МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

МИКОЛАЙСЬКА Аліна Андріївна

Методика оцінки кіберризиків в хмарних сервісах / Methodology for Assessing Cyber Risks in Cloud Services

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -21
А. А. Миколайська

Науковий керівник
д.т.н., професор В. В.Яцків

Кваліфікаційну роботу
допущено до захисту:

«____» _____ ___2025 р.

Завідувач кафедри
_____ **В.В.Яцків**

ТЕРНОПІЛЬ - 2025

Факультет комп'ютерних інформаційних технологій

Кафедра кібербезпеки

Освітній ступінь «магістр»

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ В.В.Яцків

«____» _____ 2024 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

МИКОЛАЙСЬКА Аліна Андріївна

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:

Методика оцінки кіберризиків в хмарних сервісах / Methodology for Assessing Cyber Risks in Cloud Services

керівник роботи д.т.н., професор В.В. Яцків

затверджені наказом по університету від 20 грудня 2024 року № 938

2. Строк подання студентом закінченої кваліфікаційної роботи 5 грудня 2025 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:

– проаналізувати сучасний стан використання хмарних сервісів та класифікувати притаманні їм кіберризики;

- виконати огляд існуючих методик і стандартів оцінки інформаційних ризиків, виявити їхні обмеження щодо застосування в хмарному середовищі;
- обґрунтувати та сформувати систему основних критеріїв оцінки кіберризиків у хмарних сервісах;
- розробити гібридну модель та алгоритм оцінки кіберризиків, що поєднують якісні експертні оцінки з бальними кількісними шкалами;

– апробувати запропоновану методику на прикладі тестового проєкту у хмарній платформі Google Cloud Platform.

5. Перелік графічного матеріалу у роботі:

– архітектури хмарних сервісів SaaS/PaaS/IaaS;

– робочий процес ISO/IEC 27005 з управління ризиками;

– приклад розрахунку ризику для двох сценаріїв;
– приклад шкал для якісно-кількісної оцінки;
– головна консоль Google Cloud із вибраним тестовим проєктом;
– результати розрахунку ризиків для прикладу Google Cloud.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 29 листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз сучасного стану кіберризиків у хмарних сервісах	12.2024 р. – 03.2025 р.	
2	Розроблення моделі та методики оцінки кіберризиків у хмарних сервісах	03.2025 р. – 06.2025 р.	
3	Практичне впровадження розробленої методики	06.2025 р. – 11.2025 р.	

Студент _____ А. А. Миколайська
(підпис)

Керівник роботи _____ В.В. Яцків
(підпис)

АНОТАЦІЯ

Миколайська А. А. Методика оцінки кіберризиків в хмарних сервісах. – Рукопис.

Дослідження на здобуття освітнього ступеня «магістр» за спеціальністю 125 «Кібербезпека та захист інформації», освітньо-професійна програма «Кібербезпека». – Західноукраїнський національний університет, Тернопіль, 2025.

У роботі запропоновано гібридну модель оцінки ризику, у якій інтегральний показник обчислюється як добуток оціненої ймовірності та зваженого впливу за складовими CIA з використанням якісно-кількісних шкал. Розроблену методику апробовано на тестовому проєкті в хмарній платформі Google Cloud Platform, де для реалістичної архітектури веб-застосунку сформовано набір активів і сценаріїв загроз, виконано розрахунок і ранжування ризиків. Показано, що методика коректно виділяє найкритичніші сценарії (витік та несанкціонований доступ до даних), чутлива до зміни ваг критеріїв і впровадження захисних заходів, а також може бути інтегрована в процеси управління кібербезпекою організації.

Ключові слова: ХМАРНІ СЕРВІСИ, КІБЕРРИЗИКИ, ОЦІНКА РИЗИКІВ, ГІБРИДНА МОДЕЛЬ, GOOGLE CLOUD PLATFORM.

ANNOTATION

Mykolayska A.A. Methodology for Assessing Cyber Risks in Cloud Services. – Manuscript.

Thesis submitted for the degree of Master in specialty 125 “Cybersecurity and Information Protection”, educational and professional program “Cybersecurity”. – West Ukrainian National University, Ternopil, 2025.

A hybrid risk assessment model is proposed, in which the integral risk indicator is calculated as the product of the estimated probability and the weighted impact across the CIA components using qualitative–quantitative scales. The developed methodology was tested on a test project in the Google Cloud Platform, where a set of assets and threat scenarios was defined for a realistic web application architecture, and risk calculation and ranking were performed. It is shown that the methodology correctly identifies the most critical scenarios (data leakage and unauthorized data access), is sensitive to changes in criterion weights and the introduction of security measures, and can be integrated into an organization’s cybersecurity risk management processes.

Keywords: CLOUD SERVICES, CYBER RISKS, RISK ASSESSMENT, HYBRID MODEL, GOOGLE CLOUD PLATFORM.

ЗМІСТ

ВСТУП

Актуальність роботи. Масове впровадження хмарних сервісів у бізнес-процеси, державне управління та освітню сферу супроводжується різким зростанням кількості кіберінцидентів, пов’язаних із витоком даних, помилками конфігурацій, зловживанням привілеями та атаками на доступність сервісів. Особливості хмарного середовища – мультиорендність, географічно розподілена інфраструктура, модель спільної відповідальності між провайдером і користувачем, широке використання API та автоматизації – формують новий профіль кіберризиків, який не може бути повністю охоплений традиційними підходами до захисту класичних дата-центрів. Існуючі стандарти та рамки управління інформаційними ризиками (ISO/IEC 27005, NIST, ENISA тощо) здебільшого мають загальний характер і вимагають адаптації до специфіки хмарних сервісів, а на практиці організації часто покладаються на фрагментарні або суто якісні оцінки, що ускладнює обґрунтування рішень щодо безпеки. Тому розроблення цілісної методики оцінки кіберризиків у хмарних сервісах, яка поєднує якісні й кількісні підходи й враховує технічні та організаційні особливості сучасних хмарних платформ, є актуальним науковим і прикладним завданням.

Мета і завдання дослідження. Метою роботи є розроблення методики оцінки кіберризиків у хмарних сервісах на основі гібридної моделі, що поєднує якісні та кількісні методи.

Досягнення визначеної мети передбачає вирішення таких завдань:

– проаналізувати сучасний стан використання хмарних сервісів та класифікувати притаманні їм кіберризики;

- виконати огляд існуючих методик і стандартів оцінки інформаційних ризиків, виявити їхні обмеження щодо застосування в хмарному середовищі;

- обґрунтувати та сформувати систему основних критеріїв оцінки кіберризиків у хмарних сервісах;

- розробити гібридну модель та алгоритм оцінки кіберризиків, що поєднують якісні експертні оцінки з бальними кількісними шкалами;
- апробувати запропоновану методику на прикладі тестового проєкту у хмарній платформі Google Cloud Platform.

Об'єкт дослідження – процес управління кіберризиками в інформаційних системах, що функціонують на базі хмарних сервісів.

Предмет дослідження – гібридна модель кількісно-якісної оцінки кіберризиків у хмарних сервісах з урахуванням їх технічних і організаційних особливостей.

Методи досліджень. Методи класифікації кіберризиків, математичне моделювання та вагове оцінювання критеріїв, експертне оцінювання для побудови якісно-кількісних шкал, а також моделювання й експеримент у тестовому проєкті на платформі Google Cloud Platform.

Наукова новизна одержаних результатів Розроблено гібридну методику оцінки кіберризиків у хмарних сервісах, яка інтегрує критерії CIA, хмарні специфічні та організаційні фактори в єдину зважену модель ризику, адаптовану до архітектури публічних хмарних платформ.

Практичне значення отриманих результатів. Розроблену методику можна використати для побудови та вдосконалення системи управління кіберризиками в організаціях, які застосовують хмарні сервіси, а також у навчальному процесі при підготовці фахівців з кібербезпеки.

Публікації та апробація КР.

1. Яцків Н., Миколайська А. Класифікація кіберризиків у хмарних сервісах. Збірник матеріалів науково-практичного симпозіуму «Технології Інтернету речей: системи та рішення» (TIP:CT - 2025), Тернопіль, 2025. - С.37-40.

2. Яцків Н., Миколайська А. Модель оцінки кіберризиків у хмарних сервісах. Матеріали науково-практичного симпозіуму "Захист інформації'2025", Тернопіль, 2025. – С. 115-118.

1. АНАЛІЗ СУЧАСНОГО СТАНУ КІБЕРРИЗИКІВ У ХМАРНИХ СЕРВІСАХ

1.1. Загальна характеристика хмарних сервісів та їх переваг

Сучасні хмарні технології розглядаються як модель надання обчислювальних ресурсів (мережа, сервери, сховища, сервіси, застосунки) за запитом користувача через мережу з можливістю швидкого масштабування й вивільнення ресурсів. Класичне визначення, запропоноване NIST SP 800-145, описує хмару через п’ять базових характеристик (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), три моделі сервісів (IaaS, PaaS, SaaS) та чотири моделі розгортання (public, private, community, hybrid) [1]. Саме ця триєдина схема сьогодні використовується більшістю міжнародних стандартів і рекомендацій (CSA, ENISA) як базова точка відліку для опису хмарних сервісів [2].

ENISA, аналізуючи ризики та переваги хмарних обчислень для організацій, підкреслює, що хмара – не просто «оренда серверів», а цілісна сервісна модель з новою економікою (OPEX замість CAPEX) та зміненою моделлю відповідальності між постачальником і споживачем [3]. Це обумовлює необхідність розуміти не лише технічні аспекти хмар, а також їх архітектуру, моделі розгортання та вплив на управління IT-інфраструктурою в цілому.

1.1.1. Визначення та моделі розгортання

Згідно з NIST, хмарні обчислення – це модель, що забезпечує зручний доступ за запитом до спільного пулу конфігурованих обчислювальних ресурсів, які можуть бути швидко надані та звільнені з мінімальними зусиллями з боку керування або взаємодії з постачальником. У рамках цієї моделі розрізняють три сервісні моделі [4]:

- IaaS (Infrastructure as a Service) – надання віртуалізованих обчислювальних ресурсів (VM, сховища, мережі);
- PaaS (Platform as a Service – платформи для розробки й розгортання застосунків без управління базовою інфраструктурою;

- SaaS (Software as a Service) – готові прикладні сервіси, доступні через мережу для кінцевих користувачів [5].

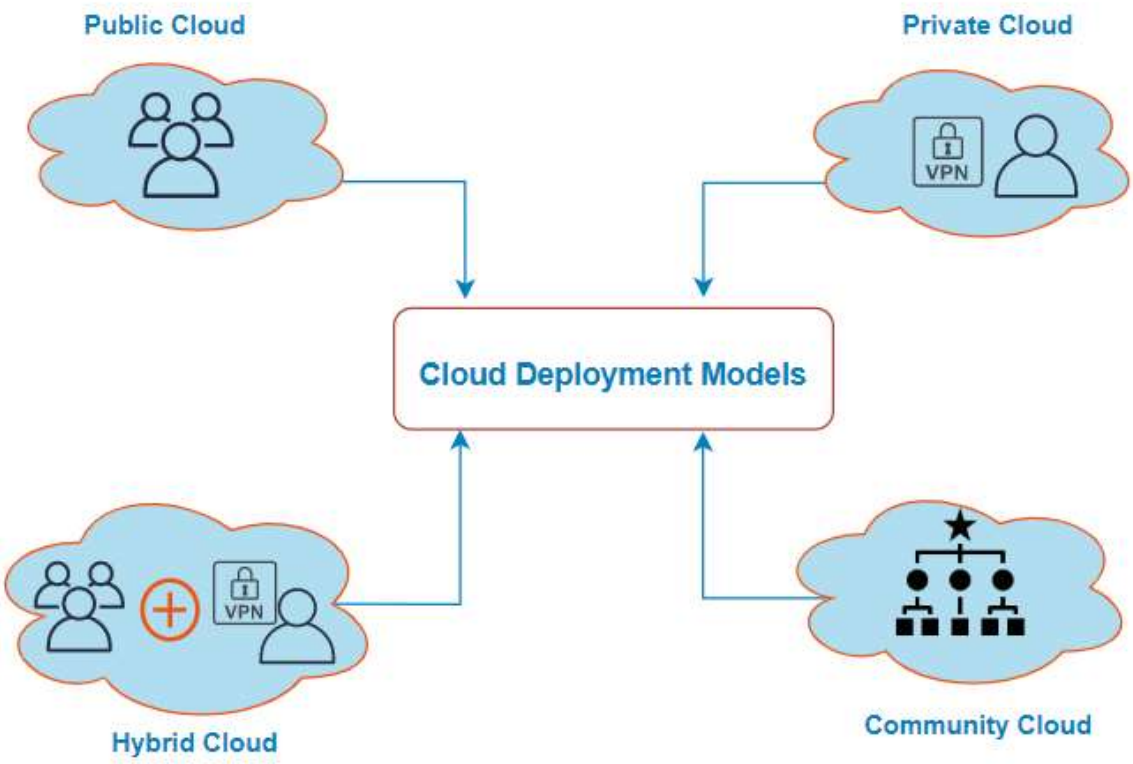

Рисунок 1.1 – Схема моделей розгортання хмарних обчислень [3]

NIST визначає чотири основні моделі розгортання: публічна хмара (public cloud), приватна (private), спільнотна (community) та гібридна (hybrid). У публічній хмарі інфраструктура належить провайдеру й використовується багатьма орендарями; приватна хмара обслуговує одну організацію; спільнотна – групу організацій зі схожими вимогами (наприклад, державні відомства); гібридна комбінує два чи більше середовища з уніфікованим управлінням і перенесенням навантаження. Вибір моделі розгортання визначається вимогами до безпеки, регуляторними обмеженнями, бюджетом та поточним IT-ландшафтом [5].

