення починається, коли клієнт переходить до оформлення. Веб-магазин запитає доступні методи оплати для вибраного магазину від PayGate і надішле відповідь із маркером безпеки, який використовується для унікальної ідентифікації транзакції. Платіжний шлюз iframe буде завантажено пізніше. Це дослідження базується на розміщеному платіжному шлюзі. Клієнт введе інформацію про платіж, і ця інформація буде зашифрована за допомогою AES 256 і надіслана до PayGate.

Веб-магазин не бачитиме дані кредитної картки, оскільки платіжні дані клієнта будуть надіслані в PayGate без передачі їх у веб-магазин. Деталі платежу включають номер кредитної картки клієнта, CVV і дані про закінчення терміну дії. Якщо перевірка платіжних даних пройде, веб-магазин надішле деталі замовлення до PayGate.

Деталі замовлення містять ім’я клієнта, дату народження клієнта, електронну адресу клієнта, адресу доставки, адресу клієнта, ідентифікатор

замовлення, позицію замовлення, кількість і ціну. На рис. 11 показано процес оформлення замовлення. Коли PayGate отримує деталі замовлення з веб-магазину, він надсилає деталі для перевірки в базі даних шахрайства. Перевірка проводиться шляхом порівняння адрес електронної пошти, адрес доставки та минулих записів транзакцій. Якщо клієнт є виявлений як шахрайський, веб-магазин буде проінформовано.

На рис. 2.7 представлено процес перевірки шахрайства. PayGate підключатиметься до рівня PSP, якщо запит надійде до обробки платіжного завдання, як показано на рис. 2.8. Рівень PSP надішле PayGate відповідь про статус транзакції на основі відповіді, отриманої від банку. Якщо платіж був відхилений банком, клієнту буде надіслано сповіщення та відбудеться скасування замовлення. Якщо платіж пройшов успішно, веб-магазин доставляє повідомлення клієнту та сповіщає про процес доставки, який не розглядається в цьому дослідженні. На рис. 2.9 представлено процес прийняття транзакції.

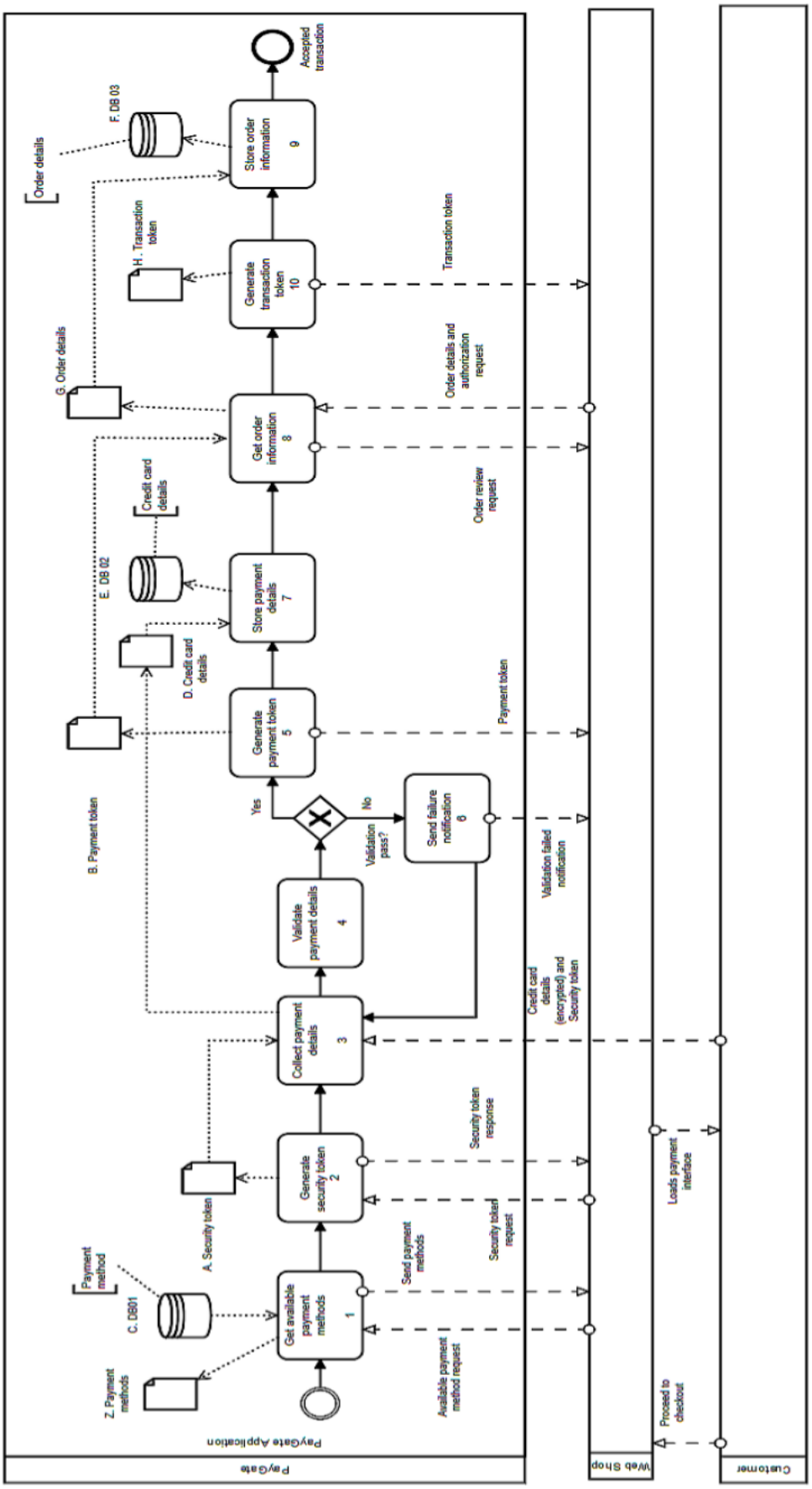

Рисунок 2.7 – Процес перевірки замовлення

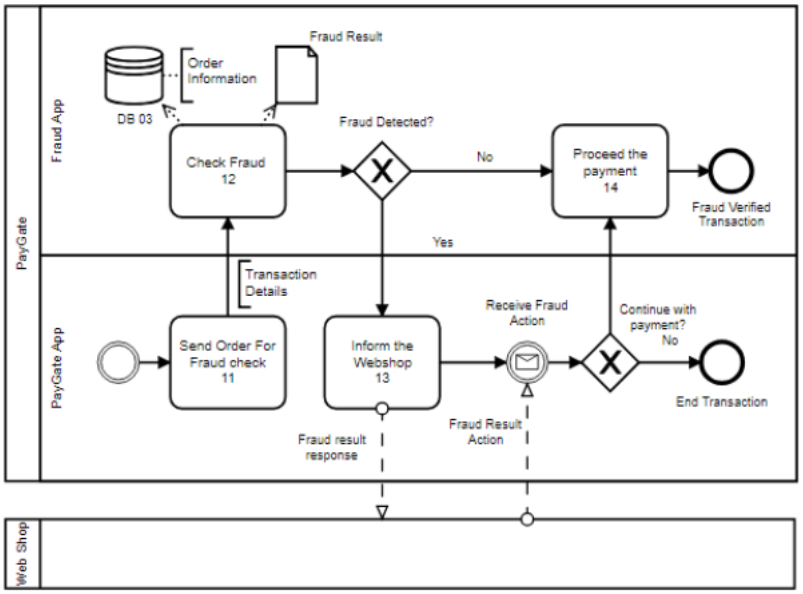

Рисунок 2.8 – Процес перевірки шахрайства

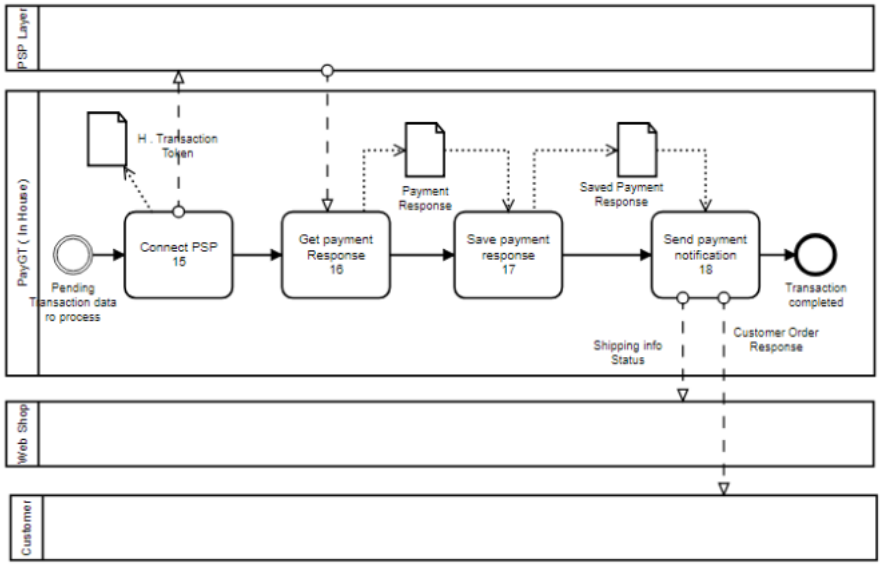

Рисунок 2.9 – Процес прийняття транзакції

2.3 Цілі безпеки бізнес-активів.

Відповідно до ISSRM, визначення цілей безпеки контексту та ідентифікованого активу зазначено як другий крок процесу ISSRM. Мета безпеки може бути узагальнена як необхідність визначення рівня гарантії або захисту інформаційних систем та інформації від будь-яких дій, які призведуть до знищення, несанкціонованого доступу, розкриття інформації, модифікації, використання систем і даних або переривання служби .

Цілі безпеки в основному класифікуються як конфіденційність, цілісність і доступність, однак рівень кожної властивості, який потрібно підтримувати, визначається критичністю активу та контекстом бізнесу [46].

Конфіденційність: Це стосується обмеження розкриття інформації сторонам, які не мають доступу до неї, з метою захисту конфіденційності людей і конфіденційної інформації. Приклад: сервер у середовищі PCI потребує належного захисту даних, оскільки він зберігає/передає інформацію кредитної картки. Якщо неавторизована сторона може переглянути інформацію про кредитну картку, це означає порушення конфіденційності інформації. Цілісність: це властивість гарантувати, що активи не будуть змінені або видалені неавторизованою стороною, і вона підтримує точність.

