

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

Факультет інформатики та обчислювальної техніки

Кафедра технічної кібернетики

«На правах рукопису»
УДК 004.042

«До захисту допущено»

Завідувач кафедри
І.Р. Пархомей
(підпис)

“ ” _____ 2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 126 «Інформаційні системи та технології»

на тему: Мінімізація ризиків інформаційної безпеки корпорації на основі хмарних обчислень

Виконав: студент другого курсу, групи ІК-71мп
(шифр групи)

Гасанов Вадим Анверович

(прізвище, ім'я, по батькові)

(підпис)

Науковий керівник професор, д.т.н., професор Стенін О.А.

(посада, науковий ступінь, вчене звання, прізвище та ініціали)

(підпис)

Консультант норм. контроль доцент, к.т.н., доцент Пасько В.П.

(назва розділу)

(посада, науковий ступінь, вчене звання, прізвище, ініціали)

(підпис)

Рецензент проректор, д.т.н., професор Новіков О.М.

(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали)

(підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

(підпис)

Київ – 2018 року

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

Факультет Інформатики та обчислювальної техніки

Кафедра Технічної кібернетики

Рівень вищої освіти – другий (магістерський)

Спеціальність 126 «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ

Завідувач кафедри

І.Р. Пархомей

(підпис)

« ___ » _____ 2018 р.

ЗАВДАННЯ

на магістерську дисертацію студенту

Гасанова Вадима Анверовича

(прізвище, ім'я, по батькові)

1. Тема магістерської дисертації «Мінімізація ризиків інформаційної безпеки корпорації на основі хмарних обчислень»
науковий керівник магістерської дисертації Стенін О.А., д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «07» листопада 2018 р. № 4112-с
2. Термін подання студентом магістерської дисертації _____
3. Об'єкт дослідження процес вибору хмарних ІТ-сервісів для впровадження у корпорації при розробці ІТ-стратегії
4. Предмет дослідження методи та моделі підтримки прийняття рішень при виборі хмарних ІТ-сервісів для впровадження в корпорації
5. Перелік завдань, які потрібно розробити – провести аналіз для визначення можливих ризиків використання хмарних середовищ у взаємозв'язку з вразливістю корпорації; визначити перелік вразливостей для кожного ризику, побудувати для них вектори системи загального обліку вразливостей; розробити алгоритм системи з урахуванням існуючих методик оцінки рівнів ризику визначити ризик-моделі; розробити інформаційно-аналітичну систему оцінки ІБ для впровадження хмарного середовища

6. Орієнтовний перелік ілюстративного матеріалу шість плакатів

7. Орієнтовний перелік публікацій три публікації

8. Консультанти розділів магістерської дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Норм. контроль	Пасько В. П., доцент ТК		

9. Дата видачі завдання 05 вересня 2017 року

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Ознайомлення з завданням	11.09.2017 – 29.09.2017 рр.	
2	Аналіз ринку для знаходження аналогів	02.10.2017 – 27.10.2017 рр.	
3	Аналіз предметної області	30.10.2017 – 01.12.2017 рр.	
4	Аналіз інформаційної безпеки	22.01.2018 – 16.02.2018 рр.	
5	Аналіз визначення можливих ризиків використання хмарних середовищ	26.02.2018 – 16.03.2018.рр.	
6	Визначення перелік вразливостей для кожного ризику	19.03.2018 – 25.05.2018.рр.	
7	Розробка алгоритму системи з урахуванням існуючих методик оцінки рівнів ризику	01.06.2018 – 29.06.2018 рр.	
8	Визначення ризик–моделі	02.07.2018 – 13.07.2018 рр.	
9	Розробка додатків	16.07.2018 – 27.07.2018 рр.	
10	Проектування бази даних	30.07.2018 – 31.08.2018 рр.	
11	Розробка інформаційно-аналітичної системи оцінки ІБ	03.09.2018 – 12.10.2018 рр.	
12	Тестування інформаційно-аналітичної системи оцінки ІБ	15.10.2018 – 26.10.2018 рр.	
13	Маркетинговий аналіз стартап-проекту	29.10.2018 – 16.11.2018 рр.	
14	Попередній захист дисертації	19.11.2018 р.	
15	Проходження норм. контролю	10.12.2018 – 14.12.2018 рр.	
16	Захист магістерської дисертації	18.12.2018 р.	

Студент

(підпис)

А.В. Гасанов
(ініціали, прізвище)

Науковий керівник дисертації

(підпис)

О.А. Стенін
(ініціали, прізвище)

АНОТАЦІЯ

Структура та обсяг роботи. Пояснювальна записка магістерської дисертації складається з 5 розділів, розмір роботи 130 сторінок, містить 26 рисунків, 43 таблиць, 6 додатків, 84 джерело.

Магістерська дисертація присвячена дослідженню проблеми ефективної оцінки ризиків інформаційної безпеки міграції корпорації до хмарного середовища для подальшого прийняття управлінських рішень, механізмів взаємодії суб'єктів у процесі нівелювання інформаційних ризиків системи, оцінці ефективності методик та ймовірності ризику реалізації загроз інформаційній безпеці як фактору переходу корпорації до хмарного ІТ-середовища.

З'ясовано сутність понять: «ризик», «інформаційний ризик», «хмарне середовище». Розглянуто актуальні теоретико-методологічні засади розробки ризик-моделей та організаційні аспекти впровадження оцінки ефективності інформаційної безпеки міграції корпорації у хмарне середовище з урахуванням тенденцій захисту інформації. Проаналізовано основні принципи функціонування складових критеріїв побудови ризик-моделі для прийняття управлінських рішень. Узагальнено світовий досвід в країнах Європи та Азії й українську специфіку застосування хмарних обчислень на основі існуючих стандартів класифікації стандартотворюючих корпорації. Розроблено інформаційно-аналітичну систему підтримки прийняття рішень інформаційних ризиків на основі позиціонування структури та зображення механізму програми.

Ключові слова: ризик, оцінка ризиків, управління ризиками, хмарні технології, прийняття управлінських рішень.

ABSTRACT

Structure and scope of work. The explanatory note of the master's dissertation consists of 5 sections, the size of the work is 130 page, contains 26 illustrations, 43 tables, 6 applications, 84 titles.

The master's dissertation is devoted to the research of the problem of effective information security risk assessment of the migration to the cloud environment for further adoption of managerial decisions, mechanisms of interaction of subjects in the process of leveling the information risks of the system, assessment of the effectiveness of the techniques and the risk of the threat of information security threats as a factor in the transition of the corporation to cloud IT-environment.

The essence of concepts is defined: "risk", "information risk", "cloud IT-environment". The current theoretical and methodological principles of risk-model development and organizational aspects of implementation of the assessment of the effectiveness of information security of corporation migration in the cloud environment are considered in the light of information protection tendencies. The basic principles of the components functioning for constructing a risk-model for making managerial decisions are analyzed. Generalized world experience in the countries of Europe and Asia and the Ukrainian specificity of the application of cloud computing on the basis of existing standardization standards of standard-setting corporations. An informational and analytical system for supporting decision-making on information risks is developed and based on the positioning of the structure and image of the program mechanism.

Keywords: risk, risk assessment, risk management, cloud technologies, management decision making.

Пояснювальна записка
до магістерської дисертації

на тему: МІНІМІЗАЦІЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАЦІЇ
НА ОСНОВІ ХМАРНИХ ОБЧИСЛЕНЬ

Київ – 2018 року

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	9
ВСТУП	10
РОЗДІЛ 1 АНАЛІЗ СУЧАСНИХ ПИТАНЬ ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ	13
1.1 Базові питання дослідження.....	13
1.2 Аналіз моделі надання послуг хмарних обчислень.....	15
1.3 Аналіз стандартів в галузі хмарних технологій.....	18
1.4 Аналіз структури ризиків втрати інформації.....	24
1.5 Системний аналіз ризиків втрати інформації в інформаційно–обчислювальних системах корпорацій.....	27
Висновки до розділу.....	33
РОЗДІЛ 2. ЗАСТОСУВАННЯ МОДЕЛЕЙ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ВИБОРІ ХМАРНИХ ІТ–СЕРВІСІВ	35
2.1 Моделі формування ризиків втрати інформації в корпоративній інформаційно–обчислювальній системі.....	35
2.2 Модель підтримки прийняття рішень про перехід до хмарних ІТ-сервісів.....	39
2.3. Оцінювання ефективності методик та їх порівняльний аналіз.....	49
Висновки до розділу.....	65
РОЗДІЛ 3. ПРОЕКТУВАННЯ ІНФОРМАЦІЙНО–АНАЛІТИЧНОЇ СИСТЕМИ.....	67
3.1 Процес вибору хмарних ІТ–сервісів.....	67
3.2 Алгоритм роботи	69
3.3. Формування архітектури та інструментів програмного продукту	77
3.4 Вибір мови програмування інформаційно-аналітичної системи	81
Висновки до розділу.....	83
РОЗДІЛ 4. ІНФОРМАЦІЙНО–АНАЛІТИЧНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ІНФОРМАЦІЙНИХ РИЗИКІВ.....	85
4.1 Позичування структури та зображення механізму програми	86
4.2 Візуалізація реалізованого продукту та опис взаємодії із користувачем	86
Висновки до розділу.....	91
РОЗДІЛ 5. МАРКЕТИНГОВИЙ АНАЛІЗ СТАРТАП–ПРОЕКТУ	93
5.1 Опис ідеї проекту	93
5.2 Технологічний аудит ідеї проекту	94
5.3 Аналіз ринкових можливостей запуску стартап–проєкту	95
5.4 Розроблення ринкової стратегії проекту.....	101
5.5 Розроблення маркетингової програми стартап–проєкту	103
Висновки по розділу	104
ВИСНОВКИ.....	105

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	107
ДОДАТКИ.....	116
ДОДАТОК А Архітектура хмарних обчислень.....	117
ДОДАТОК Б Схема суб'єктів хмарних обчислень.....	119
ДОДАТОК В Методика підтримки прийняття рішень при виборі хмарних ІТ-сервісів для впровадження в корпорації.....	121
ДОДАТОК Г Функціональна модель оцінки і аналізу корпоративних ІТ-додатків.....	123
ДОДАТОК Д ER-Діаграма на рівні атрибутів.....	125
ДОДАТОК Е Візуальна репрезентація інформаційно-аналітичної системи	127

ПЕРЕЛІК СКОРОЧЕНЬ

CCRA – Corporation Cloud Risk Assessment;

IT – інформаційні технології;

НСД – несанкціонований доступ;

IoT – інтернет речі;

CVSS – система загального обліку вразливостей;

NVS – база даних вразливостей;

ISO – міжнародна організація зі стандартизації;

ITU – міжнародний союз електрозв'язку;

IEC – міжнародна електротехнічна комісія;

CEN – європейський комітет зі стандартизації;

ІБ – інформаційна безпека;

УРІБ – управління ризиками інформаційної безпеки;

СЗІ – система захисту інформації;

СЗОВ – система загального обліку вразливостей;

SLA – угода про рівень послуг;

SSL – зашифрований канал зв'язку;

ОПР – особа, яка приймає рішення;

ЦОД – центр обробки даних;

АНР (MAI) – Analytic Hierarchy Process (метод аналізу ієрархій);

JTC – Об'єднаним технічним комітетом;

ВСТУП

До хмарних технологій проявляють зацікавленість як великі компанії, які намагаються оптимізувати свої витрати на ІТ—інфраструктуру корпорації, так і малі компанії, які не мають можливості відразу розгорнути свою власну інфраструктуру. Зростання інтересу до технології хмарних обчислень пов'язано з економічним ефектом від їх використання. Однак, незважаючи на явні переваги, під час використання хмарних обчислень необхідно вирішувати і ряд проблемних питань. Основними з них є довіра до постачальника сервісу, забезпечення конфіденційності, цілісності, справжності та неспростовності інформації на усіх етапах її існування, безперебійність в роботі, захист від несанкціонованого доступу (НСД) та збереження особистих даних користувачів, які передаються та обробляються в хмарі.

Поштовхом до стрімкого розвитку хмарних технологій стало реалізація підключення різноманітних пристроїв до глобальної мережі, так званих інтернет речей (Internet of Things – IoT).

Зростаюча кількість підключень до інтернету мобільних пристроїв з використанням соціальних мереж та хмарною інфраструктурою для вирішення різноманітних задач характеризується Третя платформа.

Часто хмари порівнюють з мейнфреймами. Відмінність хмари від мейнфреймів, в не обмеженості (теоретично) його обчислювальній потужності, а також взаємодії користувача з відправленим на обробку завданням.

В хмарі термінал є потужним обчислювальним пристроєм, який не тільки накопичує проміжні результати, а й безпосередньо керує глобальною системою обчислювальних ресурсів.

Концепція Третьої платформи ґрунтується на чотирьох елементах: великих даних, мобільних пристроях, хмарних сервісах і соціальних технологіях.

Третя Платформа ґрунтується на хмарних рішеннях, завдяки наданню віддаленого доступу до інформаційних ресурсів, у тому числі за допомогою різноманітних мобільних пристроїв.

За даними компанії IDC, на розвиток рішень на базі Третьої платформи впливають такі фактори:

- **Доступність.** Забезпечення доступу у будь-який час, в будь-якому місці і через будь-який пристрій.
- **Вартість.** Гнучкість моделей ціноутворення, вартість встановлюється за фактичне споживання.
- **Канали збуту.** Доступ до додатків здійснюється з використанням хмарних технологій.
- **Самообслуговування.** Зниження витрат і прискорення процесу впровадження ІТ—рішень за рахунок їх оренди.

В хмарі існують:

1. переваги:

- спеціалізований персонал (фахівці в галузі безпеки інформації);
- централізоване керування, конфігурація системи безпеки та її аудит;
- стійкість платформи (автоматизація діяльності щодо забезпечення безпеки, тестування та виправлення помилок у компонентів платформи);
- наявність ресурсів (динамічне масштабування ресурсів системи, резервування та аварійного відновлення);
- резервне копіювання і відновлення (більш високий рівень резервного копіювання і відновлення);
- мобільність кінцевих клієнтів;
- концентрація даних (єдине місце для зберігання та обробки даних).

2. недоліки з точки зору безпеки інформації:

- складність системи (велика кількість компонентів, з яких складається хмара);
- загальне багатокористувальницьке середовище;
- однорідність програмного та апаратного складу платформи (вплив недоліка у хмарі на усіх користувачів послуг).
- використання інтернету (незахищеність мережі інтернет)

– втрата контролю (передача контролю над інформацією провайдеру хмари, що несе додаткові ризики для безпеки інформації).

Будь-яка діяльність у галузі ІТ вимагає прийняття певних рішень, а це в свою чергу пов'язане з оцінюванням майбутнього. Таке оцінювання реалізується шляхом максимального врахування невизначеностей та активних дій елементів середовища і завжди є певною мірою ризикованим.

Головною проблемою наукового визначення поняття “ризик” є його комплексний, системний характер, що вимагає залучення широкого кола вчених – представників багатьох дисциплін. Саме тут вимагається застосування методів системного аналізу, врахування всіх факторів, що сприяють виникненню критичних ситуацій, і аналізу всіх наслідків, до яких вони можуть призвести.

Загалом ризик потрібно розглядати як суспільне явище, що має власну сутність, відповідні закономірності розвитку й управління в ситуації невизначеності.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ ПИТАНЬ ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ

1.1 Базові питання дослідження

На сучасному етапі розвитку ІТ важливу роль для корпорацій стали грати хмарні обчислення. Все більше корпорацій розглядають можливість переходу до хмарних технологій, які мають величезний потенціал. Популярність хмарних ІТ доводиться тим, що за результатами досліджень аналітичних компаній Forrester Research, IDC [1-4], обсяг світового ринку хмарних технологій до 2020 року зросте до \$ 160 млрд.

Однак для того, щоб реалізувати переваги і отримати максимальну віддачу від своїх інвестицій, корпорації повинні брати до уваги різні проблеми і особливості впровадження хмарних ІТ, унікальні у кожному конкретному випадку [5, 6].

При виборі хмарних ІТ–сервісів з'являються такі складності:

- розгляд безліч функціональних сфер корпорації, які потребують модернізації відповідно до вимог бізнесу;
- розгляд безліч альтернатив для впровадження; визначення типу хмарної моделі і моделі розгортання;
- визначення здійсненності міграції/впровадження (технічні можливості);
- визначення переваг для бізнесу і ризиків, пов'язаних з впровадженням.

Потенційні порушення в галузі безпеки є основною перешкодою на шляху впровадження хмарних технологій [7-11]. Проблема розробки ІТ–стратегії впровадження полягає в тому, що ще на стадії її формування важливо визначити, які програми найбільше будуть задовольняти бізнес–стратегії корпорації, оцінити провайдерів хмарних послуг з точки зору надійності і безпеки і провести аналіз задоволеності співробітників [12-15].

Мета дослідження: Підвищення ефективності управлінських рішень при розробці ІТ–стратегії шляхом використання інформаційно-аналітичної системи

для оптимальної підтримки прийняття рішень при виборі хмарних ІТ–сервісів для корпорації..

Для досягнення мети вирішуються наступні завдання:

1. Дослідження проблем, що стоять перед корпорацією при виборі хмарних ІТ–сервісів для впровадження.

2. Аналіз існуючих:

– методів, моделей і програмних продуктів оцінки ефективності та ризиків впровадження інвестиційних ІТ–проектів на предмет їх можливого використання для обґрунтування рішень при впровадженні хмарних технологій в умовах невизначеності;

– методик підтримки прийняття рішень при виборі хмарних ІТ–сервісів для впровадження в корпорації.

3. Використання існуючих:

– систем критеріїв та показників оцінки результативності впровадження хмарних технологій;

– моделей оцінки результативності впровадження хмарних ІТ–сервісів на основі запропонованої системи критеріїв.

4. Розробка програмного забезпечення інформаційної системи підтримки прийняття рішень при виборі хмарних ІТ–сервісів, яке реалізує математичні моделі оцінки.

При виконанні магістерської дисертаційної роботи застосовуються методи системного аналізу, метод аналізу ієрархій, метод експертних оцінок, багатокритерійний підхід.

В процесі розробки програмного забезпечення направлено на вирішення проведення кількісної оцінки та побудови ризик–моделі хмарного середовища необхідно вирішити наступні задачі:

1. Визначити та описати можливі ризики використання хмарних середовищ в взаємозв'язку з вразливостями корпорації;

2. Визначити перелік вразливостей для кожного ризику, побудувати для них вектори системи загального обліку вразливостей (CVSS);

3. Розробити алгоритм системи з урахуванням існуючих методик оцінки рівнів ризику, де під ризиком буде розумітися комбінація частоти появи та відповідного впливу потенційно небажаних подій, які частіше за все пов'язані з загрозою інформаційної безпеки. На основі базових, часових та інфраструктурних показників CVSS–метрик будуть розраховуватися показники частоти та впливу, що призведе до більш детального розгляду як поточних положень CVSS, та їх адаптації для розрахунку задачі частоти та можливого впливу;

4. Визначити ризик–моделі на підставі отриманих рівнях впливу вразливостей. Згрупувати вразливості по принципу належності до одного рівня впливу. У зв'язку з чим необхідно в алгоритмі інформаційно-аналітичної системи використати формалізовану задачу визначення сервісного рівня, який відображає потенційний ризик, у вигляді Марковського процесу з безперервним часом. Загальне представлення можливих сервісних рівнів і інтенсивності переходів між ними дозволить у результаті виконання роботи надати прогнозовані рівні ризиків в певний момент часу.

Об'єкт дослідження: процес вибору хмарних ІТ–сервісів для впровадження для корпорації при розробці ІТ–стратегії.

Предмет дослідження: методи, моделі підтримки прийняття рішень при виборі хмарних ІТ–сервісів для впровадження в корпорації.

1.2 Аналіз моделі надання послуг хмарних обчислень

За моделлю розгортання хмари поділяють на приватні, загальнодоступні (публічні) та гібридні [16, 17].

Приватні хмари – це внутрішні хмарні інфраструктури і служби корпорації, які знаходяться в межах корпоративної мережі. Корпорація може керувати приватною хмарою як самостійно так і доручити це завдання зовнішньому підряднику.

Інфраструктура може розміщуватися:

- в приміщеннях замовника;

- у зовнішнього оператора;
- частково у замовника і частково у оператора.

Ідеальний варіант приватної хмари – хмара, розгорнута на території корпорації, яка обслуговується і контролюється її працівниками.

Загальнодоступні (публічні) хмари – це хмарні послуги, що надаються постачальником. Вони знаходяться за межами корпоративної мережі. Користувачі даних хмар не мають можливості керувати даними хмарами або обслуговувати їх, вся відповідальність покладена на власника цієї хмари. Постачальник хмарних послуг приймає на себе обов'язки по установці, управлінню, наданню та обслуговуванню ПЗ, інфраструктури додатків або фізичної інфраструктури. Замовники сплачує тільки за час використання ресурси.

Абонентом пропонованих сервісів може стати будь-яка компанія і індивідуальний користувач. Вони пропонують легкий і доступний за ціною спосіб розгортання веб-сайтів або бізнес-систем з великими можливостями масштабування, які в інших рішеннях були б недоступні. Приклади: онлайн-сервіси Amazon EC2 і Amazon Simple Storage Service (S3), Google Apps / Docs, Salesforce.com, Microsoft Office Web.

Разом з тим послуги публічних хмар в основному надаються у вигляді стандартних конфігурацій, тобто виходячи з умов найбільш поширених випадків використання. Це означає, що у користувача залишається менше можливостей по вибору конфігурації в порівнянні з системами, в яких ресурсами управляє сам споживач. Слід також мати на увазі, що, оскільки споживачі слабо контролюють інфраструктуру, процеси, що вимагають суворих заходів безпеки і відповідності нормативним вимогам, не завжди підходять для реалізації в загальнодоступному хмарі.

Гібридні хмари представляють собою поєднання загальнодоступних і приватних хмар. Зазвичай вони створюються корпорацією, а обов'язки з управління ними розподіляються між корпорацією і постачальником загальнодоступного хмари. Гібридна хмара надає послуги, частина яких

відноситься до загальнодоступних, а частина – до приватних. Зазвичай такий тип хмар використовується, коли корпорація має сезонні періоди активності. Іншими словами, як тільки внутрішня ІТ-інфраструктура не справляється з поточними завданнями, частина потужностей перекидається на публічну хмару (наприклад, великі обсяги статистичної інформації, які в необробленому вигляді не становлять цінності для корпорації), а також для надання доступу користувачам до ресурсів корпорації (до приватної хмари) через публічну хмару. Добре продумана гібридна хмара може обслуговувати як вимагає безпека критично важливі процеси, такі як отримання платежів від клієнтів, так і більш другорядні.

Основним недоліком цього типу хмари є складність ефективного створення подібних рішень і управління ними. Необхідно отримувати послуги з різних джерел і організувати їх так, як якщо б це було єдине джерело. Взаємодія між приватними і загальнодоступними компонентами може ще більше ускладнити рішення. Оскільки це відносно нова архітектурна концепція в сфері хмарних обчислень, для цієї моделі з'являються все нові і нові практичні рекомендації та інструменти, і її широке поширення може затягнутися до тих пір, поки вона не буде краще вивчена.

На думку Тома Біттман, віце-президента і провідного аналітика американської дослідницької і консалтингової компанії "Gartner" [18, 19], серед перерахованих вище трьох моделей розгортання хмар найбільш актуальною для бізнесу в даний момент є приватні хмари. Біттман виділив п'ять основних моментів, які допомагають отримати більш точне уявлення про будову приватного хмари.

Важливою особливістю приватної хмари є те, що корпорація само здійснює налаштування та підтримку хмари. Складність і вартість створення внутрішньої хмари можуть бути дуже високі, а витрати на її супроводження може перевищувати вартість використання загальнодоступних хмар.

Слід зазначити, що у приватних хмар є переваги перед загальнодоступними: більш детальний контроль над різними ресурсами хмари забезпечують компанії та доступні варіанти конфігурації. Крім того, приватні

хмари ідеальні, коли потрібно виконувати роботи, які не можна довірити загальнодоступній хмарі з міркувань безпеки.

Типові рішення моделей хмарних послуг можна згрупувати для чотирьох типів компаній: малих і середніх корпорацій, великих корпорацій, державних корпорацій і постачальників телекомунікаційних і ІТ–послуг.

Використовуючи існуючі ІТ–ресурси при одночасній інтеграції в публічні та приватні хмарні середовища, гібридні хмари набувають широкого поширення на ІТ–ринку. Корпорації отримують більший контроль над їх даними, поліпшують продуктивність додатків і можливість розширеної взаємодії. Такі середовища допомагають централізувати управління ІТ–ресурсами, і в результаті корпорація скорочує витрати і підвищує ефективність роботи.

Мережева хмара не є рішенням «на всі випадки життя» – підхід залежить від потреб і пріоритетів конкретної установи. Підбір моделі сервісів і розгортання здійснюється відповідно вимогам установи та робочими навантаженнями.

1.3 Аналіз стандартів в галузі хмарних технологій

Для проведення адекватного оцінювання інформаційних ризиків застосовуються підходи та процедури, що спираються на існуючі міжнародні стандарти з ризиків інформаційної безпеки.

Без наявності відповідних нормативних документів, що описують правові норми, проблеми, ризики і способи їх мінімізації неможливе ефективне впровадження сучасних інформаційних технологій таких як Web–, Cloud–, IoT– (Internet of Things) та інші.

Для підвищення довіри до онлайн-операцій, пом'якшення наслідків кібер–атак необхідно здійснювати розробку і впровадження міжнародних стандартів в галузі безпеки інформаційних технологій.

В сучасному інформаційному просторі, де продукти, процеси і послуги розробляються і постачаються по всьому світу з приховуванням від споживача

особливостей хмарної інфраструктури провайдера такі стандарти набувають актуальності та особливої важливості.

На сьогоднішній день ведеться активна розробка стандартів та настанов, призначених для хмарних обчислень [19]. Значна кількість стандартів, які сьогодні застосовуються до хмарних обчислень, були розроблені для «дохмарних» технологій, таких як веб-сервіси, платіжні системи.

Завдяки тому, що споживачі і провайдери хмарних послуг нерідко знаходяться в різних країнах світу набувають особливої ролі міжнародні стандарти у сфері хмарних обчислень.

Щороку у відкритому доступі з'являються нові роботи, присвячені огляду та поточному стану стандартів в сфері хмарних обчислень [19-25].

Відповідно до існуючої класифікації стандартоутворюючих корпорації та органи мають наступну ієрархію рівнів:

- Міжнародний (ISO / IEC [26, 27, 37, 38], ITU [28-36, 39]);
- Міждержавний (форуми і консорціуми [21, 23]);
- Регіональний (європейські CEN / CENELEC [22]);
- Національний (державні закони та стандарти, відомчі нормативні документи, керівництва, інструкції та ін. [20, 24, 40]).

Для стандартизації хмарних технологій державні кордони відступають, так як надавачі послуг в більшості знаходяться в різних країнах та континентах.

З причин відсутності міжнародних стандартів по сертифікації елементів хмарної інфраструктури та актуальності інформаційної безпеки елементи (дата-центри, канали і мережі комунікацій та інші) використовують сертифікати безпеки стандартів, як міжнародних, так і інших країн, суміжних напрямків.

Міжнародні корпорації, які займаються стандартами в сфері інформаційної безпеки [20] представлені на рис. 1.1. В кожній країні також існують регіональні корпорації і відомства, що займаються розробкою нормативних документів у сфері інформаційної безпеки. На рис. 1.2 представлена схема взаємодії міжнародних і регіональних стандартоутворюючих корпорацій в сфері хмарних технологій [9].

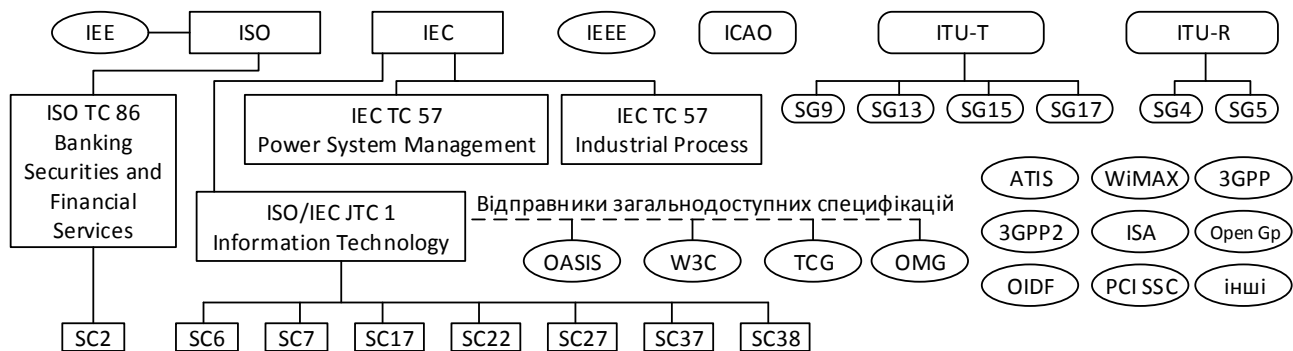


Рисунок 1.1 – Міжнародні корпорації, приймаючі участь в розробці міжнародних стандартів в галузі інформаційної безпеки хмарних технологій

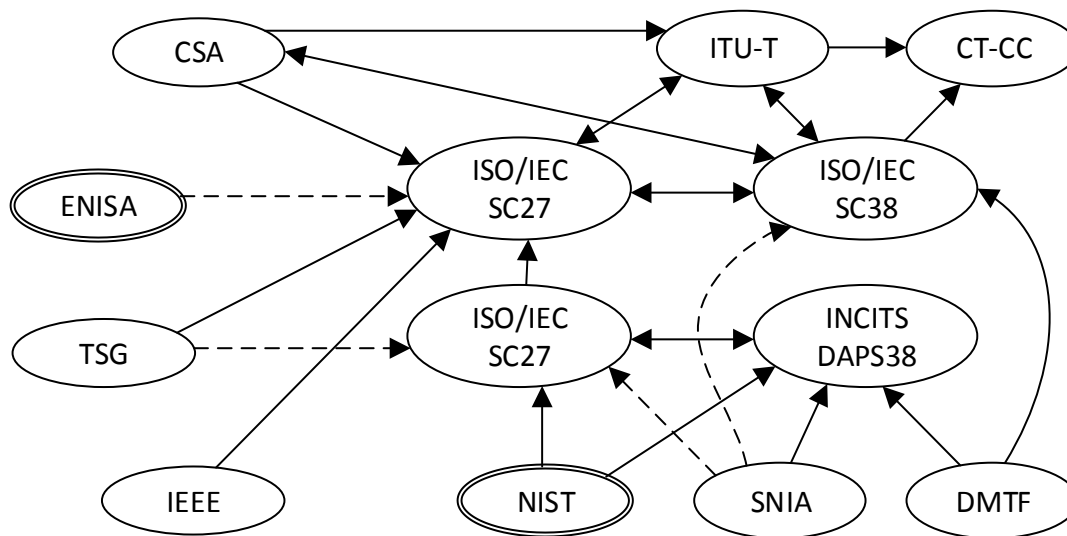


Рисунок 1.2 – Схема взаємодії між регіональними та міжнародними стандартоутворюючими корпораціями

— – Функціональна

----- – Інформаційна

Базові види хмарних послуг визначено відповідно до ISO 17788 (додаток А):

Інфраструктура як послуга (infrastructure as a service (IaaS)) – категорія хмарних послуг, в яких типом хмарних можливостей, що надаються споживачу хмарної послуги, є можливості інфраструктури. Примітка – споживач хмарної послуги не здійснює контроль або управління щодо внутрішніх фізичних або віртуальних ресурсів, але здійснює контроль над операційними системами, запам'ятовуванням і розгорнутими додатками, які використовують фізичні і віртуальні ресурси. Споживач хмарної послуги може також мати обмежену

можливість контролю над певними компонентами мережі (наприклад, брандмауерами хост–комп'ютерів);

Платформа як послуга (platform as a service (PaaS)) – категорія хмарних послуг в яких типом хмарних можливостей, які надаються споживачу хмарної послуги, є можливість платформи;

Програмне забезпечення як послуга (software as a service (SaaS)) – категорія хмарних послуг в яких типом хмарних можливостей, які надаються споживачу хмарної послуги, є можливість додатків.