1.1.2. Основні архітектурні риси

Однією з базових архітектурних рис хмар є ресурсний пулінг та багатокористувацькість (multi-tenancy): фізичні ресурси агрегуються в спільні

пули, які динамічно розподіляються між багатьма споживачами за допомогою віртуалізації та оркестрації. Це забезпечує високе завантаження інфраструктури та гнучкий розподіл навантаження, але вимагає додаткових механізмів ізоляції даних і безпеки між «орендарями». Другою критичною рисою є швидка еластичність – можливість автоматичного масштабування ресурсів відповідно до поточних потреб (auto-scaling), що реалізується через API-керування ресурсами та системи моніторингу [6].

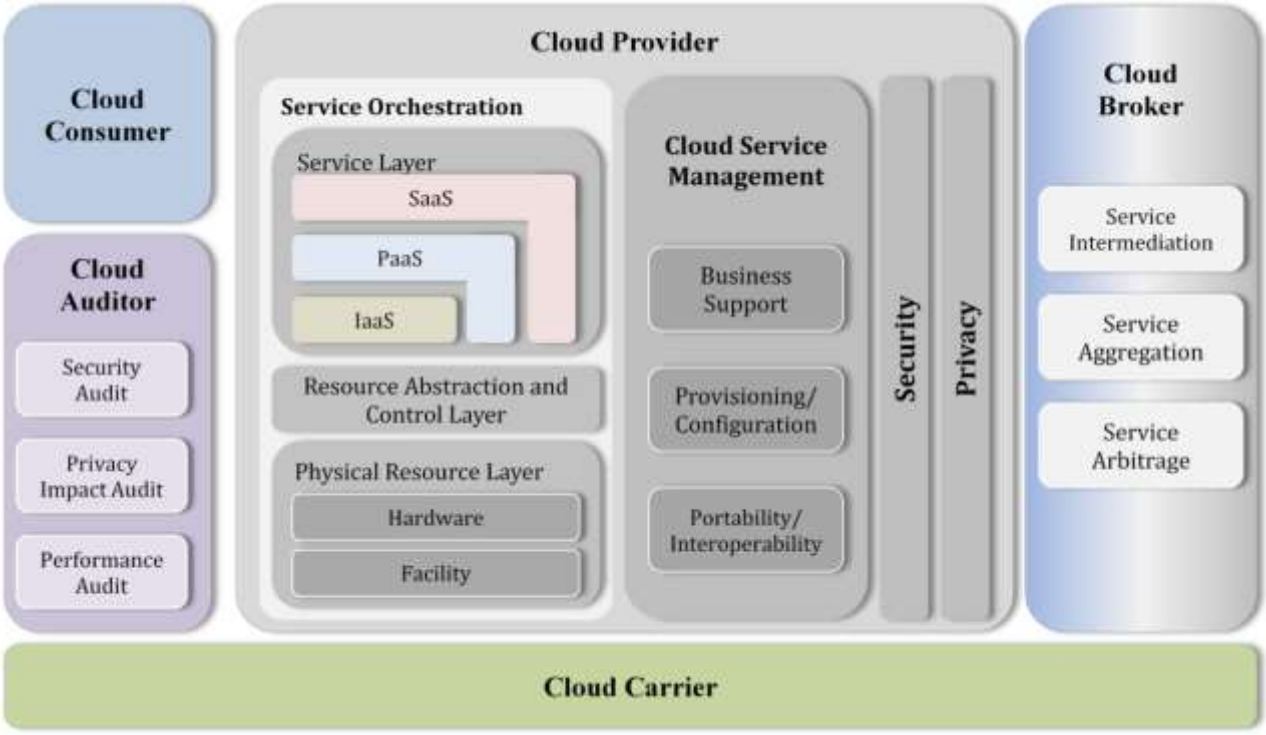

Рисунок 1.2 – Концептуальна референтна архітектура хмарних обчислень від NIST [6]

NIST Cloud Computing Reference Architecture виділяє п’ять ключових акторів (cloud provider, consumer, broker, auditor, carrier) та показує багатошарову структуру хмари: від фізичної інфраструктури й шару абстракції ресурсів до сервісного шару (SaaS/PaaS/IaaS) і керівних функцій (управління сервісами, безпека, портативність, взаємодія) [6]. Хмарні системи зазвичай будуються як API-орієнтовані платформи, де всі операції (створення VM, налаштування мережі, розгортання застосунків) автоматизуються інфраструктурним кодом (IaC) та інтегруються в CI/CD-процеси. Cloud Security Alliance додатково підкреслює важливість «метаструктури» – керувальної

площини, яка забезпечує централізоване керування, моніторинг і політики безпеки для всіх шарів хмарної архітектури [2].

1.1.3. Основні переваги для організацій

Головні переваги хмар для організацій традиційно пов’язані з гнучкістю та економією витрат. Модель «оплата по мірі використання» дозволяє уникнути великих капітальних витрат (CAPEX) на закупівлю серверів та ліцензій, замінюючи їх операційними витратами (OPEX) за фактичне використання ресурсів. ENISA відзначає, що концентрація ресурсів у хмарі дозволяє будувати масштабовані й економічно ефективні рішення, які важко реалізувати у традиційних дата-центрах невеликих організацій [3].

Другий блок переваг стосується швидкості впровадження та інновацій. Готові PaaS- та SaaS-сервіси, глобальна мережа дата-центрів і можливість автоматичного масштабування дають змогу значно скоротити час «від ідеї до прототипу» та до промислової експлуатації, що критично для сучасних цифрових продуктів (рис.1.3).

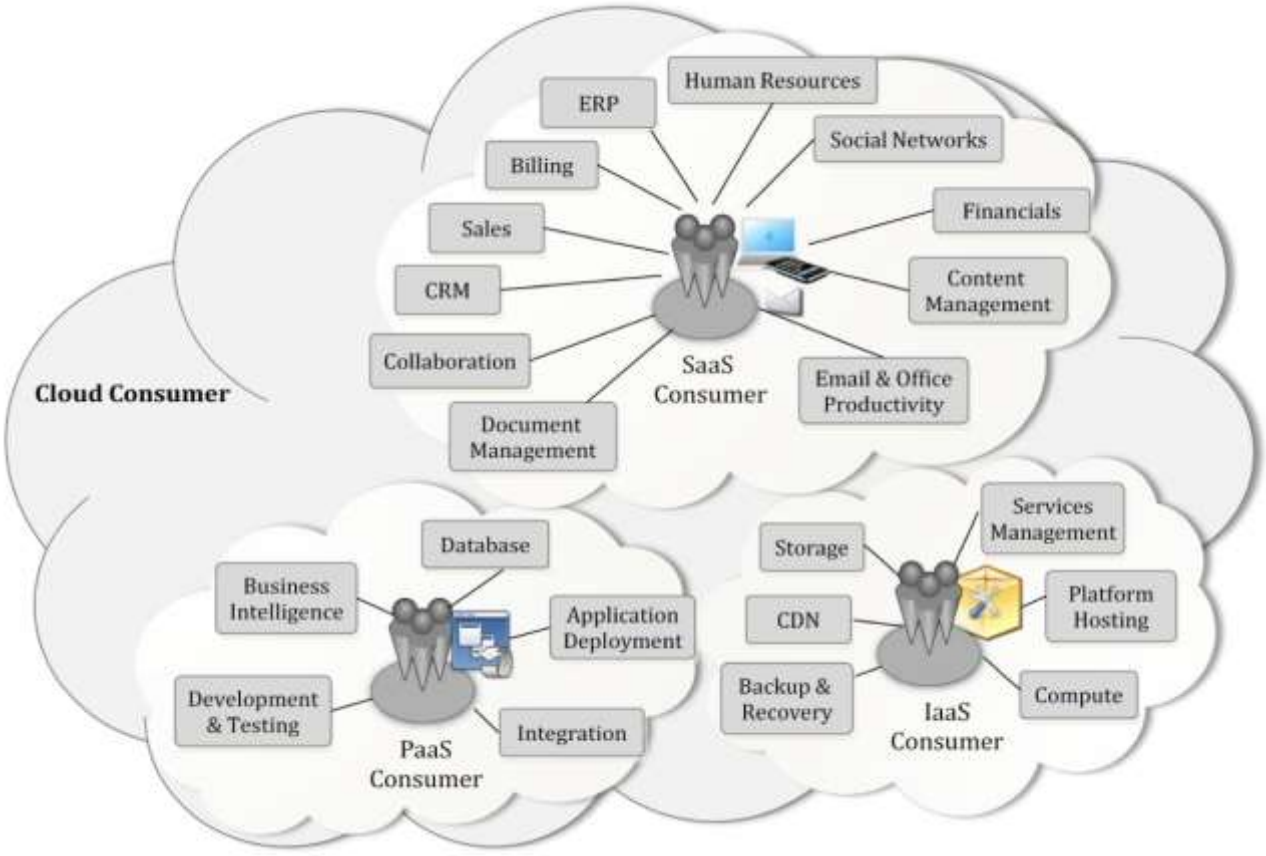

Рисунок 1.3 – Приклад архітектури хмарних сервісів SaaS/PaaS/IaaS [6]

CSA у своїй «Security Guidance» прямо вказує, що коректне використання хмарно-нативних сервісів (контейнери, serverless, керовані бази даних) підвищує не лише гнучкість, а й базовий рівень безпеки за рахунок стандартних оновлень, централізованих механізмів IAM, шифрування та журналювання [2].

Третя важлива група переваг пов’язана з надійністю та стійкістю: великі хмарні провайдери пропонують вбудовані механізми резервування, географічного розподілу навантаження та аварійного відновлення, які складно або занадто дорого відтворити на власній інфраструктурі. Дослідження NIST і ENISA підкреслюють, що за умови правильної архітектури хмара дозволяє покращити показники доступності, бізнес-безперервності та кіберстійкості, хоча й вимагає переосмислення підходів до управління ризиками та безпекою [6].

1.2. Класифікація кіберризиків у хмарних технологіях

Кіберризики у хмарних середовищах зазвичай систематизують навколо класичної тріади конфіденційність – цілісність – доступність (CIA), а також окремо виділяють архітектурні, управлінські та організаційні аспекти, які посилюються через модель спільної відповідальності між постачальником та споживачем хмарних послуг. ENISA, NIST та Cloud Security Alliance (CSA) у своїх доповідях підкреслюють, що саме порушення конфіденційності, помилки конфігурації, слабке управління доступом та недостатня архітектурна зрілість є серед домінуючих причин інцидентів у хмарі [6].