Приклад 1: зловмисник змінює повторювану інформаційну згоду клієнта, і з клієнта не стягуватиметься відповідна сума грошей за підписку на послугу. Доступність: властивість, яка гарантує, що авторизовані активи можуть бути доступні без будь-яких перерв протягом необхідного часу.

Приклад 2: зловмисник використовує ресурси платіжного шлюзу та робить платіжний віджет недоступним для користувачів, які хочуть придбати товар у веб-магазині. Ризик безпеки може завдати шкоди одній або кільком цілям безпеки бізнесу. Існують допоміжні цілі безпеки для властивостей CIA, пов’язані з користувачами, які використовують інформацію або взаємодіють з різними бізнес-активами. Автентифікація означає перевірку того, ким ви є, використовуючи те, що ви знаєте, що ви є або що у вас є [47].

Авторизація визначає, який рівень дозволу конкретна особа мала намір отримати після авторизації. Невідмовність означає, що запевнення, надане щодо конкретної діяльності, не може бути відхилено чи спростовано, або не можна нести відповідальність за дії. Визначення рівня цілей безпеки в різних середовищах може відрізнятися один від одного. Розуміння цілей безпеки та оцінка елементів керування для захисту може бути дещо складним у хмарній інфраструктурі, оскільки відповідальна сторона безпеки не може бути обмежена постачальником послуг або покупцем/клієнтом.

Це можна визначити як рукостискання, коли обидві сторони однаково сприяють і повинні бути обережними щодо безпеки, оскільки порушення з будь-якої сторони може призвести до серйозних катастроф і порушити властивості безпеки.

У таблиці 2.2 наведено бізнес-активи, отримані з діаграми BPMN, із метою безпеки кожного активу.

Таблиця 2.2 – Бізнес-активи та цілі безпеки BPMN

BPMN довідка	Бізнес-актив	Основні цілі безпеки		
A	Маркер безпеки	C	I	A
B	Платіжний маркер	x	x	
D	Інформація про кредитну картку	x	x	x
G	Деталі замовлення	x	x	x
H	Маркер транзакції	x	x	x
Z	Методи оплати		x	x
Y	Результати шахрайства		x	x

2.4 Системні активи системи платіжного шлюзу

Після виявлення бізнес-активів і визначення цілей безпеки було обрано один актив для подальшого моделювання та розширення технологічного рівня. Це розширення було змодельовано за допомогою ArchiMate. Деталі замовлення були вибрані серед виявлених бізнес-активів. На рис. 2.10 і 2.11 показано розширення обох інфраструктур.

Рис. 2.10 і 2.11 були змодельовані на основі представленої архіматної діаграми першого рівня. Деталі замовлення були отримані з процесу платіжної операції та технологічний рівень було розширено на основі відображення бізнесу та програми технологічного рівня.

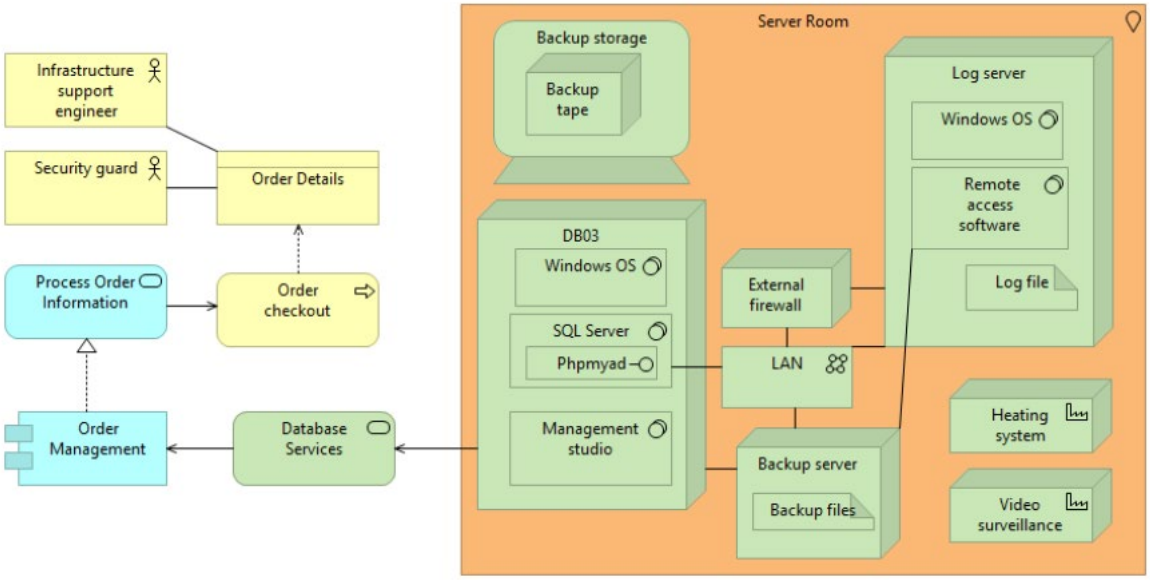

Рисунок 2.10 – Деталі замовлення, зіставлені з компонентами архітектури внутрішньої компанії.

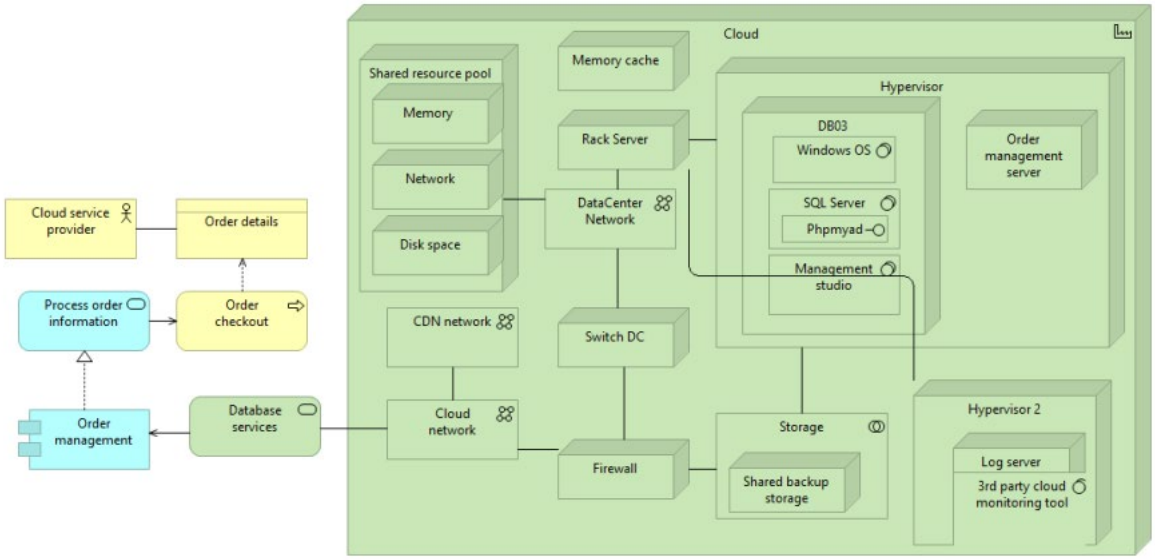

Рисунок 2.11 – Деталі замовлення, зіставлені з компонентами архітектури Cloud.

У таблиці 2.3 показано компоненти системних активів внутрішньої архітектури та хмарної архітектури, які використовуватимуться для аналізу ризиків. Ця таблиця не є порівнянням активів IS, які можуть існувати у внутрішній і хмарній інфраструктурі. Деякі активи, представлені у внутрішній системі, також можуть бути представлені в хмарі. Однак причиною, чому його було показано в таблиці, є передумови, на яких він базується.

Таблиця 2.3 – Системні активи інфраструктур.

Components of In-house Architecture	Components of Cloud Architecture
External firewall	Cloud service provider
Security guard	Shared resource pool
Video surveillance	CDN network
Backup tapes	3rd party monitoring tool
Infrastructure support engineer	Shared backup storage
DB03 (Server name)	DB03
Heating system	Log server
Log server	

2.5 Висновок до другого розділу

Було проведено пошук архітектурних відмінностей внутрішньої та хмарної інфраструктури. Спочатку було проведено ретельний аналіз внутрішнього центру обробки даних шляхом опитування людей та аналізу документів, пов'язаних із навколишнім середовищем. Хмарну модель створено на основі загальнодоступних дослідницьких моделей. Моделювання ЕА було використано для візуалізації відмінностей на абстрактному рівні, щоб отримати розуміння відмінностей до і після міграції до хмарної інфраструктури. Внутрішнє середовище базується на невіртуалізованому середовищі, а хмарна інфраструктура в ЕА базується на віртуалізованому середовищі. У хмарному середовищі постачальник хмарних послуг матиме доступ до середовища, тоді як власний охоронець не буде представлений у хмарі. Основна зміна компонентів технологічного рівня, яку можна побачити, — це зміни на основі віртуалізації, такі як спільний пул ресурсів і конфігурації мережі, специфічні для хмари.

3 АНАЛІЗ РИЗИКІВ СИСТЕМИ ПЛАТІЖНИХ ШЛЮЗІВ

3.1 Огляд глобальних ризиків, пов'язаних із оплатою

Розділ присвячено висвітлення наданню відповідей на питання: Які ризики безпеки змінюються, коли система платіжного шлюзу переходить із внутрішньої інфраструктури на хмарну? Воно складається з трьох підзапитань, а розділ містить аналіз ризиків безпеки та надає сценарії ризиків безпеки внутрішньої та хмарної інфраструктури.

ЗП 3. 1: Які загрози безпеці у внутрішній і хмарній інфраструктурі?

ЗП 3. 2: Які ризики безпеки у внутрішній і хмарній інфраструктурі?

ЗП 3. 3: Які відмінності та схожість ризиків безпеці після міграції?