Хмарні послуги мають позначення «X» aaS («послуга» as a service, «X» як сервіс).

Спочатку хмарна парадигма включала три види послуг [41,42]: IaaS, PaaS, SaaS. Починаючи з 2013 року в стандартах почали вводитись назви нових видів хмарних послуг, а саме **мережа як послуга (network as a service (NaaS))** – категорія хмарної послуги, в якій можливість, що надається споживачеві хмарної послуги, ставиться до можливостей транспортного сполучення та пов'язаним з ним мережевим можливостям [36];

З прийняттям у 2014 році міжнародного стандарту ISO17788 [26] регламентовано 7 репрезентативних категорій хмарних послуг:

- Communications as a Service (CaaS);
- Compute as a Service (ComaaS);
- Data Storage as a Service (DSaaS);
- Infrastructure as a Service (IaaS);
- Network as a Service (NaaS);
- Platform as a Service (PaaS);
- Software as a Service (SaaS).

У додатку Б цього стандарту наводиться порівняльна таблиця, в якій перераховані додаткові категорії хмарних послуг:

- Database as a Service;
- Desktop as a Service;
- Email as a Service;

- Identity as a Service;
- Management as a Service;
- Security as a Service.

Перший нормативний документ регламентуючий поняття хмарних технологій [41] не містить інформації про надавачів послуг. Надалі фахівці NIST [43] визначили 2 типу надавачі послуг:

- Cloud provider;
- Cloud consumer.

В NIST SP 800–146 [42] – визначено cloud consumer, cloud provider, а також поняття client, та акцентується увага на складність визначення ролей і відповідальності в хмарній моделі, зазначається «брокер».

Фахівці NIST в нормативних документах NIST SP 500–291[24], NIST SP 500–299 [44] визначили більш складну модель взаємодії, яка наведена на рис. 1.3, що включає:

- Cloud Consumer Person;
- Cloud Provider Person;
- Cloud Auditor;
- Cloud Broker;
- Cloud Carrier.

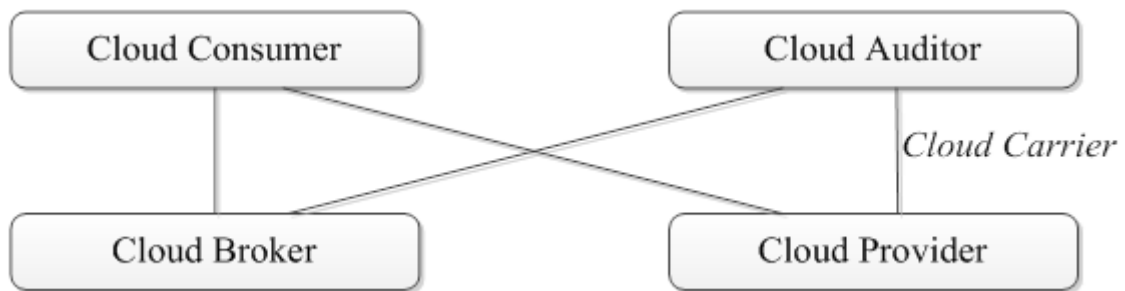


Рисунок 1.3 – Модель взаємодії учасників процесу представлення хмарних послуг згідно NIST SP 500–291:2011

Міжнародний стандарт ISO 17789 [27] вводить розширену класифікацію учасників хмарного ринку, наведена на рис. 1.4.

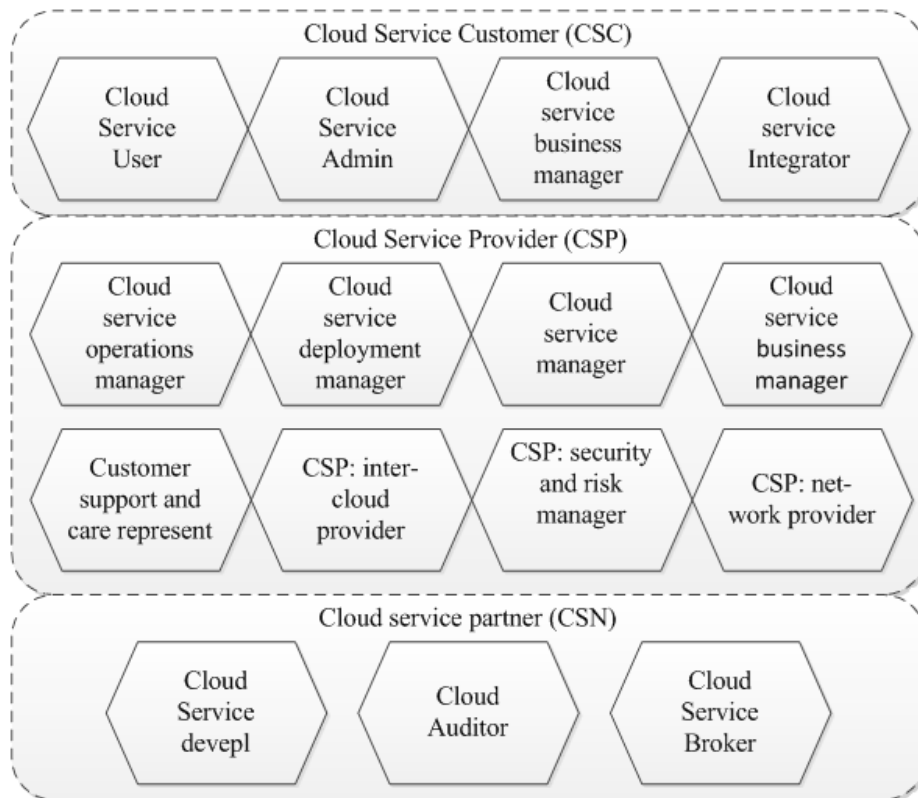


Рисунок 1.4 – Ролі учасників процесу представлення хмарних послуг згідно ISO 17789:2014

Рольова модель, прийнята в ISO 17788 [26] була врахована в керівництві ITU.T X1601 [31] в якому розглядаються такі визначення учасників:

- Споживач хмарної послуги (cloud service customer): сторона (фізична особа або корпорація), яка складається в ділових відносинах стосовно використання хмарних послуг;
- Партнер хмарної послуги (cloud service partner): партнер, що бере участь в підтримці діяльності або постачальника хмарної послуги або споживача хмарної послуги або ж надає допомогу в цій діяльності;
- Постачальник хмарної послуги (cloud service provider): сторона, яка надає хмарні послуги;
- Користувач хмарної послуги (cloud service user): особа, пов'язана зі споживачем хмарної послуги, яке користується хмарними послугами;
- Група внутрішніх користувачів (tenant): група користувачів хмарної послуги, спільно використовують доступ до набору фізичних і віртуальних ресурсів.

Останнім часом в стандартних визначеннях властивість «security» зазнає змін, поступово розширюється наповнення категорії «security». в останніх редакціях нормативних документів [26, 37] до трійки базових складових: конфіденційності, цілісності, доступності додають такі складові, як:

- Автентичність;
- Підзвітність;
- Неможливість відмови від авторства;
- Надійність.

Більш того, в стандарті [38] «security» визначається як стан захисту інформаційних активів, а конфіденційність, цілісність і доступність наводяться як окремий приклад цих активів.

У керівництві [39] дано визначення кібер–безпеки (cybersecurity), як набору інструментальних засобів, стратегії, принципів забезпечення безпеки, гарантій безпеки, керівних принципів, підходів до управління ризиками, дій, професійної підготовки, практичного досвіду, страхування і технологій, які можуть бути використані для захисту кібер–середовища, ресурсів корпорації і користувача.

У розробках NIST також зустрічаються терміни «network security», «Control system security», «IT security». Такі тенденції розширення категорії «security» знаходять застосування в нормативних документах сфери хмарних обчислень, оскільки хмарні інфраструктури безпосередньо підтримують мережеві, керуючі та інформаційні технології.

1.4 Аналіз структури ризиків втрати інформації

При визначенні ризику ключовими словами є “невизначеність”, “майбутнє”, “можливість”, “ймовірність”, “втрати”, “збитки”, “діяльність”, “вибір” і є спільним, незалежно від сфери його застосування, практично для всіх визначень терміну “ризик”.

Основні характеристики (складові) ризику[45-47]:

– чистий ризик (Pure Risk) – можливість отримання збитків або нульового результату, можливість несподіваних або незапланованих втрат без альтернативи можливого виграшу;

– спекулятивний ризик (Speculative Risk) – ймовірність отримати як негативний, так і позитивний результат, можливість не тільки не втратити, а й отримати певні вигоди з різних варіантів розвитку подій.

“Чистий ризик” за своєю суттю визначає втрати (результатом є негативні наслідки), а “спекулятивний ризик” – прибуток.

Існування ризику пов’язано з неможливістю повністю передбачити майбутнє.

Ризик існує в тих випадках, коли необхідно приймати рішення та є суб’єктивною причиною появи ризику.

Величина ризику оцінюється об’єктивно і суб’єктивно.

Об’єктивна міра ризику базуються на даних про минулі втрати, на гіпотези про тенденції, стани і можливі розвитку ймовірності втрат сьогодні і в майбутньому.

Основними параметрами оцінок ступеня ризику є такі:

1. ймовірність втрат (чим вона вища, тим більший ризик);
2. величина втрат (чим вона більша, тим небезпечніший ризик).

Ієрархічна структура складових ризику наведена на рис. 1.5.

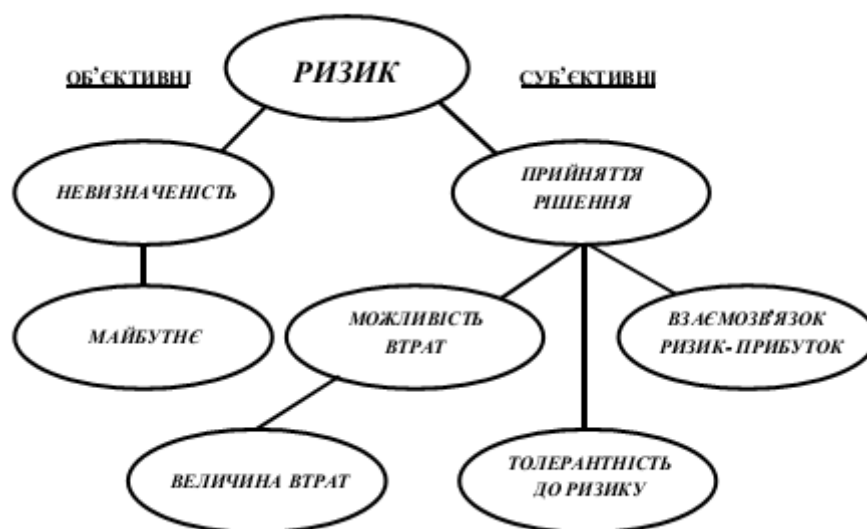


Рисунок 1.5 – Ієрархічна структура складових ризику

Отже, ризик це можливість недосягнення суб'єктом поставленої мети, зумовлена необхідністю прийняття рішення в умовах невизначеності (в недетермінованій системі).

Проблема ризику пов'язана з невизначеністю (неточністю, недостовірністю, ненадійністю) знань про умови та процеси, які відбуваються в об'єкті та зовнішньому середовищі, з ймовірнісним характером виникнення небажаних подій. Дослідження ризиків пов'язане з аналізом невизначеності, а ефективні шляхи для попередження небажаних подій, зменшення рівня ризиків при прийнятті рішень пов'язані із цілеспрямованою мінімізацією невизначеності.

Невизначеність передбачає наявність факторів, при яких результати дій не є детермінованими, а ступінь можливого впливу цих факторів на результати невідома (неповнота або неточність інформації).

Оскільки невизначеність складова ризику, вона є джерелом ризику. Для зменшення ризику необхідно мінімізувати невизначеність, тобто, перевести невизначеність у повну визначеність за рахунок отримання якісної, вичерпної та достовірної інформації у потрібний момент часу.

При прийнятті рішень в умовах невизначеності необхідно визначити, формалізувати та оцінити ризики, джерелом яких є ця невизначеність.

При визначенні ризиків слід враховувати:

1. точність визначення ризику;
2. мінімізацію одного ризику, яка може викликати зростання інших ризиків;
3. кількість ризиків, їх характеристики та особливості, методи боротьби з ними.

Фактори впливу на ризикову ситуацію мають певні ознаки, за якими їх можна класифікувати:

- можливість керування (зовнішні та внутрішні фактори);
- складність дії (одиночної та комплексної дії);
- вплив на ризик (прямого та опосередкованого впливу).

Всі ці характеристики (ознаки) тісно переплетені у факторі впливу (рис. 1.6).

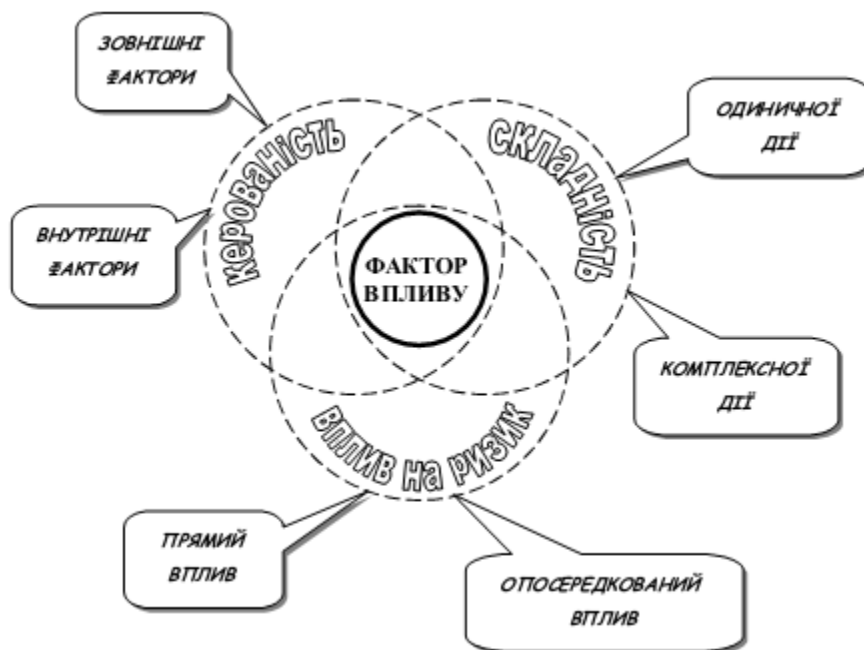


Рисунок 1.6 – Класифікація факторів впливу на ризикову ситуацію

Для адекватного та ефективного реагування на ризики та їх передбачення необхідно якомога точніше та різнобічно визначити предмет дослідження, класифікувати і формалізувати його та оцінити реальні можливості його реалізації.

1.5 Системний аналіз ризиків втрати інформації в інформаційно–обчислювальних системах корпорацій.

Не зважаючи на величезну популярність та свої численні переваги хмарні технології не позбавлені ризиків в таких галузях, як безпека, конфіденційність і доступність даних.

Створенню єдиної методики оцінки ризиків хмарних обчислень перешкоджає відсутність єдиної, стандартної, структурованої платформи, яка могла б допомогти корпораціям в оцінці і зниженні ризиків хмарних технологій. Так існують методи, які дозволяють зробити систему безпечною спочатку, замість того щоб використовувати атестати безпеки постачальника послуг хмарних обчислень.

Особливістю прийняття управлінських рішень являється необхідність врахування впливу невизначених факторів і розгляд усіх можливих наслідків та альтернатив.

Розробка моделей прийняття рішень в умовах невизначеності має велике практичне значення.

Вагомою загрозою для працездатності корпорації являється порушення цілісності інформації.

В теперішній час спостерігається зростання числа загроз і вразливостей інформації, таких як шахрайство, шпигунство, вандалізму, пожежі або повені. Оцінка ризиків є важливою частиною для визначення масштабу та ймовірності реалізації загроз безпеці інформації.

В процесі оцінки ризику здійснюється оцінювання:

- ймовірності і потенційний збиток від виявлених загроз, заходи рівня ризику інформаційних активів, а також ставляться їх до конфіденційності, цілісності та доступності;

- ефективності існуючих заходів для визначення найбільш критичних активів корпорації та визначення пріоритетів і рекомендацій для захисту активів.

Під інформаційними ризиками прийнято розуміти загрозу виникнення втрат або збитків у результаті використання інформаційних технологій. Інформаційні ризики пов'язані з обробкою інформації (створенням, передачею, збереженням) з використанням електронних носіїв або інших засобів зв'язку.

Інформаційні ризики, які виникають в межах корпорації, відносять до внутрішніх.

Інформаційні ризики, які виникають внаслідок дії зовнішніх факторів, відносять до зовнішніх.

В інформаційних відносинах корпорації наявні загрози:

- пов'язані з посяганнями на інформаційні ресурси корпорації;
- що виникають під час формування інформаційного середовища корпорації.

Способами реалізації інформаційних загроз є [48,49]:

- маніпулювання інформацією (дезінформація, тощо);

- порушення доступу до інформації (НСД, необґрунтоване обмеження доступу до інформаційних ресурсів тощо);
- руйнування та використання несанкціонованих інформаційних ресурсів;
- інформаційний тероризм (розповсюдження шкідливого ПЗ).

За чинним законодавством України, інформація є об'єктом права власності, а також об'єктом володіння, використання та розпорядження. Інформаційні ризики слід розглядати і враховувати як економічні (майнові, виробничі, фінансові) [50]. Детальну класифікацію інформаційних ризиків наведено на рис. 1.7.

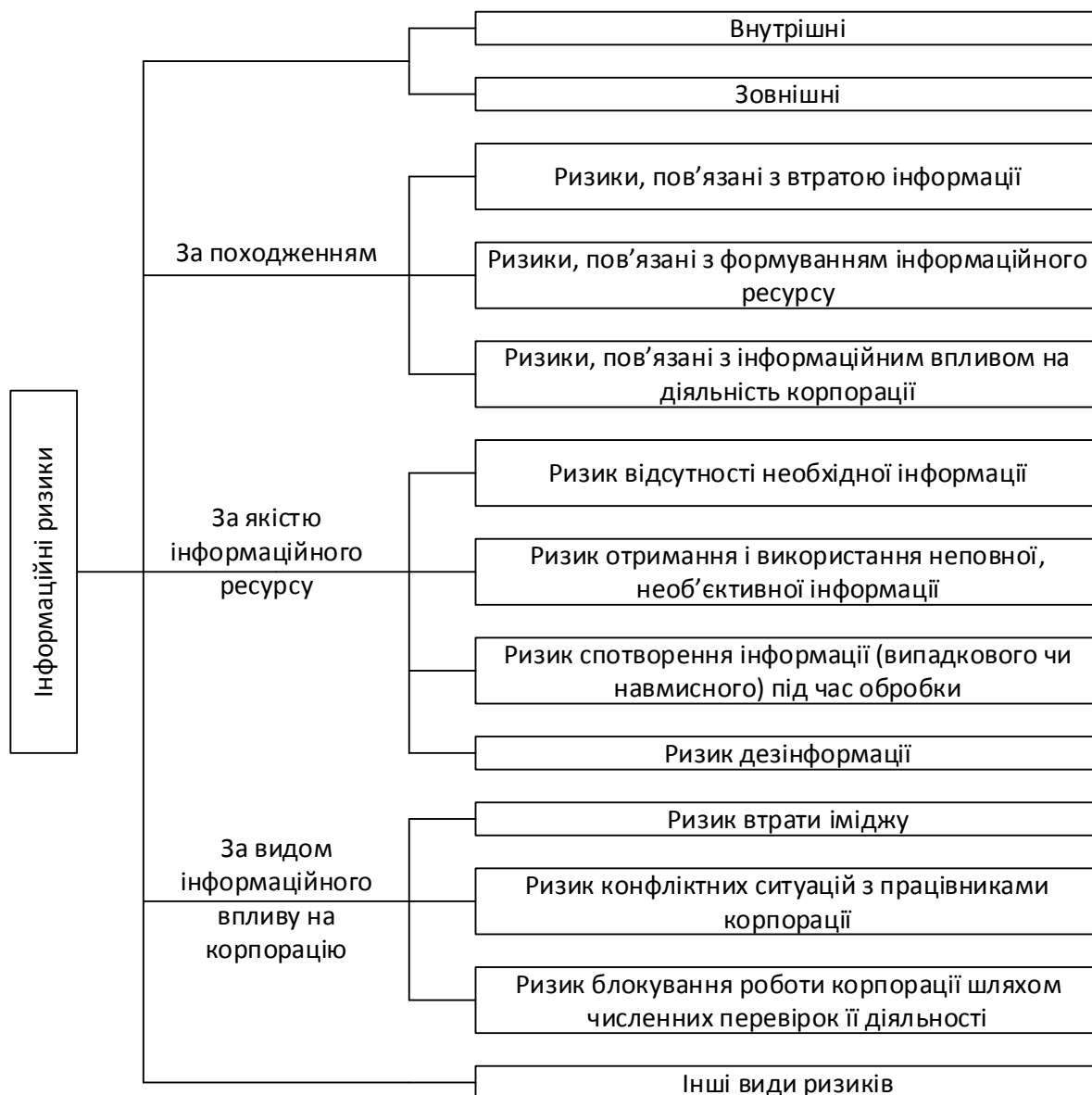


Рисунок 1.7 – Класифікація інформаційних ризиків

За своїм походженням інформаційні ризики поділяються на три категорії [51]:

– ризики, пов’язані з втратою інформації (витоком, руйнуванням, знищенням). Особливо небезпечним є ризик втрати інформації з обмеженим доступом;

– ризики, пов’язані з формуванням інформаційного ресурсу – ризики збору інформації, ризики узагальнення і класифікації інформації, ризики обробки інформації, ризики представлення інформації;

– ризики, пов’язані з інформаційним впливом на діяльність корпорації (поширення неправдивої, негативної інформації).

Процес аналізу ризиків складається з етапів:

– визначення видів ризиків, існуючих або тих що можуть з’явитися та впливати на діяльність корпорації;

– оцінки впливу на діяльність корпорації та оцінки ймовірної шкоди, що може бути заподіяна внаслідок реалізації того або іншого ризику.

Для управління інформаційними ризиками потрібно ідентифікувати всі можливі небезпеки, які загрожують інформаційній системі корпорації. Найчастіше під час розрахунку ризиків використовується формула [49,52, 83]:

$$AV * EF * ARO = ALE, \quad (1.1)$$

де AV (Asset Value) — вартість ресурсу;

EF (Exposure Factor) — міра вразливості ресурсу до загрози;

ARO (Annual Rate of Occurrence) — оцінка ймовірності реалізації загрози;

ALE (Annual Lost Exposure) — підсумкові очікувані втрати від конкретної загрози за певний період часу.

Нехай є n активів, відносна вартість активу a_j ($j = 1, n$). Також нехай c_{ij} - це вплив вразливості v_i на актив a_j . Тоді сукупний вплив вразливості v_i на активи корпорації обчислюється за формулою:

$$V_i = \sum_{(j=1)}^n v_{ij} * C_j \quad (1.2)$$

Нехай є p загроз, які впливають на V вразливостей, а d_{ki} - це потенціал впливу загрози t_k уразливості v_i . Тоді відносний сукупний вплив загрози T_k визначається за формулою:

$$T_k = \sum_{(i=1)}^m d_{ki} * V_i \quad (1.3)$$

Нехай є q засобів управління, які можуть пом'якшити p загроз, а e_{lk} - вплив засобів контролю Z_0 на загрозу t_k . Тоді відносний сукупний вплив засобів контролю Z_0 визначається за формулою:

$$Z_0 = \sum_{(i-1)}^p e_{0i} * T_i \quad (1.4)$$

Модель формування ризиків втрати інформації повинна:

- враховувати найбільшу кількість впливових факторів;
- дозволяти розраховувати ймовірність виникнення вразливостей та реалізації загрози;
- вирахувати часові межі для реалізації загроз і наслідки у вигляді збитків;
- визначати доцільність застосування запропонованих засобів захисту з оцінкою ступеня захищеності системи.

Моделювання та отримання цих показників дозволяє корпорації прийняти рішення щодо безпеки інформації в інформаційно-обчислювальній системі корпорації, а саме управляти ризиками інформаційної безпеки[53, 54].

Вартість ресурсів складається з вартості апаратного та ПЗ, інформації. Міра вразливості ресурсу до загрози (Exposure Factor) вказує на вразливість ресурсу по відношенню до даної загрози. Для якісної оцінки ризиків цей показник знаходиться в діапазоні від 1 до 3, де:

1. мінімальна міра вразливості (слабка дія);
2. ресурс підлягає відновленню (середня дія);
3. ресурс вимагає повної заміни після реалізації загрози (максимальна дія).

Оцінка ймовірності реалізації загрози також знаходиться в діапазоні від 1 до 3 (низька, середня, висока) та вказує, наскільки ймовірна реалізація певної загрози за певний період часу (як правило, протягом року).

Управління ризиками призначене для зниження високих і середніх ризиків до значень низких ризиків. Зниження показників ризику досягається за рахунок зменшення складових (AV , EF) шляхом вживання відповідних заходів.

Ризик може бути:

- прийнятий – корпорація згодна на ризик і пов'язані з ним витрати, інформаційна система працює у звичайному режимі;

- скасований – вживання заходів щодо ліквідації джерела ризику (видалення із системи програмного забезпечення, що істотно порушує вимоги інформаційної безпеки тощо);
- знижений – з метою зменшення показника ризику будуть вжиті відповідні заходи;
- переданий – компенсацію потенційного збитку корпорація передає іншій відповідній фірмі (установі).

На рис. 1.8 представлені три способи, за допомогою яких можна провести оцінку інформаційних ризиків:

- методи;
- управляючі документи;
- інструменти.



Рисунок 1.8 – Способи оцінки інформаційних ризиків.

Під методом розуміється сукупність дій, які необхідно зробити для вирішення певної задачі або досягти поставленої мети, а саме провести оцінку ризиків. Метод – це покрокова інструкція плюс інструмент для проведення оцінки ризиків корпорації.

Методи оцінки ризику поділяються на:

- кількісні – використовуються вимірні, об'єктивні дані для визначення вартості активів, ймовірність втрати і пов'язаних з ними ризиків;
- якісні – використовується відносний показник ризику або вартості активу;
- змішаний – комбінація кількісного і якісного методу, сукупність переваг і недоліків вище згаданих методів.

Висновки до розділу

У першому розділі проведено аналіз літературних джерел за темою магістерською дисертації. Досліджено існуючі стандарти в області створення хмарних інформаційно–обчислювальних систем, визначені основні проблеми, пов’язані з використанням хмарних технологій.

Розглянуті розповсюджені в Україні та світі моделі архітектурних рівнів обчислювальної хмари і визначені їх переваги та недоліки. Проведено порівняння їх характеристик з зазначенням ступенів реалізації та функціональних можливостей.

Проведено аналіз:

- джерел виникнення ризикових ситуацій та запропоновано класифікацію ризиків втрати інформації корпорації;
- впливу ризиків втрати інформації на ефективність роботи і конкурентоспроможність корпорації.

Зроблено висновок, що у корпораціях, які використовують гібридні хмари, є вибір: коли використовувати хмарне середовище, а коли – традиційну ІТ–інфраструктуру. Такий підхід покращує функціональні можливості і відповідність сучасним вимогам до гнучкості, високої надійності, відмовостійкості та безпеки середовища, а також гарантує дотримання вимог чинного законодавства в галузі ІТ–технологій. Добре продумана гібридна хмара може обслуговувати критично важливі процеси відповідно до вимог безпеки інформації.

Міжнародні стандарти мають переважно концептуально–рекомендаційний характер і не враховують багатьох факторів, котрі суттєво впливають на точність та об’єктивність оцінювання ризиків.