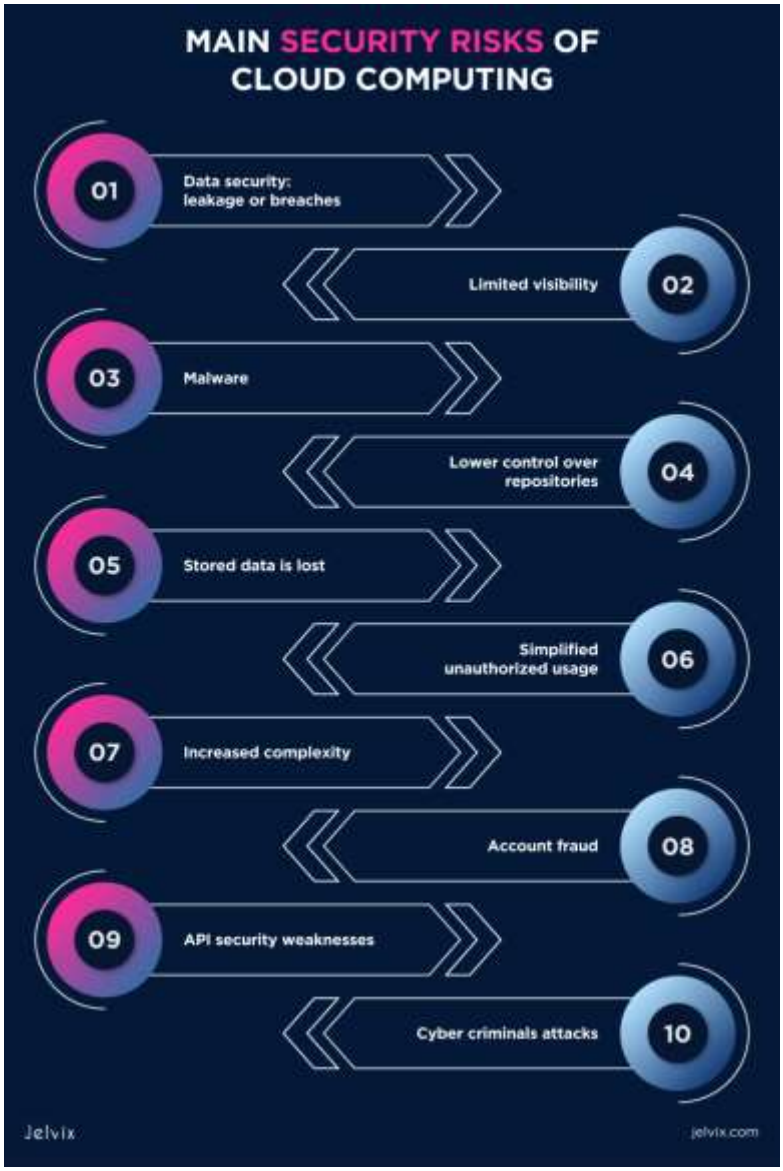

Рисунок 1.4 – Основні області ризиків хмарної безпеки [8]

Нижче наведено класифікацію основних груп кіберризиків у хмарних технологіях, релевантну для оцінки безпеки як публічних, так і приватних/гібридних хмар: ризики конфіденційності та витоку даних, доступності сервісів, цілісності та маніпуляцій даними, архітектурні й управлінські ризики, ризики у сфері ідентифікації та управління доступом (IAM), а також ризики, пов’язані з конфігураціями та помилками адміністраторів. Така структура узгоджується з підходами ENISA до оцінювання ризиків і сучасними оглядами загроз до хмарних обчислень [6].

1.2.1. Ризики, пов’язані з конфіденційністю та витоком даних

Порушення конфіденційності є одним із найкритичніших ризиків хмарних технологій і стабільно очолює рейтинги загроз CSA. До цієї групи належать несанкціонований доступ до даних у сховищах, перехоплення трафіку між сервісами, витоки резервних копій та журналів, а також побічне розкриття даних у багатокористувацьких середовищах. Причинами виступають слабка або відсутня криптографія, неправильно налаштовані списки контролю доступу до storage-сервісів, недостатній контроль над ключами шифрування, компрометація облікових записів адміністраторів, використання небезпечних API чи сторонніх сервісів.

Наслідки витоку даних у хмарі включають фінансові втрати, штрафи за порушення регуляцій (GDPR, HIPAA тощо), репутаційні збитки та втрату довіри до постачальника/організації. NIST SP 800-144 окремо наголошує, що при аутсорсингу даних до публічної хмари необхідно враховувати як технічні загрози (компрометація інфраструктури CSP, вразливі механізми ізоляції), так і організаційні – наприклад, доступ персоналу постачальника, юрисдикцію зберігання даних, можливість запитів правоохоронних органів.

Мінімізація цих ризиків базується на застосуванні наскрізного шифрування даних у стані спокою та у процесі передавання, використанні керованих сервісів управління ключами (KMS/HSM), сегментації даних, а також впровадженні політик Data Loss Prevention (DLP) та класифікації даних. ENISA рекомендує будувати моделі загроз для критичних наборів даних та періодично проводити оцінку ризиків з урахуванням розвитку хмарної інфраструктури.

1.2.2. Ризики доступності

Доступність у хмарі залежить як від надійності інфраструктури постачальника, так і від коректності архітектури рішень клієнта. До ризиків цієї групи належать відмови дата-центрів та регіонів, збої мережевої інфраструктури, помилки у механізмах балансування навантаження та авто-масштабування, DDoS-атаки на публічні інтерфейси, а також додаткові

затримки/втрати продуктивності, спричинені перевантаженням ресурсів. ENISA і CISA у своїх референс-архітектурах підкреслюють, що хмарна модель не гарантує абсолютної доступності: користувач має самостійно будувати надлишковість [9].

Особливий ризик полягає в тому, що одна точка відмови (наприклад, помилка в центральному сервісі авторизації чи DNS-конфігурації) може зупинити одразу багато хмарних застосунків. Також під час міграції до хмари організації часто недооцінюють вплив змін на існуючі бізнес-процеси, SLA з клієнтами, RTO/RPO, що призводить до невідповідності фактичної доступності очікуваному рівню.

Зниження ризиків доступності включає проєктування стійкої архітектури (fault-tolerant design), автоматизацію резервного копіювання, регулярне тестування сценаріїв відновлення (disaster recovery drills), використання послуг захисту від DDoS, а також чітку фіксацію вимог до доступності в договорах (SLA/OLA) з постачальником. NIST та CISA рекомендують інтегрувати забезпечення доступності в загальну рамку управління ризиками й zero-trust-архітектуру, а не розглядати його як окремий технічний параметр [10].

1.2.3. Ризики цілісності та маніпуляцій даними

Ризики порушення цілісності в хмарі стосуються як даних (бази даних, об’єктне сховище, резервні копії), так і конфігурацій, журналів, контейнерних образів, артефактів CI/CD. Вони включають несанкціоноване або непомітне модифікування інформації, ін’єкційні атаки на рівні застосунку/API, компрометацію комунікацій розгортання, внесення змін до політик безпеки чи IAM-ролей, а також маніпуляції журналами аудитів з метою приховування слідів атак. Наукові огляди ризиків хмарних інфраструктур прямо класифікують загрози за впливом на цілісність – від помилкових транзакцій до повної компрометації репозиторіїв коду [11].

Особливістю хмари є високий рівень автоматизації (IaC, CI/CD, autoscaling), що робить будь-яку помилку або компрометацію на одному з етапів потенційно масштабованою на сотні й тисячі інстансів. Ін’єкція

шкідливого коду в контейнерний образ або змога змінювати параметри середовища (environment variables, secrets) фактично дає зловмиснику контроль над поведінкою сервісів. Якщо при цьому не впроваджено суворий контроль версій, підписування артефактів і захист журналів, виявлення і доведення факту маніпуляцій стає нетривіальним [12].

Для мінімізації цих ризиків застосовують криптографічні механізми контролю цілісності (MAC, цифрові підписи для даних і образів), версіонування та незмінні сховища (WORM-storage), контроль цілісності журналів (append-only, remote logging), а також практики secure DevOps (DevSecOps): обов'язковий code review, підписування контейнерних образів, політики «only signed images», сегрегація робочих та привілейованих облікових записів у CI/CD-ланцюзі. Рекомендації NIST і ENISA з безпечної розробки та експлуатації хмарних сервісів прямо включають контроль цілісності як окремий клас заходів [13].

1.2.4. Архітектурні та управлінські ризики

Архітектурні та управлінські ризики пов'язані з тим, що хмарні рішення будується поверх багаторівневої ланцюга поставок (supply chain): базова інфраструктура CSP, керовані сервіси, PaaS-компоненти, сторонні SaaS-сервіси, бібліотеки з відкритим кодом, інтеграції з партнерами, підрядниками тощо. CSA у звітах «Top Threats» окремо виділяє «відсутність архітектури та стратегії хмарної безпеки» та «зловживання та неправомірне використання хмарних сервісів», підкреслюючи, що відсутність цілісної архітектури та неконтрольоване використання third-party-сервісів різко збільшує поверхню атаки.

До цієї групи відносять ризики, пов'язані з помилковим трактуванням моделі спільної відповідальності, відсутністю єдиної стратегії безпеки для multi-cloud / hybrid-cloud, обмеженою видимістю щодо активів і потоків даних, юрисдикційними питаннями (де фізично зберігаються дані і хто має до них доступ), а також залежністю від конкретного постачальника (vendor lock-in). Окрему загрозу становлять компрометації на рівні supply chain –

скомпрометовані бібліотеки, небезпечні оновлення third-party, уразливі керовані сервіси постачальника [14.

Зменшити ці ризики можна через формалізовані процеси управління постачальниками й третіми сторонами: проведення попередньої оцінки, використання рамок ENISA/NIST/CSA, вимоги до відповідності стандартам (ISO/IEC 27001, ISO/IEC 27017, SOC 2, CSA STAR), регулярні аудити й тестування безпеки, чітко прописані SLA й розподіл ролей у договорах. CISA у Cloud Security Technical Reference Architecture наголошує також на необхідності централізованої моделі управління безпекою для всіх хмарних провайдерів та сервісів [12].

1.2.5. Ідентифікація, автентифікація та доступ

Недостатній контроль ідентичностей, облікових даних та доступу входить до топ-загроз CSA і є одним з головних факторів, що призводять до компрометацій хмарних середовищ. Типові проблеми: відсутність або вибіркове застосування багатофакторної автентифікації, надмірні привілеї, використання спільних облікових записів та довгоживучих ключів доступу, погана сегрегація обов'язків (SoD), несвоєчасне відкликання доступу співробітників, які звільнились чи змінили роль.

У хмарній моделі IAM стає центральним контрольним механізмом, що визначає, хто може робити що, де і звідки. NIST Cloud Computing Security Reference Architecture прямо вказує на те, що управління ідентичністю й доступом має бути інтегроване на рівні архітектури, включно з федерацією ідентичностей, єдиним входом (SSO), делегуванням авторизації між сервісами. Помилки в IAM-конфігураціях (наприклад, роль, яка дозволяє повний доступ до усіх контеєрів або керування ключами шифрування) нерідко призводять до повного захоплення середовища атакувальником.

Зниження цих ризиків передбачає побудову моделі найменші привілеї та *нульова довіра*: обмеження прав до мінімально необхідних, використання ролей замість статичних ключів, обов'язкова MFA для адміністративних і високоризикових операцій, періодичні перегляди доступів, захист

привілейованих облікових записів (PAM), а також моніторинг аномальної автентифікації та операцій (аналітика поведінки). Методи й рекомендації з IAM детально описані в документах NIST і CSA як ключова складова хмарної безпеки.

1.2.6. Ризики пов’язані з конфігураціями та помилками адміністраторів

Масштабованість і гнучкість хмар тісно пов’язані зі складністю конфігурацій. Сучасні дослідження показують, що помилки конфігурації (misconfigurations) є провідною причиною інцидентів безпеки у хмарних середовищах: відкриті сховища, відсутність шифрування, неправильно налаштовані security-groups / firewall-правила, доступ «0.0.0.0/0» до адмін-інтерфейсів, експоновані секрети в репозиторіях коду тощо. CSA відносить «Неправильна конфігурація та недостатній контроль змін» до топ-загроз, а низка аналітичних звітів стверджує, що більшість зламів у хмарі прямо або опосередковано пов’язана з конфігураційними помилками.

Фактор людської помилки посилюється використанням multi-cloud, високим темпом змін (безперервна доставка), ручним налаштуванням через консолі провайдерів, відсутністю єдиних шаблонів та стандартів. З іншого боку, адміністратори часто перебувають під тиском бізнес-вимог до швидкого розгортання сервісів, що призводить до компромісів на користь зручності (наприклад, тимчасово відкрити доступ для усіх – і «забути» закрити) [15].