Серед цифрових покупців 42% вважають за краще оплачувати кредитні картки [48]. Ці платежі обробляються системами платіжних шлюзів. Платіжні шлюзи зберігають і передають дані кредитної картки, а також особисту інформацію, яка є цінною для організацій і має значення для моніторингу. Платіжний домен є ціллю агентів загроз через інформацію, яку він обробляє. Платіжний шлюз або будь-яка інша організація, яка обробляє дані власників карток, має відповідати стандарту PCI DSS. PCI DSS є стандартом, і його сумісність не гарантує усунення ризиків безпеки.

Вперше в історії онлайн-шахрайство з кредитними картками перевищило показники особистого шахрайства, що призвело до 58% онлайн-шахрайства з картками та 42% особистого шахрайства [49]. Існують суворі вказівки для компаній, що займаються обробкою платежів, щодо управління та захисту конфіденційних даних клієнтів. Кембриджський університет провів аналіз кіберризиків [51] у всьому світі, надавши тематичні дослідження. Атаки на відмову в обслуговуванні все ще є серйозною проблемою в кібербезпеці, яка відрізняється від традиційних підходів, таких як атака на всю інфраструктуру, але зосереджена на інфраструктурних компонентах. «Звіт про глобальні ризики даних» [52] Вароніса показує, що 58% організацій не належним чином керували правами папок, що призвело до того, що 100 000 папок стали доступними для

громадськості. Наразі очевидно, що технологічний прогрес не може гарантувати підвищення рівня безпеки в системах, а зменшення ризиків може бути складним завданням через складність систем і невизначені ризики.

У таблиці 3.1 представлено порушення, пов'язані з платежами, які сталися у 2018 році, і те, як атаки вплинули на фінансові компанії. У ньому робиться висновок, що кількість кібератак, спрямованих на індустрію обробки платежів, почастішала.

Таблиця 3.1 – Зловживання платіжних карток у 2018 р. [53]

Company Name	**Company Domain**	**Month**	**Impact and Reason**	**Potential Reason for breach**
British Airways	Airline	September	Personal and Financial 380000 customers	Payment form script modification
Dixons Carphone	Electronics retailer	July	Personal and Financial 105000 customers	No chip and Pin protection
Ticketmaster UK	Entertainment ticket seller	June	40000 Personal and Financial	Due to a malicious software third-party application
Rail Europe	Train ticket distributor	April	Personal and Financial (The entire system was compromised)	Credit card-skimming malware in website
One Plus	Smart Phone manufacturer	January	40000 c/c details compromised	Malicious code in payment gateway

3.2 Аналіз ризиків безпеки системи платіжного шлюзу.

Уразливість є слабким місцем [5] активу IS і може існувати в програмному додатку, мережі, об'єкті, обладнанні та людях, пов'язаних з організацією. Агенти загроз використовують слабкі місця в активах системи. Жодна організація не може стверджувати, що інформаційні системи вільні від уразливостей, оскільки зловмисники знаходять уразливості нульового дня, щоб використовувати інформаційні системи. Тому виявлення вразливостей на підприємстві є безперервним процесом. Тому системи, які обробляють платіжні дані, щоквартально проводять оцінку вразливості як вимога PCI [54].

Агентом загрози може бути будь-хто, хто використовує метод атаки для використання вразливості в системі IS. Цілі агента загрози відрізняються залежно від мотивації, знань і рівня досвіду. У звіті [55] показано, що 90% підприємств

уразливі до атак з боку інсайдерів через погане керування привілеями доступу, складність технологій і можливість доступу до конфіденційних даних з різних пристроїв. У дослідженні було введено класифікацію на основі того, як зміняться ризики після міграції.

На рис. 3.1 представлено категорію ризику.

Нові ризики: Ризик, який не буде існувати у внутрішній системі, але буде доступний у хмарі після міграції. Приклад: Хмарна інфраструктура має спільні пули ресурсів, і загроза для цих пулів не існуватиме у внутрішній системі, оскільки IS не існує у внутрішній інфраструктурі.

Залишкові ризики: ризик безпеки, який існуватиме в хмарі та внутрішній інфраструктурі. Імовірність ризику безпеки може збільшуватися або зменшуватися. (Матриця ризиків виходить за рамки, тому не буде оцінено, які ризики підвищаться, а які зменшаться.) Приклад: ін’єкційна атака на рівні програми не усуне, коли інфраструктура зміниться. Але ймовірність може змінитися залежно від захисту від глибинних технологій, які використовуються в хмарі.

Усунення ризиків: ризики безпеки, які існують у внутрішній інфраструктурі, але ніколи не існують у хмарній інфраструктурі. Приклад: фізичні атаки на внутрішню інфраструктуру не будуть застосовні в хмарі, оскільки внутрішні співробітники не мають доступу до хмарного центру обробки даних, а також дані розподіляються.

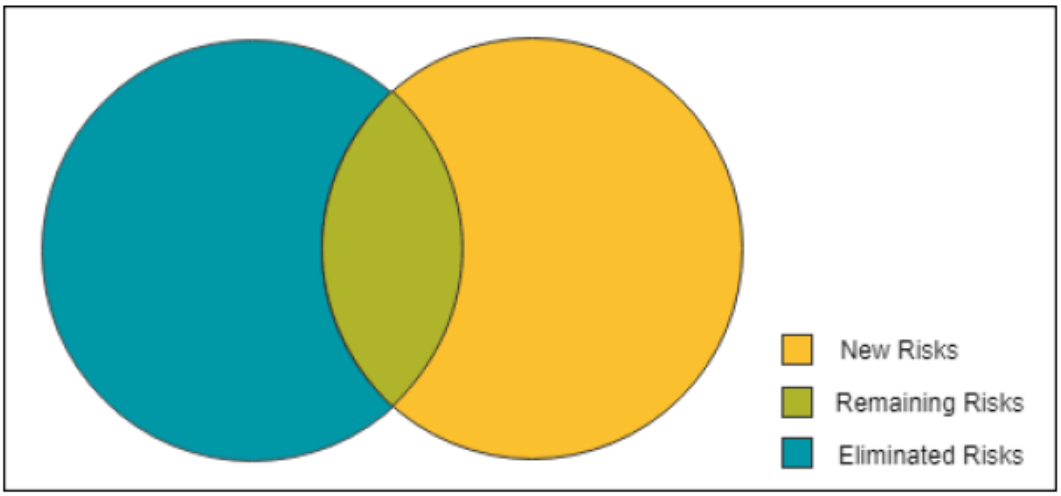

Рисунок 3.1 – Категорія ризику

3.3 Аналіз загрози та наслідків на основі.

STRIDE Через складний характер платіжного шлюзу аналіз загроз буде проведено для активів IS, які підтримують бізнес-актив із інформацією про замовлення. Деталі замовлення, надіслані продавцем, містять ім’я клієнта, дату народження клієнта, електронну адресу клієнта, адресу доставки, адресу клієнта, ідентифікатор замовлення, позицію замовлення, кількість і ціну.

Буде використано підхід, орієнтований на активи на основі STRIDE, оскільки програмне забезпечення, пов’язане з активами ISSRM, розглядатиметься як актив, а зловмисники будуть розглядати інфраструктуру. Нерозумно думати лише про минулі атаки та перевіряти, чи є вони потенційними ризиками в обох інфраструктурах, оскільки можуть існувати загрози, які ще не були скомпрометовані агентом загрози.

Вплив через ризик безпеки може призвести до пошкодження як бізнес-активів, так і допоміжних активів (активи IS). Категоризація STRIDE раніше використовувалася кінцевими елементами компонентів. У таблиці 8 представлені сценарії загроз для пошуку різних ризиків у кожній інфраструктурі.

Тому метою є не знайти найкращий сценарій ризику, а надати практичний приклад. Активи IS, які існують лише у внутрішній інфраструктурі, розглядаються, оскільки загроза використовує вразливість в активі IS, і якщо вибрана IS не представлена в хмарі, це означає, що ризик, представлений для внутрішньої інфраструктури, ніколи не відбудеться в хмарному середовищі. Тому розрахунки на основі матриці ризиків безпеки не потрібні. Це має бути так само, коли виявляють загрози активам ІС хмарної інфраструктури, які підтримують бізнес-актив «Деталі замовлення».

Для визначення унікальних ризиків під час представлення сценаріїв ризику було зроблено три обмеження:

1. Для формування сценарію ризику використовуються унікальні компоненти кожної архітектури.

2. Бізнес-актив внутрішньої та хмарної інфраструктури для певної категорії STRIDE має бути схожим.

3. Бізнес-об’єкт усіх сценаріїв залишиться незмінним.

Таблиця 3.2 – Аналіз загрози та впливу на основі STRIDE

Тип загрози	**Внутрішня інфраструктура**	**Хмарна інфраструктура**
Spoofing	Актив інформаційної системи: Охоронець, Серверна кімната. Уразливість: неправильний механізм автентифікації у серверній кімнаті. Агент загрози: неавторизований співробітник. Мотивація: вкрасти бекап для особистої вигоди. Ресурси: Підроблений ідентифікатор. Рівень знань: середній. Спосіб атаки: Перейти до серверної кімнати. Показ фальшивого посвідчення та представлення уповноваженим новим працівником. Отримати доступ до серверної кімнати (доступ лише до серверної кімнати під контролем охоронця). Крадіжка резервних бекапів замовлень. Наслідки: Втрата конфіденційності замовлення, деталі та втрата надійності резервного копіювання.	Актив IS: постачальник хмарних послуг, DB03 Уразливість: слабка політика обробки запитів користувачів у хмарі. Агент загрози: Співробітник за контрактом, Мотивація: Продавати деталі замовлення Ресурси: Навички соціальної інженерії, Адреса електронної пошти організації Рівень досвіду: Проміжний Метод атаки: Надішліть електронний лист постачальнику хмарних послуг за електронною адресою групи. Згадка про зовнішнє пентестування та запит на зміну правил брандмауера. Співробітник за контрактом підмінив ідентифікацію законного користувача, тому постачальник послуг Cloud приймає запит на дозвіл трафіку зі зловмисної IP-адреси. Відскануйте DB03. Знайдіть загальнодоступний експлойт і перейдіть до деталей замовлення. Наслідки: втрата конфіденційності деталей замовлення. Ураження репутації компанії.