Провідними корпораціями, що займаються питаннями безпеки в хмарі, є Альянс безпека в хмарі (Cloud Security Alliance, CSA), що складається з представників ІТ–індустрії, а також дві державні корпорації Європи та США: Європейське агентство мережної та інформаційної безпеки (ENISA) і Національний інститут стандартів і технологій (NIST).

Кожна з корпорацій створила відповідний документ з класифікацією всіх існуючих проблем ІБ в хмарі.

При формуванні стратегії розвитку корпорації слід приділити увагу питанням безпеки. ІТ-фахівці повинні оцінювати ризики, пов'язані з безпекою хмарної архітектури. Крім того, стратегія повинна враховувати подальший розвиток хмарної моделі і дії.

Для прийняття рішення щодо безпеки інформації в інформаційно-обчислювальній системі корпорації, а саме для управління ризиками інформаційної безпеки необхідно створити модель формування ризиків втрати інформації, а саме:

- враховувати найбільшу кількість впливових факторів;
- дозволяти розраховувати ймовірність виникнення вразливостей та реалізації загрози;
- обчислювати час реалізації загрози і можливі збитки;
- визначати ефективність впровадження засобів захисту та ступінь захищеності системи.

РОЗДІЛ 2. ЗАСТОСУВАННЯ МОДЕЛЕЙ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ВИБОРІ ХМАРНИХ ІТ–СЕРВІСІВ

2.1 Моделі формування ризиків втрати інформації в корпоративній інформаційно–обчислювальній системі.

Модель формування ризиків втрати інформації повинна:

- враховувати найбільшу кількість впливових факторів;
- дозволяти розраховувати ймовірність виникнення вразливостей та реалізації загрози;
- обчислювати час реалізації загрози і можливі збитки;
- визначати ефективність впровадження засобів захисту та ступінь захищеності системи.

Моделювання та отримання цих показників дозволяє корпорації прийняти рішення щодо безпеки інформації в інформаційно–обчислювальній системі корпорації, а саме для управління ризиками інформаційної безпеки.

Основною моделлю управління ризиками інформаційної безпеки (далі – УРІБ) є процесна модель, що відображена в усіх стандартних підходах до УРІБ і являє собою основу ISO/IEC 27005 і BS 7799–3. УРІБ не є математичною моделлю, вона дає перелік і послідовність етапів, які необхідні для УРІБ корпорації:

- планування – визначається політика та методологія управління ризиками, здійснюється оцінювання ризиків (інвентаризація активів, складання профілів загроз і вразливостей, оцінювання ефективності контрзаходів і потенційного збитку, визначення допустимого рівня залишкових ризиків);
- реалізації – виконуються роботи з обробки інформації про ризики, оцінювання критичності ризиків, планування та впровадження заходів щодо кожного з ризиків. За результатами етапу планування керівництво корпорації приймає рішення стосовно кожного з ідентифікованих ризиків: проігнорувати, уникнути, передати зовнішній стороні або мінімізувати та розробляє і впроваджує план протидій по кожному з ризиків;

- перевірки – проводиться аналіз функціонування відповідних механізмів мінімізації ризиків;
- дії – за результатами постійного моніторингу та проведених перевірок виконується коригування, яке включає в себе переоцінювання ризиків, коригування політики і методології управління ризиками, а також план обробки ризиків [55].

Такі методики, як CRAMM, FRAP, OCTAVE, є класичними та базуються на використанні процесної моделі з опитувальною схемою, з використанням готових міжнародних стандартів, із яких необхідно вибрати оптимальні для інформаційно-обчислювальної системи корпорації та оцінити їх за наданою системою критеріїв оцінювання:

- класифікація та перелік ресурсів – визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання ресурсів;
- класифікація та набір вразливостей – визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання вразливостей;
- класифікація та набір ризиків – визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання ризиків;
- класифікація та набір засобів і заходів безпеки – визначений перелік якісних і чисельних (у тому числі складених) критеріїв оцінювання вартості та надійності засобів і заходів безпеки.

За результатами відповідей на запитання процесної моделі з опитувальною схемою обчислюються показники та виводяться за пріоритетністю перелік вразливостей, ризиків, набір протидій та дані щодо ефективності їх впровадження.

Головними відмінностями класичних методологій УРІБ є набір критеріїв оцінювання ресурсів, вразливостей, ризиків та формалізація обчислення кількісних показників.

За методикою **CRAMM** цінність даних і програмного забезпечення визначається в таких ситуаціях:

- недоступність ресурсу протягом певного періоду часу;

- руйнування ресурсу – втрата інформації, отриманої з часу останнього резервного копіювання, або повне руйнування бази даних;
- порушення конфіденційності у випадках отримання несанкціонованого доступу до інформації;
- модифікація (помилки персоналу, програмні тощо);
- помилки, пов'язані з передачею інформації (відмова від доставки, неповна доставка інформації тощо).

Для оцінювання можливого збитку CRAMM рекомендує використовувати такі параметри:

- збитки для репутації корпорації;
- порушення чинного законодавства;
- збитки для здоров'я персоналу;
- збитки, пов'язані з розголошенням персональних даних;
- фінансові втрати від розголошення інформації;
- фінансові втрати, пов'язані з відновленням ресурсів [56].

У методології CRAMM для кожної групи ресурсів і кожного із 36 типів загроз програмним забезпеченням генерується список питань, що допускають однозначну відповідь.

Рівень загроз оцінюється, як дуже високий, високий, середній, низький і дуже низький, рівень вразливості – як високий, середній і низький. На основі цієї інформації розраховуються рівні ризику від 1 до 7.

За методикою **Facilitated Risk Analysis Process (FRAP)** оцінювання рівня ризику здійснюється для незахищеної інформаційно–обчислювальної системи, що дозволяє показати ефект від впровадження системи захисту інформації (СЗІ).

Оцінювання здійснюється за такими показниками:

1. Ймовірність (Probability):

- висока (High Probability) – дуже ймовірно, що загроза реалізується упродовж наступного року;
- середня (Medium Probability) – можливо, загроза реалізується упродовж наступного року;

– низька (Low Probability) – малоімовірно, що загроза реалізується упродовж наступного року.

2. Збиток (Impact) – міра показника втрат або шкоди, що наноситься активу:

– високий (High Impact) – зупинка критично важливих процесів, яка призводить до істотних збитків, втрати іміджу або неотримання істотного прибутку;

– середній (Medium Impact) – короточасне переривання роботи критичних процесів;

– низький (Low Impact) – перерва в роботі, що не спричиняє відчутних фінансових втрат.

Оцінка визначається відповідно до правила, що задається матрицею ризику (табл. 2.1) [57].

Таблиця 2.1 – Матриця ризику за методом FRAP

		ЗБИТОК		
		Високий	Середній	Низький
Ймовірність	Висока	A	B	C
	Середня	B	B	C
	Низька	B	C	B

A – роботи з виправлення мають бути виконані негайно;

B – роботи з виправлення слід виконати найближчим часом;

C – необхідно моніторити ситуацію;

D – дії з виправлення та даний час не потрібні.

Методика **OCTAVE** передбачає три фази аналізу ризику:

– розробка профілю загроз: актив (asset), тип доступу до активу (access), джерело загрози або суб'єкт загрози (actor), тип порушення або мотив (motive), результат (outcome) і посилання на опис загрози в загальнодоступних каталогах;

– ідентифікація інфраструктурних вразливостей;

– розробка стратегії та планів безпеки.

Відповідно від типу джерела, загрози в **OCTAVE** поділяються на класи:

– загрози від людини–порушника, яка діє через мережу передавання даних;

- загрози від людини–порушника, яка використовує фізичний доступ;
- загрози, пов'язані зі збоями в роботі системи;
- інші.

Результатом реалізації загрози може бути розкриття (disclosure), зміна (modification), втрата або руйнування (loss/destruction) інформаційного ресурсу, відсутність доступу до ресурсу або відмова в обслуговуванні (interruption).

Майже в усіх методиках базою для визначення рівня ризику є ймовірність виникнення тієї чи іншої події, яка впливає на ймовірність реалізації загрози. У більшості методик визначення ймовірності здійснюється експертним методом або за базу береться статистика минулих періодів.

Для розробки моделі управління ризиками інформаційної безпеки корпорації необхідно вибрати таку модель або комбінацію моделей, яка б включала в себе якомога більше результуючих факторів, притаманних даній системі, та найбільш достовірно визначала ймовірність найгіршого сценарію реалізації загрози. При цьому така модель повинна динамічно змінювати вихідні результати (кількість користувачів, кількість комутаційного обладнання, швидкість каналу передавання даних тощо).

Керувати ризиком означає застосовувати дії, що направлені на підтримання такого рівня, що відповідає меті управління.

Основні задачі управління ризиком:

- підтримка ризику на рівні, не вищому заданого;
- мінімізація ризику при заданих умовах.

2.2 Модель підтримки прийняття рішень про перехід до хмарних ІТ-сервісів

Рішення, пов'язані з міграцією корпоративних додатків в хмару, можна вважати стратегічними, так як вони пов'язані зі значними витратами різних ресурсів і значною часткою невизначеності середовища прийняття рішень, несуть довгострокові надзвичайні наслідки для корпорації [21].

Після відбору хмарних ІТ-сервісів, які будуть ефективні для впровадження в корпорації, необхідно порівняти їх між собою. Це дозволить виявити найбільш підходящі сервіси для роботи в хмарному середовищі.

Для підтримки прийняття рішень про міграцію корпоративних додатків в хмарне середовище пропонується наступна модель до оцінки додатків які використовуються з точки зору придатності їх для роботи в хмарі.

Цей підхід має багатовимірну експертну оцінку. Корпоративні додатки пропонуються оцінювати за трьома груповим критеріями:

- Бізнес-цінність. Яку бізнес-цінність може отримати корпорація, перемістивши додатки в хмару?
- Технічна можливість. Чи реально перенести додатки в хмару?
- Ступінь ризику. Який ризик перенесення додатків в хмару?

Кожен з цих критеріїв має вирішальне значення для прийняття позитивного або негативного рішення щодо перенесення додатків в хмару. Наприклад, додаток може отримати високі оцінки по бізнес-цінності та технічної можливості, але може не бути хорошим кандидатом на перенесення в хмару, якщо рівень ризику перевищує допустимий для конкретної корпорації [78, 79].

Оцінка додатків в кожному з цих критеріїв є багатофакторним аналізом рішень. На рис. 2.1 продемонстровані етапи оцінки у вигляді схеми.

В першу чергу з самого початку із процесу оцінки виключаються ті додатки, які явно не підходять для роботи в хмарі, наприклад, такі, які не зможуть реалізувати поставлені завдання в хмарі або мають особливі вимоги до безпеки. Це робиться на 2-му етапі пропонованої методики («Оцінка результативності») по Інтегральній моделі. Виключаються ті додатки, у яких бал менше 0,5.

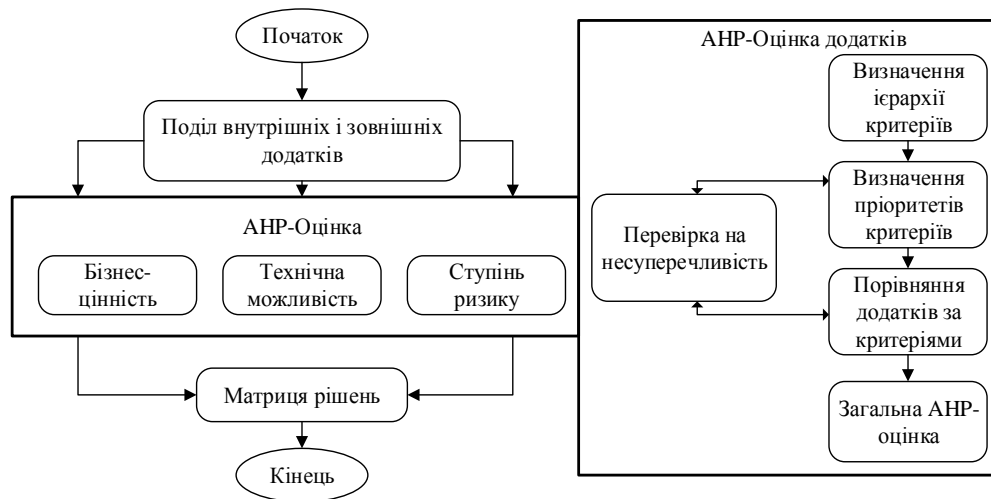


Рисунок 2.1 – Схема етапів оцінки за моделлю підтримки прийняття рішень про перехід до хмарних ІТ-сервісів

На першому етапі - поділ додатків на внутрішні і зовнішні. Ці види додатків оцінюються окремо, оскільки мають різну природу і значення. Внутрішні додатки - це додатки, доступ до яких здійснюється тільки всередині корпорації і які захищені мережевим екраном; до зовнішніх додатків можна звернутися і в обхід мережевого екрану [94]. Аргументом на користь того, що кожен тип додатків заслуговує окремого розгляду, є той факт, що питання безпеки набагато більш актуальні для зовнішніх додатків, ніж для внутрішніх.

На другому етапі здійснюється власне експертна оцінка додатків в контексті трьох критеріїв. Кожен з представлених критеріїв (бізнес-цінність, технічна можливість і ступінь ризику) має кілька підкритеріїв; вони в свою чергу можуть мати кілька рівнів підкритеріїв. При цьому важливо враховувати різний вплив рівневих підкритеріїв, тобто їх вага (значимість).

Для формалізації експертних знань і розрахунку експертних оцінок пропонується використовувати метод аналізу ієрархій, розроблений американським вченим Томасом Сааті [3, 6]. Метод аналізу ієрархій дозволяє розглядати ієрархію критеріїв за рівнями, проводити порівняння критеріїв на основі попарних порівнянь, а також формалізовувати як кількісну, так і якісну експертну інформацію.

Для кожного пропонованого групового критерію розробляється своя ієрархія критеріїв.

На третьому етапі після виконання АНР-оцінки розраховані бали додатків перетворюються в лінгвістичні оцінки. Статус «висока» присвоюється додатком, якщо його бал $(Sx) > 1/n$, де n - кількість оцінюваних додатків. Якщо бал $(Sx) < 1/n$ - присвоюється статус «низька».

Потім по матриці рішень (табл. 2.2) формуються рекомендації щодо вибору хмарних ІТ-сервісів для впровадження. Додатки, що входять у верхні рядки матриці будуть найбільш підходити для розгортання в хмарному середовищі.

Таблиця 2.2 – Приклад матриці рішень придатності додатків для міграції в хмару

АНР-оцінка: Бізнес-цінність	АНР-оцінка: Технічна можливість	АНР-оцінка: Ступінь ризиків	Придатність
Висока	Висока	Низька	Підходить за всіма критеріями. Додатки цієї групи найбільше підходять для впровадження або перенесення в хмару
Висока	Низька	Низька	Підходить за двома критеріями. Додатки цієї групи придатні для хмарних обчислень
Низька	Висока	Низька	Підходить за двома критеріями
Низька	Низька	Низька	Підходить по одному критерію. Додатки в цій групі не є ідеальними кандидатами
Низька	Низька	Висока	Не підходить ні за одним критерієм. Додатки цієї групи найкраще залишити без змін

Так, наприклад, якщо оцінюються 4 додатки, то статус «висока» матимуть додатки, чий бал більше 0,25; від 0,167 до 0,25 - «середній»; менше 0,167 - «низький».

Застосування методу аналізу ієрархій для визначення загальної оцінки переходу до хмарних обчислень

Для підвищення обґрунтованості рішень, прийнятих експертом, про пріоритети альтернатив на практиці часто використовується метод аналізу ієрархій (МАІ), що дозволяє відображати якісні оцінки експерта [21]. Основні питання МАІ були розроблені американським математиком Саати Т.Л. і

опубліковані ним в 1977 р. Даний метод використовується для вирішення слабоструктурованих і неструктурованих проблем. Принцип рішення таких проблем ґрунтується на системному підході, при якому проблему розглядають як результат взаємодії, а також взаємозалежності різних об'єктів. Особливість МАІ полягає в можливості отримання ранжируваних оцінок альтернатив на основі суб'єктивних думок експерта. У методі виробляють декомпозицію проблеми на більш прості складові елементи і роблять обробку суджень експерта.

В результаті визначають відносну значимість розглянутих альтернатив за всіма критеріями, які перебувають в ієрархії. Відносна значимість виражається чисельно у вигляді пріоритетів (векторів). Отримані значення векторів будуть оцінками у шкалі відносин і відповідати «жорстким» оцінками. Результатом даного методу буде визначення більш кращого варіанту і конкретне обґрунтування у виборі і розподілі варіантів, що дозволить в цілому досліджувати задачу докладно.

У МАІ використовується методологія дерева цілей [84]. Також заснований на формуванні ієрархії цілей і засобів по типу шарів. Даний метод призначений для вибору можливих засобів для вирішення складної багатофакторної проблеми і передбачає декомпозицію мети на більш прості складові (кошти і підцілі) і подальшої оцінки всіх цих складових елементів за допомогою парних порівнянь. Результатом буде чисельна оцінка важливості елементів ієрархії, яка використовується для вибору найкращих альтернатив рішення для вихідної проблеми [24, 29].

Процес використання МАІ для оцінки можливості для роботи в хмарі складається з декількох компонентів. Основні кроки методу аналізу ієрархії:

1. Ієрархічне представлення проблеми.
2. Побудова безлічі матриць парних порівнянь.
3. Визначення векторів локальних і глобальних пріоритетів.
4. Перевірка узгодженості отриманих результатів.
5. Обчислення загальної АНР-оцінки.

Крок № 1. Як правило, ієрархія будується з вершини - глобальної мети з точки зору вирішення проблеми, через проміжні рівні, від яких залежить мета, до самого нижнього рівня, який зазвичай є переліком альтернатив. Кожен з представлених критеріїв (бізнес-цінність, технічна можливість і ступінь ризику) має кілька підкритеріїв. Вони в свою чергу можуть мати кілька рівнів підкритеріїв. На рис. 2.2 представлена ієрархія для оцінки набору додатків за критерієм бізнес-цінність роботи в хмарі із застосуванням МАІ. Наведені критерії мають підкритерії, які всі разом утворюють групу критеріїв [81].

Аналогічним чином будуються ієрархії для інших двох критеріїв. У табл. 2.3 наведено приклад ієрархії критеріїв оцінки для всіх трьох групових критеріїв, свого роду дерево критеріїв.

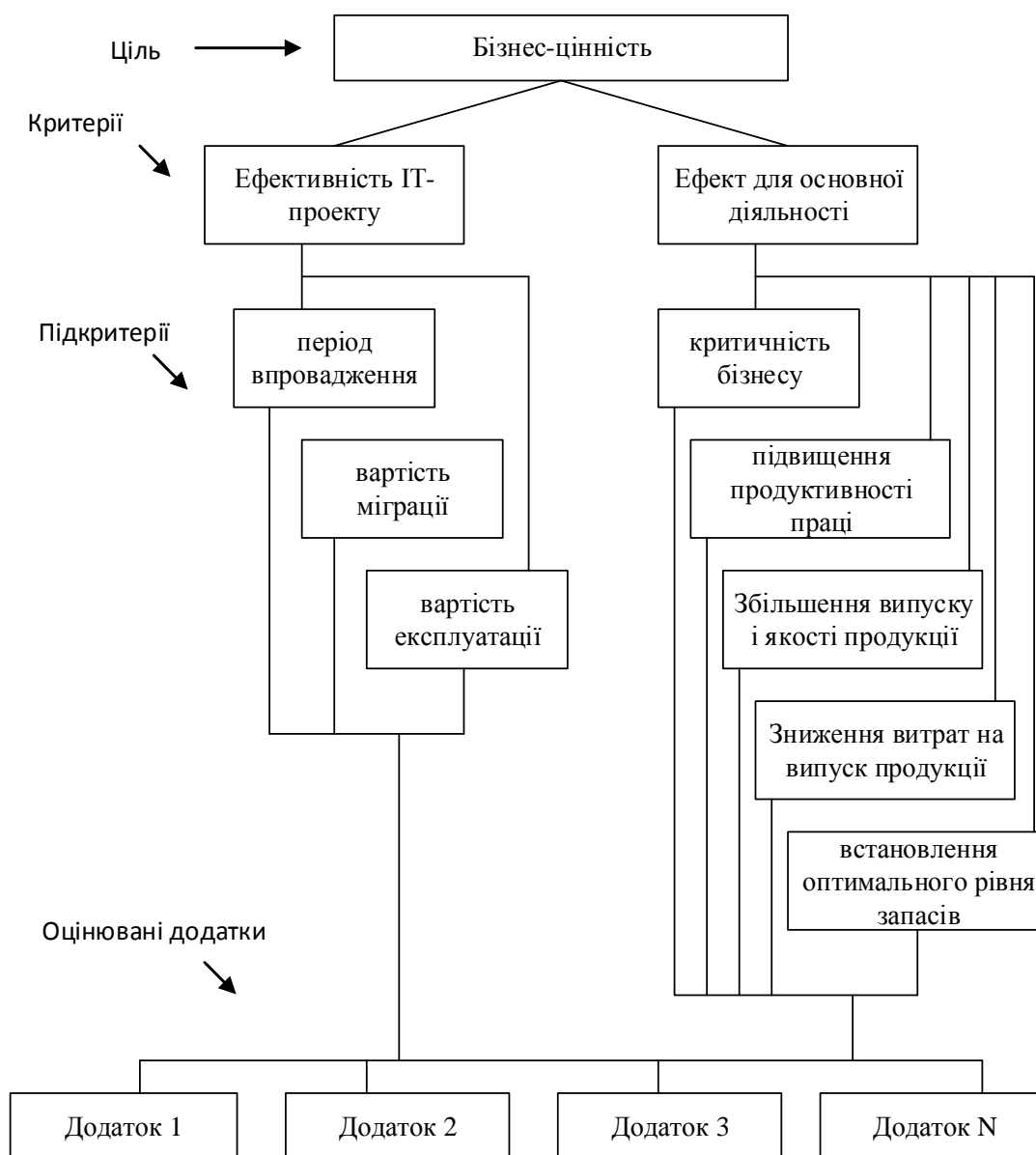


Рисунок 2.2 – Ієрархія для оцінки набору додатків за критерієм бізнес-цінність

Таблиця 2.3 – Ієрархія критеріїв для трьох групових критеріїв

Бізнес-цінність	ефективність ІТ-проекту	невеликий період впровадження
		низька вартість міграції
		низька вартість експлуатації
	Ефект для основної діяльності підприємства	критичність для бізнесу
		підвищення продуктивності праці
		збільшення випуску і якості продукції (послуг)
		зниження витрат на випуск продукції
		встановлення оптимального рівня запасів
ступінь ризику	незавершеність	нечітка ліцензія COTS
		відсутність стандартів
		передчасне пропозиція від постачальника
		нечітка модель оплати за використання
	втрата керованості	відсутність керівництва
		невідповідність корпоративної політики
	Правові-нормативні питання	Невиконання SLA
		відповідність нормативним документам
	проблеми безпеки	відсутність ізоляції даних
		захист даних
		відсутність аудиту
	технічна можливість	простота інтеграції
кількість пристроїв для інтеграції		
чітко визначена точка інтеграції		
простота міграції		Непропріетарний код
		функціональна складність
		розмір програми
		розмір бази даних
технологічний стек		середовище виконання
		бази даних
		Операційна система
дизайн програми		заснований на сервісах дизайн
		використання віртуалізації

Крок № 2. Експерт повинен скласти матрицю попарних порівнянь для критеріїв кожного рівня, висловлюючи свою думку про відносні пріоритети критеріїв відповідно до АНР-шкалою, представлені в табл. 2.4 (від 1 до 9).

На цьому кроці проводиться оцінка корпоративної програми за кількісними і якісними критеріями.

Оцінка за кількісним критерієм. При оцінці додатки за кількісним критерієм додатка порівнюються один з одним із урахуванням кількісного значення критерію:

– Бал додатка за критерієм, що має позитивний ефект, розраховується шляхом нормування значень на одиницю. Для ряду чисел $r_i, i = 1 \dots n$ нормоване значення r_{in} являє собою r_i , поділене на суму всіх наступних чисел в наборі:

$$r_{in} = \frac{r_i}{\sum_{i=1}^n r_i} \quad (2.1)$$

– За критерієм, що має негативний ефект, відносний бал додатка розраховується шляхом визначення зворотних значень і подальшої їх нормалізації. Зворотне значення - це зворотне значення числа $x: 1/x$.

Для якісного критерію відносний бал додатка розраховується шляхом попарного порівняння з використанням АНР-шкали (від 1 до 9). Процес аналогічний визначенню пріоритетів для критерію.

Таблиця 2.4 – Шкала відносної важливості

Оцінка важливості	Визначення	Пояснення
1	однакова важливість	2 елементи однаково беруть участь в досягненні мети
3	помірна важливість	один елемент краще іншого
5	суттєва важливість	досвід і судження дають сильну перевагу одному елементу над іншим
7	значна важливість	одному елементу дається настільки сильна перевага, що воно стає практично значним
9	дуже сильна перевага	очевидність переваги одного елемента над іншим підтверджується найбільш сильно
2,4,5,8	проміжні значення	застосовуються в компромісному випадку

Крок № 3. На основі кожної з побудованих матриць парних порівнянь формуються набори локальних пріоритетів, які відображають відносні пріоритети (цінність, важливість, силу впливу) порівнюваних елементів по відношенню до направляемому елементу. Для цього потрібно обчислити безліч власних векторів для кожної матриці, а потім нормалізувати результат до одиниці, одержуючи тим самим вектор пріоритетів. Одним з найкращих шляхів обчислення власних векторів є геометричне середнє. Його можна отримати, перемножая елементи в кожному рядку і витягуючи коріння n-го ступеня, де n - число елементів. Отриманий таким чином стовпець чисел нормалізується розподілом кожного числа у сумі всіх чисел.

$$a'_i = \sqrt[n]{\prod_{j=1}^n a_{ij}}, \quad (2.2)$$

$$a_i = a'_i / \sum_{i=1}^n a'_i \quad (2.3)$$

Підкритеріям має як локальний, так і глобальний пріоритет. Глобальний пріоритет -це твір його власного пріоритету (локальний пріоритет) і пріоритету батьківського критерію.

Крок № 4. При складанні матриць парних порівнянь експертні судження не повинні порушувати аксіоми впорядкованості. Зокрема, якщо один елемент кращий за інший, а той, у свою, чергу, краще третього, то перший також повинен бути краще третього, причому сила переваги першого елемента над третім повинна бути більше, ніж першого над другим і другого над третім. Однак людям властиво помилятися. Тому матриці парних порівнянь, засновані на суб'єктивних судженнях, можуть бути неузгодженими. Для оцінки ступеня відхилення від узгодженості використовується, так званий, індекс узгодженості (ІЗ).

Індекс узгодженості обротносиметричної матриці парних порівнянь обчислюється за формулою: $IЗ = (\lambda_{max} - n)/(n - 1)$,

де n - розмірність матриці (число порівнюваних елементів), λ_{max} - найбільше власне значення матриці.

Найбільше власне значення обчислюють таким чином. Спочатку необхідно підсумувати кожен стовпець матриці, потім отриману суму першого

стовпчика множать на значення першої компоненти у нормалізованого вектора пріоритетів, суму другого шпальти - другу компоненту і т. Д. Потім отримані числа підсумовують.

Узгодженість матриці можна визначити по обчисленому для неї індексу узгодженості. Для цього потрібно порівняти цей ІЗ з індексом, який обчислено для не узгодженою матриці, отриманої при випадковому виборі суджень. У табл. 2.5 наводяться середні значення випадкової узгодженості для матриць різної розмірності.

Таблиця 2.5 – Індеси узгодженості для випадкових матриць різного порядку

Розмір матриці	1	2	3	4	5	6	7	8	9	10
Випадкова узгодженість (ВУ)	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Якщо розділити ВУ на число, відповідне випадкової узгодженості матриці того ж порядку, буде отримано відношення узгодженості ($ВУ' = ІЗ/ВУ$). Величина ВУ' повинна бути близько 10% або менше, щоб бути прийнятною. У деяких випадках допускається 20%, але не більше. Якщо ВУ' виходить з цих меж, то слід перевірити судження і переглянути їх.

Крок № 5. Загальний АНР-бал додатка для критерію розраховується як сума добутку його відносного пріоритету за кожним критерієм і відносного пріоритету відповідного критерію:

$$S_x = \sum_{i=1}^M \sum_{j=1}^{N_j} (P_i) * (p_{ij}) * (S_{ijx}) \quad (2.4)$$

де: S_x - АНР-бал для х-го додатка;

M - число груп критеріїв;

N_j - число елементів в j-ої групи критеріїв;

P_i - значення пріоритету i-ої групи критеріїв;

p_{ij} - значення пріоритету j-го критерію, що належить i-ої групи критеріїв;

S_{ijx} - бал порівняння х-го додатка по j-му критерію в i-ої групи критеріїв.

Далі бали додатків зіставляються в матриці рішень. Матриця дасть цілісне уявлення про результати перенесення в хмару різних корпоративних додатків для різних критеріїв і допоможе в прийнятті обгрунтованого рішення [77].

2.3. Оцінювання ефективності методик та їх порівняльний аналіз

Для вирішення поставлених задач в магістерській дисертації будуть застосовані методики вразливості які на далі будемо розуміти як дефекти, котрі або мають патчі з виправленнями, або патчі застосовуються з часовою затримкою. Загроза безпеки – це потенційно небажане побія в об’єкті оцінки, яке може призвести к успішному використанню експлойта з небажаним впливом на конфідційність, цілісність, доступність активів об’єкту оцінки. Результатом використання вразливостей деякі загрози можуть призвести до появи небажаного події, яке будемо називати злонамірним використанням [58].

Необхідно відмітити, що злонамірне використання може виникнути лише у випадку одночасного існування як загрози, так і вразливості, тому розглядена вразливість може бути використана конкретною загрозою як наведено на рис.2.3.



Рисунок. 2.3 – Взаємозв’язок між загрозою і вразливістю

Це значить, що множина всіх потенційних злонамірних подій є підмножиною набору вразливостей та набору потенційних загроз

$$M \subset ST \cap SV, \quad (2.5)$$

де M – це набір злонамірних подій,

ST – множина загроз,

SV – множина вразливостей.