Зменшення цих ризиків базується на переході до інфраструктура-як-код (infrastructure-as-code, IaC) та безпека як код (security-as-code): усі зміни в інфраструктурі фіксуються в коді (Terraform, CloudFormation тощо), проходять перевірке коду, автоматичний аналіз на відповідність політикам безпеки та тестування. Додатково застосовуються інструменти класу CSPM/CNAPP для безперервного виявлення небезпечних конфігурацій, централізоване управління політиками, формалізовані процеси управління змінами та регулярні тренінги для адміністраторів щодо типових помилок у хмарних середовищах. Рекомендації щодо цього підходу системно представлені у CISA Cloud Security Technical Reference Architecture та керівництвах CSA [16].

1.3. Огляд сучасних методик оцінки ризиків

Сучасні підходи до оцінки кіберризиків спираються на стандартизовані рамки (NIST, ISO, ENISA), які задають процес: від ідентифікації активів та загроз до вибору варіантів обробки ризику. NIST SP 800-30 та ISO/IEC 27005 розглядають оцінку ризиків як частину загального циклу управління ризиком, а не як одноразову задачу [17].

У хмарному контексті до цього додаються спеціалізовані методики ENISA, європейських регуляторів (CNIL) і Cloud Security Alliance, а також інструменти для безперервної оцінки стану безпеки (CSPM/CNAPP, вбудовані сервіси AWS/Azure/GCP).

1.3.1. Стандартні підходи та рамки

До базових міжнародних стандартів управління ризиками належать ISO/IEC 27005 (інформаційна безпека), ISO 31000 (загальне управління ризиками) та NIST SP 800-30 / 800-39 для IT-та кіберризиків. ISO/IEC 27005 дає процес: встановлення контексту, ідентифікація, аналіз, оцінювання, обробка, моніторинг і комунікація ризиків у рамках ISMS за ISO/IEC 27001. NIST SP 800-30 зосереджений на методиці проведення оцінки ризиків: моделі ризику, вибір підходу (кількісний/якісний), опис кроків оцінки загроз, вразливостей, ймовірності та впливу [18].

ENISA дає огляд різних risk-management – стандартів і пропонує узагальнену схему процесу, що узгоджується з ISO 27005 (контекст → оцінка → обробка → моніторинг) [11]. У сфері кібербезпеки також використовують методології OCTAVE, TARA, COBIT-орієнтовані підходи, які структурують аналіз активів, загроз та вразливостей і часто комбінують з ISO/NIST [9].

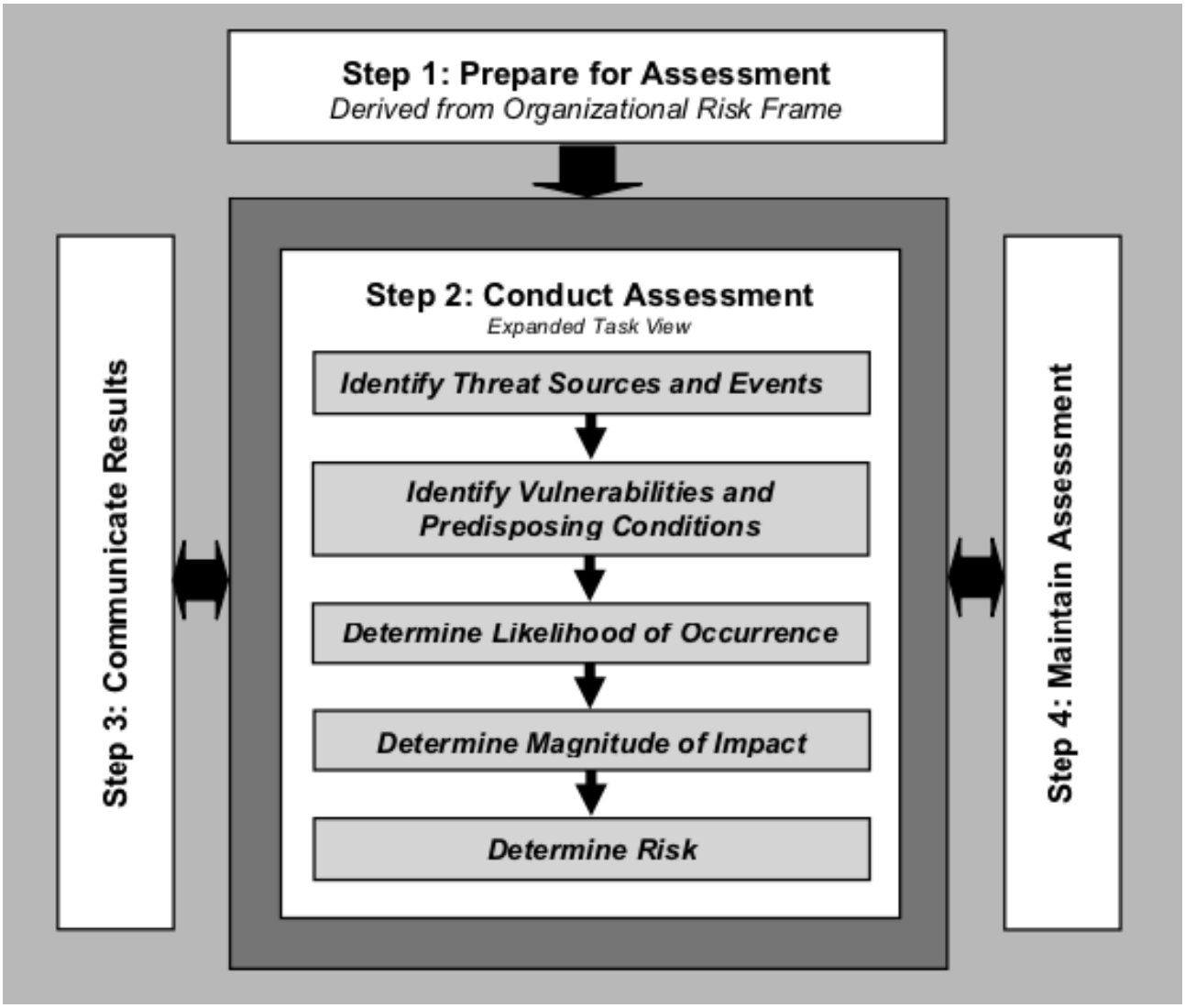

Рисунок 1.5 – Процес оцінки ризиків за NIST SP 800-30 [7]

1.3.2. Кількісні та якісні методи

Якісні методи домінують у більшості організацій, оскільки прості в застосуванні й добре інтегруються зі стандартами ISO/IEC 27005 та NIST SP 800-30. Ризики оцінюють за матрицею «ймовірність × вплив» із використанням шкал 3–5 рівнів, часто з додатковими критеріями (вплив на конфіденційність, цілісність, доступність окремо). Плюс – зрозумілість для менеджменту; мінус – суб’єктивність і складність порівняння ризиків між підрозділами або у грошовому вимірі.

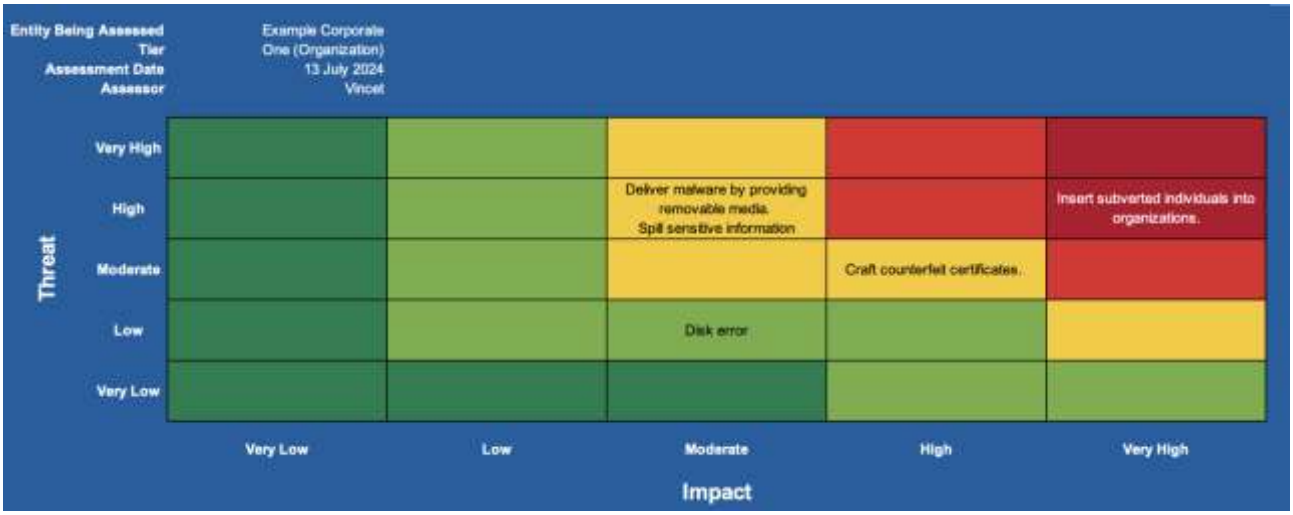

Рисунок 1.6 – Приклад ризик-матриці (імовірність × вплив) [8]

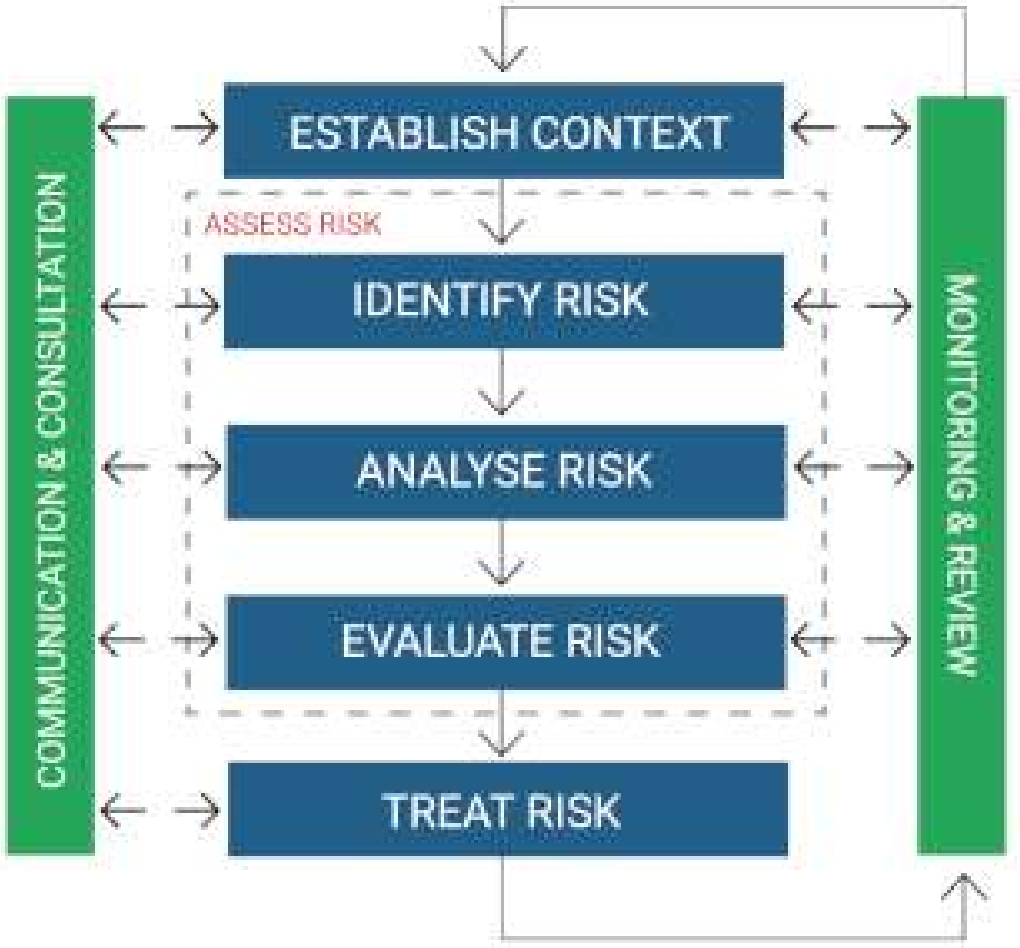

Рисунок 1.7 – Робочий процес ISO/IEC 27005 з управління ризиками

Кількісні методи, такі як: ALE, Monte Carlo, FAIR прагнуть перевести ризик у фінансові показники: очікуваний річний збиток, розподіли можливих

втрат, інтервали довіри. FAIR (Factor Analysis of Information Risk) є де-факто стандартом для кількісного аналізу кіберризиків, який описує частоту подій та величину збитку й дозволяє обраховувати ризик у грошах. На базі FAIR працюють платформи RiskLens та інші CRQ-рішення, що автоматизують моделювання та репорти для С-рівня.