Тип загрози	**Внутрішня інфраструктура**	**Хмарна інфраструктура**
	Актив IS: Співробітник (стажист) Вразливість: відсутність досвіду безпеки та схильність до соціальної інженерії Агент загроз: зловмисний співробітник, Мотивація: підсадити троян для особистої вигоди Ресурси: Навички соціальної інженерії Рівень знань: середній Метод атаки: зв'яжіться зі стажером і вдайте, що зловмисник намагається допомагати. Отримайте облікові дані БД від стажера, вдаючи, що він збирається допомогти. Журнал у DB03 з обліковими даними стажерів і запустіть шкідливий сценарій. Вплив: втрата конфіденційності деталей замовлення. Втрата надійності в DB03.	

Тип загрози	Внутрішня інфраструктура	Хмарна інфраструктура
Tampering	Актив IS: резервні стрічки, серверна кімната Уразливість: ненадійно збережена резервна копія стрічки Агент загроз: зловмисний співробітник, Мотивація: знищити резервні стрічки для особистої вигоди. Ресурси: Тісний контакт з охороною Рівень знань: середній Спосіб атаки: доступ до серверної кімнати шляхом атаки соціальної інженерії на Охоронець. Вставте резервні стрічки в а пристрій і змінювати дані резервних стрічок. Вплив: втрата доступності замовлення деталі. Втрата цілісності деталей замовлення. Пошкодити дані на резервній стрічці.	Актив IS: DB03, сервер журналу, сторонній інструмент моніторингу, протокол передачі Уразливість: неналежна безпека протоколу передачі в 3 руки інструменту моніторингу Агент загроз: зловмисник, Мотивація: Замітати сліди про попередній напад Ресурси: Знання про вразливий сторонній хмарний моніторинговий інструмент Рівень знань: середній / просунутий Метод атаки: знайти те, що є інтеграційне програмне забезпечення, що використовується для вилучення даних від сервера журналу до порталу моніторингу. Вставте зловмисне програмне забезпечення в плагін. Змінити журнал файли реквізитів замовлення, тому не буде видимі для моніторингу. Наслідки: втрата конфіденційності замовлення деталі. Втрата цілісності порядку деталі. Втрата довіри до третьої сторони інструменту моніторингу.

Тип загрози	Внутрішня інфраструктура	Хмарна інфраструктура
Repudiation	Актив IS: сервер журналу, співробітник Уразливість: несанкціоноване сповіщення механізм на сервері журналу Агент загрози: підкуплений працівник, Мотивація: особиста вигода Ресурси: Інфраструктура компанії Знання Рівень знань: середній Спосіб атаки: перейдіть до серверної кімнати. Підключіть USB-накопичувач із руткітом шкідливих програм. Отримати доступ до сервера журналу. Віддалено змінювати файли журналів деталей замовлення. Наслідки: втрата конфіденційності замовлення деталі. Втрата цілісності деталей замовлення. Втрата довіри до сервера журналу	Актив IS: резервне сховище Уразливість: неоновлений доступ привілеї для внутрішніх користувачів Агент загрози: Внутрішній зловмисник, Мотивація: Здійснити відповідь на приниження його становища Ресурси: Технічні знання про механізм резервного копіювання, має обліковий запис користувача для доступу до серверів журналу Рівень знань: середній Метод атаки: увійдіть на сервер журналу зі своїм дійсним посвідченням особи. Змініть завдання cron розклад, щоб уникнути створення резервних копій. Очистити сліди його присутності в серверній . Логи в той період будуть недоступні для подальших досліджень. Вплив: втрата доступності замовлення подробиці Журнали.
Information Disclosure	Актив IS: серверна кімната, резервні стрічки Уразливість: ненадійно збережені незашифровані резервні стрічки Агент загроз: зловмисний співробітник, Мотивація: особиста вигода Ресурси: резервні знання Рівень знань: середній	Актив IS: резервне сховище Уразливість: неправильне виведення з експлуатації апаратних ресурсів у резервному сховищі Агент загрози: зловмисний співжильник, Мотивація: особиста слава Ресурси: знання резервного копіювання та відновлення,

<table>
<tr><th>Тип загрози</th><th>Внутрішня інфраструктура</th><th>Хмарна інфраструктура</th></tr>
<tr><td rowspan="2"></td><td>Метод атаки: співробітник із доступом до серверної кімнати проникає. Клонує дані в дату резервного копіювання. Доступ до даних, що зберігаються у вигляді звичайного тексту. Деталі замовлення на продаж.
Вплив: втрата конфіденційності деталей замовлення. Втрата довіри до механізму зберігання даних.</td><td>інструменти криміналістичної експертизи
Рівень знань: середній
Метод атаки: співорендар купує Advance Forensic Tool. Виконати програма та відновлення файлів резервних копій даних DB03. Поруште шифрування файлів, щоб переглянути деталі замовлення.
Наслідки: втрата конфіденційності замовлення деталі.</td></tr>
<tr><td colspan="2">Актив IS: DB03
Уразливість: неправильний контроль доступу користувачів на рівні програми
Агент загрози: неавторизований інсайдер,
Мотивація: переглянути всю інформацію, пов’язану з деталями замовлення (особиста вигода)
Ресурси: знання контролю доступу користувачів, співробітник компанії
Рівень знань: середній
Метод атаки: неавторизований інсайдер виявляє, що його роль доступу користувача була оновлена. Увійдіть до DB03 і отримайте деталі замовлення з DB03.
Вплив: втрата конфіденційності деталей замовлення та втрата довіри до DB03</td></tr>
</table>

Тип загрози	Внутрішня інфраструктура	Хмарна інфраструктура
Denial of Service	Актив IS: Система опалення, Серверна Уразливість: слабкий механізм моніторингу тепла Агент загроз: зловмисний інсайдер, Мотивація: особиста вигода (образа) Ресурси: Знання організації Рівень досвіду: Початківець Спосіб атаки: доступ до серверної кімнати. Вимкнути систему опалення. Сервер перегрівається та не працює. Це призведе до порушення роботи служби. Вплив: втрата доступності деталей замовлення, втрата надійності DB03 і шкода серверу DB03.	Актив IS: мережа CDN, DB03 Уразливість: неправильна маршрутизація запитів та обробка відповідей у мережі CDN [52] [53] Агент загрози: зловмисний співжильник, Мотивація: особиста вигода Ресурси: знання мережі та маршрутизації Рівень досвіду: просунутий Спосіб атаки: . Співнаймач маніпулює процесом пересилання. Створіть цикл пересилання в мережі CDN (атака циклу пересилання). Пересилання цикл повторюватиме один запит. Зробіть несподіване масове споживання ресурсів. Ці запити приведуть до DOS Вплив: втрата доступності в деталях замовлення
Elevation of Privilege	Актив IS: DB03, камера Уразливість: неправильний контроль доступу до USB Агент загроз: зловмисний співробітник, Мотивація: особиста вигода Ресурси: Технічні знання та обладнання Рівень знань: середній Спосіб атаки: перейдіть до серверної кімнати.	Актив IS: DB03, спільний пул ресурсів Уразливість: неправильна ізоляція ресурсів у спільному пулі ресурсів Агент загрози: зловмисний орендар, Мотивація: особиста вигода Ресурси: знання віртуалізації Рівень досвіду: просунутий Метод атаки:

Тип загрози	**Внутрішня інфраструктура**	**Хмарна інфраструктура**
	Підключіть гумову качечку до DB03 03. Отримайте віддалений доступ до DB03. Отримати деталі замовлення, які включають особисту інформацію, щоб знайти дохід веб-магазину з деталей замовлення. Вплив: втрата конфіденційності деталей замовлення	Орендар купує кілька VMS у хмарного постачальника. Отримайте карту інфраструктури та розподіл IP-адрес за допомогою атаки на боковий канал. Використовуйте кеш спільної пам'яті. 4. Отримайте доступ до кешу DB03 і розкрийте деталі замовлення. Вплив: втрата конфіденційності деталей замовлення. Пошкодити надійність пулу спільних ресурсів.
	Asset IS: інтерфейс phpMyAdmin Уразливість: неправильна конфігурація інтерфейсу phpMyadmin DB03 Загрозливий агент: зловмисник, Мотивація: отримати доступ до деталей замовлення та зробити копію для продажу в темній мережі (особиста вигода) Ресурси: знання злому програм Рівень знань: середній Метод атаки: досліджуйте вразливості, пов’язані з phpmyadmin. Дослідіть розташування інтерфейсу phpMyadmin. Завантажте бекдор за допомогою функції файлу дампа та підвищте привілеї Вплив: втрата конфіденційності деталей замовлення та втрата довіри до PayGate	

Аналіз ризиків на основі STRIDE.

В даний час організації використовують різні методи для проведення аналізу ризиків. Загроза та комбінація вразливостей системних активів, які можуть вплинути на активи [5], створюють ризики для безпеки. Виявлення ризиків безпеки на ранніх стадіях робить процедуру обробки ризиків плавною.

Еволюція відбувається постійно разом із технологічним розвитком, і для того, щоб залишатися на ринку, потрібне впровадження. Ідентифікатори ризиків безпеки на основі різних категорій загроз сформульовані таким чином у таблиці 2.3.

Таблиця 3.3 – Ризики безпеки на основі STRIDE у внутрішній та хмарній інфраструктурі

Тип загрози	**Внутрішня інфраструктура**	**Хмарна інфраструктура**
Spoofing	SP. A. R1: Неавторизований працівник із засобами доступу до серверної кімнати для викрадення резервних стрічок із деталями замовлення, використовуючи неналежний механізм автентифікації в серверній кімнаті, що призводить до втрати конфіденційності деталей замовлення та втрати надійності резервних стрічок.	SP. B. R1: Співробітник за контрактом, який може продавати деталі замовлення, використовуючи слабку політику обробки запитів користувачів постачальником хмарних послуг, що призводить до втрати конфіденційності деталей замовлення та заплямує репутацію компанії.
	SP. B. R1: Зловмисний співробітник із засобами встановлення трояна для отримання деталей замовлення з DB03, використовуючи облікові дані бази даних стажера за допомогою атаки соціальної інженерії, що призводить до втрати конфіденційності деталей замовлення та втрати надійності в DB03.	