Для вирішення поставлених задач представимо методику оцінки ризиків у вигляді послідовно зв’язаних процесів (табл. 2.6). На верхньому рівні

застосованої методики по оцінці ризиків включає два основних етапи. Перший етап описує керований ризиком аналіз, включаючий оцінювання набору злочинамирних використань та пов'язаних з ними рівні ризиків, які будуть визначатися результатом кроків 2, 3, 4 використаної методики з подальшим порівнянням отриманих значень з критеріями прийняття ризику, визначених на першому кроці. Результатом цього етапу є отримання наборів ризиків потребуючих подальшої обробки [59, 60].

Таблиця 2.6 Методика оцінки ризику

Крок	Опис процесу/дії	Пояснення процесу/дії
1-й	Ідентифікація контексту оцінки ризику	1.1. Ідентифікація мети і масштабу оцінки 1.2. Опис об'єкта мети, бізнес-вимог і безпекового середовища 1.3. Визначення власників процесу 1.4. Ідентифікація активів і класифікація активів з боку власників 1.5. Опис графа активів і власників 1.6. Опис політики безпеки 1.7. Ідентифікація та опис критеріїв прийняття ризиків
2-й	Ідентифікація ризику	2.1. Ідентифікація загроз безпеки і їх впливу на активи 2.2. Ідентифікація вразливостей об'єкта оцінки, принципів забезпечення, процесів, процедур і середовища безпеки 2.3. Документування сценаріїв не коректного використання і їх угруповання
3-й	Аналіз ризику	3.1. Оцінка рівня впливу не коректного використання 3.2. Оцінка частоти не коректного використання

Продовження таблиці 2.6

4-й	Оцінювання ризику	4.1. Визначення рівня ризику для кожного набору частоти і впливу 4.2. Оцінювання ризику і порівняння з критеріями прийняття ризику 4.3. Категоризація ризику для обробки в набори ризиків 4.4. Визначення внутрішніх взаємозв'язків між наборами ризиків 4.5. Ідентифікація конфліктів між наборами ризику
-----	-------------------	--

		4.6. Призначення пріоритетів наборів і ризиків 4.7. Рішення знайдених конфліктів
5-й	Обробка ризику	5.1. Ідентифікація альтернативних рішень по забезпеченню безпеки і угруповання їх у набори 5.2. Ідентифікація ефекту і цілі альтернативних систем захисту інформації (СЗІ) 5.3. Моделювання СЗІ 5.4. Оцінка і пошук оптимальної СЗІ або набір рішень по забезпеченню безпеки

Набір ризиків для обробки, набір альтернативних рішень та інших компромісних параметрів, відповідних при розробці даної інформаційно-аналітичної системи, є вхідними даними для другого етапу методики. На цьому етапі ризики інформаційної безпеки розглядаються як проблеми та виклики, потребуючі рішення у вигляді доступних альтернативних механізмів безпеки.

В рамках першого етапу розглянутих подій включають в собі ключові елементи аналізу: набір загроз, вразливостей, злонамірне використання, його частоту і вплив, ризик інформаційної безпеки, критерії прийняття ризику. Основні сутності першого етапу підходу по оцінці ризику та їх взаємозв'язок наводяться на рис. 2.4. Всі наведені елементи необхідні для визначення рівня ризику об'єкту оцінки та його оцінки з метою з'ясування, який із ризиків потребує обробки.

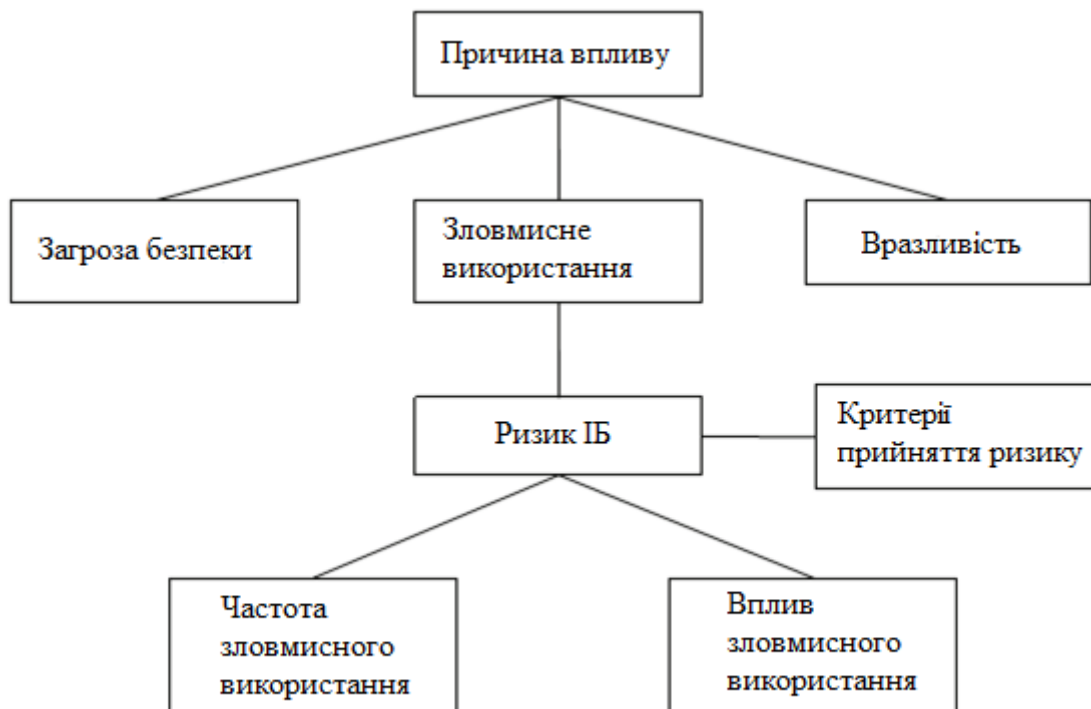


Рисунок. 2.4 – Показники для розрахунку рівня ризику в рамках першого етапу методики

В роботі алгоритма інформаційно-аналітичної системи ризик розраховується для кожного злонамірного використання шляхом комбінації його частоти з одним з впливів. Це означає, що злонамірне використання призводить к появі одного або декількох ризиків інформаційної безпеки, які залежать від кількості зв'язаних впливів. Обидва показники (частота та вплив) будуть визначені за допомогою кількісного методу оцінки на основі даних із загальнодоступних джерел, одним із яких є база даних вразливостей NVS і система загального обліку вразливостей – CVSS.

Частота злонамірного використання та його вплив будуть наведені у вигляді кількох показників: певне число проявів у проміжку тимчасового інтервалу або у ймовірній появі злонамірного використання в певний період часу. Вплив буде надаватися у вигляді фінансових втрат, втрат репутації [61, 62].

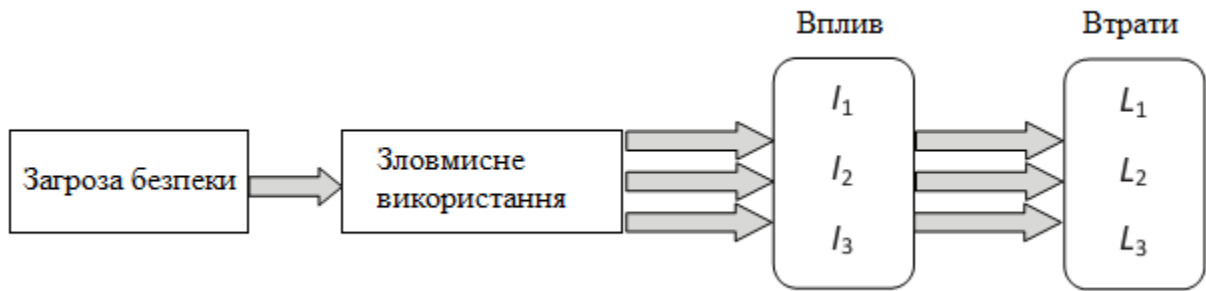


Рисунок 2.5 – Приклад ризик-моделі

Розглянемо більш детально наведену на рис. 2.5 ризик-модель втрат застосовану у алгоритмі, пов'язаних з певною погрозою інформаційної безпеки, яка буде наведена у наступному вигляді:

$$\{(I_1, F_1), (I_2, F_2), \dots, (I_n, F_n)\}, \quad (2.6)$$

де F_i – інтенсивність потоку подій або ймовірність появи злонамірної події, яка може призвести до виникнення впливу I_i .

Це призводить до безлічі втрат $\{L_1, L_2, L_3\}$, котрі будуть наведені у вигляді статистичних очікуваних втрат SOP :

$$SOP = \{(I_1, F_1)L_1 + (I_2, F_2)L_2 + \dots + (I_n, F_n)L_n\}, \quad (2.7)$$

При використанні виразу (2.6) і (2.7) в якості бази для оцінки, наведемо далі основні положення загальної системи обліку вразливостей CVSS, наведемо їх характеристику та інтерпретацію показників, яка була стосована до середовища хмарних обчислень.

Загальна система обліку вразливостей CVSS на сьогоднішній час достатньо широко використовується та все більш приймає вигляд стандарту для визначення та оцінки вразливостей [63]. Основна задача системи полягає в оцінці рівня серйозності вразливості та представлення рекомендацій щодо пом'якшення наслідків появи зв'язаних погроз. Також слід відмітити, що загальна система обліку вразливостей представляє собою інструмент для аналізу характеристик та впливів вразливостей, незалежно від вендорів (поставщиків), тому була використана для класифікації вразливостей хмарних середовищ. Набір метрик наведений на рис.2.6.

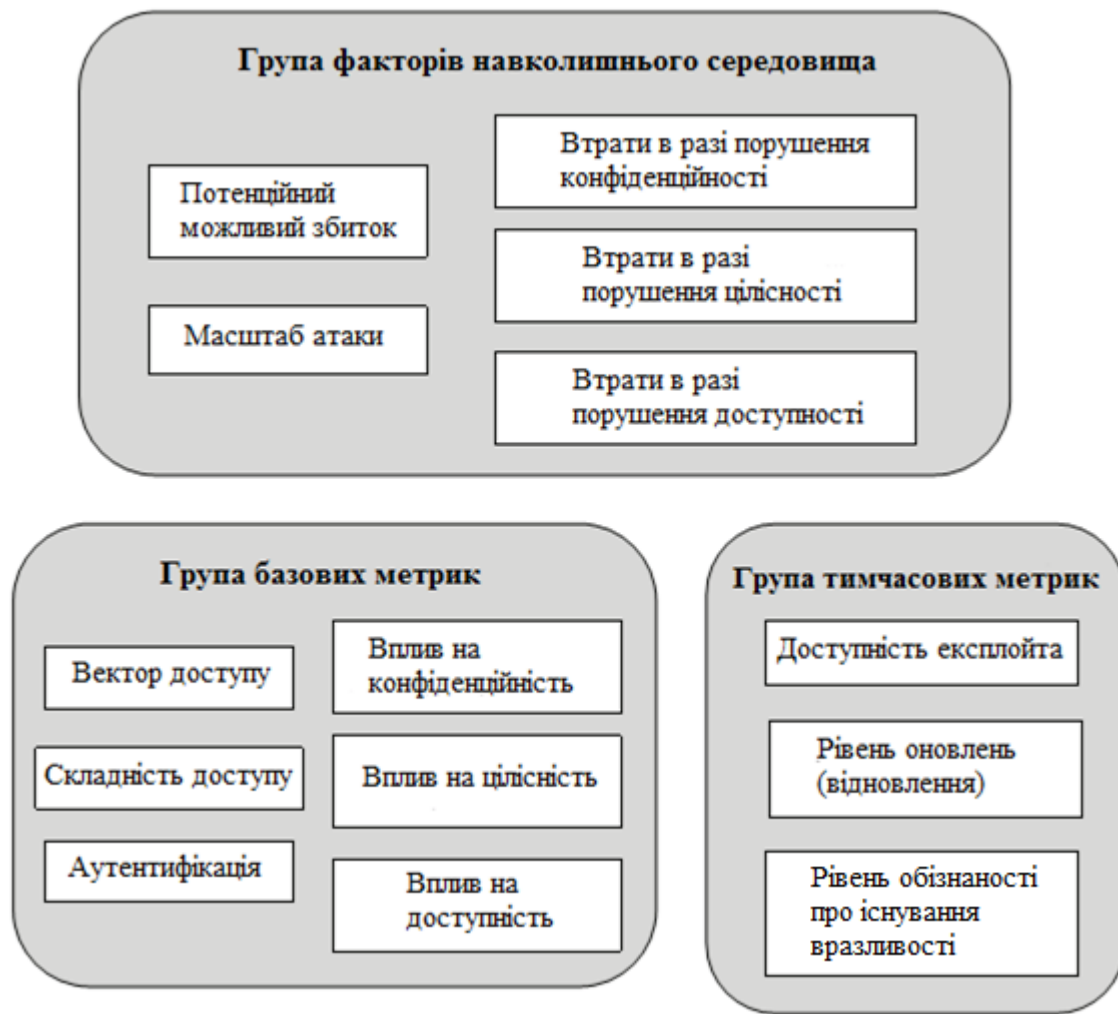


Рисунок 2.6 – Набір метрик CVSS

Розглянемо стислий опис основних груп метрик застосованої системи (для кожного показника визначена вага у відповідності з даними із керівництва по CVSS) [63].

Базова метрика. Показники базової групи описують характеристики вразливостей, які визначаються постійними і не залежать ні від часу, ні від інфраструктури. До данної групи відносяться:

- вектор доступу – відображає, яким доступом має володіти зловмисник для експлуатації вразливостей (табл. 2.7);

Таблиця 2.7 – Показники вектора доступу

Показник	Опис показника	Вага
Локальний доступ <i>L</i>	Вразливість експлуатується тільки в разі локального доступу, вимагає від зацікавленої особи фізичного доступу або локального облікового запису. Стосовно до хмарних обчислень локальним доступом володіє тільки адміністратор хмарного дата-центру	0,395

Сполучена мережа A	Вразливість вимагає від зацікавленої особи мати доступ до широковещательного домена, до домена колізій. Прикладами сполученої мережі можуть бути локальна мережа, Bluetooth, IEEE 802.11 і локальний сегмент Ethernet	0,646
Мережа N	Уразливість експлуатується віддалено і не вимагає локального або фізичного доступу	

– складний доступ – описує складність атаки, необхідної для експлуатації вразливостей, слід зауважити, чим нижчий рівень складності, тим вище показник вразливості (табл. 2.8);

Таблиця 2.8 – Показники складності доступу

Показник	Опис показника	Вага
Висока H	Для експлуатації уразливості потрібно «особлива умова», наприклад привілеї адміністратора з доступом до управління гіпервізором, віртуальним машинам	0,35
Середня M	Для експлуатації уразливості потрібно виконати ряд додаткових дій. Атака може бути здійснена тільки з певного облікового запису, вимагає збір інформації (пасивної розвідки)	0,61
Низька L	Не існує особливих умов або ускладнення обставин. Вразливий продукт має доступ до великої кількості користувачів, часто анонімних і не довірених. Показник характерний для хмарних середовищ з загальнодоступним типом розгортання, до якого має доступ велика кількість користувачів. Проведення атаки не вимагає спеціальних програмних засобів.	0,71

– аутентифікація – описує кількість необхідних сеансів аутентифікації цілі при експлуатації вразливостей. Показник не враховує складність даного процесу, а лише характеризує саму необхідність аутентифікації для використання вразливостей. Аутентифікація відбувається лише у тому випадку, якщо доступ к ресурсу вже отриман (табл. 2.9);

Таблиця 2.9 – Показники аутентифікації

Показник	Опис показника	Вага
Багаторазова аутентифікація	Експлуатація вразливості вимагає, щоб користувач провів аутентифікацію кілька разів. Наприклад, користувачу необхідно здійснити вхід в ОС, а потім в бізнес-додаток	0,450
Одноразова аутентифікація	Експлуатація вразливості вимагає проходження аутентифікації один раз	0,560
Аутентифікація відсутня	Експлуатація вразливості не вимагає аутентифікації	0,704

– вплив на конфіденційність – зміна ступеня порушення конфіденційності в результаті позитивної експлуатації вразливості (табл. 2.10);

Таблиця 2.10 – Показники впливу на конфіденційність

Показник	Опис показника	Вага
Відсутній <i>N</i>	Конфіденційність не порушена	0
Часткове <i>P</i>	Значне розкриття інформації та доступ на читання до деяких системних файлів, до даних певного клієнта. При цьому конфіденційність інших клієнтів хмари не порушена	0,275
Повне <i>C</i>	Повне розкриття конфіденційної інформації всіх клієнтів хмари, при якому всі файли користувача і системні файли відомі зловмиснику	0,660

– вплив на цілісність – вимірюється ступеню порушення цілосності в результаті позитивної експлуатації вразливостей (табл. 2.11);

Таблиця 2.11 – Показники впливу на цілісність

Показник	Опис показника	Вага
Відсутній <i>N</i>	Цілісність не порушена	0
Часткове <i>P</i>	Можлива зміна деяких системних або інформативних файлів, але атакуючий або не має можливості вибирати, що змінювати, або частина файлів, які зловмисник може міняти, невелика	0,275

Повне С	Повна компрометація цілісності системи. Повна втрата систем захисту, атакуючий може змінити будь-який файл	0,660
---------	---	-------

– вплив на доступність – вимірюється ступеню порушення доступності в наслідок успішної експлуатації вразливості (табл. 2.12). Розрахунок базової метрики відбувається за наступною формулою:

$$BS = \text{round_to_1_decimal}\{[(0,6 * imp) + (0,4 * Exp) - 1,5] + f(imp)\}, (2.8)$$

де BS – базова метрика;

imp – загальний вплив (втрата), визначається, як

$$imp = 10,41[1 - (1 - Confimp) * (1 - Intimp)(1 - Avimp)], (2.9)$$

де $Confimp$ – втрата конфіденційності;

$Intimp$ – втрата цілосності;

$Avimp$ – втрата доступності;

Exp – доступність використання експлойта, визначається за наступною формулою

$$Exp = 20 * AccVec * AccCom * Aut, (2.10)$$

де $AccVec$ – вектор доступу;

$AccCom$ – вектор складності;

Aut – аутентифікація;

$f(imp) = 0$, якщо $imp = 0$, в інших випадках $f = 1,176$.

Таблиця 2.12 – Показники впливу на доступність

Показник	Опис показника	Вага
Відсутній N	немає впливу на доступність хмарної ІС, всі компоненти хмари функціонують в штатному режимі	0
Часткове P	Можливе зменшення продуктивності, потребує додаткове підключення хмари розриву	0,275
Повне C	Повна втрата доступності всіх компонентів хмарної ІС. Запити користувачів не обробляються, бізнес-додатки недоступні	0,660

Часова метрика. Часова метрика описує показники загрози, які реалізують дану уразливість, і включає наступні показники:

– доступність коду і техніки експлойта – характеризує доступність і техніку (код) експлойта. Загальнодоступність робочого експлойта (відкритого коду) різко підвищує кількість потенційних зловмисників (табл. 2.13);

Таблиця 2.13 – Показники доступності коду і техніки експлойта

Показник	Опис показника	Вага
Теорія (немає доказів) <i>U</i>	Можливість використання експлойта існує тільки в теорії, реальних практичних реалізацій немає	0,85
Експеримент <i>POC</i>	Використання експлойта було реалізовано у вигляді експерименту, де практично була доведена можливість проведення атаки. Розроблено код, який вимагає високого рівня підготовки	0,90
Функціональна <i>F</i>	Вразливістю може скористатися атакуючий за допомогою готового і доступного експлойта	0,95
Висока <i>H</i>	Експлойт реалізований у вигляді функціонального, незалежно чинного модуля. Код експлойта працює в будь-якій ситуації, реалізується за допомогою автономних мобільних агентів («черви» або вірус)	1,00
Не визначена <i>ND</i>	Інформації немає, показник не впливає на загальну оцінку обліку вразливостей	1,00

– ступінь готовності рішення для ліквідації наслідків вразливості. У загальному випадку вразливість після її появи протягом певного часу не має виправлень у вигляді патча або офіційного оновлення. У зв'язку з цим існує ряд тимчасових рішень, які можуть бути використані в даний період для часткової ліквідації наслідків або повного їх усунення (табл. 2.14);

Таблиця 2.14 – Показники ступеня готовності рішення

Показник	Опис показника	Вага
Офіційний патч OF	Виробник ПО випустив остаточний офіційний патч для закриття вразливостей	0,87
Тимчасове рішення TF	Виробник ПО випустив тимчасовий, але офіційний патч для закриття вразливостей	0,90
Рішення на основі порад і рекомендацій W	Існує неофіційне рішення, призначений для користувача патч	0,95
Відсутній U	Рішення немає або їм неможливо скористатися	1,00
Не визначена ND	Інформації немає, показник не впливає на загальну оцінку обліку вразливостей	1,00

– ступінь достовірності інформації про вразливість – відображає ступінь достовірності джерел про існування самої вразливості, а також можливості використання технічних деталей експлойта (табл. 2.15).

Таблиця 2.15 – Показники ступеня достовірності інформації

Показник	Опис показника	Вага
Носить гаданий характер UC	Інформація про експлойтів суперечлива, ряд джерел суперечить одне одному	0,90
Не опрацьована UR	Інформацію про експлойтів коментують дослідні антивірусні компанії	0,95
Підтверджена C	Вразливість була підтверджена виробником ПО	1,00
Не визначена ND	Інформації немає, показник не впливає на загальну оцінку обліку вразливостей	1,00

Розрахунок часової метрики включає ваги часових показників з їх комбінацією з базовою оцінкою, при цьому результат знаходиться в діапазоні 0 ÷ 10. Підсумкова оцінка часової метрики не перевищує базової оцінки, але повинна бути не менше 33% від неї:

$$TempSc = round_to_1_dec(BaseSc * Exp * Rem * Rep), \quad (2.11)$$

де $TempSc$ – часова метрика;

BaseSc – базова метрика;

Exp – доступність коду і техніки експлойта;

Rem – ступінь готовності рішення;

Rep – достовірність інформації.

Метрики середовища експлуатації (інфраструктури). До даної групи метрик відносяться наступні показники:

– супутній потенційний збиток – описує можливі втрати (фінансові) в результаті успішної експлуатації вразливості (табл. 2.16);

Таблиця 2.16 – Показники супутнього потенційного збитку

Показник	Опис показника	Вага
Відсутнє <i>N</i>	В результаті успішної експлуатації вразливості втрат немає	0
Низький <i>L</i>	В результаті успішної експлуатації вразливості відбувається незначне зниження продуктивності, збиток мінімальний	0,1
Низький–середній <i>LM</i>	В результаті успішної експлуатації вразливості відбувається зниження продуктивності хмарної ІС, запити користувачів обробляються довше, ніж визначено в SLA, що може спричинити зниження доходу від використання хмарних сервісів	0,3
Середній–високий <i>MH</i>	В результаті успішної експлуатації вразливості відбувається істотне зниження продуктивності, фінансовий збиток серйозний	0,4
Високий <i>H</i>	В результаті успішної експлуатації вразливості клієнту хмарної ІС наноситься катастрофічний збиток	0,5
Не визначена <i>ND</i>	Інформації немає, показник не впливає на загальну оцінку обліку вразливостей	0

– розподіл цільових систем – описує, яка частина компонентів хмарної ІТКМ схильна до вразливості (табл. 2.17);

Таблиця 2.17 – Показники розподілу цільових систем

Показник	Опис показника	Вага
Немає розподілу	Жоден з компонентів хмарної інформаційно–телекомунікаційної системи не схильний до вразливості	0
Низький <i>L</i>	1–25% компонентів хмарної ІС схильні до вразливості	0,25
Середнє <i>M</i>	26–75% компонентів хмарної ІС схильні до вразливості	0,75
Високий <i>H</i>	76–100% компонентів хмарної ІС схильні до вразливості	1,00
Не визначена <i>ND</i>	Інформації немає, показник не впливає на загальну оцінку обліку вразливостей	1,00

– вимоги до безпеки – дозволяє спеціалісту по ІБ визначити пріоритет і важливість ключових вимог безпеки: конфіденційність, цілісність, доступність. При цьому особлива увага приділяється тому, наскільки критично для існуючих бізнес–функцій підтримання на необхідному рівні одного з вимог.

Загальний ефект інфраструктурного показника залежить від відповідних значень приватних показників з базовою метрикою – шкоди для конфіденційності, цілісності та доступності. Слід взяти до уваги, що якщо в базовій метриці шкоди для конфіденційності відсутня, то вимога до забезпечення конфіденційності не чинитиме жодного впливу на розрахунок сукупного інфраструктурного показника. Збільшення вимоги конфіденційності з «середнього» до «високого» не змінить інфраструктурного показника, якщо базовий показник втрати конфіденційності приймає значення «повний», тому що проміжний показник (частина базового показника шкоди конфіденційності) вже прийняв максимальне значення. Значення показників для конфіденційності, цілісності та доступності описані в табл. 2.18.

Таблиця 2.18 Показники вимог до безпеки

Показник	Опис показника	Вага
Низькі <i>L</i>	Втрати конфіденційності (цілісності, доступності) має обмежений ефект для корпорації	0,50
Середні <i>M</i>	Втрати конфіденційності (цілісності, доступності) має серйозний ефект для корпорації	1,00
Високі <i>H</i>	Втрати конфіденційності (цілісності, доступності) має катастрофічний ефект для корпорації	1,51
Не визначена <i>ND</i>	Значення метрики не визначене і на загальний рахунок не впливає	1,00

Розрахунок інфраструктурної метрики проводиться за формулою:

$$EnvSc = round_to_1_dec[(AdTem + (10 - AdTem) * CollDamPot)TarDis], \quad (2.12)$$

де *EnvSc* – інфраструктурна метрика;

TarDis – розподіл цільових систем;

CollDamPot – супутній потенційний збиток;

AdTem – скоригована оцінка часової метрики, перерахована з урахуванням вимог безпеки та шкоди з базової метрики (*Adjimp*):

$$Adjimp = \min[10,41 * (1 - (1 - Confimp * ConfReq)(1 - Intimp * IntReq)(1 - Avimp * AvReq))], \quad (2.13)$$

де *ConfReq*, *IntReq*, *AvReq* – вимоги до конфіденційності, цілісності, доступності.

Таким чином, отримуємо базовий, часовий і інфраструктурний вектори, відповідні групі метрик, наведеної в табл. 2.19.

Таблиця 2.19 Показники вимог до безпеки

Група метрик	Вектор
Базова	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/ C:[N,P,C]/I:[N,P,C]/A:[N,P,C]

Часова	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/ RC:[UC,UR,C,ND]
Інфраструктурна	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/ CR:[L,M,H,ND]/IR:[L,M,H,ND]/AR:[L,M,H,ND]

Використовуючи базовий, часовий і інфраструктурний вектори, визначимо два основних інтегральних показника, що впливають на оцінку ризику. Чим вище рівень схильності вразливості (тобто застосування експлойта), тим більше шансів у зловмисника провести успішну атаку і тим більше значення показника частоти не коректного використання F. Розрахунок цього показника для кожної вразливості, представленої в ризик–моделі хмарної середовища, ґрунтується на положенні, що основні характеристики вразливості описуються базовою метрикою, а облік показників часової метрики дозволяє зменшити ймовірність успішного застосування експлойта. Той же принцип стосується і до втрат (впливу): потенційний вплив визначається як шкоди, що залежить від показників вразливості в базовій метриці. У той же час воно може бути збільшена або зменшена в залежності від вимог до конфіденційності, доступності та цілісності, визначених у інфраструктурній метриці.

Далі для вимірювання рівня ризику вводиться поняття рівня сервісу, представленого у вигляді Марківського процесу з безперервним часом. Сервісні рівні залежать від проектного рішення і варіанти реалізації ІС, структури ІС і набору додатків, іншими словами, від способу використання інформаційної системи.

Побудова ризик–моделі досягається за рахунок виконання двох послідовних кроків:

1. визначення стану моделі виходячи з оцінки шкоди при успішній реалізації експлойта;
2. визначення стану моделі з оцінки частоти застосування експлойта.

На першому кроці визначається список вразливостей на підставі загальнодоступних даних, наприклад з офіційних повідомлень про уразливість,

стану баз даних (NVD) або шляхом запуску спеціалізованих сканерів (Nessus). Якщо ж по ряду технічних причин (наприклад, заборона відкриття потрібних портів в брандмауері, скрутне визначення місця розташування ІС) застосування спеціалізованих сканерів утруднено, тоді необхідно провести розрахунок частоти застосування експлойта і можливого шкоди для кожної уразливості.

Втрати від успішного застосування експлойта описує серйозність уразливості, але це зовсім не означає, що дві вразливості, що призводять до однакового втрат, мають схожий рівень впливу для даної середовища і призводять до пропорційного зменшення сервісного обслуговування. У зв'язку з цим необхідно вирішити задачу визначення інтервалів рівнів впливу вразливостей з подальшим визначенням для них сервісних рівнів. В результаті виходить набір рівнів сервісу: від рівня без надання сервісів до повного набору сервісів, описаних у вигляді моделі станів.

Далі, на другому кроці, досліджується модель переходів станів, отримана на першому кроці, і доповнюється інтенсивністю переходів. Інтенсивність переходів визначає, з якою ймовірністю можливий перехід з одного стану в інший і з якою ймовірністю можливе знаходження в цьому стані в певний інтервал часу t . У моделі оцінки рівнів ризику кожне стан посилається на сукупний рівень впливу набору вразливостей. Таким чином, модель переходів станів описує різні рівні ризику, характерні для даної середовища в момент часу t .

Для визначення інтенсивності переходів враховується сукупна частота використання експлойта в певний інтервал часу. На іншому кроці, досліджується модель переходів станів, отримана на першому кроці, і доповнюється інтенсивністю переходів. Інтенсивність переходів визначає, з якою ймовірністю можливий перехід з одного стану в інший і з якою ймовірністю можливе знаходження в цьому стані в певний інтервал часу t . У моделі оцінки рівнів ризику кожен стан посилається на сукупний рівень впливу набору вразливостей. Таким чином, модель переходів станів описує різні рівні ризику, характерні для даної середовища в момент часу t . Для визначення

інтенсивності переходів враховується сукупна частота використання експлоїта в певний інтервал часу.