Практично, більшість організацій комбінує обидва підходи: на рівні каталогу ризиків використовуються якісні матриці, а для критичних сценаріїв (cloud outage, витік великого масиву даних, компрометація хмарного провайдера) застосовують кількісні моделі (FAIR, ALE, Monte Carlo). Окремі статті та кейси демонструють, як переводити ISO/NIST-ризики в кількісні моделі, щоб обґрунтувати інвестиції в безпеку [14].

1.3.3. Спеціалізовані методики для хмарних сервісів

Для хмарних середовищ класичні ISO/NIST-підходи доповнюються галузевими методиками. ENISA у своєму «Cloud Computing Security Risk Assessment» пропонує специфічний для хмари каталог загроз і методику оцінки: для кожної події аналізуються ймовірність, вплив, рівень ризику та рекомендовані контрзаходи. Окремі дослідження пропонують моделі оцінки ризиків при виборі cloud-провайдера, де враховують юрисдикцію, сертифікації, технічні та організаційні контролі [19].

Регулятори на кшталт французької CNIL публікують власні методики оцінки приватності в хмарі, зосереджені на ризиках для персональних даних. Також широко застосовуються артефакти Cloud Security Alliance: CAIQ (опитувальник для провайдера) і CCM Cloud Controls Matrix), які дозволяють зіставити ризики та контролі в хмарі із вимогами ISO 27001, NIST, PCI DSS тощо [11]. Фактично, для хмарних сервісів стандартною практикою є: базова методика ISO 27005 / NIST 800-30 + спеціалізований cloud-каталог ризиків (ENISA/CSA) + окремий аналіз підрядників та ланцюга постачання.

1.3.4. Автоматизація та неперервна оцінка

NIST SP 800-137 вводить поняття Information Security Continuous Monitoring (ISCM) – підтримання постійної поінформованості про стан безпеки, вразливості та загрози для підтримки рішень у рамках управління ризиками [12]. Тобто оцінка ризиків перестає бути раз на рік, а перетворюється на цикл: збір даних → аналіз → репорти → реакція → оновлення стратегії. Цей підхід прямо вбудований у NIST RMF та NIST CSF 2.0, а також підтримується сучасними інструментами безперервного моніторингу [20].

У хмарі основою безперервна оцінка є CSPM/CNAPP-рішення та провайдер-нативні сервіси, які постійно сканують конфігурації, права доступу та сховища на предмет помилок, вразливостей і невідповідності стандартам (CIS, NIST, ISO). На цю телеметрію «накладаються» ризик-орієнтовані моделі: автоматичне присвоєння оцінки ризику об’єктам (акаунти, VPC, bucket-и, кластери), кореляція з бізнес-критичністю активів, тригери для оновлення реєстру ризиків і планів обробки.

У результаті, безперервна оцінка – це зв’язка: формальна методика (ISO/NIST/FAIR), дані з автоматизованих сканерів (CSPM, CWPP, CIEM, сканери вразливостей), та регулярні рев’ю ризиків з боку SOC/команд безпеки. Багато сучасних практик, як CTEM (Continuous Threat Exposure Management), прямо описують кроки переходу від одиничних аудитів до постійного, метрик-орієнтованого управління ризиком [21].

1.3.5. Приклади інструментів та сервісів

Для хмарних середовищ зараз домінують кілька класів інструментів оцінки ризиків і стану безпеки:

CSPM / CNAPP / CWPP / CIEM – платформи, що виявляють помилки конфігурації, надлишкові права, вразливості робочих навантажень, корелюють їх із вимогами стандартів і будують risk-score. Оглядові статті виділяють серед популярних рішень: Wiz, Prisma Cloud, Orca, Lacework, Tenable, Cyera тощо [22].

Нативні сервіси провайдерів:

- AWS Security Hub / GuardDuty – агрегують сигнали з різних сервісів AWS, зіставляють їх із CIS/NIST та формують зведений risk-/compliance-score;
- Microsoft Defender for Cloud (колишній Azure Security Center) – CSPM/CNAPP-платформа для Azure та multi-cloud;
- Google Cloud Security Command Center (SCC) – централізований сервіс для моніторингу вразливостей, помилок конфігурації, прав доступу та загроз у GCP (та частково multi-cloud) [23].

Платформи кіберризик-квантифікації на базі FAIR (RiskLens, SAFE One, інші CRQ-рішення), які інтегруються з вихідними даними з SIEM/CSPM та дозволяють переводити ризики в грошові показники для прийняття рішень на рівні бізнесу [24].

Інструменти відповідності та cloud-compliance – орієнтовані на аудит налаштувань і безперервну перевірку відповідності (SOC 2, ISO 27001, GDPR, HIPAA тощо) у хмарі. Такі рішення (у т.ч. згадані SentinelOne, інші cloud-compliance-платформи) автоматизують збір доказів, мапінг контролів і формування звітів для аудиторів [25].

1.4. Проблеми та виклики у сфері кібербезпеки для хмарних сервісів

Попри очевидні переваги хмарних технологій, їх використання супроводжується низкою специфічних викликів безпеки, пов’язаних із моделлю спільної відповідальності, багатокористувацькістю, динамічністю середовища та складним юридичним полем (GDPR, галузеві регуляції тощо). ENISA, CSA та недавні промислові звіти показують, що більшість інцидентів у хмарі зумовлена поєднанням обмеженої видимості, людського фактору, помилок конфігурації та нових типів атак на ланцюги постачання й хмаро-нативні технології (контейнери, serverless, API) [26].

Нижче розглянуто основні групи проблем, що безпосередньо впливають на ефективність систем управління кібербезпекою у хмарних середовищах.

1.4.1. Прозорість та контроль

Одна з базових проблем хмарної безпеки – обмежена видимість активів, конфігурацій і потоків даних. Перехід до multi-cloud та широке використання керованих сервісів призводять до ситуації, коли організація не має єдиного «інвентаризаційного» зрізу: які ресурси створені, які сервіси активні, де фізично зберігаються дані, які політики застосовані. Оглядові статті прямо вказують недостатній контроль та видимість як один із топ-викликів захисту multi-cloud-середовищ [27].

ENISA й CSA підкреслюють, що видимість у хмарі ускладнюється додатковими шарами абстракції: частина інфраструктури повністю управляється провайдером, а у клієнта є доступ лише до логів, метрик та API. Це створює «сліпі зони» для класичних SIEM/SOC-підходів, якщо не інтегрувати провайдер-нативну телеметрію (CloudTrail, Activity Logs тощо) та CSPM/CNAPP-рішення. Звіти також показують, що відсутність повної картини, яка активно пов’язана з помилками конфігурації та витоками даних [28].

1.4.2. Динамічність середовища

Хмарне середовище надзвичайно динамічне: ресурси створюються й знищуються за хвилини, контейнери та serverless-функції живуть секунди – хвилини, конфігурації змінюються через IaC-скрипти та CI/CD-пайплайни. Дослідження хмарних викликів відзначають, що така динамічність ускладнює застосування традиційних статичних методів контролю (періодичні аудити, ручні контрольні списки), оскільки стан системи може повністю змінитися між двома перевірками.

Додатковий фактор – розмаїття сервісів: віртуальні машини, керовані бази даних, Kubernetes-кластери, FaaS, керовані черги, API-шлюзи тощо. Кожен із цих компонентів має власну модель конфігурації та прав доступу. Помилка в одному IaC-шаблоні або конвеєрі може тиражуватися на сотні інстансів. Оглядові публікації прямо пов’язують зростання динамічності з підвищенням складності управління політиками безпеки та збільшенням поверхні атаки [29].

1.4.3. Юридичні та виклики відповідності

Хмарні сервіси працюють у контексті складного правового поля: національне законодавство, GDPR, галузеві регуляції (HIPAA, PCI DSS тощо), а також експортний контроль, вимоги до збереження логів, шифрування та локалізації даних. Дослідження щодо відповідності GDPR у хмарі демонструють, що користувачі стикаються з довготривалими проблемами: рознесеність дата-центрів між юрисдикціями, непрозорість суб-процесорів, складність доведення відповідності вимогам контролерів/процесорів даних [30].

ENISA у своїх звітах про хмарну безпеку окремо виділяє правові та комплаєнс-ризики: lock-in до провайдера, складність міграції, різночитання законодавства різних країн, а також труднощі з доведенням виконання договірних зобов'язань щодо безпеки та приватності. Для організацій це означає необхідність побудови комплексної стратегії відповідності в хмарі, яка охоплює вибір провайдера, архітектуру розміщення даних, договірну базу (DPA, SCC, SLA), технічні та організаційні заходи (шифрування, псевдонімізація, логування, контролі доступу).

1.4.4. Людський фактор та організаційні проблеми

За останні роки людський фактор вийшов на перше місце серед загроз для хмарних середовищ. Звіт Cloud Security Alliance 2024 прямо зазначає, що людський фактор – топ-загроза, а більшість інцидентів пов'язана з помилками конфігурації, некоректним управлінням ідентичностями та правами доступу, а також браком кваліфікації персоналу [31].

Наукові роботи, що аналізують помилки конфігурації в хмарі через призму HFACS, показують: неправильна конфігурація – це багаторівнева проблема, де на помилки операторів нашаровуються організаційні чинники: відсутність стандартів конфігурації, недостатні процедури перевірки, перевантаження команд, «культура швидкого релізу». Додаються типові організаційні виклики: нечітко розподілена відповідальність за безпеку між Dev/Ops/безпекою, відсутність зрозумілого трактування моделі спільної

відповідальності з провайдером, конфлікти між бізнес-цілями (time-to-market) та вимогами безпеки.

1.4.5. Нові типи загроз і еволюція атак

Хмарні платформи створюють ґрунт для нових типів атак або переосмислення старих: атаки на ланцюги постачання (supply chain), компрометація CI/CD-процесів, атаки на контейнерні та serverless-архітектури, зловживання API, масштабні DDoS проти хмарної інфраструктури. ENISA Threat Landscape 2023 фіксує зростання атак на ланцюги постачання, стійкий рівень DDoS, а також домінування ransomware як однієї з ключових загроз, що активно використовує хмарну інфраструктуру як ціль і як інструмент (рис.1.8) [16].

Рисунок 1.8 – Огляд загроз ENISA 2022 – Основні загрози

Звіт CSA щодо хмарних загроз 2023 року показує понад 300% річне зростання атак на програмні ланцюги постачання та різноманітні техніки

обходу захисту в хмаро-нативних середовищах [17]. Окремі аналітичні матеріали фіксують різке зростання інцидентів, пов’язаних із serverless-архітектурами, а також активну експлуатацію вразливих контейнерних образів та відкритих хмарних API. Додатково в останні роки зростає роль хмари в контексті AI: моделі й дані для навчання розміщуються в хмарі, а звіт CSA 2025 вказує на те, що незахищені AI-системи стають відчутним новим класом ризиків [32].

2 РОЗРОБЛЕННЯ МОДЕЛІ ТА МЕТОДИКИ ОЦІНКИ КІБЕРРИЗИКІВ У ХМАРНИХ СЕРВІСАХ

2.1 Визначення основних критеріїв оцінки ризиків

Чітко визначені критерії оцінки ризиків є вихідною точкою будь-якої методики, оскільки саме вони задають, що саме вважається критичним для організації, як вимірюється рівень ризику та які події вимагають пріоритетного реагування. Міжнародні стандарти ISO/IEC 27005 та NIST SP 800-30 наголошують, що рівень ризику розглядається як функція ймовірності реалізації загрози та тяжкості її наслідків для інформаційних активів, які підтримують бізнес-процеси організації [1].

У контексті хмарних сервісів до цього додаються специфічні фактори: модель надання сервісу (IaaS/PaaS/SaaS), тип хмари (публічна/приватна/гібридна), розподіл відповідальності між провайдером і споживачем, багатокористувацькість (multi-tenancy), географічне розміщення даних тощо [20].

Розглянемо основні критеріїв, які доцільно використовувати при оцінці кіберризиків у хмарних сервісах.