Тип загрози	**Внутрішня інфраструктура**	**Хмарна інфраструктура**
Tampering	TA. A. R2: Зловмисний працівник із засобами для знищення резервних стрічок шляхом викрадення картки-токена через неналежний механізм доступу в серверній кімнаті, що призводить до втрати доступності в деталях замовлення, втрати цілісності в деталях замовлення та пошкодження даних у резервній стрічці.	TA. B. R2: Зловмисник із засобами для приховування слідів попередньої атаки на сервері журналу шляхом використання неправильного протоколу передачі безпеки, який використовується в сторонньому інструменті моніторингу, інтегрованому з сервером журналу, що веде до до втрати конфіденційності деталей замовлення, втрати цілісності деталей замовлення та втрати довіри до інструменту моніторингу третьої сторони.
	Без сценарію ризику	
Repudiation	RE. A. R3: Внутрішній співробітник підкупив засіб видалення журналів деталей замовлення, щоб встановити зловмисне програмне забезпечення на фізичному пристрої через неправильно налаштований механізм сповіщення про несанкціоновані випадки на сервері журналу, що призводить до втрати конфіденційності деталей замовлення, втрати цілісності деталей замовлення та втрати довіра до сервера журналу 1	RE. B. R3: Внутрішній зловмисник із засобами змінити розклад завдань Cron, щоб уникнути створення резервних копій, використовуючи неоновлені привілеї доступу для внутрішніх користувачів, що призводить до втрати конфіденційності в журналах деталей замовлення та втрати доступності в журналах деталей замовлення.
	Без сценарію ризику	

Тип загрози	**Внутрішня інфраструктура**	**Хмарна інфраструктура**
Information Disclosure	IN. A. R4: Зловмисний власний співробітник із засобами для отримання деталей замовлення для продажу особистої інформації в темній мережі за допомогою незахищено збережених незашифровані стрічки резервного копіювання в серверній кімнаті, що призводить до втрати конфіденційності деталей замовлення та втрати довіри до механізму зберігання даних.	IN. B. R4: Зловмисний співорендар з метою продати деталі замовлення шляхом відновлення видалених файлів за допомогою невідповідного апаратного ресурсу виведення з експлуатації резервного сховища, що призводить до втрати конфіденційності деталей замовлення.
	IN. AB. R4: Неавторизований інсайдер із засобами для перегляду всієї інформації, пов'язаної з деталями замовлення з DB03, використовуючи неналежні привілеї ролі доступу користувача DB03, що призводить до втрати конфіденційності деталей замовлення та втрати надійності механізму доступу DB03.	
Denial of Service	DE. A. R5: Внутрішній співробітник із засобами для знищення служб сховища даних DB03, використовуючи систему опалення в серверній кімнаті, яка не контролюється, що призводить до втрати доступності деталей замовлення, втрати надійності DB03 і шкоди серверу DB03.	DE. B. R5: Зловмисний спільний орендар із засобами для неочікуваного великого споживання ресурсів шляхом використання неправильної маршрутизації запитів і обробки відповідей у CDN, що призводить до втрати доступності в деталях замовлення, шкоди функціональності DB03 і репутації організації PayGate.

Тип загрози	**Внутрішня інфраструктура**	**Хмарна інфраструктура**
	Без сценарію ризику	
Elevation of Privilege	EL. A. R6: Зловмисний інсайдер отримує деталі замовлення, вводячи в оману систему безпеки особистий з атакою соціальної інженерії в серверній кімнаті та отриманням доступу до DB03, що призводить до втрати конфіденційності деталей замовлення.	EL. B. R6: Зловмисний співкористувач отримує доступ до деталей замовлення, використовуючи неправильну ізоляцію ресурсів у спільному пулі ресурсів, і отримує доступ до DB03, що призводить до втрати конфіденційності деталей замовлення.
	EL. AB. R6: Зловмисник із засобами для отримання деталей замовлення отримує доступ до інтерфейсу phpMyAdmin DB03, використовуючи неправильну конфігурацію DB03, що призводить до втрати конфіденційності деталей замовлення та втрати довіри до веб-магазину.	

Відмова в обслуговуванні DE. A. Ризик R5 існує через вразливість внутрішньої системи опалення серверної кімнати. Агент загрози зміг зайти до серверної кімнати та пошкодити систему опалення, що призвело до перегріву обладнання в серверній кімнаті. Цей ризик не існує в хмарі, тому що працівник PayGate ніколи не матиме доступу до хмарного центру обробки даних.

DE. AB. R5 пояснює ризик на рівні програми. Щоб обслуговувати законний запит, сховища даних повинні мати належну обробку запитів. Підвищення ризику безпеки привілеїв EL. A. R6 – це усунутий ризик, коли систему платіжного шлюзу перенесено в хмару. Співробітники PayGate не знатимуть, де зберігаються дані в хмарі, а фізичний доступ до хмарного центру обробки даних суворо заборонено.

Тому працівник не зможе підключити пристрій, який міг би отримати віддалений доступ у хмарному середовищі. EL. B. R6 пояснює ескалацію привілеїв у хмарному середовищі, яка можлива завдяки пулам спільних ресурсів

у хмарі. У внутрішній невіртуалізованій інфраструктурі спільні пули ресурсів не можна побачити. Тому ризик ніколи не існуватиме у внутрішньому середовищі. EL. AB. R6 – це загроза безпеці на основі програми, а інфраструктура, яку розміщує програма, не усуне ризик.

Уразливість [56], яка існує в інтерфейсі phpMyAdmin, залишиться у внутрішній та хмарній інфраструктурі. Таблиці призначені лише для ілюстрації деяких прикладів сценаріїв ризику. Відсутність сценарію ризику означає, що сценарій ризику не представлено в таблиці.

Аналіз загроз було проведено в системі платіжного шлюзу, розміщеній у внутрішній інфраструктурі та хмарній інфраструктурі. Аналіз показує, як загрозлива подія формулюється агентом загрози та методом загрози. Мета цього розділу — проілюструвати сценарії ризику на основі STRIDE. Аналіз також показує, які ризики безпеки залишаться після міграції.

У роботі моделювання архітектури підприємства використовується для демонстрації абстрактного рівня системи реального платіжного шлюзу. Хмарна інфраструктура, яку було змодельовано за допомогою Archi-Mate, є узагальненням інформації, зібраної від основних хмарних постачальників, і моделі в дослідницькій статті «Моделювання загроз для інфраструктур хмарних центрів обробки даних» [33]. Реальна хмарна інфраструктура може мати різні компоненти.

Також у цьому дослідженні розглядається лише модель IaaS. Але результати можуть бути різними, якщо той самий підхід використовувати для SaaS і PaaS. Представлена система платіжного шлюзу змодельована на основі інтерв'ю з існуючою компанією. Інтеграція системи платіжних шлюзів може бути іншою для іншої компанії, тому це суб'єктивно.

ЗП 1: Які архітектурні відмінності між внутрішньою інфраструктурою та хмарною інфраструктурою? Вибране дослідження базується на фактично існуючому платіжному шлюзі. Тому перед моделюванням системи за допомогою ArchiMate було проведено аналіз внутрішньої інфраструктури компанії. Поділ шарів і взаємозалежність у ArchiMate були використані для переведення сценарію реального світу в абстрактну візуалізацію, щоб знайти зв'язки кожного

компонента. Порівняння діаграм ArchiMate показало, що є зміни в групах користувачів, прикладному рівні та технологічному рівні. Подальший аналіз показав, що всередині компанії є невіртуалізоване середовище та ручні методи захисту, тоді як хмарна архітектура відображає компоненти віртуалізації та зміни групи користувачів через те, що хмарний провайдер також має доступ до середовища.

ЗП 2: Що таке бізнес-активи та активи допоміжної інформаційної системи? З моделей корпоративної архітектури, процес платіжних транзакцій було обрано як основне дослідження серед чотирьох бізнес-процесів, які були виявлені на бізнес-рівні обох інфраструктур. Технологічний рівень моделі архітектури підприємства – це абстрактний погляд на систему PayGate. Діаграма BPMN не охопила всі архітектурні компоненти, видимі навіть в анотації першого рівня. Тому процес платіжної транзакції було змодельовано з використанням мови BPMN, щоб отримати бізнес-активи від процесу платіжної транзакції.

Процес платіжної транзакції в ArchiMate складався з трьох підпроцесів: оформлення замовлення, перевірка шахрайства та прийняття транзакції. Кожен був представлений у роботі окремо, щоб мати кращу наочність.

З діаграми BPMN було отримано 6 бізнес-активів. Цілі безпеки бізнес-активів представлені за допомогою властивостей конфіденційності, доступності та цілісності. Мета безпеки кожного бізнес-активу була визначена шляхом проведення інтерв'ю з технічним менеджером із продуктів PayGate, щоб зрозуміти, наскільки актив є важливим для організації. Було обрано один бізнес-актив, і розширення технологічного рівня було змодельовано знову для цього конкретного активу з використанням ArchiMate як абстракції другого рівня, щоб отримати активи IS із внутрішньої інфраструктури та хмарної інфраструктури. Системними активами хмари, які підтримують бізнес-актив Деталі замовлення, є технологічні компоненти на основі віртуалізації, постачальник хмарних послуг. Модель внутрішньої інфраструктури складалася з охоронця, який підтримує захист інформації в серверній кімнаті, засобів, які підтримують захист цілей безпеки деталей замовлення.

ЗП 3: Які ризики безпеки змінюються, коли система платіжних шлюзів переходить із внутрішньої до хмарної інфраструктури?

Метою є порівняння ризиків безпеки у внутрішній і хмарній інфраструктурі на основі підходу, орієнтованого на загрози, з використанням STRIDE. Через складний характер дослідження було обрано лише один бізнес-актив. Друга абстракція діаграми рівня ArchiMate моделюється, щоб показати взаємозалежність одного бізнес-активу з відповідним технологічним рівнем. Така ж процедура була дотримана для хмарної інфраструктури. Активи IS, які підтримують бізнес-актив Деталі замовлення, використовуються для пошуку загроз і відмінностей ризиків. Перш ніж визначити актив IS для сценаріїв загрози, рішення було прийнято на основі:

• Порівняння ризиків у кожній категорії STRIDE має враховувати лише один бізнес-актив. Причини обмежень: ризик можна або повністю усунути, збільшити рівень ризику, знизити рівень ризику, або ризики можуть бути введені з міграцією. По-перше, для пошуку сценаріїв розглядалася лише обмежена кількість активів. Сценарії були обрані на основі категорій STRIDE. Наведені результати показують, що результат ризику безпеки можна розділити на три категорії: новий ризик, усунутий ризик і ризик, що залишився. Прогалина в безпеці — це зміни ризику, які можуть статися внаслідок міграції інфраструктури для конкретного бізнес-об’єкта. Це пояснення показує, як знайти ризики в двох різних інфраструктурах і як їх можна класифікувати на основі підходу STRIDE.