Висновки до розділу

У другому розділі проведено:

- аналіз існуючих моделей формування ризиків втрати інформації при переході корпорації до хмарного середовища;
- оцінювання ефективності методик та їх порівняльний аналіз.

При впровадженні хмарних технологій необхідний стратегічний план, який допоможе правильно поставити цілі і побачити їх досягнення, контролювати і коригувати рух до досягнення результату.

Проблема розробки ІТ-стратегії впровадження полягає в тому, що ще на стадії її формування важливо визначити, які моделі формування ризиків втрати інформації будуть задовольняти корпорацію при переході до хмарного середовища, оцінити провайдерів хмарних послуг з точки зору надійності і безпеки.

Потенційні порушення в сфері інформаційної безпеки є базовою основною перешкодою на шляху впровадження хмарних технологій на практиці управління адміністративними процесами. Проблема розробки ІТ-стратегії впровадження полягає в тому, що ще на стадії її формування важливо визначити, які моделі підтримки прийняття рішень при виборі хмарних ІТ-сервісів для впровадження в корпорації найбільше будуть задовольняти бізнес-стратегії корпорації, сумісність діючого способу організації взаємодії серед суб'єктів системи в корпорації, оцінити провайдерів хмарних послуг з точки зору надійності, достовірності, оперативності та безпеки інформаційних потоків.

Майже в усіх методиках базою для визначення рівня ризику є допустимість появи тієї чи іншої події, яка визначає рівень ймовірності реалізації загрози. В основу методик визначення ймовірності найчастіше закладається експертний метод або використовується дані статистики попередніх періодів.

Для розробки моделі управління ризиками інформаційної безпеки корпорації необхідно вибрати таку модель або комбінацію моделей, яка б включала в себе визначення, збір та обробку даних про результуючі фактори, які притаманні системі, та дозволяє з високим рівнем ймовірності визначити найгірший сценарій для реалізації загрози. Дана модель має бути адаптивною та оперативно змінюватись з урахуванням вихідних результатів (кількості користувачів, кількості обладнання, швидкості каналу передачі даних тощо).

Таким чином, доцільна розробка програмного забезпечення підтримки прийняття рішень при виборі хмарних ІТ-сервісів для впровадження в корпорації з використання існуючих методик та моделей, які були розглянуті в другому розділі.

3.1 Процес вибору хмарних ІТ–сервісів

Для прийняття обґрунтованого рішення при виборі хмарних ІТ–сервісів для впровадження в корпорацію необхідно провести аналіз зібраних даних про хмарних сервісах і провайдерів для визначення витрат і вигод, результативності та ризиків від їх застосування. Існують різні методики по визначенню ефективності, ризиків, пов'язаних з впровадженням ІТ, а також інструменти при стратегічному плануванні, проте для проведення всебічного аналізу необхідно застосувати системний підхід, виділивши важливі етапи.

Основною операцією системного підходу є поділ цілого на складові частини. Завдання може розпадатися на підзадачі, цілі – на підцілі і т. д. При необхідності даний процес може повторюватися, що призведе до деревовидним ієрархічним структурам. Процес вибору хмарних ІТ–сервісів складний, погано формалізований, слабо структурований, тому операцію декомпозиції важливо чітко продумувати. Один із способів спрощення складного – це метод декомпозиції, який полягає в розділенні цілого складного на прості і більш дрібні частини.

У зв'язку з цим обґрунтуємо декомпозицію концепції вирішення проблеми відповідно до методики, розробленої Ф.П. Перегудова і В.З. Ямпольським [64, 65]. Глобальна мета – вибір хмарних ІТ–сервісів для впровадження в корпорацію ґрунтується на формуванні стратегії, яка включає в себе три складові: корпоративна стратегія, стратегія бізнесу та функціональна стратегія [13]. Далі за ознакою «життєвий цикл» для функціональної стратегії виділимо (декомпозицію) стандартні етапи:

- збір та аналіз даних;
- оцінка даних;
- прийняття рішень [67] (рис. 3.1).

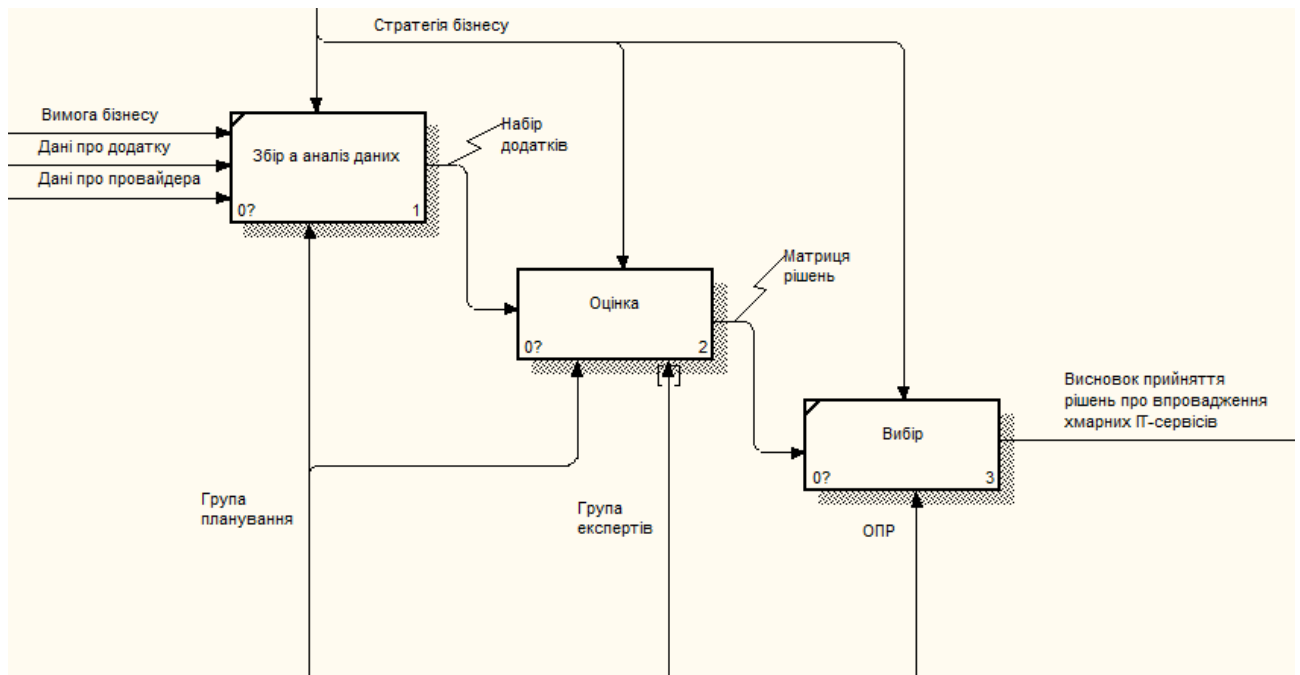


Рисунок. 3.1 – Декомпозиція процесу прийняття рішення при виборі хмарних ІТ-сервісів

Вхідною інформацією для аналізу буде: визначення високорівневих вимог бізнесу; визначення моделі хмарного сервісу і моделі розгортання; дані про провайдерів та додатки тощо. На виході процесу аналізу буде отримано набір додатків, який піддається оцінці. За результатами оцінки отримуємо бал для кожної програми, на основі якого приймається рішення про впровадження.

Процес оцінки згідно ознакою «простір ініціювання цілей» декомпозіруем на 2 етапи: оцінка результативності та оцінка можливості переходу. На першому етапі визначається відповідність стандартам і тим самим можливість застосування в корпорації додатків що оцінюються. На другому етапі після відсіву додатків, які не відповідають стандартам, проводиться аналіз можливості переходу додатків до хмарних технологій в порівнянні з іншими альтернативами, де визначається їх пріоритет для впровадження. Оцінка проводиться групою експертів у відповідності до завдань на експертизу. На рис. 3.2 представлена декомпозиція процесу оцінки. На виході процесу оцінки отримуємо матрицю рішень про впровадження хмарних ІТ-сервісів.

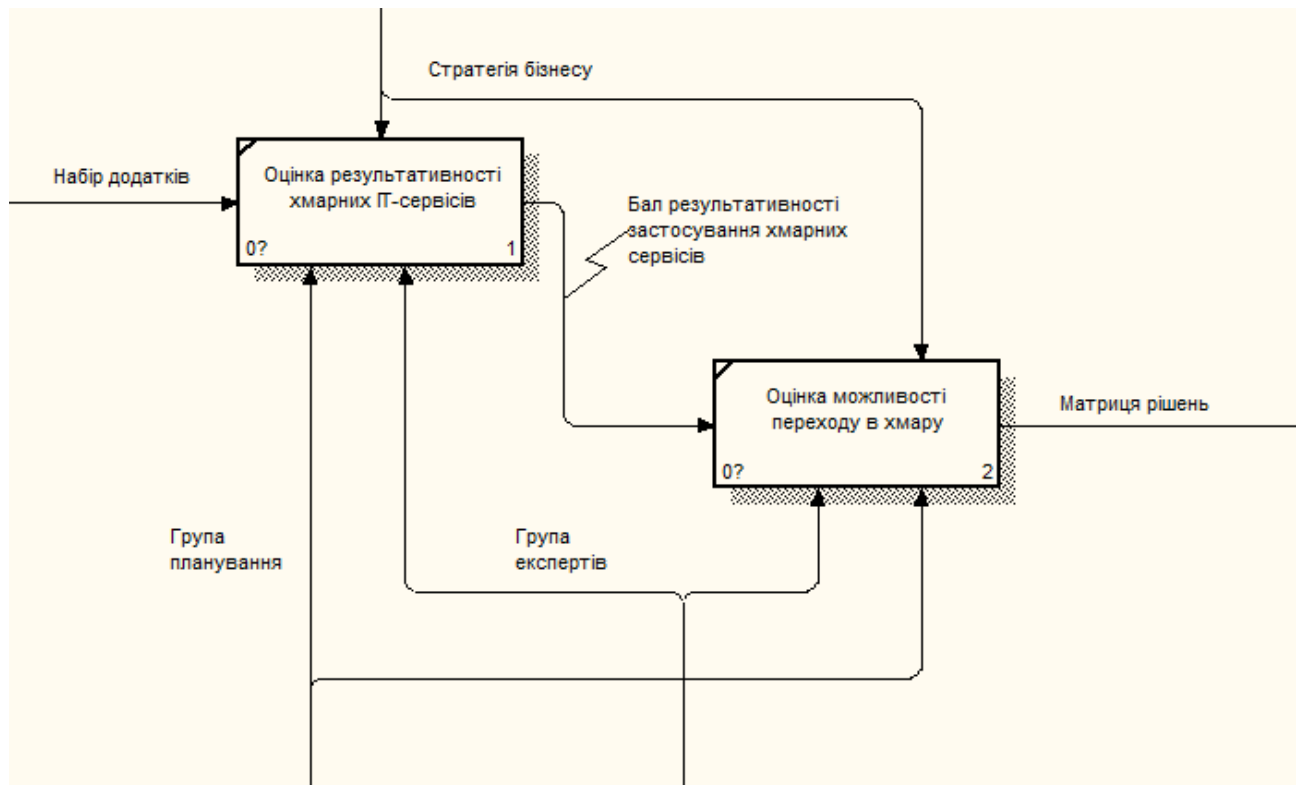


Рисунок. 3.2 – Декомпозиція процесу оцінки

На останньому етапі «Вибір» робиться висновок ОПР про впровадження хмарних IT-сервісів в корпорації.

Розроблена методика підтримки прийняття рішень при виборі хмарних IT-сервісів для впровадження в корпорації на основі системного підходу.

За даною методикою розглядається поетапна концепція вирішення проблеми із застосуванням двох запропонованих моделей.

3.2 Алгоритм роботи

А для забезпечення безпроблемного переходу і досягнення оптимального результату корпорація повинна, перш за все, розробити всебічну стратегію впровадження хмарних технологій, спрямовану на вирішення специфічних проблем корпорації. Розглянемо застосування запропонованої методики і моделей підтримки прийняття рішень при виборі хмарних технологій.

Оцінка проводиться експертами відповідно до зібраної інформації всередині корпорації, отриманою інформацією від провайдера і при вивченні наданих документів (договорів з додатками).

Корпорація процесу прийняття управлінських рішень на впровадження хмарних технологій повинна здійснюватися на основі результатів оцінки їх економічної ефективності та ризиків використання. Прийняття рішень при стратегічному плануванні практично завжди відбувається в умовах неточності та невизначеності інформації. Експерт в таких умовах виробляє в основному якісну оцінку. Знання та інтуїція експерта будуть головними вирішальними факторами при виборі хмарного додатка. При прийнятті рішення важливо враховувати не тільки якісні, а й кількісні критерії в оцінці. Кількісна оцінка виглядає наочно і зрозуміло для керівника (ОПР) [65, 68]. Цю проблему можна вирішити, застосувавши багатокритерійний підхід підтримки прийняття рішень і експертних оцінках, за допомогою яких можна моделювати при формальному аналізі альтернатив узагальнений (інтегральний) показник, який дозволяє визначити компроміс між різними оцінюються критеріями. У таких моделей можна використовувати для оцінки альтернатив і прийняття рішень кількісну експертну інформацію нарівні з якісною [69, 70].

Концепція вирішення проблеми за запропонованою методикою наведена у додатку В.

На першому етапі «Визначення витрат і вигод» формується набір додатків для оцінки і визначаються витрати і вигоди впровадження хмарних сервісів. На етапі визначення високорівневих вимог бізнесу необхідно виявити.

1. Функції бізнесу.
2. Головні причини, які спонукають бізнес впроваджувати хмарні сервіси (стратегічні цілі).
3. Хмарні сервіси, які могли б підтримувати бізнес–процеси.
4. Вимоги законодавства, які мають значення.
5. Фізичне розміщення систем, що забезпечують надання послуг (на території корпорації, що не на його території, в певній географічній точці) і хто буде відповідати за надання послуг.

Далі визначається, який тип хмарної моделі (SaaS, PaaS, IaaS) потрібен корпорації, а також яка модель розміщення хмари (публічне, приватне, суспільне, гібридне) найкраще підійде.

Наступний етап – визначення стартової / базової моделі хмарного сервісу з точки зору ризику. Тут визначаються області ризику, які необхідно прийняти до уваги і заходи щодо зниження ризику в виявлених областях до рівня, прийняттого з точки зору корпорації.

При вирішенні цього етапу визначити заходи мінімізації ризику втрати інформації:

- шифрування даних клієнтом для їх захисту від несанкціонованого доступу з боку персоналу хмарного провайдера;

- резервне копіювання даних/відстеження аудиту клієнтом на своїй території на випадок втрати доступу до хмарного сервісу;

- ясно або повно сформульовані SLA (Service Level Agreement), що включають пункт про право на аудит [71, 72];

- складання і здійснення внутрішнього плану відновлення після аварії.

Це дозволить аудиторам вжити заходів при розгляді інших хмарних моделей і визначиться:

- зниження витрат при зміні моделі надання / розміщення хмарних сервісів;

- дозволить використання приватного, громадського або гібридного хмари відмовитися від деяких заходів з безпеки, необхідних в публічному хмарі;

- вдасться скоротити витрати на зниження ризику, пов'язаного з прив'язкою до певного виробника, за рахунок використання моделі PaaS або IaaS замість SaaS.

На другому етапі «Оцінка результативності» проводиться оцінка кожного з наявної програми і/або того додатку, який припускають впроваджувати в корпорацію відповідно до функціональних і юридичними вимогами бізнесу (встановленими на етапі 1).

В оцінці ризиків для існуючого / впроваджуваного додатку визначається наступне:

1. Области, в яких ризик перевищує прийнятний для корпорації рівень і повинен бути знижений.

2. Заходи, які допоможуть знизити ризик до прийнятного рівня (наприклад, використовувати приватне хмара, щоб не ділити майданчик із іншими корпораціями, провести оцінку постачальника, а також його сертифікатів і т. д.).

3. Порівняння подібного з подібним. Для цього необхідно проаналізувати області ризику, що існує для поточної технології, щоб переконатися, що в оцінці існуючого і майбутнього стану враховано одне і теж.

Після аналізу розраховуються критерії та інтегральний показник по запропонованій системі критеріїв оцінки переваг і інтегральної моделі на основі багатокритеріального підходу прийняття рішень. У розрахунку критерію K_{ecs} і показників ефективності та ризиків необхідно підключити до роботи експертів, фінансовий відділ і використовувати корпоративні стандарти.

На третьому етапі «Аналіз можливості переходу до хмарних технологій» визначається ієрархія критеріїв. Далі проводиться розрахунок балів додатків по 3-м критеріям відповідно до запропонованої моделі. В результаті розрахунків складається матриця прийняття рішень про можливість переходу додатків в хмарну середу і приймається рішення щодо вибору хмарних ІТ-сервісів для впровадження в корпорацію [73, 74].

У запропонованій методиці підтримки прийняття рішень вибору хмарних ІТ-сервісів для впровадження можна виділити наступну послідовність дій у вигляді блок-схеми (рис. 3.3), по якій здійснюється оцінка та відбір програм для впровадження в корпорацію з застосуванням запропонованих моделей.

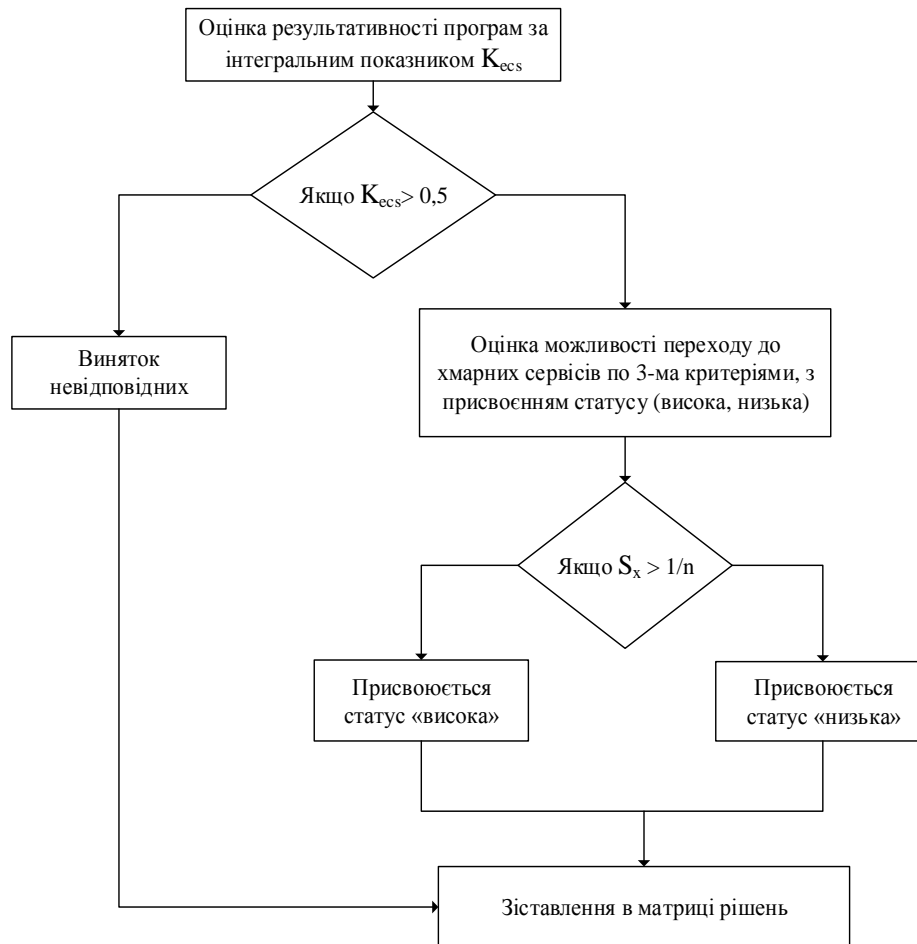


Рисунок. 3.3 – Схема оцінки та відбору хмарних ІТ-сервісів для впровадження в корпорацію з застосуванням запропонованих моделей підтримки прийняття рішень

Для кращого розуміння всіх виявлених в літературі переваг, витрат, вигод і ризиків від впровадження хмарних сервісів наведемо їх у табл. 3.1

Для кращого розуміння прорахунку відсотка ймовірності втрати інформації по всіх виявлених видах ризиків від впровадження хмарних сервісів наведемо їх у таблицях.

Таблиця 3.1 Ризики при використанні хмарних сервісів

Види ризиків	Пояснення ризиків при використанні хмарних технологій
Обмеження можливостей настройки додатків	Неможливість перенастроювання хмарного додатка при будь-якій зміні бізнес-процесу. Так як модифікації неможлива або виробляється за окрему плату.

Продовження таблиці 3.1

Дотримання законних вимог	Вступ операцій в протиріччя з діючими правовими нормами (причому це не буде своєчасно помічено). Проблема через повсюдності доступності хмарних сервісів і еволюції регулюючих вимог.
Безпека	З хмарними обчисленнями пов'язані як традиційні, так і нові ризики в галузі безпеки, які враховують специфіку хмарних ІТ. Провайдер і клієнт повинні враховувати ці ризики і приймати адекватні заходи для їх зниження.
Несумісність	Несумісність хмарних сервісів з наявною ІТ-інфраструктурою або зі специфічними системами, які повинні бути інтегровані з сервісами.
Безперервна робота	Нездатність гарантувати час безперебійної роботи, обумовлений в контракті. Крім того, збої можуть викликатися іншими факторами.
Переплата за схемою pay-as-you-go	Залучені додаткові ресурси можуть залишитися підключеними після закінчення пікового попиту.
Прив'язка до апаратної платформи або постачальнику	Прив'язка замовника до певної хмарної технології або постачальнику хмарних сервісів, неможливість перейти на іншу платформу.
Втрата внутрішніх компетенцій	Важливі внутрішні навички в сфері ІТ будуть втрачені. Можливо, вона могла б стати одним з моментів стратегічного диференціювання компанії.
Продуктивність	Зниження продуктивності систем, якщо провайдер використовує модель поділу ресурсів при наданні сервісів декільком замовникам і припускається помилки при плануванні потужностей. Швидкість доступу в Інтернет також може позначитися на продуктивності.
Консьюмеризація хмари	Бізнес-одиниці можуть замовляти хмарні сервіси без участі ІТ-департаменту через широкого поширення простих хмарних сервісів.

На підставі чого були сформульовані основні групи джерел:

- нормативно–правові питання в оцінці ризиків і технічна реалізація міграції: «Стандарти та керівництва з використання хмарних обчислень» [75];
- ризики, пов'язані з інформаційною безпекою: стандарти ІБ [75, 76];
- ефективність і результативність застосування хмарних ІТ для бізнесу: методичні рекомендації для оцінки ефективності інвестиційних проектів [77];
- методи [5, 6, 78].

Пропонується наступний метод оцінки результативності застосування хмарних ІТ–сервісів, в основі якого лежить оцінка 6–й групових критеріїв. Їх огляд наведено в табл. 3.2 [79, 80, 81].

Слід зазначити, що наведені в таблиці критерії та показники, складені на основі досліджуваної літератури, в якій в тому чи іншому вигляді заявлені всі ці показники. Винятком є ті, які в явному вигляді не вказані в літературі, але виявлено, що вони мають важливість в оцінці результативності.

Таблиця 3.2 Система критеріїв оцінки результативності застосування хмарних ІТ–сервісів в корпорації

Критерії і показники результативності	Роль показника в оцінці
Ефективність для бізнесу (<i>Еб</i>)	
Зростання швидкості (гнучкості) (<i>Зш</i>)	Швидкість допомагає знизити витрати на підключення нових користувачів (масштабування) і нового функціоналу
Продуктивність роботи користувачів (<i>Прк</i>)	Визначається скорочення витрат і термінів на обробку інцидентів і змін
Оптимізація використання ресурсів (<i>Овр</i>)	Встановлюється скорочення простоїв обчислювальних систем, тому що компанії використовують тільки ті обчислювальні ресурси, які необхідні
Критичність для бізнесу (<i>Кб</i>)	Визначається важливість хмарного додатка при підставі нового бізнесу або вихід на новий ринок, а також у відповідності з бізнес стратегією корпорації
Фінансові переваги (<i>Фп</i>)	
Витрати на хмарні сервіси (вартість міграції) (<i>Вхс</i>)	Витрати на впровадження сервісу (капітальні, операційні та потенційні витрати)

Фінансові переваги (<i>Фп</i>)	
Економія коштів (<i>Ек</i>)	Оцінка скорочення капітальних і операційних витрат від хмарних сервісів
Критерій технічного пріоритету (<i>Тп</i>)	
Інтеграція (<i>І</i>)	Визначається простота інтеграції
Можливість міграції додатків в хмару (<i>Ммдх</i>)	Функціональна складність міграції та розмір додатків
Технологічний стек (<i>Тс</i>)	Середовище роботи додатка (операційна система, база даних)
Дизайн додатка (<i>Дд</i>)	Зручність інтерфейсу і використання віртуалізації
Критерій надійності роботи та інформаційної безпеки (<i>Іб</i>)	
Збереження даних (<i>Зд</i>)	Робота провайдера щодо забезпечення збереження даних
Захист даних при передачі (<i>Здп</i>)	Забезпечення збереження даних провайдером при їх передачі (це повинно бути як всередині хмари, так і на шляху від/до хмари)
Аутентифікація (<i>А</i>)	Розпізнавання провайдером автентичності клієнта
Ізоляція користувачів (<i>Ік</i>)	Відділення даних і додатків одного клієнта від даних і додатків інших клієнтів
Безперебійна робота і доступність (<i>Бр</i>)	Нездатність гарантувати час безперебійної роботи, обумовлений в контракті
Критерій ступеня ризику використання хмарного сервісу (<i>Ср</i>)	
Нормативно–правові питання (<i>Нпн</i>)	Ступінь використання провайдером законів і правил, які можуть застосовуватися до сфери хмарних обчислень
Реакція на події (прив'язка до постачальника) (<i>Рп</i>)	Реагування провайдера на події, ступінь залучення клієнтів в інфідент, можливість передачі деяких ризиків хмарного провайдера
Несумісність (<i>Н</i>)	Визначається сумісність хмарних сервісів з наявною ІТ–інфраструктурою
Відновлення конфіденційності та даних (<i>Вкд</i>)	Обумовлюється в контракті, яким чином буде проводитися відновлення даних в разі інциденту
Переплата за схемою pay–as–you–go (<i>П</i>)	Залучені додаткові ресурси можуть залишитися підключеними після закінчення пікового попиту

Для забезпечення відповідності критерії мають ранг (коефіцієнти вагомості). Результати досліджень показують, що є відмінності між вагами, які призначає сам аудитор, і тими, які виявляються на основі його дій. Зазвичай можуть недооцінювати вагомості найбільш істотних критеріїв і завищуватиметься у незначних. Тому при призначенні ваг для згладжування суб'єктивізму використовується метод попарних порівнянь [82, 69].

3.3. Формування архітектури та інструментів програмного продукту

Проектування архітектури програмного забезпечення є важливою складовою життєвого циклу розроблювального проекту, що в майбутньому заощадить багато сил, часу та грошей.

Процес розробки та супроводження архітектури майбутнього програмного забезпечення передбачає такі вимоги, як: простоту, ефективність, розуміння, масштабованість, гнучкість, тестованість та відгладжуваність. Далі сформулюємо наступний перелік висуваємих критеріїв:

- Ефективність. В першу чергу програмне забезпечення повинна вирішувати поставлені завдання і добре виконувати свої функції, причому в різних умовах. Сюди відносяться такі характеристики, як надійність, безпеку, продуктивність, здатність адаптуватись зі збільшенням навантаження (масштабованість), тощо.

- Розуміння. Над розробкою програмного забезпечення, як правило, працює безліч людей - одні йдуть, інші приходять. Після впровадження програмного забезпечення, супроводити його, як правило, доводиться людям, які не брали участі в його розробці. Тому правильно спроектована архітектура дає можливість відносно легко і швидко розібратися новим людям. Програмне забезпечення повинна бути добре структурована, не містити дублювання, мати добре оформлений код і бажано документацію. І по можливості в системі краще застосовувати стандартні, загальноприйняті рішення звичні для програмістів. Чим специфічне програмного забезпечення, тим складніше його зрозуміти іншим розробникам (Принцип найменшого подиву - Principle of least

astonishment. Зазвичай, він використовується відносно призначеного для користувача інтерфейсу, але застосовується і до написання коду).

– Гнучкість. Будь-яке програмне забезпечення доводиться міняти з часом – змінюються вимоги, додаються нові. Чим швидше і зручніше можна ввести зміни в існуючий функціонал, чим менше проблем і помилок це викличе - тим гнучкіше і конкурентоздатніше програмне забезпечення. Тому в процесі розробки треба оцінювати те, що виходить, на предмет того, як це потім, можливо, доведеться міняти. Запитайте у себе: «А що буде, якщо поточне архітектурне рішення виявиться невірним?», «Яка кількість коду піддасться при цьому змін?». Зміна одного фрагмента системи не повинно впливати на її інші фрагменти. По можливості, архітектурні рішення не повинні «вирубувати в камені», та наслідки архітектурних помилок повинні бути в розумній мірі обмежені.

– Можливість розширення. Можливість додавати в систему нові сутності та функції, не порушуючи її основної структури. На початковому етапі в систему має сенс закладати лише основний і необхідний функціонал. Але при цьому архітектура повинна дозволяти легко нарощувати додатковий функціонал по мірі необхідності. Причому, щоб внесення найбільш ймовірних змін вимагало найменших зусиль.

Вимога, щоб архітектура програмного забезпечення володіла гнучкістю і розширюваністю (тобто була здатна до змін і еволюції) є настільки важливим, що вона навіть сформульована у вигляді окремого принципу - «Принципу відкритості/закритості» (Open-Closed Principle - другий з п'яти принципів SOLID) : Програмні суті (класи, модулі, функції, тощо) повинні бути відкритими для розширення, але закритими для модифікації.