2.1.1. Загальні принципи формування критеріїв

При формуванні критеріїв оцінки ризиків доцільно спиратися на такі принципи (узгоджені з ISO/IEC 27005 та NIST SP 800-30) [1]:

1) зв’язок з бізнес-цілями та контекстом організації. Критерії мають відображати, наскільки подія впливає на ключові бізнес-процеси, виконання договірних зобов’язань, доступність критичних сервісів для клієнтів, фінансові показники, репутацію тощо;

2) вимірюваність та відтворюваність. Формулювання критеріїв повинно дозволяти їх застосування різними експертами з мінімальною суб’єктивністю. Це досягається через шкали (якісні – «низький/середній/високий»; кількісні – бали, ймовірність у рік, очікувані збитки у грошовому вираженні);

3) сумісність зі стандартами та нормативними вимогами. Критерії мають відповідати вимогам ISO/IEC 27001/27005, NIST SP 800-30, а також законодавству (наприклад, вимоги щодо захисту персональних даних, галузеві регуляції), що критично для хмар, де часто обробляються персональні та чутливі дані;

4) урахування апетиту до ризику та толерантності організації. Одна й та сама подія може бути прийнятною для невеликої компанії, але неприйнятною для критичної інфраструктури. Тому критерії рівнів ризику (низький/допустимий/недопустимий) мають бути узгоджені з керівництвом;

5) орієнтація на хмарний контекст. Критерії повинні враховувати динамічність хмарної інфраструктури, автоматичне масштабування, гнучке виділення ресурсів, багатокористувацькість, використання загального підґрунтя (shared infrastructure) та розподілене зберігання даних.

2.1.2. Критерії, пов’язані з активами та вимогами безпеки

Перший блок критеріїв стосується цінності та властивостей інформаційних активів, які розміщуються чи обробляються у хмарному середовищі. ISO/IEC 27005 рекомендує починати оцінку з інвентаризації та класифікації активів за критичністю [21].

Основні критерії:

1. Критичність активу для бізнес-процесів.

Чи є сервіс/дані необхідними для безперервності основних операцій?

Чи вплине втрата доступу до них на доходи, послуги клієнтам, виконання контрактів?

Приклад: збій хмарної CRM-системи може повністю зупинити продажі, тоді як втрата допоміжної Wiki матиме значно менший вплив.

2. Рівень конфіденційності даних. Класифікація за типами: публічні, внутрішні, конфіденційні, строго конфіденційні (наприклад, персональні дані, фінансова інформація, комерційна таємниця). Порушення конфіденційності в хмарі спричиняє ризики несанкціонованого доступу, витоків та порушення вимог захисту даних (GDPR та ін.) [22].

3. Вимоги до цілісності.

– Наскільки критична точність і повнота даних?

– Чи призведе модифікація (навмисна або випадкова) до фінансових втрат, помилкових управлінських рішень, збоїв у технологічних процесах?

Для хмарних застосунків важливо враховувати ризики порушення цілісності через атаки на API, помилки синхронізації, уразливості в CI/CD-ланцюгах.

4. Вимоги до доступності.

Визначаються допустимий час простою (RTO), допустима втрата даних (RPO), вимоги до безперервності сервісів та допустимі вікна обслуговування. У хмарі на доступність впливають не лише технічні збої, а й відмова сервісу провайдером, DDoS-атаки, проблеми з мережею.

5. Додаткові властивості безпеки.

У низці випадків доцільно виділяти критерії для:

– автентичності (гарантія, що суб’єкт/об’єкт є тим, за кого себе видає);

– невідмовності (non-repudiation) – особливо для журналів подій, фінансових транзакцій, логів доступу в хмарному середовищі;

– контрольованості та прозорості – наскільки повно організація бачить події, логування, метрики провайдера.

2.1.3. Критерії оцінки ймовірності реалізації загроз

Другий ключовий блок – критерії, що характеризують ймовірність (частоту) реалізації загроз. NIST SP 800-30 пропонує розглядати ймовірність як комбінацію мотивації та можливостей зловмисника, наявних уразливостей і «предрасположуючих умов» системи [23].

Для хмарних сервісів доцільно враховувати:

1. Тип та мотивація загроз:

– зовнішні зловмисники (кіберзлочинність, APT-групи, хактивісти);

– внутрішні порушники (співробітники клієнта, персонал провайдера, підрядники);

– випадкові помилки (людський фактор, помилки конфігурації).

Для кожної групи визначається типова частота/імовірність дій.

2. Рівень експонованості активів:

– наявність публічних інтерфейсів (Web/API);

– використання відкритих портів, доступних з Інтернету;

– інтеграція з третімі сторонами через API.

Чим ширший «периметр» хмарного сервісу, тим вища ймовірність сканування, виявлення вразливостей і атак.

3. Стан уразливостей та контрольних заходів:

– результати тестів на проникнення, сканування вразливостей;

– наявність і стан механізмів автентифікації, авторизації, шифрування, сегментації мережі;

– зрілість процесів управління змінами та патч-менеджменту.

Якщо уразливість відома, але не усунута, ймовірність реалізації загрози значно зростає.

4. Модель надання хмарних послуг та розподіл відповідальності.

Ймовірність інцидентів залежить від того, які рівні стека контролює клієнт, а які – провайдер (shared responsibility model). Наприклад, у SaaS клієнт має менше технічного контролю, але більше залежить від безпеки постачальника.

5. Історичні дані та статистика інцидентів.

ENISA та інші організації рекомендують враховувати історію інцидентів, як всередині організації, так і в галузі (витоки даних, збої великих хмарних провайдерів, масові атаки на певну технологію) [24].

Імовірність часто оцінюють за упорядкованою шкалою (наприклад, 1–5), де кожне значення має текстовий опис (наприклад, «очікувано кілька разів на рік», «малоймовірно, не частіше ніж раз на 10 років»), або в термінах «подій на рік» для більш зрілих кількісних моделей.

2.1.4. Критерії оцінки впливу інцидентів

Третій блок – критерії впливу (impact), які показують, наскільки суттєвими будуть наслідки реалізації ризику. NIST SP 800-30 та ENISA

рекомендують розглядати декілька вимірів впливу: фінансовий, операційний, юридичний, репутаційний тощо [25].

Основні підкритерії:

1. Фінансові втрати:

– прямі: штрафи, компенсації клієнтам, витрати на відновлення (форензіка, нове обладнання, додаткові сервіси);

– непрямі: втрата доходу через простій сервісу, відтік клієнтів, зниження продажів.

Для важливих хмарних сервісів доцільно переводити оцінку в грошові показники (очікуваний розмір збитків).

2. Порушення доступності сервісів:

– час простою (у годинах/днях);

– кількість користувачів, що зазнали впливу;

– вплив на критичні бізнес-процеси (наприклад, неможливість проводити платежі, реєструвати замовлення, надавати послуги).

3. Порушення конфіденційності та цілісності даних:

– кількість скомпрометованих записів;

– тип даних (персональні, фінансові, медичні, державна таємниця тощо);

– можливі наслідки для суб’єктів даних (крадіжка особистості, шахрайство, дискримінація).

4. Юридичні та комплаєнс-наслідки:

– штрафи регуляторів;

– розірвання контрактів або позови з боку клієнтів;

– необхідність сповіщення регуляторів та суб’єктів даних про інцидент (наприклад, у разі витоку персональних даних).

5. Репутаційні втрати.

Оцінюються через можливе зниження довіри з боку клієнтів, партнерів, акціонерів, згадки в медіа, позиції в рейтингах. Для хмарних провайдерів та сервісів, що працюють B2B, це часто одна з найчутливіших складових впливу.

Як і для ймовірності, вплив часто оцінюють за шкалою (1–5) з чіткими текстовими описами для кожного рівня – наприклад, від «незначний вплив, не впливає на бізнес-процеси» до «катастрофічний вплив, зупинка критичних операцій, суттєві фінансові та репутаційні наслідки».

2.1.5. Специфічні для хмарних сервісів критерії

Окремо доцільно виділити критерії, характерні саме для хмарних середовищ, які ENISA та інші організації визначають як відмінність хмарних ризиків від традиційної IT-інфраструктури [20].

1. Модель розгортання та багатокористувацькість (multi-tenancy).

– публічна, приватна, гібридна, community-хмара;

– ступінь ізоляції між клієнтами;

– спільне використання фізичних ресурсів (гіпервізори, мережеві пристрої, сховища).

Високий рівень багатокористувацькості без достатньої ізоляції підвищує ризик побічного витоку даних (side-channel), атак між тенантами, ескалації привілеїв.

2. Географічне розміщення даних та юрисдикція.

– розташування дата-центрів (країна, регіон);

– застосовні закони щодо захисту даних, експортних обмежень, доступу правоохоронних органів;

– відповідність вимогам замовника (наприклад, зберігання даних виключно в межах ЄС або України).

3. Рівень прозорості та контрольованості провайдера.

– наявність сертифікацій (ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 та ін.);

– доступність звітів про аудити, незалежні оцінки безпеки;

– наявність механізмів моніторингу, логування, SIEM-інтеграції, API для отримання подій.

Низька прозорість ускладнює оцінку реального рівня захищеності.

4. Параметри SLA та механізми резервування/відновлення.

– гарантований рівень доступності (наприклад, 99,9 %);

– умови компенсацій;

– наявність георезервування, можливість відновлення після катастрофи (Disaster Recovery), частота резервного копіювання та перевірки відновлюваності.

5. Залежність від провайдера (vendor lock-in).

Оцінюється складність міграції даних і сервісів до іншого постачальника, наявність стандартних форматів даних та відкритих API, ризики зупинки бізнесу в разі банкрутства або зміни політики провайдера.

2.1.6. Організаційні та процесні критерії

Крім технічних аспектів, важливу роль відіграють організаційні та процесні критерії, які ENISA виділяє як ключовий компонент сучасних підходів до управління ризиками [26].

1. Зрілість системи управління інформаційною безпекою (ISMS):

– наявність політик та процедур безпеки;

– регулярність перегляду та актуалізації;

– інтеграція процесів управління ризиками в загальний цикл управління (plan–do–check–act).

2. Управління людським фактором:

– рівень підготовки персоналу, проведення навчань щодо роботи з хмарними сервісами;

– наявність процедур доступу, звільнення, розподілу повноважень;

– контроль привілейованого доступу та діяльності адміністраторів.

3. Процеси реагування на інциденти та безперервність бізнесу:

– визначеність ролей та відповідальності при інциденті (хто за що відповідає зі сторони клієнта і провайдера);

– наявність планів реагування та відновлення, проведення навчальних тренувань;

– вимоги до часу виявлення та реагування (MTTD, MTTR).

4. Управління постачальниками та третімі сторонами:

– наявність критеріїв оцінки безпеки провайдера до укладання договору;

– положення в договорах щодо безпеки, аудиту, повідомлення про інциденти;

– періодичний перегляд та моніторинг постачальників.

2.1.7. Узагальнення системи критеріїв

На основі наведених положень можна сформувати інтегровану систему критеріїв оцінки кіберризиків у хмарних сервісах, що включає такі групи:

1) критерії активів та вимог безпеки: критичність активу, рівень конфіденційності, вимоги до цілісності, доступності, додаткові властивості (автентичність, невідмовність);

2) критерії ймовірності реалізації загроз: тип загроз і їх мотивація, експонованість сервісів, стан уразливостей і контролів, модель надання сервісу, історичні дані;

3) критерії впливу: фінансові втрати, порушення доступності, порушення конфіденційності та цілісності, юридичні та комплаєнс-наслідки, репутаційні втрати;

4) специфічні хмарні критерії: модель розгортання й багатокористувацькість, географія та юрисдикція, прозорість провайдера, параметри SLA і DR, ризик залежності від провайдера;

5) організаційні та процесні критерії: зрілість ISMS, управління людським фактором, процеси реагування на інциденти та безперервність, управління постачальниками.

У наступному підрозділі ці критерії будуть формалізовані у вигляді моделі оцінки ризиків, де кожному критерію призначаються вагові коефіцієнти, шкали та правила агрегування, що дозволяє переходити від якісних експертних оцінок до порівнюваних кількісних показників для різних хмарних сервісів та сценаріїв загроз.

2.2 Гібридна модель оцінки кіберризиків у хмарних сервісах

На основі критеріїв, визначених у підрозділі 2.1, розроблено гібридну модель оцінки кіберризиків для хмарних сервісів. Модель враховує такі компоненти ризику.

1. Ймовірність реалізації загроз. Кожному сценарію загрози призначається оцінка ймовірності (частоти) її виникнення. Це може бути якісна категорія (наприклад, низька, середня, висока) або числова шкала (наприклад, 1 – 5 балів). Оцінка враховує статистичні дані про інциденти або експертні судження щодо того, наскільки часто може відбутися реалізація загрози. Відповідно до підходів стандартів (ISO/IEC 27005, NIST SP 800-30), ризик розглядається як функція ймовірності загрозової події та потенційних наслідків для організації. Так, NIST SP 800-30 пропонує розраховувати рівень ризику шляхом комбінування оціненої ймовірності загрози та впливу її реалізації [1].