Більшість сценаріїв ризику, представлених у компанії, базуються на фізичних атаках. Унікальні сценарії ризику на основі хмари здебільшого пов’язані з середовищем віртуалізації. Таким чином, внутрішні ризики фізичної безпеки усуваються в хмарі, а ризики, засновані на віртуалізації, будуть знову запроваджені. Однак це не означає, що хмара не має фізичних атак.

Але ризики безпеки внутрішніх співробітників PayGate не будуть у хмарі через розподілену природу даних у хмарі та недоступність хмарного центру обробки даних.

Ризики безпеки в програмах, які розміщені в обох середовищах, класифікуються як ризики, що залишилися, оскільки ризики безпеки на основі

коду та веб-програми не змінюватимуться залежно від компонентів інфраструктури. Але ймовірність використання системи загрозливим агентом може бути дуже малоймовірною через різні механізми захисту, що використовуються в різних інфраструктурах.

В організаціях моделюванням бізнес-процесів займається бізнес-аналітик. Існує ізоляція між технічною групою користувачів і групою нетехнічних користувачів. Ідентифікація активів для RA на основі діаграм BPMN може містити недоліки, такі як неідентифіковані активи IS. Тому в цьому дослідженні використовується моделювання EA, щоб показати відображення бізнес-рівня та технологічного рівня, щоб мати кращу видимість компонентів інфраструктури та взаємозв'язків кожного рівня.

3.4 Висновок до третього розділу

Підсумовуючи, аналіз показує, що модель EA допомагає ідентифікувати активи IS, якими можна було б знехтувати на діаграмі бізнес-процесів. Це також допомагає порівнювати та вловлювати відмінності в архітектурі. ISSRM добре узгоджено з моделями EA та полегшує ідентифікацію активів. Зміни архітектурних компонентів у моделях допомагають ідентифікувати активи ІБ, які можуть становити загрозу та становити ризик для організації. Разом з міграцією інфраструктури ризик може бути усунутий, привнесений, існуючий ризик може збільшитися або зменшитися. Ризик було визначено для обох інфраструктур на основі підходу до загроз STRIDE. Перевірка роботи була представлена шляхом опитування експертів в організації, де розміщено PayGate, і кількох зовнішніх думок про придатність підходу, використаного в дослідженні.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності. Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам законодавства. Працівник має право відмовитися від дорученої роботи, якщо створилася виробнича ситуація, небезпечна для його життя чи здоров'я або для людей, які його оточують, або для виробничого середовища чи довкілля. Він зобов'язаний негайно повідомити про це безпосереднього керівника або роботодавця. Факт наявності такої ситуації за необхідності підтверджується спеціалістами з охорони праці підприємства за участю представника профспілки, членом якої він є, або уповноваженої працівниками особи з питань охорони праці (якщо професійна спілка на підприємстві не створювалася), а також страхового експерта з охорони праці. Завдання охорони праці – звести до мінімуму ушкодження та захворювання працівника з одночасним забезпеченням комфорту при максимальній продуктивності праці. Основними цілями охорони праці є формування в спеціалістів необхідних знань і практичних навичок по правових і організаційних питаннях охорони праці, виробничій санітарії, техніці безпеки, пожежній безпеці.

4.1 Загальна характеристика приміщення і робочого місця

Розробка системи керування виконується в приміщенні, яке знаходиться на четвертому поверсі восьмиповерхового будинку з загальним та місцевим освітленням. В приміщенні одностороннє освітлення, вікна орієнтовані на схід, на вікнах є ролети. Стеля білого кольору з коефіцієнтом відбиття 0,7, стіни цегляні світлого кольору з коефіцієнтом відбиття 0,5. В приміщенні працює 4 людини,

відповідно до цього отримуємо вхідні дані для аналізу потенційно-небезпечних і шкідливих виробничих факторів, які наведено в табл. 4.1.

Таблиця 4.1 – Вхідні дані

Параметри приміщення	Значення
Довжина х ширина х висота	6,6 х 6,1 х 2,7 м
Площа	40,26 м^2
Об’єм	108,70 м^3
Номер робочого місця	Специфіка роботи
І робоче місце	Front-end програміст (спеціаліст з розробки клієнтської частини веб- застосунків)
ІІ робоче місце	Back-end програміст (спеціаліст з розробки серверної частини веб застосунків та проектування баз даних)
ІІІ робоче місце	Бізнес-аналітик (також виконує роль менеджера продукту)
IV робоче місце	UI-UX веб-дизайнер
Технічні засоби (кількість)	Назва та характеристики
Монітор (4 шт.)	HP 22Xi/21,5"/1920x1080px/IPS
Комп’ютер (4 шт.)	HP ProBook 440 G6, екран 14" IPS (1920x1080) Full HD, Intel Core i7-8565U (1.8 - 4.6 ГГц)/RAM 16 ГБ/SSD 256 ГБ
Підлоговий кулер (1 шт.)	CRYSTAL YLR3-5V208
Кондиціонер (1 шт.)	DEKKER DSH105R/G/26м^2/2,65кВт-2,9кВт/25х74,5х19,5см/9 кг
Світильники загального призначення (3 шт.)	Світильник растровий вмонтований 4х18W
Світильники (4 шт.)	DeLux Décor TF-05 / 1 х 40Вт

Згідно НПАОП 0.00-7.15-18 площа S$^{'}$, виділена для одного робочого місця з персональною ЕОМ, повинна бути не менше 6 м^2 і об’єм – не менше 20 м^3. У приміщенні розташовано 4 робочі місця, що повністю відповідає необхідним нормам.

Розрахуємо фактичні значення цих показників, розділивши об’єм приміщення та загальну площу на кількість працюючих.

Отже, виходячи з отриманих результатів за характеристиками площі та об’єму, приміщення відповідає нормам.

Можна зробити висновок, що розміри робочого місця програміста відповідають встановленим нормам, виходячи з заданих параметрів.

Таблиця 4.2 – Характеристики робочого місця

№	Найменування параметру	Значення	
		фактичне	нормативне
1.	Висота робочої поверхні, мм	780	680 – 800
2.	Ширина робочої поверхні, мм	1500	не менше 600
3.	Глибина робочої поверхні, мм	750	не менше 600
4.	Висота простору для ніг, мм	750	не менше 600
5.	Ширина простору для ніг, мм	800	не менше 500
6.	Глибина простору для ніг, мм	750	не менше 450
7.	Висота поверхні сидіння, мм	480	400 – 500
8.	Ширина сидіння, мм	500	не менше 400
9.	Глибина сидіння, мм	500	не менше 400
10.	Висота опорної поверхні спинки, мм	550	не менше 300
11.	Ширина поверхні спинки, мм	470	не менше 380
12.	Довжина підлокітників, мм	300	не менше 250
13.	Ширина підлокітників, мм	60	50 – 70
14.	Відстань від очей до екрану, мм	650	600 – 700

4.2 Аналіз потенційно небезпечних і шкідливих виробничих факторів на робочому місці

При створенні системи аналізу та візуалізації робота виконується сидячи без фізичних зусиль, тому відноситься до категорії легка Іа.

Під час роботи на працівника діє ряд небезпечних і шкідливих чинників, які наведені у табл. 4.3 та табл. 4.4.

У таблиці 4.5 та 4.6 наведені нормативні та фактичні показники мікроклімату.

Таблиця 4.3 – Шкідливі чинники на робочому місці

Фізичні	Психофізіологічні
Підвищений рівень шуму	Розумове перенапруження
Підвищений рівень електромагнітного випромінювання	Монотонність праці
Підвищений рівень статичної електрики	Перенапруження аналізаторів
Недостатній рівень освітленості	
Неоптимальний мікроклімат	

Таблиця 4.4 — Аналіз шкідливих факторів, пов’язаних з мікрокліматом

№	Шкідливий фактор	Наслідки
1	Відхилення вологості повітря від оптимальних параметрів	Тимчасове погіршення самопочуття і зниження працездатності, хвороби, роздратованість
2	Відхилення t від оптимальних параметрів	Відсутність теплового комфорту, тимчасове погіршення самопочуття і зниження працездатності, хвороби
3	Відхилення V руху повітря від оптимальних параметрів	Тимчасове погіршення самопочуття і зниження працездатності, хвороби

Таблиця 4.5 – Мікроклімат в теплий період року

Параметр мікроклімату			
Найменування	Значення		
	Фактичне		Оптимальне
t, °C	21	21 – 23	18 –27
w, %	55	60 – 40	до 75
V, м/с	0,2	0,3	0,4 – 0,2

Таблиця 4.6 – Мікроклімат в холодний період року

Параметр мікроклімату			
Найменування	Значення		
	Фактичне		Оптимальне
t, °С	18	21 – 23	18 –27
w, %	70	60 – 40	до 75
V, м/с	0,4	0,3	0,4 – 0,2

Заходи для запобігання встановлених мікрокліматичних порушень норм подані в таблиці 4.7.

Джерелами шуму в приміщенні є вентилятор системного блоку, ноутбуку та кондиціонер (табл. 4.8). Звук, що створюється вентилятором та кондиціонером, можна класифікувати як постійний.