Іншими словами, повинна бути можливість розширити чи змінити поведінку системи без зміни або переписування вже існуючих частин системи.

Це означає, що систему слід проектувати так, щоб зміна її поведінки і додавання нових функцій була досягнута за рахунок написання нового коду (розширення), і при цьому не доводилося б змінювати вже існуючий код. В такому випадку поява нових вимог не спричинить за собою модифікацію

існуючої логіки, а зможе бути реалізовано перш за все за рахунок її розширення. Саме цей принцип є основою «плагін архітектури» (Plugin Architecture).

– Масштабованість. Можливість скоротити термін розробки за рахунок додавання до проекту нових людей. Архітектура повинна дозволяти розподілити процес розробки так, щоб безліч людей могли працювати над програмним забезпеченням одночасно.

– Тестованість. Код, який простіше тестувати, буде містити менше помилок і надійніше працювати. Але тести не тільки покращують якість коду. Вимога «проста тестованість» є також спрямовуючою силою, автоматично веде до зручного дизайну, і одночасно одним з найважливіших критеріїв, дозволяючи оцінити його якість.

Не дивлячись на різноманітність критеріїв, все ж головним при розробці великих систем вважається завдання зниження складності. А для зниження складності нічого, крім поділу на частини, поки не придумано. Це називають принципом «розділяй і володарюй» (divide et impera), але по суті мова йде про ієрархічної декомпозиції. Складна система повинна будуватися з невеликої кількості простіших підсистем, кожна з яких, в свою чергу, будується з частин меншого розміру, тощо, до тих пір, поки самі невеликі частини не будуть достатньо прості для безпосереднього розуміння і створення.

Дане рішення є не тільки єдино відомим, а й універсальним. Крім зниження складності, воно одночасно забезпечує гнучкість системи, дає хороші можливості для масштабування, а також дозволяє підвищувати стійкість за рахунок дублювання критично важливих частин.

Відповідно, коли мова йде про побудову архітектури програмного забезпечення, створенні його структури, під цим, головним чином, мається на увазі декомпозиція програмного забезпечення на підсистеми (функціональні модулі, сервіси, шари, підпрограми) і організація їх взаємодії один з одним і зовнішнім світом. Причому, чим більш незалежні підсистеми, тим безпечніше зосередитися на розробці кожної з них окремо в конкретний момент часу і при цьому не піклуватися про всі інші частини.

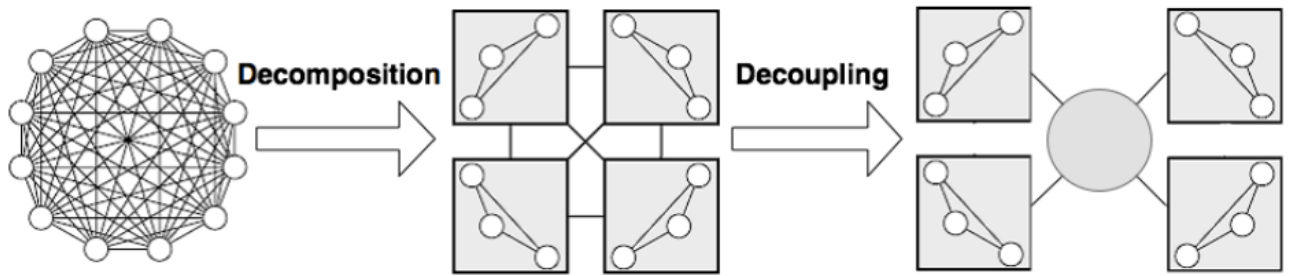


Рисунок 3.4 – Приклад ієрархічної декомпозиції архітектури

Під час проектування архітектури інформаційно-аналітичної системи проводилася декомпозиція ієрархічно – спочатку систему розбили на великі функціональні модулі, що описують її роботу в найзагальнішому вигляді (рис. 3.4). Потім, отримані модулі, аналізували більш детально і, в свою чергу, поділили на під-модулі та на об'єкти.

При проектуванні інформаційно-аналітичної системи застосовано «спагетті-код» який перетворюється в конструктор, що складається з набору модулів та підпрограм, що взаємодіють один з одним по визначеним і простим правилам, що власне і дозволяє контролювати її складність, а також дає можливість отримати переваги, які зазвичай співвідносяться з поняттям правильна архітектура:

- Масштабованість. Можливість розширювати систему і збільшувати її продуктивність, за рахунок додавання нових модулів;
- Ремонтопридатність. Зміна одного модуля не вимагає зміни інших модулів;
- Замінність модулів. Модуль легко замінити на інший;
- Можливість тестування. Модуль можна від'єднати від всіх інших і протестувати або полагодити;
- Перевикористання. Модуль можна бути перевикористати в іншому програмному забезпеченні та іншому оточенні;
- Супроводження. Розбите на модулі програмне забезпечення простіше розуміти і супроводжувати.

Під час проектування інформаційно-аналітичної системи застосовувалася архітектура, така як, Модель-Вид-Контролер (MVC). Всього-на-всього в відділенні подання від бізнес-логіки, де користувальницький додаток спочатку

ділиться на два модуля - один з яких відповідає за реалізацію власне самої бізнес-логіки (Модель), а другий – за взаємодію з користувачем (для користувача графічний інтерфейс). Після чого, для того щоб ці модулі розроблялися незалежно один від одного, зв'язок між ними послаблюється за допомогою паттерна «Спостерігач», чим саме отримали один з найпотужніших і полярних «шаблонів», які використовуються в даний час (рис. 3.5).

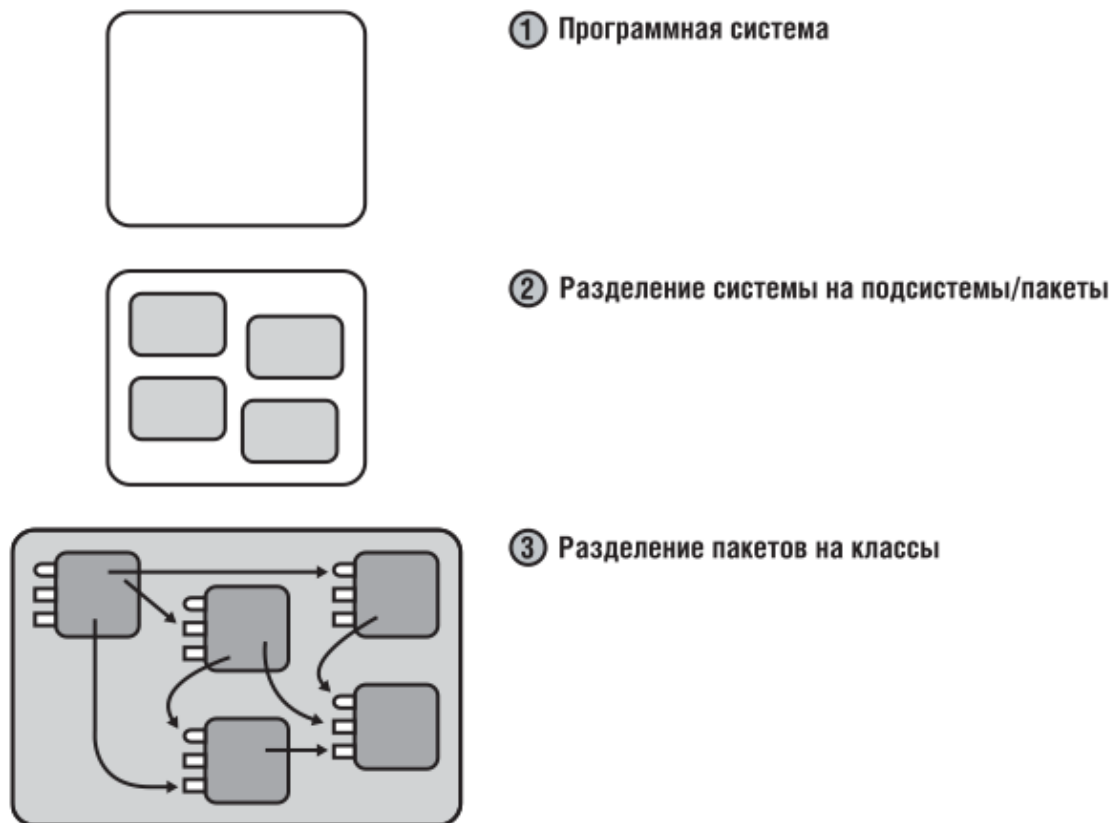


Рисунок 3.5 – Схематичне представлення архітектури інформаційно-аналітичної системи

3.4 Вибір мови програмування інформаційно-аналітичної системи

На сьогоднішній день представлено безліч мов програмування. Проте найпопулярнішими, для розробки, є С подібні мови. Серед них найпопулярнішими є С# та Java. Обидві мови кросплатформенні та мають схожий з С\С++ синтаксис. Щоб обрати відповідну, треба розглянути особливості, переваги та недоліки кожної з них.

С# та Java кросплатформенні, тому повинні працювати у “віртуальних машинах”. Для С# це CLR (Common Language Runtime), а для Java – JVM (Java

Virtual Machine). Кожен додаток транслюється у проміжну мову, а він вже запускається у віртуальній машині. Загалом ці мови схожі на Assembler, проте в C# має поліморфні інструкції (загальні), а Java має різні інструкції для різних типів даних. Вибір x86 інструкцій в C# лягає на JIT, компілятор реального часу. Це може призвести до трохи повільнішого першого запуску, порівняно з Java, проте надалі, ця інструкція буде краще підібрана для конкретної машини.

Обидві мови підтримують Generics. Проте в Java безпека типів доступна лише на рівні компілятора, а в C# вона як на рівні компілятора, так і на рівні рантайму. Це надає C# безпеку типів, надає можливість рефлексії, зменшує кількість Boxing/Unboxing.

C# та Java мови з некерованою пам'яттю. Це означає, що розробнику треба менше приділяти увагу виділенню та очищенню пам'яті, так як за нього це зробить “збирач сміття”. В обох мовах можливо задати деструктори та самостійно налагодити роботу збирача.

Як Java так і C# мають вбудовані типи. Кожен тип унаслідуються від Object. Проте в Java неможливо розробити власні примітивні типи. Також, в C# всі примітивні типи (крім string) знаходяться в стеку, а не в керованій купі, що значно збільшує його швидкість.

Порівнюючи ці мови, слід прийняти до уваги, що в C# набагато більше можливостей ніж в Java:

- Властивості та автовластивості
- Делегати
- Події
- Анонімні на лямбда-вирази
- Можливість роботи з C++ та Assembler компонентами
- Вбудована мова LINQ
- Перевантаження операторів
- Індексатори
- Рефлексія
- Асинхронність та зручна реалізація многопоточності

Враховуючи вище наведені особливості мов програмування, було обрано C#. Ця мова програмування є частиною .Net Framework, тож для зручної роботи зразу будуть доступні такі додаткові інструменти:

- Visual Studio – зручна середовище розробки, з підтримкою NuGet, IntelliSense. Можливе інсталиювання додаткових плагінів;
- NuGet – система керування додатковими пакетами, що вбудована в Visual Studio;
- WCF – фреймворк для налагодження обміну даними між додатками. Можливо реалізувати за допомогою нього сервіс, який не потребуватиме конкретної мови програмування у клієнтському додатку;
- WPF – система для побудови клієнтських додатків, що використовує векторну графіку для візуалізації інтерфейсу. Можливо використовувати апаратне прискорення, що ще більше збільшує її продуктивність;
- EF – ORM технологія, для зручної роботи з БД.

Мова має строгу статичну типізацію, підтримує поліморфізм, переваження операторів, вказівники на функції–члени класів, атрибути, події, властивості, винятки, коментарі у форматі XML.

Варто зазначити, що C# розроблена Microsoft, тож в цій мові можлива зручна реалізація взаємодії із системою Windows. Наприклад, push-повідомлення у Windows 8+, меню, що викликається на праву кнопку миші по іконці в треї у Windows 7+ та можливість доступу до зовнішніх пристроїв комп'ютера.

Висновки до розділу

В третьому розділі була використана:

- система критеріїв і показників для оцінки результативності хмарних IT-сервісів. Дані показники були сформовані відповідно до основних груп джерел: «Стандарти та керівництва з використання хмарних обчислень», офіційним

документам Cisco, ДСТУ з інформаційної безпеки, методичних рекомендацій з оцінки ефективності інвестиційних проектів, окремих публікацій по хмарним ІТ;

– інтегральна модель оцінки результативності впровадження хмарних технологій в корпорації відповідно до необхідних стандартів, в основі якої лежить оцінка 6–ти групових критеріїв. В результаті розрахунку інтегрального показника результативності визначено, що якщо значення $K_{\text{ecs}} > 0,5$, то додаток підходить за критеріями і задовольняє бізнес–стратегії корпорації і відповідає стандартам по використанню хмарних обчислень;

– модель підтримки прийняття рішень про перехід ІТ–додатків в хмарне середовище на основі методу аналізу ієрархій, яка дозволяє здійснювати оцінку можливості впровадження ІТ–додатків в хмарне середовище по трьом груповим критеріями: бізнес–цінність, технічна можливість і ступінь ризику; дозволяє отримувати рекомендації щодо прийняття рішення на основі матриці узагальнення.

У цьому розділі було розглянуто та обрано основні технології для розробки системи. Для розробки БД було обрано MsSQL Server, а для розробки клієнтського додатку та серверу – платформу .Net та мову програмування C#. Після вибору технологій була спроектована структура бази даних. Вибір технологій дає можливість визначити мінімальні вимоги для обладнання користувача та перейти до створення інтерфейсу користувача та тестування додатку.

Процес вибору хмарних ІТ–сервісів складний, погано формалізований, слабо структурований, тому операцію декомпозиції важливо чітко продумувати. Для прийняття обґрунтованого рішення при виборі хмарних ІТ–сервісів для впровадження в корпорації необхідно зібрати дані та провести їх аналіз для визначення витрат і вигод, результативності та ризиків від їх застосування. На виході процесу аналізу буде отримано набір даних для попереднього аналізу та оцінки інформаційних ризиків. За результатами оцінки отримуємо ваговий коефіцієнт для кожного провайдера, на основі якого приймається рішення про впровадження.

РОЗДІЛ 4. ІНФОРМАЦІЙНО–АНАЛІТИЧНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ІНФОРМАЦІЙНИХ РИЗИКІВ

Слід підкреслити, що до теперішнього часу немає єдиної думки про методи оцінки придатності хмарних обчислень, але цього важко досягти, оскільки в галузі відсутня єдина, стандартна, структурована платформа, яка могла б допомогти корпораціям в оцінці і зниженні ризиків «хмарних» обчислень.

Функціональна модель оцінки і аналізу корпоративних ІТ–додатків представлена в додатку Г. Розглянемо кожну функцію докладніше.

1. Облік даних про провайдерів і надаються хмарних сервісах. Вхідна інформація: інформація про провайдерів і хмарних сервісах; характеристики хмарних сервісів. Вихідна інформація: звіт про провайдерів і надання хмарних сервісах.

2. Оцінка придатності ІТ–додатків для переходу в хмару. Вхідна інформація про: критерії оцінки; корпоративні ІТ–додатки; експертні оцінки. Вихідна інформація: звіт «Бізнес–цінність переходу в хмару»; звіт «Ступінь ризику переходу в хмару».

Для опису концептуальних схем предметної області застосована ER–діаграма. З її допомогою виділені ключові сутності і позначені зв'язки, які можуть встановлюватися між цими сутностями.

На рівні ключів, крім імен сутностей і зв'язків, представлені первинні, альтернативні і зовнішні ключі сутностей. Вказуються також специфіковані властивості зв'язків (їх кардинальність та ідентифікація). На рівні атрибутів представлені всі атрибути сутностей. Ця діаграма містить повні визначення структури створюваної системи. Діаграма представлена в додатку Д.

Для функціонування будь–якої програми необхідно створити ряд об'єктів інформаційної системи. В даному випадку це довідники, документи, звіти. ІАС оцінки та аналізу корпоративних ІТ–додатків для міграції в хмару містить дві підсистеми: Оцінка ІТ–додатків корпорації і Облік витрат. Розглянемо деякі об'єкти розробленої ІАС з прикладами діалогових вікон.

4.1 Позиціювання структури та зображення механізму програми

Розрахунок інтегрального показника включає наступні етапи:

1) Збір даних. Визначення кількісних і якісних показників, виходячи з відповідей провайдера хмарного ІТ-сервісу, контрактів, договорів, прайс-листів. Ця робота проведена на першому етапі пропонованої методики вибору хмарних ІТ-сервісів.

2) Бальна оцінка експертом всіх показників відповідно до запропонованої шкалою переваг. Для розуміння необхідних стандартів слід використовувати документи – «Стандарти та керівництва з використання хмарних обчислень», розроблені в 2014 році Об'єднаним технічним комітетом ЛТС 1 [73]. Також в якості стандартних значень показників можуть виступати: показники лідера-конкурента на ринку, показники аналога-конкурента, власне уявлення експерта.

3) Розрахунок коефіцієнтів вагомості для критеріїв.

4) Розрахунок значень критеріїв.

5) Розрахунок інтегрального показника результативності хмарного сервісу (K_{ecs}).

Рішення, пов'язані з міграцією корпоративних додатків в хмару, можна вважати стратегічними, так як вони пов'язані зі значними витратами різних ресурсів і значною часткою невизначеності середовища прийняття рішень, несуть довгострокові надзвичайні наслідки для корпорації.

Після відбору хмарних ІТ-сервісів, які будуть ефективні для впровадження в корпорацію, необхідно порівняти між собою. Це дозволить виявити найбільш підходящі сервіси для роботи в хмарному середовищі.

4.2 Візуалізація реалізованого продукту та опис взаємодії із користувачем

Взаємодія експерта з інформаційно-аналітичною системою CCRA розпочинається з авторизації користувача (рис. 4.1). Користувачу для авторизації потрібно заповнити поля «Логін» та «Пароль». При переході до наступного кроку відбувається ідентифікація користувача в CCRA.

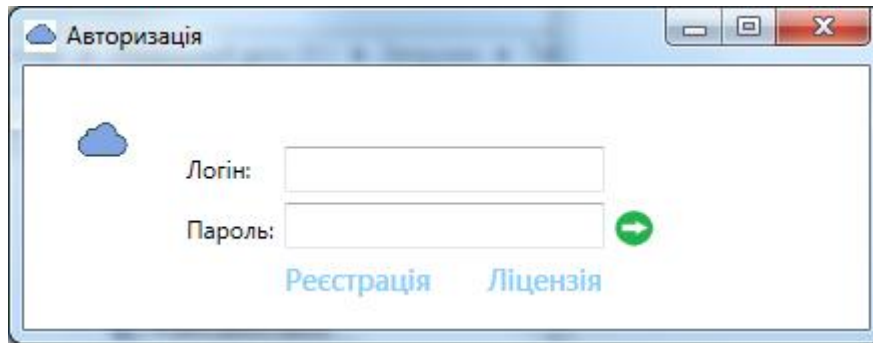


Рисунок 4.1 – Авторизація користувача в ССРА

Після проходження авторизації користувачу надається можливість вибору (рис. 4.2):

- створити нову виборку ризику інформаційної безпеки для корпорації;
- обрати раніше створену виборку ризику інформаційної безпеки для певної корпорації.

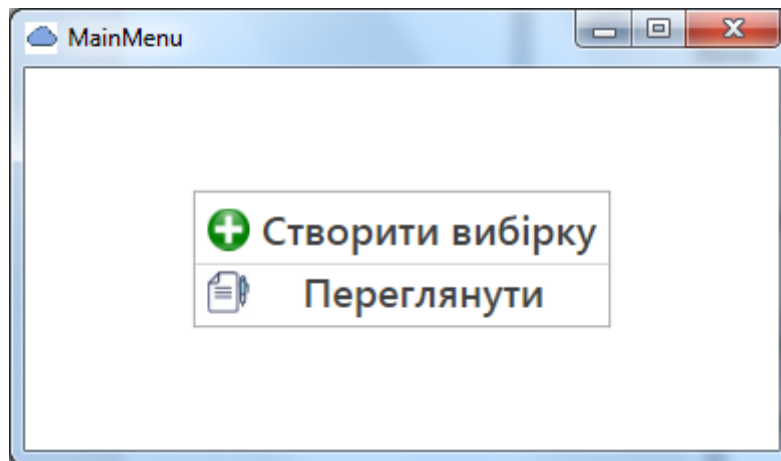


Рисунок 4.2 – Головне меню

На наступному кроці користувачу надаються наступні варіанти взаємодії:

- якщо було обрано «Створити нову виборку ризику інформаційної безпеки для корпорації» пропонується ввести назву корпорації або обрати із запропонованого списку після чого відбувається перехід до функціоналу модулю «Вхідні дані» (рис. 4.3);

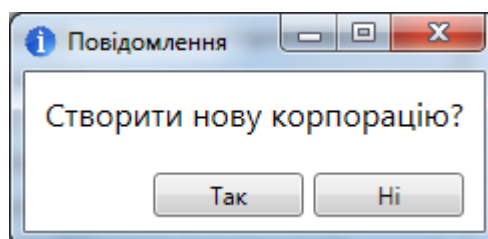


Рисунок 4.3 – Вибір при створенні нової корпорації

– якщо було обрано «Обрати раніше створену виборку ризику інформаційної безпеки для певної корпорації» відбувається перехід до функціоналу модулю «Вхідні дані» (рис. 4.4).

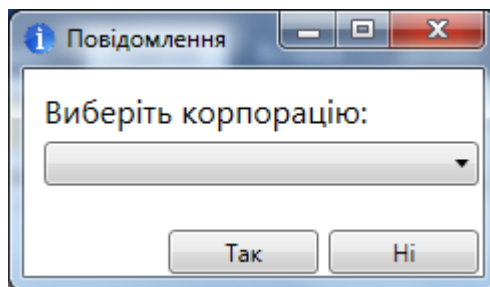


Рисунок 4.4 – Вибірка корпорації

Модулю «Вхідні дані» є функціонально складним, який консолідує усі функції даної системи.

На першому етапі (рис. 4.5) користувач заповнює зведену інформацію щодо ІТ—інфраструктури корпорації, а саме:

- наявність власного ЦОДу, при наявності власного ЦОД вказується які моделі обслуговування підтримує частна хмара;
- перелік та назва існуючих баз даних із зазначенням для кожної з них видів інформаційних ризиків та оціночною характеристикою існуючого рівня інформаційної безпеки;
- перелік існуючих додатків;
- пропускна спроможність інформаційних каналів зв'язку;
- тощо.

Після внесення зведеної інформації щодо ІТ—інфраструктури корпорації автоматично формуються три окремих матриці: матрицю загроз, матрицю вразливостей і матрицю контролю. За допомогою цих матриць збираються дані для аналізу ризиків. [27, 28].

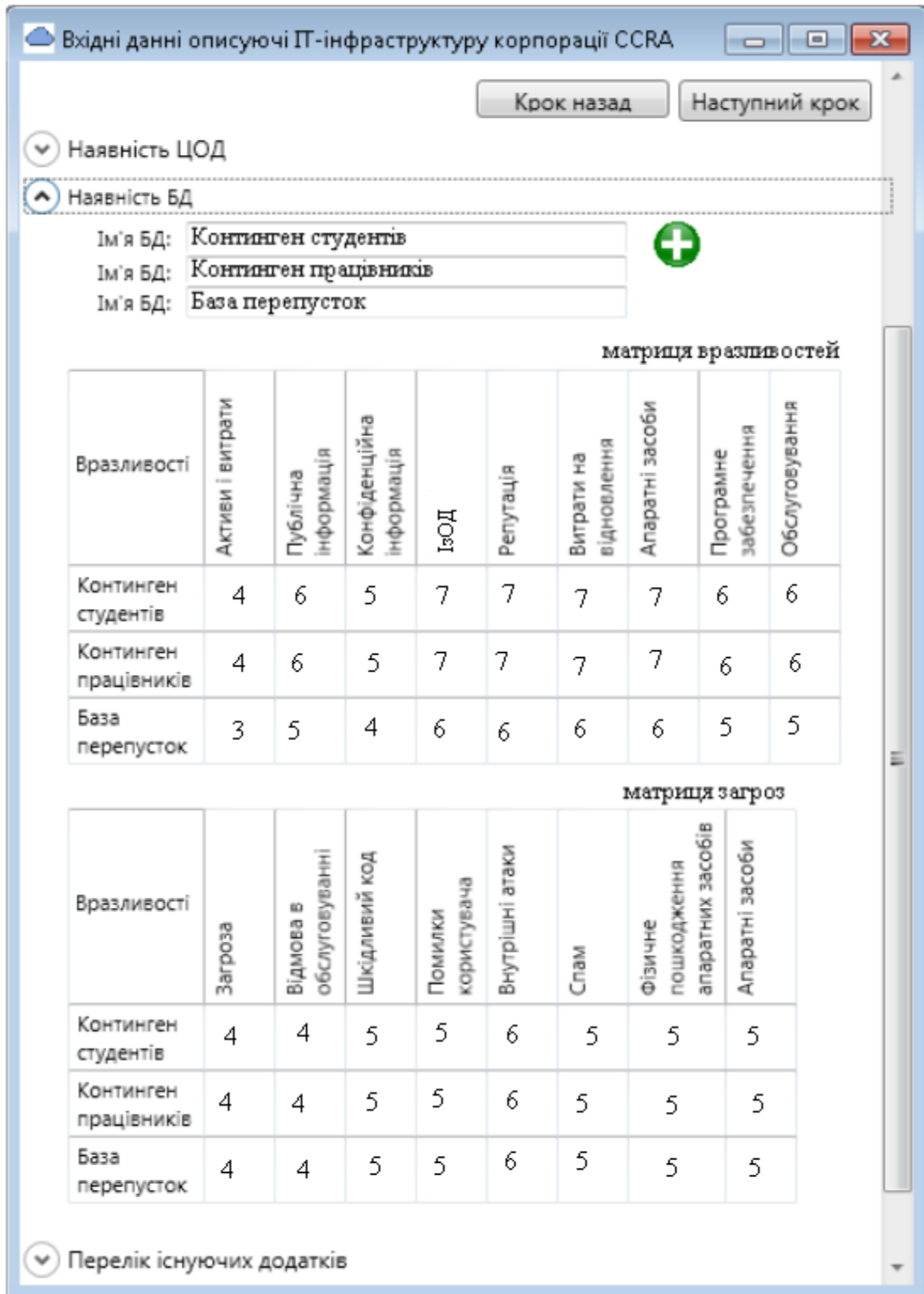


Рисунок 4.5 – Перший етап вхідних даних

Всі матриці пов'язані між собою. Матриця вразливостей містить кореляційний зв'язок між активами і вразливостями, матриця загроз відображає причинно-наслідковий зв'язок вразливостей та загроз, а матриця контролю демонструє співвідношення між загрозами і засобами управління. Значення, отримане в результаті аналізу, в кожній відповідній комірці матриці

характеризує цінність відносини між елементом рядка і стовпця.

Використовується така система оцінок: низька, середня і висока.

Таблиця 1 – шкала оцінок

0	1	2	3	4	5	6	7	8	9
немає впливу	слабкий вплив	...	помірний вплив	сильний вплив

В процесі первинного аналізу формуються списки активів, вразливостей, загроз і засобів управління. Матриці заповнюються шляхом додавання даних про зв'язок елемента стовпця матриці з елементом рядка. Потім дані з матриці вразливостей переносяться в матрицю загроз. Далі за таким же принципом дані з матриці загроз заносяться в матрицю контролю.

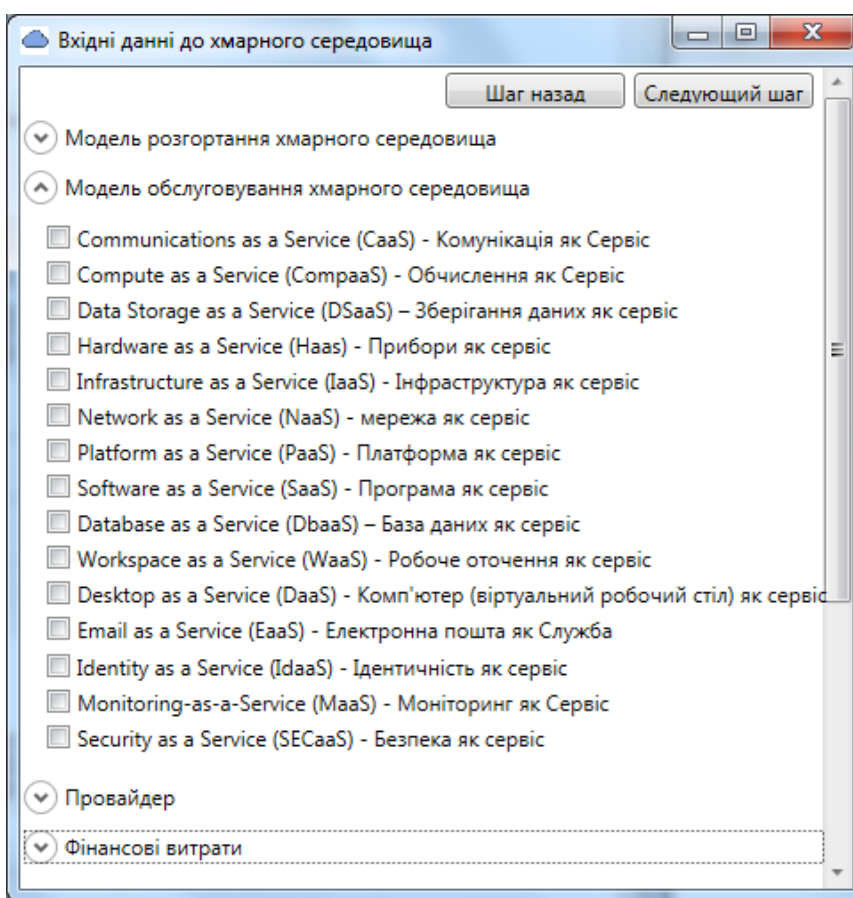


Рисунок 4.6 – Другий етап вхідних даних

На другому етапі (рис. 4.6) користувач заповнює інформацію щодо вимог до хмарного середовища, а саме:

- модель розгортання хмари;
- моделі обслуговування хмари;
- країна, розміщення серверів провайдера;
- провайдер, за ліцензією надання послуг;

- плануєма сума витрат на місяць за публічну хмару;
- тощо.