2. Вплив на активи (конфіденційність, цілісність, доступність). Для кожного активу оцінюється потенційний вплив інциденту за трьома класичними критеріями інформаційної безпеки: конфіденційність, цілісність і доступність. Ці критерії відображають, наскільки серйозними будуть наслідки компрометації активу в разі порушення кожної з указаних характеристик. Згідно з рекомендаціями ISO/IEC 27005, аналіз інцидентів має фокусуватися на компрометації конфіденційності, цілісності та/або доступності інформації. У моделі для кожної з трьох властивостей встановлюються якісні або бальні оцінки впливу (наприклад, 1 – незначний, 5 – катастрофічний вплив). Вплив може оцінюватися в грошовому еквіваленті (кількісно) або за допомогою експертних рангів (якісно), залежно від наявних даних. Важливо, що модель дозволяє врахувати відмінності у важливості цих властивостей для різних активів: вводяться вагові коефіцієнти для кожної складової впливу (наприклад, для конфіденційності, цілісності, доступності), щоб відобразити пріоритети організації. Таким чином, сумарний вплив на актив I_{total} розраховується як зважена сума оцінок впливу на конфіденційність I_C, цілісність I_I та доступність I_A.

Хмарні особливості. Модель інтегрує специфічні ризик-фактори, притаманні хмарному середовищу:

3. Мультиорендність (multi-tenancy). У хмарних сервісах ресурси спільно використовуються багатьма клієнтами, що створює ризик ізоляційних збоїв. У разі компрометації механізмів ізоляції (гіпервізора тощо) зловмисник може отримати несанкціонований доступ до даних інших орендарів в тій самій інфраструктурі. Хоча такі атаки реалізувати складніше, ніж атаки на традиційні ОС, мультиорендність підвищує масштаб впливу – потенційно порушення може зачепити відразу кількох клієнтів. Таким чином, фактор мультиорендності враховується при оцінці ймовірності та впливу: наприклад, для загроз, пов'язаних з ізоляційним провалом, встановлюється вища оцінка ймовірності та ширший вплив (адже під ударом кілька організацій одночасно) [4].

Географічний розподіл та юрисдикції. Дані і сервіси в хмарі можуть розміщуватися в дата-центрах різних країн, що породжує ризики, пов'язані з законами та регуляціями. Зберігання даних у кількох юрисдикціях з недостатнім рівнем верховенства права чи непередбачуваним правовим полем може призвести до примусового розкриття або вилучення даних місцевою владою [27]. Наприклад, якщо дані знаходяться в країні з агресивними правоохоронними органами, існує ризик, що сервери можуть бути конфісковані, зачепивши при цьому і дані добросовісних користувачів. Окрім того, глобальний розподіл сервісів ускладнює реагування на інциденти та дотримання різних регуляторних вимог щодо приватності (GDPR та ін.), що підвищує регуляторні та репутаційні наслідки інцидентів. У моделі цей фактор відбивається через підвищення оцінки впливу на конфіденційність (через можливі юридичні штрафи та втрату довіри) і доступність (через потенційно ширший масштаб збою в разі відмови цілої регіональної зони) [28].

Модель спільної відповідальності. У хмарних сервісах відповідальність за безпеку розподілена між постачальником (CSP) та клієнтом. Помилкове припущення, що провайдер повністю захищає всі аспекти, призводить до прогалин у безпеці на стороні клієнта. Провайдер забезпечує безпеку хмари

(інфраструктури), а користувач – безпеку в хмарі (налаштування сервісів, дані, доступи). Неправильна конфігурація сервісів або відсутність необхідних контролів з боку клієнта є суттєвими ризиками в хмарному середовищі [29]. Модель враховує цей момент при оцінюванні ймовірності: наприклад, ризик зловживання конфігурацією або вразливості через неуважність клієнта буде мати вищу ймовірність у разі відсутності належних процесів управління конфігураціями. Також враховується, чи забезпечує провайдер достатні засоби безпеки за замовчуванням та чи зрозумілі межі відповідальності – нечіткість ролей підвищує сукупний ризик.

Організаційні аспекти. Внутрішні процеси та ресурси організації також впливають на ризик.

Система управління інформаційною безпекою (СУІБ). Наявність у організації сформованої СУІБ (наприклад, відповідно до ISO/IEC 27001) опосередковано знижує ризики. Це означає, що ризики ідентифіковано, впроваджено відповідні контролі та моніторинг. Стандарт ISO/IEC 27005 наголошує, що управління ризиками має здійснюватися системно в рамках ISMS, що забезпечує раціональне впровадження та підтримку захисних заходів відповідно до виявлених ризиків. У моделі це проявляється в тому, що для організацій із зрілою СУІБ ймовірність успішної реалізації багатьох загроз оцінюється нижче (через наявність контролів, політик, регулярного аналізу вразливостей тощо). Фактично, рівень ризику може перераховуватися на резидуальний з урахуванням ефективності впроваджених заходів безпеки: наприклад, множенням на фактор, що відображає ступінь захищеності (чим кращі контролі – тим менший підсумковий ризик) [7].

Людський фактор. Кваліфікація та поведінка персоналу істотно впливають на кіберризики. Помилки адміністраторів, нехтування політиками безпеки чи успішні фішингові атаки на співробітників підвищують ймовірність інцидентів. З іншого боку, програми навчання і підвищення обізнаності зменшують цю ймовірність. Окремо слід виділити ризик зловмисних інсайдерів: хоча ймовірність навмисних дій від інсайдера зазвичай низька, потенційна шкода від нього дуже велика. У хмарному контексті існують

високоризикові ролі – наприклад адміністратори провайдера з широкими привілеями, компрометація яких матиме критичні наслідки. Модель враховує людський фактор переважно через компонент ймовірності: для сценаріїв, де основною причиною є помилка людини або навмисні дії, ймовірність оцінюється на основі наявних організаційних заходів (тренінги, ротація кадрів, політика розподілу обов'язків тощо) [8].

Угода про рівень обслуговування (SLA). SLA між замовником і постачальником хмарної послуги визначає гарантії доступності, цілісності даних, часові рамки реагування на інциденти, штрафні санкції за порушення тощо. Чітко прописані показники рівня послуг та безпекові вимоги в SLA сприяють кращому управлінню ризиками – необхідність кількісно оцінити ризикові сценарії і можливі збитки (для включення штрафів у SLA) мотивує провайдера впроваджувати належні заходи безпеки. З іншого боку, якщо в угодах відсутні зобов'язання щодо безпеки або доступності, виникає розрив у захисті – деякі аспекти можуть залишитися без належних гарантій [10, 11]. У моделі цей фактор може враховуватися при оцінці впливу: наприклад, наявність суворого SLA з компенсаціями частково знижує фінансовий вплив простою, в той час як відсутність SLA підвищує оцінку впливу для замовника. Також відповідність провайдера умовам SLA опосередковано впливає на ймовірність – низький рівень виконання обіцянок може свідчити про вищу ймовірність збоїв.

Логіка та гібридний підхід моделі. Запропонована модель є гібридною, тобто поєднує якісні та кількісні методи оцінювання. В основі лежить загальноприйнята формула одного сценарію загрози [9]:

$$R = P \cdot I_{total},$$

де

R – інтегральна оцінка ризику;

P – ймовірність реалізації загрози;

I_{total} – сумарний вплив інциденту.

Такий підхід відповідає рекомендаціям провідних стандартів і методик: зокрема, ISO/IEC 27005 пропонує оцінювати імовірність (ймовірність виникнення інциденту) та вплив (наслідки для активів) або в кількісній, або в

якісній формі, залежно від контексту, а за потреби – комбінувати обидва підходи. ENISA також рекомендує визначати рівень ризику на основі зіставлення ймовірності сценарію та його негативного впливу [12].

У практичній реалізації гібридного підходу використовується шкалювання експертних оцінок у бали. Спочатку ризикові фактори оцінюються якісно експертами (наприклад, ймовірність: середня; вплив на конфіденційність: високий тощо). Потім цим категоріям присвоюються числові значення за узгодженою шкалою – наприклад, низька = 1, середня = 3, висока = 5. Таким чином, якісні судження переводяться в кількісні оцінки. Далі шляхом застосування формули обчислюється інтегральний показник ризику. Подібний напівкількісний метод дозволяє підвищити об'єктивність порівняння ризиків: числові результати дають більш чітку градацію, ніж просто вербальні категорії, і водночас зберігають гнучкість експертної оцінки там, де відсутні точні дані. Це узгоджується з підходом NIST SP 800-30, де після аналізу загроз і контролів ризики ранжуються за рівнями на основі оцінок ймовірності та впливу, щоб визначити пріоритети обробки ризиків [11].

Для поєднання різнорідних критеріїв (кількісних і якісних) у моделі можуть використовуватися методи нормалізації та вагового коефіціювання. Наприклад, окремі бали (ймовірність, впливи на CIA) можуть нормуватися до єдиної шкали (0–1 або 0–5) і зважуватися. Вагові коефіцієнти затверджуються експертно або на основі аналізу пріоритетів організації. ISO/IEC 27005:2022 заохочує організації розробляти власні підходи до оцінки ризиків, у тому числі гібридні, що найкраще відповідають їхнім потребам [12]. Наш підхід якраз є таким: він адаптує загальну методику під специфіку хмарних сервісів, комбінуючи якісні рейтинги експертів з кількісним рахуванням балів.

На основі зазначеної логіки формалізуємо обчислення ризику.

Сумарний вплив за CIA:

$$I_{total} = w_C \cdot I_C + w_I \cdot I_I + w_A \cdot I_A,$$

де

I_C – вплив на конфіденційність;

I_I – вплив на цілісність;

ІА – вплив на доступність;

w_C, w_I, w_A – вагові коефіцієнти відповідних складових,

причому:

$$w_C + w_I + w_A = 1.$$

Тоді повна формула обчислення ризику набуває вигляду:

$$R = P \cdot (w_{\mathrm{C}} \cdot I_{\mathrm{C}} + w_I \cdot I_I + w_A \cdot I_A),$$

де P – оцінка ймовірності реалізації загрози (наприклад, від 0 до 1, або за 5-бальною шкалою);

I_{C}, I_I, I_A – оцінки впливу інциденту на конфіденційність, цілісність і доступність;

w_C, w_I, w_A – вагові коефіцієнти значущості кожного виду впливу.

Наприклад, якщо для захисту даних конфіденційність критичніша за доступність, організація може встановити вагу $w_C = 0.5$, тоді як w_A і w_I – по 0.25 кожний. У формулі всі три складові впливу сумуються з урахуванням ваг, утворюючи сумарний зважений показник впливу. Множення на P дає числовий рейтинг ризику R. Чим вище R, тим більш неприйнятним є ризик і тим вищий пріоритет його обробки.

Варто зазначити, що додаткові фактори можуть бути інтегровані в формулу за потреби. Зокрема, хмарні особливості та організаційні аспекти можуть враховуватися через модифікацію вихідних оцінок P, I_{C}, I_I, I_A або через введення поправочних множників.

Один із підходів – обчислювати спочатку власний (інтринсичний) ризик без врахування компенсуючих заходів, а потім розраховувати залишковий ризик.

3. Власний і залишковий ризик

Власний і залишковий ризик, можна записати так:

– власний ризик:

$$R_{intrinsic} = P \cdot I_{total};$$

– залишковий ризик з урахуванням ефективності контролів:

$$R_{residual} = f_{control} \cdot R_{intrinsic,}$$

де $f_{control} \in (0,1]$ – коефіцієнт, що відображає ефективність впроваджених заходів безпеки.

У межах розроблюваної моделі для спрощення організаційні та хмарні чинники вже відображені у відповідних оцінках ймовірності та впливу на етапі їх визначення експертами. Це означає, що експерт, виставляючи бали P або I, враховує контекст: наприклад, високий рівень захищеності приведе до нижчого P, а мультиорендність з підвищеним потенційним масштабом шкоди – до вищого I_C, чи I_A тощо.

Приклад. Зведена матриця оцінки ризиків. Для ілюстрації роботи моделі наведемо приклад зведеної матриці оцінки двох різних ризикових сценаріїв (табл.2.1). У цьому прикладі використано 5-бальну шкалу для ймовірності і впливів, а вагові коефіцієнти встановлено як $w_C = 0.5,\ w_I = 0.25,\ w_A = 0.25.$

Матриця демонструє розрахунок сумарного балу ризику і його якісного рівня.