Таблиця 4.7 — Запобіжні заходи в теплий та холодний періоди року

№	Технічні	Організаційні	ЗІЗ
1	Контроль параметрів за допомогою анемометра Extech AN100; використання кондиціонеру DEKKER DSH105R/G (для кондиціонування і провітрювання)	відсутні	відсутні
2	Контроль параметрів за допомогою термометра La Crosse WS8005; використання кондиціонеру DEKKER DSH105R/G (для кондиціонування і провітрювання)	Перерви в роботі з метою провітрювання кімнати; вологе прибирання на робочих місцях	відсутні
3	Контроль параметрів за допомогою психрометра Т-04; використання зволожувача повітря ZELMER AH1500	Перерви в роботі з метою провітрювання кімнати; вологе прибирання на робочих місцях	відсутні

Приміщення для роботи мають бути обладнані системами опалення, кондиціонування повітря або припливно-витяжною вентиляцією відповідно до ДБН В.2.5-67:2013. Нормовані параметри мікроклімату, іонного складу повітря, вмісту шкідливих речовин відповідають вимогам ДСН 3.3.6.042-99, ГН 2152-80, ГОСТ 12.1.005-88, ДСТУ ГОСТ 12.0.230:2008 та ДСТУ ГОСТ 12.4.041:2006. Під вентиляцією розуміють сукупність заходів та засобів, призначених для забезпечення на постійних місцях та зонах обслуговування приміщень метеорологічних умов та чистоти повітряного середовища, що відповідають гігієнічним та технічним вимогам. Основне завдання вентиляції – вилучити із приміщення забруднене, вологе або нагріте повітря та подати чисте свіже повітря.

Таблиця 4.8 – Джерела шуму

Джерело шуму	Фактичний рівень шуму, дБ	Оптимальний рівень шуму, дБ	Час роботи, год.
Кондиціонер DEKKER SH105R/G	22	< 50	8
Кулер комп’ютеру HP Probook 4530s	20		8

Наслідки шуму та вібрації подано у таблиці 4.9.

Таблиця 4.9 – Шум і вібрація

Шкідливий фактор	Наслідки
Підвищений рівень шуму	Погіршення слуху, підвищення ймовірності виникнення помилки, зниження продуктивності роботи
Вібрації на робочому місці	Роздратування, зниження працездатності, погіршення самопочуття

Запобіжні заходи, які здійснюються для уникнення наслідків шкідливих факторів, наведено в табл. 4.10.

Таблиця 4.10 – Запобіжні заходи

№	Технічні	Організаційні	ЗІЗ
1	Контроль параметрів за допомогою приладу для виміру шуму DT-8852; якісний монтаж окремих вузлів комп'ютера	Проведення планового попереджувального ремонту (чищення від пилу і інших забруднень)	Відсутні
2	Контроль параметрів за допомогою приладу для виміру вібрацій TV260; встановлення спеціальної підставки під ноутбук	Проведення планового попереджувального ремонту (чищення від пилу й інших забруднень)	Відсутні

Відповідно до ДБН В.2.5-28:2018 робота відноситься до розряду зорових робіт. Передбачається використання природного, штучного та змішаного освітлення. В табл. 4.11 наведені шкідливі фактори порушень норм яскравості світла.

Таблиця 4.11 – Шкідливі фактори порушень норм яскравості світла

№	Шкідливий фактор	Наслідки
1	Недостатня освітленість робочої зони	Погіршення зору і самопочуття, втомлюваність, підвищення ризику здійснення помилки
2	Підвищена яскравість світла	

У таблиці 4.12 відображено фактичні та оптимальні значення для параметрів освітлення.

Таблиця 4.12 – Параметри освітлення

Найменування	Значення	
	Фактичне	Оптимальне
При змішаному освітленні	450	400
При загальному освітленні	300	300
Коефіцієнт природного освітлення	1,23	1,2

Для уникнення наслідків неправильного освітлення вживаються такі запобіжні заходи (табл. 4.13):

Таблиця. 4.13 – Запобіжні заходи

№	Технічні	Організаційні	ЗІЗ
1	Контроль параметрів за допомогою люксметра DT-1308; використання нових світильників загального призначення ELSTEAD FINSBURY PARK FP6 POL NICKEL; урахування природного освітлення кімнати	Встановлення мінімального рівня освітлення; чищення скла вікон та світильників; заміна ламп, що перегоріли	Додаткове освітлення на робочих місцях (світильники DeLux Décor TF-05); окуляри для роботи з комп'ютером.
2	Контроль параметрів за допомогою люксметра DT-1308; використання регульованих пристроїв для відкривання вікон, а також жалюзі; використання світильників нового типу	Відсутні	Окуляри для роботи з комп'ютером.

ЕОМ є однофазним споживачем електроенергії, що живиться від змінного струму 220В від мережі із заземленою нейтраллю. IBM PC відноситься до електроустановок до 1000В закритого виконання, всі струмопровідні частини

знаходяться в кожухах. За способом захисту людини від ураження електричним струмом, ЕОМ і периферійна техніка повинні відповідати 1 класу захисту.

Технічні методи захисту від ураження струмом зводиться до застосування струму безпечної напруги, захисту у випадку випадкового доторкання до струмоведучих частин і від надмірних струмів, захисту у випадку переходу напруги на неструмоведучі металеві частини установки.

Безпечну напругу одержують від сітки підвищеної напруги (110-120 В) за допомогою знижувальних трансформаторів.

Захисту від доторкання до струмоведучих частин установки досягають за допомогою ізоляції, відгородження застосування блокуючих пристроїв запобіжної сигналізації та неприступності розташування установок.

Розподільні щитки поміщають у закриті металеві кожухи-ящики.

Запобіжну сигналізацію застосовують у вигляді плакатів і надписів. Найкращими світловими сигналізаціями є подвійні, яких при наявності напруги горить червона лампочка, а при її відсутності - зелена.

Захист від надмірних струмів – короткого замикання і струмів перевантаження, які можуть спричинити займання ізоляції, здійснюється запобіжниками й автоматичними вимикачами, а захист від переходу напруги на струмоведучі частини за допомогою захисного заземлення і захисного вимикання.

В табл. 4.14 наведені небезпечні фактори ураження людини електричним струмом.

Таблиця 4.14 – Небезпечні фактори ураження людини електричним струмом

№	Шкідливий фактор	Наслідки	Заходи
1	Небезпечний рівень напруги струмопровідних частин обчислювальної та побутової техніки	Зростання ризику ураження електричним струмом	Релейний захист струму дотику, захисні заземлюючі корпуси. Попереджувальні знаки про рівень напруги.

У таблиці 4.15 відображено фактичні та оптимальні значення для параметрів електропостачання.

Таблиця 4.15 – Параметри електропостачання на робочому місці

Значення	Напруга, В	Частота, Гц	Тип розетки/вилки	Тип фази
Фактичне	220	50	F	Однафазна, трипровідна
Оптимальне	220	50	C, F	Однофазна, трипровідна

Вживаються такі запобіжні заходи для уникнення наслідків ураження людини електричним струмом (табл. 4.16):

Таблиця 4.16 – Запобіжні заходи

№	Технічні	Організаційні	ЗІЗ
1	Релейний захист струму дотику, захисні заземлюючі корпуси	Проведення робіт з електричним обладнанням лише проінструктованим персоналом. Створення плану короткострокових відпочинків.	відсутні

Запобігання пожежі досягається виключенням утворення джерел загорянь і горючого середовища. У таблиці 4.17 приведено шкідливі фактори.

Таблиця 4.17 — Шкідливі фактори, пов’язані з пожежною безпекою

№	Шкідливий фактор	Наслідок
1	Коротке замикання, електротравми, пожежі, летальні наслідки	Коротке замикання, пожежі, електротравми, летальні наслідки
2	Коротке замикання	Електротравми, пожежі, летальні наслідки
3	Порушення протипожежного режиму	Електротравми, пожежі, летальні наслідки

В цьому приміщенні можливі пожежі таких класів: А – горіння твердих речовин, Е – горіння електроустановок під напругою. Для забезпечення цих категорій застосовуються заходи, що вказані в таблиці 4.18.

Таблиця 4.18 – Запобіжні заходи

№	Технічні	Організаційні	ЗІЗ
1	Контроль параметрів за допомогою термометра La Crosse WS8005; використання кондиціонеру DEKKER DSH105R/G (для кондиціонування і провітрювання)	Розвантаження електровузлів після виконання роботи; ознайомлення з інструкціями по використанню електроприладів;	відсутні
2	Наявність вогнегасника порошкового типу ОП-5 та автоматичної системи “ГАРАНТ-Р” (ПО-2), узгоджений план евакуації	Ознайомлення з інструкціями по використанню протипожежних засобів; узгоджений план евакуації	відсутні
3	Наявність вогнегасника порошкового типу ОП-5 та автоматичної системи “ГАРАНТ-Р” (ПО-2), узгоджений план евакуації	Ознайомлення з інструкціями по використанню протипожежних засобів; узгоджений план евакуації	відсутні

4.3 Висновок до четвертого розділу

Аналіз умов праці в розглянутому робочому приміщенні показав, що умови праці з ПЕОМ відповідають нормативам.

Інструктаж і навчання всіх працюючих безпечних методів роботи –основна передумова різкого зниження і навіть повної ліквідації травматизму.

Головне завдання навчання та інструктажу полягає в тому, щоб робітники до вступу на роботу одержали необхідні знання прийому безпечної роботи і вивчили правила техніки безпеки.

ВИСНОВКИ

Робота висвітлює основне дослідницьке питання, яке полягає в тому, яку процедуру можна використати для виявлення відмінностей ризиків безпеки у внутрішній інфраструктурі та хмарній інфраструктурі.

Ця робота сприятиме організаціям, які планують перенести свої платіжні шлюзи на хмарну інфраструктуру за допомогою аналізу прогалин безпеки на основі STRIDE.

Процедура ілюструє, як захопити активи інформаційної системи за допомогою корпоративної архітектури. Робота виділяє бізнес-актив із процесу платіжної транзакції та представляє взаємозв’язок з інформаційними системами за допомогою ArchiMate.

В першому розділі кваліфікаційної роботи освітнього рівня «Магістр» описано з методи і мови моделювання, використаних у дослідженні, представляючи обґрунтування обраного методу.

В другому розділі кваліфікаційної роботи розглянуто типи платіжних шлюзів і огляд інфраструктур, використаних у дослідженні. Крім того, тут представлено корпоративну архітектуру внутрішньої та хмарної інфраструктури для визначення контексту та зв’язку бізнес-активів і допоміжних активів за допомогою моделювання корпоративної архітектури.

В третьому розділі кваліфікаційної роботи описано процес виявлення активів і представлено цілі безпеки бізнес-активів. Розділ зосереджено на пошуку загроз для активів інформаційної системи у внутрішній інфраструктурі та хмарній інфраструктурі за допомогою методу моделювання загроз STRIDE. Крім того, буде обговорено, як ризики будуть диференціюватись на основі міграції інфраструктури.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 12 Benefits of Cloud Computing and Its Advantages. Salesforce.com. URL : https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/.