На четвертому етапі, на основі графіку кореляції величини збитку та ймовірності події (та запропонованого експертом оптимального варіанту), команда починає обговорення обґрунтованої пропозиції щодо розробки стратегії рішень відповідно до цього варіанту (рис. 4.7).

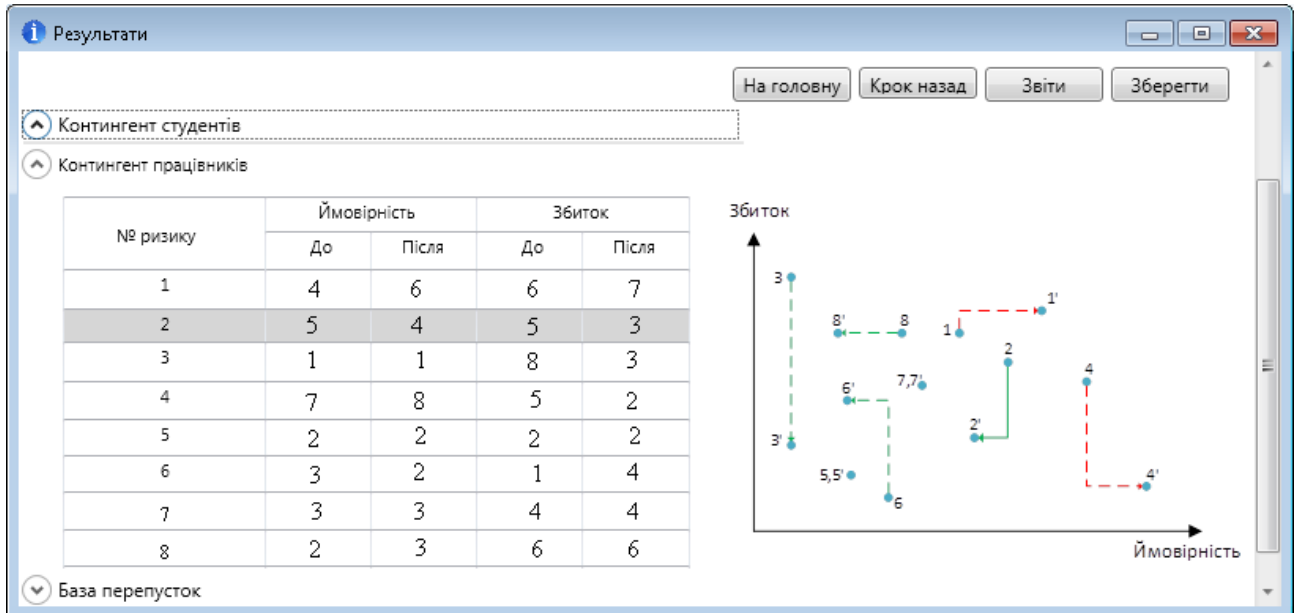


Рисунок 4.7. – Результати кореляційної величини збитку та ймовірності події

Висновки до розділу

Майже в усіх методиках базою для визначення рівня ризику є допустимість появи тієї чи іншої події, яка визначає рівень ймовірності реалізації загрози. В основу методик визначення ймовірності найчастіше закладається експертний метод або використовується дані статистики попередніх періодів.

Для розробки моделі управління ризиками інформаційної безпеки корпорації необхідно вибрати таку модель або комбінацію моделей, яка б включала в себе визначення, збір та обробку даних про результуючі фактори, які притаманні системі, та дозволяє з високим рівнем ймовірності визначити найгірший сценарій для реалізації загрози. Дана модель має бути адаптивною та оперативно змінюватись з урахуванням вихідних результатів (кількості користувачів, кількості обладнання, швидкості каналу передачі даних тощо).

В четвертому розділі представлено графічний інтерфейс розробленої інформаційно-аналітичної системи, яка надає аналіз ризиків втрати інформації при переході корпорації до хмарного середовища.

Розроблена інформаційно-аналітична система, повністю задовольняє вимогам, які були визначені при проектуванні.

Розроблена система проста в експлуатації. Інтуїтивно–зрозумілий інтерфейс дозволяє скоротити час на обробку даних і отримання результату. Вимоги до апаратного забезпечення необхідні для роботи з даною системою мінімальні.

В автоматизованій системі оцінки ризику повністю реалізовані описані в роботі механізми визначення критичної групи загроз.

РОЗДІЛ 5. МАРКЕТИНГОВИЙ АНАЛІЗ СТАРТАП–ПРОЕКТУ

Однією з основних причин створення, успішного розвитку та подальшого існування стартапів вважають неповороткість і повільність великих корпорацій, які успішно використовують уже наявні продукти, а розробкою і створенням нових майже не займаються. Тому стартапи, завдяки своїй мобільності в плані втілення нових ідей становлять конкуренцію великим корпораціями.

Основним ресурсом для створення нового стартапу служить хороша новаторська ідея. Власне за свіжими і незвичайними ідеями женуться багато і часто купуючи їх не шкодують великі суми. Сама ідея, яка не має ніякого матеріального втілення, а існує тільки на папері або на словах (план стартапу), може коштувати дуже багато. Іншим фактором успішності цієї ідеї є її затребуваність (ступінь необхідності для споживача), адже ідея може бути незвичайної і новою, але користі від неї буде мінімум.

Стартапи покликані вирішувати проблеми і завдання, які з часом стає можливим вирішити завдяки використанню результатів технічного прогресу.

5.1 Опис ідеї проекту

Таблиця 4.1. Опис ідеї стартап–проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Розрахунок мінімізації ризику на основі хмарних технологій та прийняття рішення щодо переведення корпорації на хмарний сервіс.	Корпорації; Аудит компанії.	Економічні Результуючі

Таблиця 4.2. Опис ідеї стартап–проекту

№	Техніко– економічні характеристики ідеї	Продукція конкурентів	W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект			
1	Визначення оцінки ризику	Застосування оцінки мінімізації ризиків для переходу на хмарні технології			+
2	Визначення відсотку втрати інформації				+
3	Прогнозування			+	
4	Вибір найкращого варіанту				+
5	Дає рішення переходу на хмарний сервіс			+	

5.2 Технологічний аудит ідеї проекту

Таблиця 4.3. Технологічна здійсненність ідеї проекту

№	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Розрахунок мінімізації ризиків на основі хмарних технологій	БД NVS	+	+
		БД CVSS	+	+
		Хмарні технології	+	+
		Матричний метод	+	+

5.3 Аналіз ринкових можливостей запуску стартап–проєкту

Таблиця 4.4. Попередня характеристика потенційного ринку

№	Показники стану ринку	Характеристика
1	Кількість головних гравців, од	Немає
2	Загальний обсяг продаж, грн./ум.од	6 000 грн. на 1 продукт
3	Динаміка ринку	Стагнує
4	Наявність обмежень для входу	Немає
5	Специфічні вимоги до стандартизації та сертифікації	Знання послугами аудита
6	Середня норма рентабельності в галузі або по ринку, %	40 %

Висновок: враховуючи кількість головних гравців по ринку, зростаючу динаміку ринку, невелику кількість конкурентів та середню норму рентабельності можна зробити висновок, що на даний момент, ринок для входження стартап–продукту є привабливим.

Таблиця 4.5. Характеристика потенційних клієнтів стартап–проєкту

№	Потреба, що формує ринок	Цільова аудиторія	Відмінності у поведінці цільових груп клієнтів	Вимоги споживачів до товару
1	Зменшення ризику втрати інформації при переході на хмарні сервіси	Аудиторські компанії	Немає відмінності у поведінці цільових груп клієнтів	Точність оцінки; Швидкість оцінювання
2	Визначення потреби переходу на хмарні технології			

Таблиця 4.6. Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
1	Кошти на розробку та підтримку продукту	Закінчення грошей та недостатнє фінансування	Залучення додаткових інвесторів, мотивація роботи на перспективу; Ітеративна розробка продукту задля покрокового виведення продукту на ринок та отримання відповіді користувачів
2	Вихід аналогу	Вихід аналогу даного товару може призвести до знецінення та безідейності даного товару	Вихід товару на ринок в коротші строки з не повною, але достатньою, функціональністю для зацікавлення усіх цільових аудиторій; Проведення рекламної компанії

Таблиця 4.7. Фактори можливостей

№	Фактор	Зміст можливості	Можлива реакція компанії
1	Новий продукт	Вихід на ринок, Надання нових рішень у сфері	Розробка нової функціональності; Вихід нової продукції на ринок; Надання різноманітних типів ліцензій в залежності від потреб користувача \ замовника.
2	Вихід аналогу	Надати продукт з певними характеристиками та можливостями що відсутні у компаній конкурентів	Аналіз ринку та користувачів задля задоволення їх потреб та надання функціональності у найкоротші строки за ціну, котра є дешевшою ніж у продуктів–замінників.
3	Зворотній зв'язок від користувачів	Можливість отримання необхідної інформації для вдосконалення продукту	Наявність вхідних даних та реакція на них з боку команди розробників задля задоволення потреб та бажань кінцевих користувачів системи кешування даних.

Продовження таблиці 4.7

4	Грошова винагорода за рекламу	<p>При достатньому попиту на систему кешування даних можлива комерціалізація продукту на основі реклами задля отримання грошової винагороди для подальшого розвитку продукту та оплати заробітної плати працівникам</p>	<p>Точкова комерціалізація продукту; Введення реклами; Ведення додаткових коштів у проект задля його подальшого розвитку.</p>
---	-------------------------------	---	---

Таблиця 4.8. Ступеневий аналіз конкуренції на ринку

№	Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1	Тип конкуренції: монополістична	<p>Товар від кожної компанії на ринку, являється недосконалим замінником товару, реалізованого іншими фірмами; На ринку є умови для входу та виходу; Ціна корелює між суперниками;</p>	<p>Розробка продукту з характеристиками, які покривають сфери вживання що не покривають інші товари–замінники; Кореляція цін у відповідності до товарів замінників; Різні типи ліцензій.</p>

Продовження таблиці 4.8

2	Рівень конкурентної боротьби: світовий	Всі продукти замітники розроблялись інтернаціональними командами з різних куточків світу, продукти не належать до певної держави, а належать команді розробників	Вихід на ринок збуту продукту з клієнто–необхідною функціональністю; Налагодження маркетингу на основних Інтернет ресурсах задля охоплення великої кількості потенційних користувачів; Надання бета–версій продукту.
3	Галузева ознака: внутрішньогалузева	Даний тип продукту може використовуватися тільки у сфері розробки ІТ додатків \ продуктів	Надання зручного, інтуїтивно зрозумілого інтерфейсу; Підтримка всім відомих методів взаємодії з середовищем розробки; Наявність документації та он–лайн підтримки.
4	Конкуренція за видами товарів: товарно–видова	Дана конкуренція – конкуренція між товарами одного виду.	Впровадження функціональності яка відсутня у товарів–замінників; Спрощення інтерфейсів; Надання підтримки.
5	Характер конкурентних переваг: цінова та не цінова	Цінові переваги – точкова комерціалізація; Не цінова – надання функціональності, що відсутня у товарах–замінниках.	Надання платних ліцензій лише на критично важливу функціональність для клієнта з певним строком підтримки, що зазначена у відповідній ліцензії; Впровадження унікальної функціональності.
6	За інтенсивністю: марочна	Наявність унікального знаку що відрізняє даний продукт від продуктів–замінників	Впровадження власної назви та власного знаку.

Таблиця 4.9. Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари–замінники
	Навести перелік прямих конкурентів	Визначити бар'єри входження в ринок	Визначити фактори сили постачальників	Визначити фактори сили споживачів	Фактори загроз з боку замінників
Висновки	Визначити інтенсивність конкурентної боротьби з боку прямих конкурентів	– чи є можливості входу в ринок? – чи є потенційні конкуренти? Строки виходу їх на ринок?	Чи постачальники диктують умови роботи на ринку? Які?	Чи клієнти диктують умови роботи на ринку? Які?	Обмеження для роботи на ринку через товари замінники

Проаналізувавши можливості роботи на ринку з огляду на конкурентну ситуацію можна зробити висновок: оскільки кожний з існуючих продуктів не впливає у великій мірі на поточну ситуацію на ринку в цілому, кожний з існуючих продуктів має свою специфічну сферу використання та свої позитивні та негативні сторони щодо рішення певних типів задач, то робота та вихід на даний ринок є можливою і реалізованою задачею.

Для виходу на ринок продукт повинен мати функціонал що відсутній у продуктів–аналогів, повинен задовольняти потреби користувачів, мати необхідний та достатній функціонал з конфігурування, підтримку зі сторони розробників та можливість розробки спеціального функціоналу за відповідною ліцензією.

Таблиця 4.10. Обґрунтування факторів конкурентоспроможності

№	Фактор конкурентоспроможності	Обґрунтування
1	Економічний	Розраховує витрати на перехід до хмарного сервісу
2	Іноваційний	На ринку немає такого продукту
3	Надійність	Використовується БД стандартів по ризикам

Таблиця 4.11. Порівняльний аналіз сильних та слабких сторін системи кешування мало змінних даних

№	Фактор конкурентоспроможності	Бали 1–20	Рейтинг товарів–конкуrentів у порівнянні з запропонованим						
			–3	–2	–1	0	+1	+2	+3
1	Економічний	14					+		
2	Іноваційний	19							+
3	Надійність	17						+	

Таблиця 4.12. SWOT аналіз стартап–проекту

<p>Сильні сторони (S):</p> <p>контроль за здійсненням витрат, пошук можливостей щодо їхнього зниження; інвестиційна привабливість підприємства; зважена цінова політика; врахування потреб споживачів.</p>	<p>Слабкі сторони (W):</p> <p>частка ринку; організація системи комунікацій.</p>
<p>Можливості (O):</p> <p>зростання грошових доходів; застосування сучасних технологій</p>	<p>Загрози (T):</p> <p>недосконалість та змінюваність законодавства; інфляційні процеси; високий рівень безробіття.</p>

Таблиця 4.13. Альтернативи ринкового впровадження стартап–проекту

№	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Стратегія нейтралізації ринкових загроз сильними сторонами стартапу.	вище середньої	1 рік
2	Стратегія підсилення сильних сторін за рахунок ринкових можливостей.	висока	6 місяців
3	Стратегія компенсації слабких сторін наявними ринковими можливостями.	середня	2 роки

5.4 Розроблення ринкової стратегії проекту

Таблиця 4.15. Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Аудит компанії	Висока	Специфічна	Помірна	Високий бар'єр входу у галузь

Відповідно до проведеного аналізу можна зробити висновок, що підходящою цільовою групою для розповсюдження даного програмного продукту є працівники аудит компанії або експерти коропрації які проводять аудит. Відповідно до стратегії охоплення ринку збуту товару обрано стратегію масового маркетингу, оскільки для аудит компаніям надається стандартизований продукт з можливістю розширення функціональності за домовленістю (відповідно до ліцензії).

Таблиця 4.16. Визначення базової стратегії розвитку

Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи
Стратегія диференціації	Передбачає надання товару важливих з точки зору споживача відмінних властивостей, які роблять товар відмінним від товарів конкурентів. Така відмінність може базуватися на об'єктивних або суб'єктивних, відчутних і невідчутних властивостях товару(у ширшому розумінні – комплексі маркетингу), бути реальною або уявною.	Реалізація цієї стратегії вимагає, як правило, більш високих витрат. Проте успішна диференціація дозволяє компанії домогтись більшої рентабельності за рахунок того, що ринок готовий прийняти більш високу ціну (цінову премію бренду).

Таблиця 4.17. Визначення базової стратегії конкурентної поведінки

Чи є проект «першопрохідцем» на ринку	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, які?	Стратегія конкурентної поведінки
Ні	Так	частково	Стратегія заняття конкурентної ніші

Таблиця 4.18. Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап–проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту
1	Відповідність чинним нормативам	Заняття конкурентної ніші	Реалізація цієї стратегії вимагає, як правило, більш високих витрат. Проте успішна диференціація дозволяє компанії домогтись більшої рентабельності за рахунок того, що ринок готовий прийняти більш високу ціну (цінову премію бренду).	Унікальність Доступна ціна Реалізація нових методів

Відповідно до проведеного аналізу можна зробити висновок, що стартап–компанія вибирає як базову стратегію розвитку – стратегію диференціації, як базову стратегію конкурентної поведінки – стратегію заняття конкурентної ніші.

5.5 Розроблення маркетингової програми стартап–проекту

Таблиця 4.19. Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
1	Розрахунок ризиків втрати інформації	Результуюча	Зменшує витрати на оцінювання ризиків

Таблиця 4.21. Визначення меж встановлення ціни

Рівень цін на товари–замінники	Рівень цін на товари–аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
6000	5000	10000	4000-6000

Таблиця 4.22. Формування системи збуту

Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
Мінімальна кількість посередників	Організувати широку мережу збуту товару	3	непряма

Таблиця 4.23. Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення
1	Обережний вибір потенційних контрагентів, що зумовлено особливістю ринку	Інтернет-розсилки	Технологія	Привернути увагу

Висновки по розділу

Стратегія лідерства за витратами дозволяє розробляти, виробляти і продавати продукти більш ефективно, ніж її конкуренти.

Ця стратегія можлива при масовому виробництві стандартизованої, як правило, дешеві продукти і налагодженими каналами збуту.

Компанія, яка здійснює цю стратегію постійно знаходиться під тиском з боку конкурентів, тому він вимагає від компанії, щоб мати оптимальні розміри виробництва, розвинена мережа продажів, захопити певну частку ринку і так далі.

ВИСНОВКИ

1. Досліджено існуючі стандарти в області створення хмарних інформаційно–обчислювальних систем, визначені основні проблеми, пов’язані з використання хмарних технологій.

Проведено аналіз:

– джерел виникнення ризикових ситуацій та запропоновано класифікацію ризиків втрати інформації корпорації;

– впливу ризиків втрати інформації на ефективність роботи і конкурентоспроможність корпорації.

2. Проаналізовано існуючі методи, моделі і програмні продукти оцінки ефективності методик та визначення ймовірності реалізації ризиків впровадження програмного забезпечення ІТ–середовища, а також методик підтримки прийняття рішень при виборі хмарних ІТ–сервісів для впровадження в корпорації.

Для розробки моделі управління ризиками інформаційної безпеки корпорації була запропонована комбінація моделей, яка включає в себе визначення, збір та обробку даних про результуючі фактори, які притаманні системі, та дозволяє з високим рівнем ймовірності визначити сценарії для реалізації загрози. Дана модель має бути адаптивною та змінюватись з урахуванням вихідних результатів (кількості користувачів, кількості обладнання, швидкості каналу передачі даних тощо).

Таким чином, доцільна розробка програмного забезпечення підтримки прийняття рішень при виборі хмарних ІТ-сервісів для впровадження в корпорації з використання існуючих методик та моделей, які були розглянуті в другому розділі.

3. Запропоновано використання системи критеріїв та показників оцінки результативності впровадження хмарних технологій, а також моделі оцінки результативності впровадження хмарних ІТ–сервісів на їх основі.

Майже в усіх методиках базою для визначення рівня ризику є допустимість появи тієї чи іншої події, яка визначає рівень ймовірності реалізації загрози. В основу методик визначення ймовірності був закладений експертний метод.

4. Розроблено програмне забезпечення інформаційно-аналітичної системи підтримки прийняття рішень при виборі хмарних ІТ-сервісів, яке реалізує математичні моделі оцінки.

В роботі розглянуто та обрано основні технології для розробки системи. Для розробки БД було обрано MsSQL Server, а для розробки клієнтського додатку та серверу – платформу .Net та мову програмування C#. Після вибору технологій спроектували структуру бази даних. Вибір технологій дає можливість визначити мінімальні вимоги для обладнання користувача та створена інформаційно-аналітична система.

В процесі розробки програмного забезпечення направлено на вирішення проведення кількісної оцінки та побудови ризик-моделі хмарного середовища були:

- визначені та описані можливі ризики використання хмарних середовищ в взаємозв'язку з вразливостями корпорації та визначений перелік вразливостей для кожного ризику, побудовані для них вектори системи загального обліку вразливостей (CVSS);
- розроблений алгоритм системи з урахуванням існуючих методик оцінки рівнів ризику;
- на підставі отриманих рівнях впливу вразливостей побудована ризик-модель.

За результатами проведених аналізів та використанням існуючих методик в роботі представлено графічний інтерфейс розробленої інформаційно-аналітичної системи, яка надає аналіз ризиків втрати інформації при переході корпорації до хмарного середовища.

Даний інтегральний підхід до оцінки ймовірності мінімізації інформаційного ризику переходу до хмарного середовища, який застосований в роботі, дозволяє оптимізувати ефективність управління ризиками в корпорації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Найдич А. Рынок SaaS и его участники в мире и в России // КомпьютерПресс 08'2013.
2. Науменко А.И. Оценка эффективности внедрения инновационных информационных технологий в банковской деятельности: автореф. дисс. канд. экон. наук: 08.00.05 – Новосибирск, 2006. – 21 с.
3. Облачные сервисы (рынок России) // TAdviser, 10.07.2014. – [Электронный ресурс]. Режим доступа: [http://www.tadviser.ru/index.php/http://www.tadviser.ru/index.php/Статья:Облачные_сервисы_\(рынок_России\)](http://www.tadviser.ru/index.php/http://www.tadviser.ru/index.php/Статья:Облачные_сервисы_(рынок_России)). Дата обращения – 4.09.2014.
4. Харатишвил Д. Рынок «облачных» услуг в цифрах и фактах // КомпьютерПресс 8'2010.
5. Арефьев Н. IaaS, PaaS, SaaS. Раздел территории между провайдерами и клиентами облачных сервисов // Защита виртуальных сред и облачных вычислений Jet Info №5, май 2013 г. – [Электронный ресурс]. Режим доступа: <http://www.jetinfo.ru/author/nikolaj-arefev/iaas-paas-saas-razdel-territorii-mezhdu-provajderami-i-klientami-oblachnykh-servisov>. Дата обращения: 12.03.2014.
6. Меднов С. Облачные вычисления // Клуб топ-менеджеров 4CIO. [Электронный ресурс]. – Режим доступа: <http://www.4cio.ru/pages/index/129>. Дата обращения: 09.04.13.
7. Нестеркина Е. Методы реализации стандартной стратегии рисков облачных вычислений (cloud computing) // ЦОД, датацентры, облачные вычисления, SaaS, 2013 [Электронный ресурс]. – Режим доступа: <http://dcnt.ru/?p=10700> (дата обращения: 12.06.2013).
8. Одегов С.В. Методика снижения рисков информационной безопасности облачных сервисов на основе квантифицирования уровней защищенности и оптимизации состава ресурсов: дисс. канд. тех. наук: 05.13.19 – Санкт-Петербург, 2013. – 107 с.

9. Полякова Т.А., Химченко А.И. Правовые проблемы обеспечения информационной безопасности при использовании облачных технологий // Правовая информатика, с. 12-16.

10. Разумников С.В. Моделирование оценки рисков при использовании облачных ИТ-сервисов // Фундаментальные исследования. - 2014 - №. 5-1. - С. 39-43.

11. Стив Балмер Облачные вычисления как настоящее и будущее ИТ // УК «Альянс. венчурный бизнес», 14.02.2011. [Электронный ресурс]. – Режим доступа: <http://venture-biz.ru/informatsionnye-tekhnologii/205-oblachnye-vychisleniya>. Дата обращения: 25.11.12.

12. Михайлов А.Г. Кому и зачем нужна ИТ-стратегия? Результаты интервьюирования ИТ-директоров // Global CIO – [Электронный ресурс]. – 2015. – Режим доступа: http://www.globalcio.ru/workshops/1118/?setstat=1&id=16915&hash=71392a5348fdbe0d7e2789c3971f06186db28010&auto_login=1&from_digest=165&item_id=165. Дата обращения – 28.09.2015.

13. Холодков А. ИТ-стратегия, часть 1: общий стратегический процесс в организации // ИТ-консультант.рф – [Электронный ресурс]. – Режим доступа: <http://www.kholodkov.ru/it/?p=671>. Дата обращения: 10.09.2015.

14. Холодков А. ИТ-стратегия, часть 2: определение, границы, содержание, процессы разработки и реализации // ИТ-консультант.рф – [Электронный ресурс]. – Режим доступа: <http://www.kholodkov.ru/it/?p=737>. Дата обращения: 10.09.2015.

15. Холодков А. ИТ-стратегия, часть 3: консалтинг в области стратегического управления ИТ // ИТ-консультант.рф – [Электронный ресурс]. – Режим доступа: <http://www.kholodkov.ru/it/?p=752>. Дата обращения: 10.09.2015.

16. Гребнев Е. Облака: от старых технологий к широким перспективам. 2012. URL: http://cloud.cnews.ru/reviews/index.shtml?2011/05/20/440918_1 (дата обращения: 29.05.2014). – 48

17. Miller R. Who Has the Most Web Servers? 2012. URL: <http://www.datacenterknowledge.com/archives/2009/05/14/whos-got-the-most-web-servers/> (дата обращения: 29.05.2014). - 1.

18. Медведев А. Облачные технологии: тенденции развития, примеры исполнения // Современные технологии автоматизации. 2013. № 2. С. 6–9. -2.

19. Храмовская, Н. Стандарты и руководства по использованию облачных вычислений [Текст] /Н. Храмовская // Information Management. – 2013. – № 3. – С. 12-21 - 1.

20. NISTIR 8074 Volume 2 (Draft) Supplemental Information for the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity [Electronic resource] // National Institute of Standards and Technology. – Access mode: http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol1_draft_report.pdf. – 24.11.2015. – 2.

21. D: A-5.1 Report on A4Cloud contribution to standards. Version 1.1. Deliverable Lead Organisation [Electronic resource] // Cloud Accountability Project (CSA). – Access mode: [http://www.a4cloud.eu/sites/default/files/D15.1 Report on A4Cloud contribution to standards.pdf](http://www.a4cloud.eu/sites/default/files/D15.1%20Report%20on%20A4Cloud%20contribution%20to%20standards.pdf). – 24.11.2015. - 3.

22. Hibbard, E. A. Latest in Cloud Computing Standards [Electronic resource] // Eric A. Hibbard. – Access mode: <http://www.slideshare.net/rnewton/summary-cloudstandardseahv2130225>. – 24.11.2015. - 4.

23. Cisco Global Cloud Index: Forecast and Methodology, 2014-2019. White Paper [Electronic resource] // Cisco. – Access mode: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf. – 24.11.2015. - 5.

24. NIST Special Publication 500-291, NIST Cloud Computing Standards Roadmap [Text]. – impl. 01.07.2011. – Gaithersburg: National Institute of Standards and Technology, 2011. – 76 p. - 6.

25. ITU-T. FG Cloud TR. Version 1.0. (02/2012). Part 6: Overview of SDOs involved in cloud computing. [Electronic resource] // Switzerland, Geneva. – Access

mode: http://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P6-PDF-E.pdf. – 24.11.2015. - 7.

26. ISO/IEC 17788:2014 Information technology - Cloud computing - Overview and vocabulary [Text]. – impl. 15.10.2014. – Brussels: European Committee for Electrotechnical Standardization, 2014. – 16 p. - 8.

27. ISO/IEC 17789:2014 Information technology - Cloud computing – impl. 10.10.2014. – Brussels: European Committee for Electrotechnical Standardization, 2014. – 53 p. - 9.

28. Recommendation ITU-T Y.3500. Information technology – Cloud computing – Overview and vocabulary [Text]. – impl. 13.08.2014. – Geneva: International Telecommunication Union, 2014. – 18 p. - 10.

29. Recommendation ITU-T Y.3501. Cloud computing framework and high-level requirements [Text]. – impl. 22.05.2013. – Geneva : International Telecommunication Union, 2013. – 26 p. – 11.

30. Recommendation ITU-T Y.3502. Information technology - Cloud computing - Reference architecture [Text]. – impl. 13.08.2014. – Geneva : International Telecommunication Union, 2014. – 62 p. – 12.

31. Recommendation ITU-T Y.3503. Requirements for desktop as a service [Text]. – impl. 22.05.2014. – Geneva: International Telecommunication Union, 2014. – 34 p. – 13.

32. Recommendation ITU-T Y.3510. Cloud computing infrastructure requirements [Text]. – impl. 22.05.2013. – Geneva: International Telecommunication Union, 2013. – 28 p. -14.

33. Recommendation ITU-T Y.3511. Framework of inter-cloud computing [Text]. – impl. 09.03.2014. – Geneva : International Telecommunication Union, 2014. – 46 p. -15.

34. Recommendation ITU-T Y.3512. Cloud computing - Functional requirements of Network as a Service [Text]. – impl. 29.08.2014. – Geneva: International Telecommunication Union, 2014. – 36 p. -16.

35. Recommendation ITU-T Y.3513. Cloud computing - Functional requirements of Infrastructure as a Service [Text]. – impl. 29.08.2014. – Geneva: International Telecommunication Union, 2014. – 26 p. – 17.

36. Рекомендация МСЭ-Т X.1601. Основы безопасности облачных вычислений [Текст]. – введ. 24.01.2014. – Женева: Международный союз электросвязи, 2014. – 32с. -18

37. ISO/IEC 27000:2014. Информационные технологии. Методы обеспечения защиты. Системы управления защитой информации. Общий обзор и словарь [Текст]. – введ. 15.01.2014. – Женева: Международная организация по стандартизации, 2014. – 44 с. -25.

38. ISO/IEC 15408-1:2009. Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model [Text]. – impl. 15.12.2009. – Brussels: European Committee for Electrotechnical Standardization, 2014. – 64 p. - 26.

39. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности [Текст]. – введ. 18.04.2008. – Женева: Международный союз электросвязи, 2008. – 64 с. – 27.

40. Department of defense (DoD). Cloud computing security requirements guide (SRG). Version 1, Release 1. – impl. 12.01.2015. – Developed by the Defense Information Systems Agency (DISA) for the Department of Defense (DoD), 2015. – 152 p. -24.

41. NIST Special Publication 800-145. The NIST Definition of Cloud Computing [Text]. – impl. 01.11.2011. – Gaithersburg: National Institute of Standards and Technology, 2011. – 7 p. - 19

42. NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations [Text]. – impl. 10.05.2012. – Gaithersburg: National Institute of Standards and Technology, 2012. – 81 p. -20.

43. NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing. [Text]. – impl. 01.12.2011. – Gaithersburg: National Institute of Standards and Technology, 2011. – 80 p. -22.

44. Cloud Computing Security Reference Architecture. Working Document. [Electronic resource] // National Institute of Standards and Technology. – Access mode: http://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf. – 24.11.2015. - 21.

45. Гольдштейн Г.Я., Гуц А.Н. Экономический инструментарий принятия управленческих решений. – Таганрог: Изд-во ТРТУ, 1999. <http://www.aup.ru/books/M69/>. (6)

46. Литовских А.М. Финансовый менеджмент: Конспект лекций. – Таганрог: Изд-во ТРТУ, 1999. – 76 с. <http://www.aup.ru/books/M68/>. (20)

47. Романов В.С. Классификация рисков: принципы и критерии. <http://www.aup.ru/articles/finance/>. (26)

48. Зинкевич В., Штатов Д. Информационные риски: анализ и количественная оценка // Бухгалтерия и банки. — 2007. — № 1. — С. 50–55. (6).

49. Зинкевич В., Штатов Д. Информационные риски: анализ и количественная оценка // Бухгалтерия и банки. — 2007. — № 3. — С. 48–53. (7)

50. Завгородний В.И. Парадигма информационных рисков — http://www.fakit.ru/main_dsp.php?top_id=591.(3)

51. Романенко Л., Коротеева А. Ризики у банківській діяльності // Фінанси України. — 2003. — № 5 — С. 121–127. (1)

52. Вуколов В. Інформаційні ризики в державному управлінні — http://archive.nbuv.gov.ua/e-journals/Patp/2010_2/10vvvrdu.pdf. (5)

53. Пасько В.П., Гасанов В.А., Гришко А.С., Максимюк А.В. Інтероперабельність матриці прийняття рішення для оцінки ризиків інформаційної безпеки // Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління» № 1 (32), 2018 – 26-30 с.

54. Пасько В.П., Гасанов В.А., Гришко А.С., Максимюк А.В. Декомпозиція методики оцінки ризиків інформаційної безпеки // XIV Международная научно-практическая конференция «Перспективные вопросы мировой науки – 2018» 15-22.12.2018, Болгария, София – 70-72 с.

55. 8 шагов к безопасным облачным системам // Information Security / Информационная безопасность. – 2013. – № 1. – С. 28–29. (1)
56. Маслов А.В., Григорьева А.А. Математическое моделирование в экономике и управлении: учебное пособие – Юрга: Изд-во Юргинского технологического института (филиала) Томского политехнического университета, 2007. – 264 с. (2)
57. Разумников С.В. Анализ существующих методов оценки эффективности информационных технологий для облачных ИТ-сервисов [Электронный ресурс] // Современные проблемы науки и образования. – 2013. – № 3. – С. 1. – (3)
58. Mell P., Grance T. The NIST Definition of Cloud Computing, Version 15, September, 2011. Available at: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
59. Царегородцев А.В., Качко А.К. Обеспечение информационной безопасности на облачной архитектуре организации // Национальная безопасность. 2011. № 5. С. 25–34.
60. Царегородцев А.В., Качко А.К. Один из подходов к управлению информационной безопасностью при разработке информационной инфраструктуры организации // Национальная безопасность. 2012 №1. С. 46-59.
61. Accorsi R., Wonnemann C. Auditing Workflow Execution against Dataflow Policies. In Proc. BIS. 2010. P. 207–217.
62. Bishop M. Computer Security: art and science. Addison Wesley Publ., 2002. 1084 p.
63. NVD Common Vulnerability Scoring System Support. Vol. 2. URL: <http://nvd.nist.gov/cvss.cfm?calculator&version=2>.
64. Корилов А.М. Теория систем и системный анализ: учеб. Пособие / А.М. Корилов, С.Н. Павлов. – 2-е изд., доп. И перераб. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2008. – 264 с.
65. Перегудов Ф.И. Основы системного анализа: учеб. – 2-е изд., доп. / Ф.И. Перегудов, Ф.П. Тарасенко. – Томск: НТЛ, 1997. – 396 с.

66. Анфилатов В.С. Системный анализ, в управлении: Учеб. Пособие / В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин; Под ред. А.А. Емельянова. – М.: Финансы и статистика, 2002. – 368 с.: ил.

67. Захарова А.А. Система поддержки принятия решений о стратегии инновационного развития региона: монография / А.А. Захарова; Юргинский технологический институт. – Томск: Изд-во Томского политехнического университета, 2011. – 144 с.

68. Маслов А.В., Григорьева А.А. Математическое моделирование в экономике и управлении: Учебное пособие – Юрга: Изд-во Юргинского технологического института (филиала) Томского политехнического университета, 2007. – 264 с.

69. Телипенко Е.В. Система поддержки принятия решений при управлении риском банкротства предприятия: автореф. дисс. канд. тех. наук: 05.13.10 – Новосибирск, 2013. – 24 с.

70. Reig G., Alonso J., Guitart J. (2010) Deadline constrained prediction of job resource requirements to manage high-level SLAs for SaaS cloud providers, Tech. Rep. UPC-DAC-RR, Dept. d'Arquitectura de Computadors, University Politècnica de Catalunya, Barcelona, Spain.

71. Wu, L., Kumar Garg, S., Buyya, R. (2012). SLA-based admission control for a Software-as-a-Service provider in Cloud computing environments. Journal of Computer and System Sciences, 78 (5), pp. 1280-1299.

72. Валентинова Т. Что в действительности представляют собой облачные сервисы // Wardwareportal.ru, 9.03.2009 [Электронный ресурс]. – Режим доступа: http://www.hwp.ru/articles/CHto_v_deystvitelnosti_predstavlyayut_soboy_oblachnie_servisi/ (дата обращения: 08.04.2013).

73. Москаленко А. Облачно и мобильно: что может спасти российский ИТ-рынок? // InLine group, 24.01.2013 [Электронный ресурс]. – Режим доступа: <http://www.inlinegroup.ru/events/press-releases/5635.php> (дата обращения: 08.04.2013).

74. Стандарты и руководства по использованию облачных вычислений.

75. Кулябов Д.С. учебно-методическое пособие по курсу «Защита информации в компьютерных сетях» Часть 1, г. Москва, 2004, с. 130 (стандарты информационной безопасности).

76. Методические рекомендации по оценке эффективности инвестиционных проектов (утв. Минэкономки РФ, Минфином РФ, Госстроем РФ 21.06.1999 N ВК 477).

77. Колесов А. Облачные вычисления: что же это такое? // PCWeek, 24.11.2011. [Электронный ресурс]. – Режим доступа: <http://www.pcweek.ru/its/article/detail.php?ID=135408>. Дата обращения: 24.11.12.

78. Razumnikov S., Prankevich D. Integrated model to assess cloud deployment effectiveness when developing an IT-strategy, Volume 127 (2016), Number 1, Tomsk – [Электронный ресурс]. – Режим доступа: <http://iopscience.iop.org/article/10.1088/1757-899X/127/1/012018> (дата обращения: 11.05.2016).

79. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решения на основе нечетких моделей. – Рига, 1990. – 180 с.

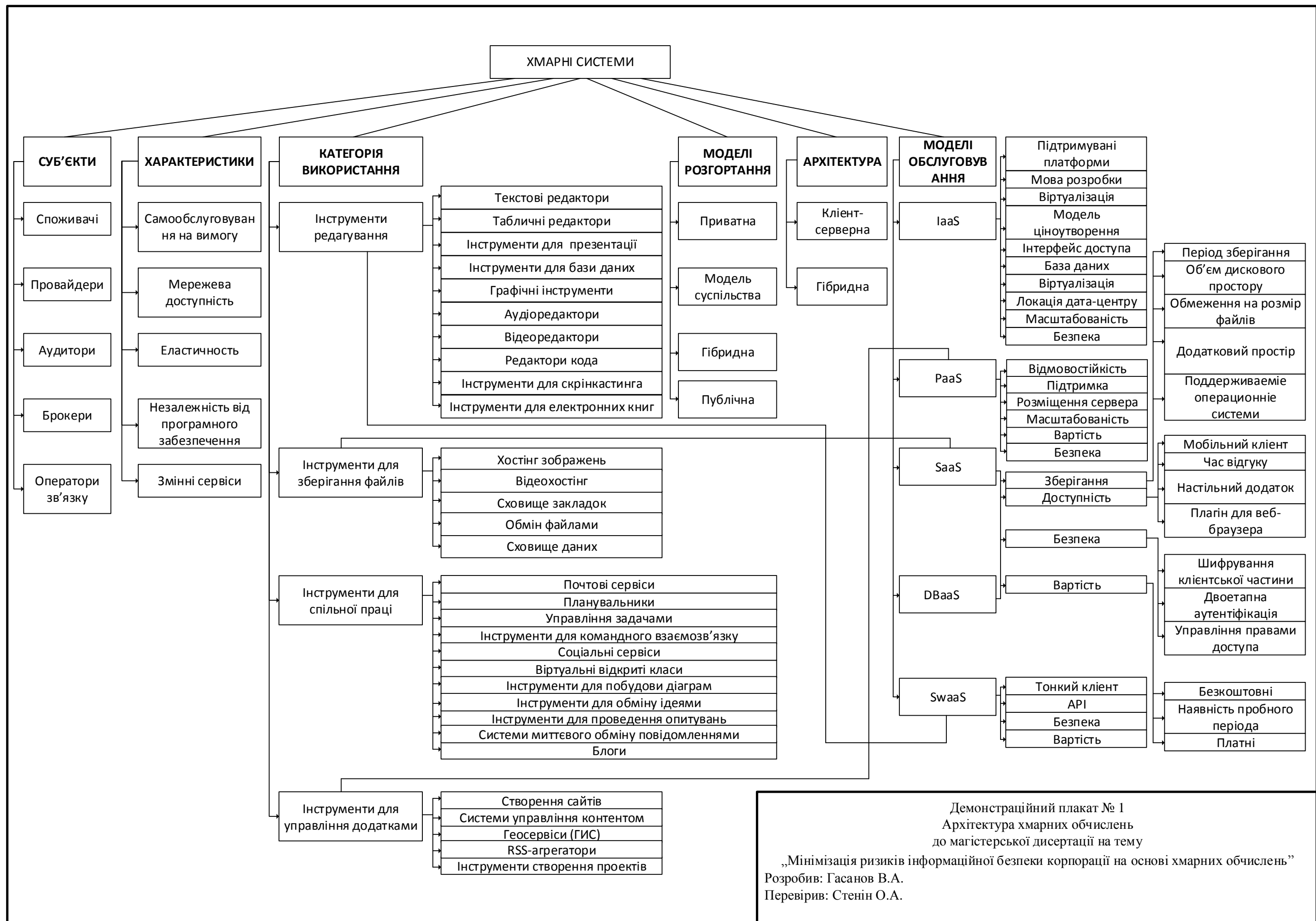
80. Разумников С.В., Захарова А.А., Кремнёва М.С. Экспертная оценка о возможности перехода корпоративных приложений в облачную среду // Инновационные технологии и экономика в машиностроении: сборник трудов V Международной научно-практической конференции: в 2 т., Юрга, 22-23 Мая 2014. - Томск: ТПУ, 2014 - Т. 2 - С. 69-74.

81. Пасько В.П., Гасанов В.А., Гришко А.С., Максимюк А.В. Інтероперабельність матриці прийняття рішення для оцінки ризиків інформаційної безпеки // Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління» № 2 (32), 2018

82. Пасько В.П., Гасанов В.А., Гришко А.С., Максимюк А.В. Декомпозиція методики оцінки ризиків інформаційної безпеки // XIV Международная научно-практическая конференция «Перспективные вопросы мировой науки – 2018» 15-22.12.2018, Болгария, София

ДОДАТКИ

ДОДАТОК А



Демонстраційний плакат № 1
 Архітектура хмарних обчислень
 до магістерської дисертації на тему
 „Мінімізація ризиків інформаційної безпеки корпорації на основі хмарних обчислень”
 Розробив: Гасанов В.А.
 Перевірив: Стенін О.А.

ДОДАТОК Б

СУБ'ЄКТИ ХМАРНИХ ОБЧИСЛЕНЬ

Споживачі

Провайдери

Оператори зв'язку

Брокери

Аудитори

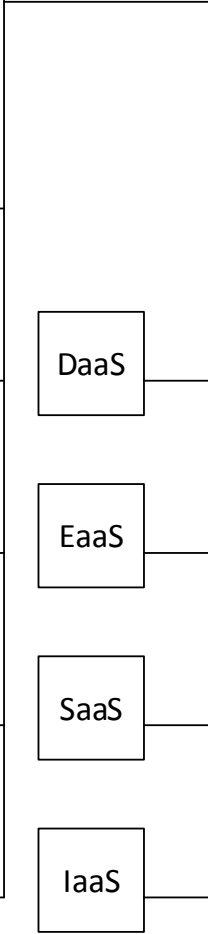
Caas

DSaaS

MaaS

Seaas

NaaS



DaaS

EaaS

SaaS

IaaS

Розгортання

Обслуговування

IdaaS

DbaaS

CompaaS

PaaS

Доступ

Розподіл

Споживання

Забезпечення

Безпека

Приватність

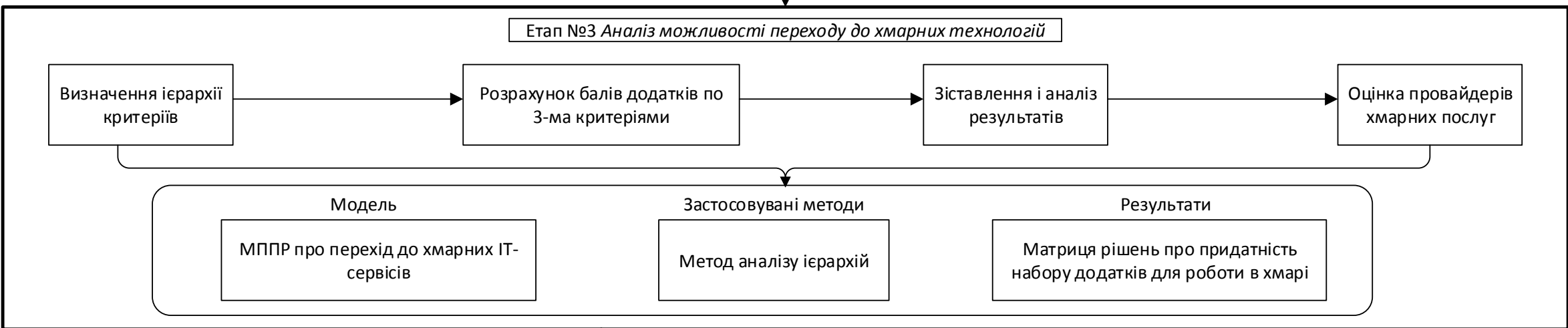
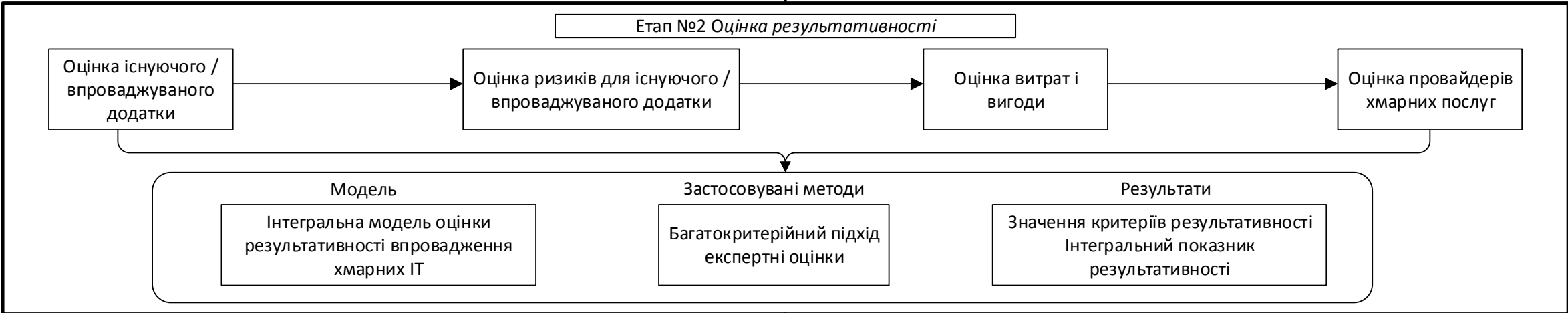
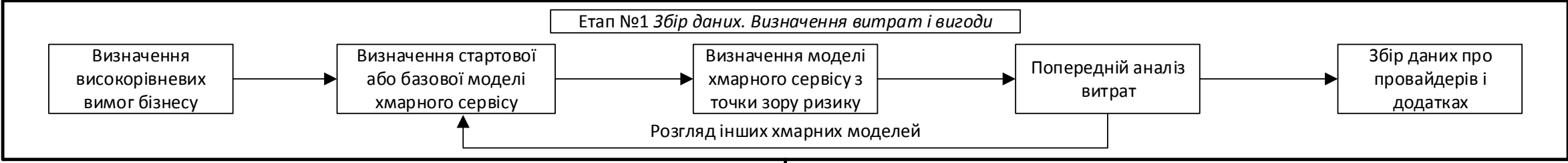
Виконання

Демонстраційний плакат № 2
Схема суб'єктів хмарних обчислень
до магістерської дисертації на тему
„Мінімізація ризиків інформаційної безпеки корпорації на основі хмарних обчислень”
Розробив: Гасанов В.А.
Перевірив: Стенін О.А.

ДОДАТОК В

ПОСТАНОВКА ПРОБЛЕМИ ВИБОРУ ХМАРНИХ ІТ-СЕРВІСІВ ДЛЯ ВПРОВАДЖЕННЯ В КОРПОРАЦІЮ

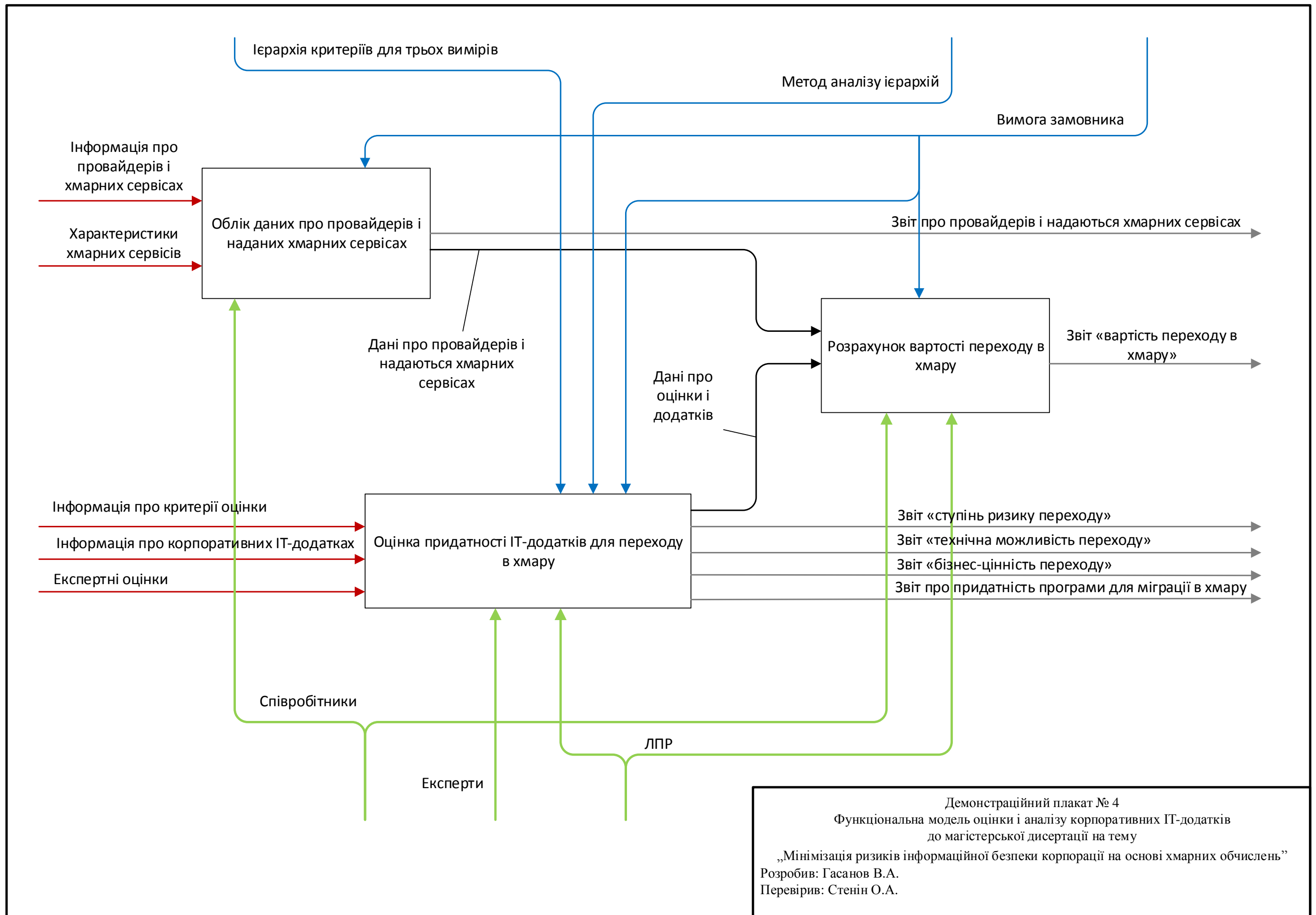
Етап №0
Формування експертної групи



УХВАЛЕННЯ РІШЕННЯ ПРО ВПРОВАДЖЕННЯ ХМАРНИХ ІТ-СЕРВІСІВ

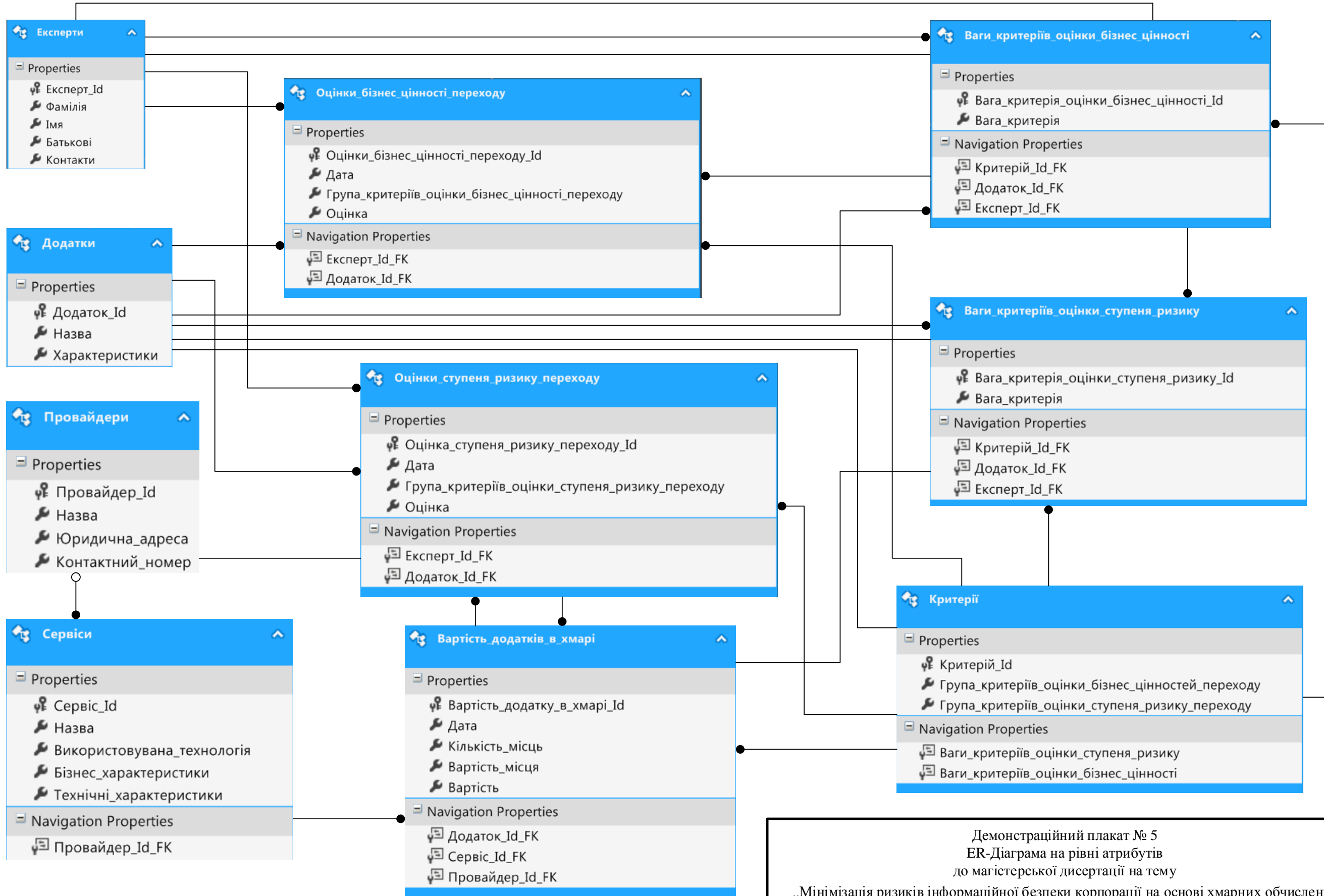
Демонстраційний плакат № 3
Методика підтримки прийняття рішень при виборі хмарних ІТ-сервісів для впровадження в корпорації
до магістерської дисертації на тему
„Мінімізація ризиків інформаційної безпеки корпорації на основі хмарних обчислень”
Розробив: Гасанов В.А.
Перевірив: Стенін О.А.

ДОДАТОК Г



Демонстраційний плакат № 4
 Функціональна модель оцінки і аналізу корпоративних ІТ-додатків до магістерської дисертації на тему
 „Мінімізація ризиків інформаційної безпеки корпорації на основі хмарних обчислень”
 Розробив: Гасанов В.А.
 Перевірив: Стенін О.А.

ДОДАТОК Д



Демонстраційний плакат № 5
 ER-Діаграма на рівні атрибутів
 до магістерської дисертації на тему
 „Мінімізація ризиків інформаційної безпеки корпорації на основі хмарних обчислень”
 Розробив: Гасанов В.А.
 Перевірив: Стенін О.А.

ДОДАТОК Е

Вхідні данні до хмарного середовища

Крок назад Наступний крок

▼ Модель розгортання хмарного середовища

▲ Модель обслуговування хмарного середовища

- Communications as a Service (CaaS) - Комунікація як Сервіс
- Compute as a Service (ComaaS) - Обчислення як Сервіс
- Data Storage as a Service (DSaaS) – Зберігання даних як сервіс
- Hardware as a Service (Haas) - Прибори як сервіс
- Infrastructure as a Service (IaaS) - Інфраструктура як сервіс
- Network as a Service (NaaS) - мережа як сервіс
- Platform as a Service (PaaS) - Платформа як сервіс
- Software as a Service (SaaS) - Програма як сервіс
- Database as a Service (DbaaS) – База даних як сервіс
- Workspace as a Service (WaaS) - Робоче оточення як сервіс
- Desktop as a Service (DaaS) - Комп'ютер (віртуальний робочий стіл) як сервіс
- Email as a Service (EaaS) - Електронна пошта як Служба
- Identity as a Service (IdaaS) - Ідентичність як сервіс
- Monitoring-as-a-Service (MaaS) - Моніторинг як Сервіс
- Security as a Service (SECaaS) - Безпека як сервіс

▼ Провайдер

▼ Фінансові витрати

Вхідні данні описуючі ІТ-інфраструктуру корпорації ССРА

Крок назад Наступний крок

▼ Наявність ЦОД

▲ Наявність БД

Ім'я БД: +

Ім'я БД:

Ім'я БД:

матриця вразливостей

Вразливості	Активи / витрати	Публічна інформація	Конфіденційна інформація	ІвОД	Репутація	Витрати на відновлення	Апаратні засоби	Програмне забезпечення	Обслуговування
Контингент студентів	4	6	5	7	7	7	7	6	6
Контингент працівників	4	6	5	7	7	7	7	6	6
База перепусток	3	5	4	6	6	6	6	5	5

матриця загроз

Вразливості	Загроза	Відмова в обслуговуванні	Шкідливий код	Помилки користувача	Внутрішні атаки	Спам	Фізичне пошкодження апаратних засобів	Апаратні засоби
Контингент студентів	4	4	5	5	6	5	5	5
Контингент працівників	4	4	5	5	6	5	5	5
База перепусток	4	4	5	5	6	5	5	5

▼ Перелік існуючих додатків

Результати

На головну Крок назад Звіти Зберегти

▲ Контингент студентів

▲ Контингент працівників

№ ризику	Ймовірність		Збиток	
	До	Після	До	Після
1	4	6	6	7
2	5	4	5	3
3	1	1	8	3
4	7	8	5	2
5	2	2	2	2
6	3	2	1	4
7	3	3	4	4
8	2	3	6	6

Збиток

Ймовірність

▼ База перепусток

Демонстраційний плакат № 6
 Візуальна репрезентація інформаційно-аналітичної системи
 до магістерської дисертації на тему
 „Мінімізація ризиків інформаційної безпеки корпорації на основі хмарних обчислень”
 Розробив: Гасанов В.А.
 Перевірив: Стенін О.А.