2 RightScale. RightScale 2018 State of the Cloud Report, 2018. URL : https://www.suse.com/media/report/rightscale_2018_state_of_the_cloud_report.pdf

3 Gartner.com. Gartner Identifies the Top 10 Trends Impacting Infrastructure and Operations for 2019. Gartner , 2018. URL : https://www.gartner.com/en/newsroom /press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras.

4 Network Security Infrastructure Report. Netscout, 2018. URL : https://www.netscout.com/report/.

5 R. Matulevičius, Fundamentals of secure system modelling. Cham: Springer, 2017. URL : https://www.researchgate.net/publication/321502403_Fundamentals _of_Secure_System _Modelling.

6 R. M. Blank and P. D. Gallagher. Guide for conducting risk assessments. 2012. URL : https://mpra.ub.uni-muenchen.de/83659/1/MPRA_paper_83659.pdf.

7 Managing Risk in the Cloud. in Cloud Computing Security, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742: CRC Press. 2016. p. 79–86.

8 PCI DSS Quick Reference Guide," p. 1–40. URL : https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

9 H. Bahtit, B. Regragui. Risk Management for ISO 27005 Decision support. Int. J. Innov. Res. Sci. Eng. Technol., vol. 2, 2013. URL : https://docplayer.net/21261061-Risk-management-for-iso-27005-decision-support-hanane-bahtit-1-boubker-regragui-2.html

10 V. Agrawal. A Framework for the Information Classification in ISO 27005 Standard. 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). New York. NY, 2017. p. 264-269.

11 IT-Grundschutz - Information Security Management." URL : https://www.tuvit.de/en/services/information-security-management/it-grundschutz.

12 ISO/IEC 27005:2018(en), Information technology — Security techniques — Information security risk management. URL : https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en.

13 M. S. Lund, B. Solhaug, and K. Stølen. Model-driven risk analysis : the CORAS approach". Springer, 2010. p. 22-28.

14 N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann and R. Wieringa. An integrated conceptual model for information system security risk management supported by enterprise architecture management. Software & Systems Modeling, 2018. p. 32-38.

15 F. Vraalsen, T. Mahler, M.S. Lund, I. Hogganvik, F. Braber, K. Stølen. Assessing Enterprise Risk Level: The CORAS approach. in Advances in Enterprise Information Technology Security, IGI Global, 1AD, 2018. p. 311–333.

16 CLUSIF. MEHARI-2010-Reference-Manual of Mehari, 2010 Knowledge Base". 2010. 128 p.

17 N. Mayer, P. Heymans, and R. Matulevičius, (2007). Design of a Modelling Language for Information System Security Risk Management, 1st International Conference on Research Challenges in Information Science, 2007. p. 121-132.

18 C. Alberts, A. Dorofee, J. Stevens and C. Woody. Introduction to the OCTAVE® Approach. Carnegie Mellon University, 2003 URL : https://www.itgovernance.co.uk/files/Octave.pdf.

19 A. Tewari. Comparison between ISO 27005, OCTAVE & NIST SP 800-30 - SISA Information Security. SISA Information Security. URL : https://www.sisainfosec.com/blogs/comparison-between-iso-27005-octave-nist-sp-800-30/.

20 Z. Jourdan, R. Rainer, Jr., T. Marshall and F. Ford. An Investigation Of Organizational Information Security Risk Analysis. Journal of Service Science (JSS), vol. 3. no. 2, 2010. p. 38-46.

21 N. Al-Safwani, S. Hassan, and N. Katuk. A Multiple Attribute Decision Making for Improving Information Security Control Assessment. Int. J. Comput. Appl., vol. 89. no. 3, 2014. p. 19–24.

22 O. Altuhhova, R. Matulevičius, and N. Ahmed. An Extension of Business Process Model and Notation for Security Risk Management. Int. J. Inf. Syst. Model. Des. vol. 4. no. 4, 2013. p. 93–113.

23 M. Välja. Improving IT Architecture Modeling Through Automation : Cyber Security Analysis of Smart Grids. PhD dissertation. Stockholm, 2018. p. 32-44.

24 P. Koning, I-to-i.nl, 2017. URL : https://www.i-to-i.nl/wp-content/uploads/2017/04/Risk-Modeling-With-ArchiMate-Pascal-de-Koning-mrt2017.pdf.

25 Opengroup.org. ArchiMate® 3.0.1 Specification. URL : http://pubs.opengroup.org/architecture/ArchiMate3-doc/chap03.html.

26 T. Sommestad, M. Ekstedt, and H. Holm. The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures. IEEE Syst. J. vol. 7. no. 3, 2013. p. 363–373.

27 H. Holm, K. Shahzad, M. Buschle and M. Ekstedt. P2CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language. in IEEE Transactions on Dependable and Secure Computing. vol. 12. no. 6, 2015. p. 626-639.

28 Foreseeti. SecuriLang Reference Manual -. URL : https://community.securicad.com/securilang-reference-manual/.

29 H. Shafiq, K. Asif, A. Shabir, R. Ghulam, and I. Sajid. Threat Modelling Methodologies: A Survey. 2014. URL : https://www.academia.edu /29215191/threat_modelling_methodologies_a_survey.

30 Shostack A. Threat modeling: Designing for Security. Wiley, 2014. p. 35-46.

31 A. Obot. Security Risk Management of E-commerce Systems. University of Tartu, 2018. p. 34-39.

32 F. Innerhofer-Oberperfler and R. Breu. Using an Enterprise Architecture for IT Risk Management. ISSA, 2006. p. 34-42.

33 N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal. Threat modeling for cloud data center infrastructures. in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). vol. 10128 LNCS, 2017. p. 302–319.

34 K. Singh and J. Aggarwal. Fear of cloud computing: Identifying risks involved using STRIDE. Troindia.in, 2017. URL : http://troindia.in/journal/ ijcesr/vol4iss11/23-30.pdf.

35 R. Matulevičius, A. Norta, C. Udokwu, and R. Nõukas. Security risk management in the aviation turnaround sector. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). vol. 10018 LNCS, 2016. p. 119–140.

36 J. Janulevičius. Method of Information Security Risk Analysis for Virtualized Systems. Vilnius Gediminas Technical University, 2016. p. 1–112.

37 I. Tovstukha. Management of Security Risks in the Enterprise Architecture using ArchiMate and Mal-activities. University of Tartu, 2017. p. 32-42.

38 W. Engelsman, B. Christophe Feltus, S. González Paredes, D. Diligens Jim Hietala, T. Open Group Henk Jonkers, and B. Sebastien Massart. Modeling Enterprise Risk Management and Security with the ArchiMate ® Language. 2015. p. 32-46.

39 Alexsoft. How to integrate payment gateways and choose a provider. 2019, URL : https://www.altexsoft.com/blog/business/how-to-choose-and-integrate-payment-gateway-online-payments-transaction-processing-and-payment-gateways-providers/.

40 P. Smirnoff. Understanding Hardware Security Modules (HSMs). 2017. URL : https://www.cryptomathic.com/news-events/blog/understanding-hardware-security-modules -hsms.

41 C. Wueest, M. Ballano Barcena, and L. O'brien. Mistakes in the IaaS Cloud could put your data at risk. Symantec, 2015. p. 32-38.

42 Zubair Lone and Aaqib Iqbal Wani. A Survey of Security Issues and Attacks in Cloud and their possible defences, 2017. p. 32-39.

43 T. Erl, R. Puttini, and Z. Mahmood, Cloud computing : concepts, technology, and architecture (1st ed.). Prentice Hall Press, 2013. p. 86-92.

44 T. Shinder. What Does Shared Responsibility in the Cloud Mean?. Microsoft Azure, 2018. URL : https://blogs.msdn.microsoft.com/azuresecurity/ 2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/.

45 H. Jonkers, M. M. Lankhorst, H. W. L. Ter Doest, F. Arbab, H. Bosma, and R. J. Wieringa. Enterprise architecture: Management tool and blueprint for the organisation. Inf Syst Front, vol. 8, 2006. p. 63–66.

46 44 U.S. Code § 3542. Legal Information Institute. URL : https://www.law.cornell.edu/uscode/text/44/3542.

47 Linda Pesante. Introduction to Information Security, 2008. URL : https://cyberdivision.net/2017/10/09/introduction-to-information-security/.

48 Statista. Digital buyers worldwide 2021 | Statistic. URL : https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/.

49 Verizon. PCI Compliance Report. URL : http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf.

50 J. Vijayan. After Target, Neiman Marcus breaches, does PCI compliance mean anything? | Computerworld. 2014. URL : https://www.computerworld.com/article/2486879/data-security/after-target--neiman-marcus-breaches--does-pci-compliance-mean-anything-.html.

51 A.W. Coburn, J. Daffron, A.Smith, J. Bordeau, É.Leverett, S. Sweeney, T. Harvey. Cyber Risk Outlook 2018. Centre for Risk Studies, University of Cambridge, 2018. p. 74-82.

52 Varonis Data Lab, “2018 Global data risk report," 2018 URL : https://info.varonis.com/hubfs/2018 Varonis Global Data Risk Report.pdf.

53 L. Irwin. Lessons to learn from recent payment card breaches - IT Governance Blog. URL : https://www.itgovernance.co.uk/blog/pci-dss-lessons-to-learn-from-recent-payment-card-breaches.

54 SecurityMetrics 2017 SecurityMetrics Guide To PCI DSS COMPLIANCE, 2017. URL : https://www.securitymetrics.com/static/resources/orange/2017-securitymetrics-pci-guide.pdf.

55 Cybersecurity Insiders. Insider Threats CA Technologies, 2018. URL : https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf.

56 S. Dhar. Code Execution and Privilege Escalation – Databases, 2016 URL : https://resources.infosecinstitute.com/code-execution-and-privilege-escalation-databases/#gref.

57 N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal. Threat Modeling for Cloud Data Center Infrastructures. 2016. URL : https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=921695.

58 P. Mell and T. Grance, Cloud Computing Security Essentials and Architecture. The NIST Definition of Cloud Computing: National Institute of Standards and Technology, Information Technology Laboratory, 2018. 16 p.

Додаток А

Тези конференцій А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

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 IT-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.