Таблиця 2.1 – Приклад розрахунку ризику для двох сценаріїв

Сценарій загрози	Ймовір-ність P (бали)	I_C	I_I	I_A	$\Sigma\, I$	$R = P \times \Sigma I$	Рівень ризику
1. Витік даних (компрометація облікових даних у мультиторентному середовищі)	5	5	1	1	3.0	15.0	Висо-кий
2. Простій сервісу (DDoS-атака на хмарний застосунок)	4	1	1	5	2.0	8.0	Серед-ній

Як видно з наведеного прикладу, запропонована модель дозволяє поєднати якісні судження з кількісним підрахунком балів, отримуючи наочну матрицю ризиків. За допомогою вагових коефіцієнтів модель гнучко налаштовується під потреби конкретної системи: якщо для певного активу критичною є доступність, ваги можна змінити таким чином, щоб A мала найбільшу частку. Тоді розрахунок пріоритезуватиме ризики, пов’язані з

простоєм, вище. Аналогічно, якщо організація більше переймається конфіденційністю даних (як у прикладі), модель це враховує, даючи витоку даних більш високий сумарний бал ризику.

Відповідність стандартам та найкращим практикам. Розроблена гібридна модель узгоджується з підходами, описаними в міжнародних стандартах та рекомендаціях. Стандарт ISO/IEC 27005 (керування інформаційними ризиками) наголошує на необхідності системного виявлення та оцінки ризиків, допускаючи як кількісні, так і якісні методи, а також їх комбінації [12]. Наш підхід реалізує саме таку комбінацію, адаптовану до специфіки хмарних обчислень (multi-tenancy, географія, спільна відповідальність тощо). Документ NIST SP 800-30 (керівництво з проведення оцінки ризиків) також підтримує практику використання матриць ризику: спочатку визначаються загрози, вразливості та передумови, потім оцінюються ймовірність та вплив для кожного сценарію, після чого комбіновані оцінки використовуються для присвоєння рівнів ризику і їх ранжування. Розроблена модель дотримується цієї логіки, додаючи деталізацію по лінії CIA та специфічних для хмари чинників [1].

Європейське агентство ENISA у своєму керівництві з оцінки ризиків хмарних обчислень наводить перелік типових сценаріїв загроз і активів, пропонуючи оцінювати рівень ризику шляхом зіставлення ймовірності сценарію та масштабу негативного впливу. Зазначений підхід є якісним і індуктивним. Наша ж модель розвиває цю ідею, дозволяючи кількісно порівнювати різні сценарії (через бальну систему) та враховувати особливості конкретного провайдера і клієнта, чого бракує загальному фреймворку ENISA [2, 13].

Таким чином, запропонована гібридна модель оцінки кіберризиків у хмарних сервісах поєднує кращі практики стандартизованого управління ризиками із урахуванням специфіки хмарного середовища. Вона забезпечує системність, відповідно до ISMS, гнучкість налаштування та наочність результатів, що полегшує подальше ухвалення рішень щодо обробки ризиків. Модель може бути використана для пріоритезації ризиків та для обґрунтування

вибору заходів безпеки, спираючись на визнані стандарти (ISO/IEC 27005, NIST SP 800-30) та рекомендації ENISA щодо кібербезпеки хмарних сервісів.

2.3. Використання кількісних і якісних методів оцінки

У попередніх підрозділах було визначено систему критеріїв (2.1) та побудовано гібридну модель оцінки ризику (2.2), яка поєднує ймовірність та вплив за складовими CIA. Логічним кроком є обґрунтувати, як саме застосовуються якісні та кількісні методи оцінювання у цій моделі, особливо в контексті хмарних сервісів.

Міжнародні стандарти не нав'язують один «правильний» метод – ISO/IEC 27005 прямо допускає використання як якісних, так і кількісних підходів (або їх комбінації), наголошуючи, що головне – узгоджені та чітко визначені шкали оцінки. NIST SP 800-30 також описує ризик як функцію ймовірності загрози та впливу інциденту і дозволяє реалізовувати як напівкількісні, так і повністю кількісні оцінки. У сфері хмарних обчислень ENISA на практиці застосовує саме напівкількісний підхід: інциденти оцінюються за ймовірністю та впливом, ризикам присвоюється числова оцінка та категорія «низький/середній/високий». [8]

Розглянуто особливості якісних, кількісних та гібридних методів у контексті хмарних сервісів та їх використання в межах запропонованої моделі.

2.3.1. Якісні методи оцінки ризиків

Якісна оцінка ризиків ґрунтується на експертних судженнях. Загрози, уразливості, наслідки та ймовірності описуються у вербальних категоріях: «низька», «середня», «висока», «критична» тощо. ISACA визначає якісну оцінку як використання експертної оцінки на основі стандартів управління ризиками з наперед визначеними рейтингами (high/medium/low), що стосуються імовірності та впливу [4].

Типові інструменти якісного підходу:

– матриця ризику з осями ймовірність та вплив;

– категоризація ризиків (низький/середній/високий/критичний);

– workshop-и/експертні сесії, де фахівці з безпеки, IT та бізнесу спільно визначають рівні ризику.

Переваги:

– не потребує точних статистичних даних;

– зрозуміла для менеджменту й нескладна для впровадження;

– швидко дає огляд «картини ризиків» для пріоритезації.

Недоліки:

– висока суб’єктивність: різні експерти можуть по-різному тлумачити «середній» чи «високий» ризик;

– категорії, як правило, не є лінійними – різниця між «середнім» та «високим» часто нечітка;

– складно безпосередньо прив’язати результат до фінансових показників або обґрунтування бюджету.

ISO/IEC 27005 прямо зауважує, що корисність якісних шкал залежить від однозначності рівнів і узгодженості інтерпретації всіма зацікавленими сторонами; рівні мають бути чітко описані, без перекриттів, із об’єктивними формулюваннями.

Застосування для хмарних сервісів.

У хмарному контексті якісні методи є природним стартовим кроком, оскільки:

– часто немає повної статистики по загрозах конкретного провайдера;

– параметри середовища (конфігурації, сервіси, тенанти) швидко змінюються;

– ризики значною мірою залежать від спільної відповідальності (cloud provider + замовник), яку складно формалізувати чисельно.

ENISA класифікує свій фреймворк оцінки ризиків для хмар як загальний якісний дедуктивний підхід, де від типових загроз і активів переходять до якісної оцінки та подальшого віднесення ризику до категорій низький/середній/високий. [29]. Це добре підходить для:

– первинного аналізу ризиків перед міграцією в хмару;

– порівняння різних моделей розгортання (публічна/гібридна/приватна хмара);

– комунікації з керівництвом на високому рівні.

2.3.2. Кількісні методи оцінки ризиків

Кількісні методи намагаються представити ризик у числовому вигляді – зазвичай як очікуваний розмір збитків у грошових одиницях або як частоту і серйозність втрат. NIST SP 800-30 підкреслює, що оцінка ризику включає оцінку ймовірності настання загрози та величини впливу, причому в разі наявності даних їх можна задавати як числові величини та навіть як розподіли ймовірностей [30].

Приклади кількісних моделей:

– класичні моделі на кшталт Annualized Loss Expectancy (ALE),

де:

Single Loss Expectancy (SLE) – збиток від одного інциденту;

Annualized Rate of Occurrence (ARO) – частота інцидентів на рік;

очікувані щорічні збитки: $ALE = SLE \times ARO$;

– сучасні підходи типу FAIR (Factor Analysis of Information Risk), який дає змогу оцінювати кіберризики у фінансових термінах, задаючи для частоти та величини збитків не детерміновані значення, а ймовірнісні розподіли (часто з використанням Монте-Карло) [19].

Переваги:

– можливість прямо оцінити фінансовий вплив і порівнювати різні ризики, інвестиції в безпеку та варіанти обробки ризиків;

– краща інтеграція з фінансовим та операційним ризиком;

– можливість використання імовірнісного моделювання (розподіли, сценарний аналіз, Монте-Карло).

Недоліки:

– потреба у значному обсязі даних (статистика інцидентів, простої, витрати на відновлення, штрафи, репутаційні втрати тощо);

– ризик помилкової точності (false precision) – модель може давати числовий результат, який створює ілюзію високої точності, тоді як вхідні дані приблизні;

– відносно висока складність для впровадження в організаціях із низькою зрілістю процесів управління ризиками.

Застосування для хмарних сервісів. У хмарному середовищі повністю кількісний підхід можливий, але ускладнюється:

– обмеженою прозорістю провайдерів (не всі публікують статистику інцидентів);

– залежністю від багатьох зовнішніх факторів (інтернет-провайдер, регіональні відмови, міжхмарні інтеграції).

Втім, кількісні методи є дуже корисними для:

– оцінки вартості простою хмарних сервісів (наприклад, за даними про доходи/годину, операційну важливість сервісу, параметри SLA);

– обґрунтування інвестицій у резервування, багаторегіональність, DDoS-захист;

– порівняння різних варіантів розгортання (один провайдер vs multi-cloud) у грошових термінах.

2.3.3. Порівняння та доцільність використання в хмарних сервісах

ENISA у своєму огляді стандартів управління ризиками підкреслює, що існує широкий спектр методик – від суто якісних до суто кількісних – і організація має обирати або комбінувати їх залежно від цілей, зрілості та доступності даних [17].

Якісні методи доцільні, коли:

– хмарна ініціатива знаходиться на ранній стадії (аналіз «go / no-go»);

– бракує статистичних даних або провайдер не надає детальної інформації;

– метою є швидка інвентаризація та ранжування ризиків, а не фінансове моделювання.

Кількісні методи доцільні, коли:

– організація має історичні дані про інциденти, простої, штрафи, витрати на відновлення;

– стоїть задача обґрунтувати інвестиції в додаткові заходи (резервні регіони, посилений SLA, SOC-моніторинг для хмари);

– керівництву потрібні числові показники для включення кіберризиків у загальний портфель ризиків.

Для хмарних сервісів чисто кількісний підхід рідко можливий «з коробки» через дефіцит даних та динамічність середовища. Тому на практиці більшість рекомендацій (той же ENISA Cloud Computing Risk Assessment) пропонують напівкількісну модель: qualitatively оцінені ймовірність/вплив переводяться у числові шкали, а далі з ними працюють як з кількісними оцінками [17].

Наша модель (розділ 2.2) якраз є прикладом такого гібридного підходу, формально сумісного з ISO/IEC 27005 та NIST SP 800-30: якісні судження експертів систематизуються у вигляді числових бальних оцінок і використовуються у формулі ризику.

2.3.4. Реалізація гібридного підходу в запропонованій моделі

У цій роботі гібридний підхід реалізується як послідовність кроків, що об’єднує якісні та кількісні елементи:

1. Якісна ідентифікація активів, загроз та сценаріїв. На основі аналізу хмарної архітектури визначаються активи (дані, сервіси, інтерфейси API, облікові записи адміністраторів, інтеграції з іншими системами), відповідні їм загрози (DDoS, витік даних через неправильну конфігурацію, зловживання обліковими даними тощо) і формуються сценарії ризику.

2. Призначення якісних рейтингів.

Для кожного сценарію експерти присвоюють:

– ймовірність (наприклад, «низька», «середня», «висока»);

– вплив на конфіденційність, цілісність, доступність (так само у вербальних категоріях).

При цьому ураховуються особливості хмар: multi-tenancy, географія дата-центрів, модель спільної відповідальності, зрілість організаційних процесів (ISMS, навчання персоналу, SLA).

3. Перехід від якісних категорій до числових значень.

Далі вербальні категорії відображаються на бальну шкалу (наприклад, 1, 3, 5 або 1–5). Це описано в стандартах як типова практика напівкількісної оцінки – перетворення якісних шкал у числові, з умовою, що всі учасники однаково розуміють, що означає кожен рівень.

Наприклад:

– «низька» → 1 бал;

– «середня» → 3 бали;

– «висока» → 5 балів.

4. Застосування формули ризику. Отримані числові значення підставляються у формулу, описану в підрозділі 2.2:

5. Перетворення результату в якісні рівні ризику.

Після розрахунку числового значення R воно може бути:

– або використане як безперервний показник для порівняння ризиків між собою;

– або віднесене до категорій (наприклад, 0–5 – низький, 6–10 – середній, понад 10 – високий), як це робить ENISA у своєму хмарному фреймворку.

6. За потреби – наближення до фінансових оцінок. Якщо організація має хоча б приблизні дані про фінансові наслідки, доцільно для кожного рівня впливу (за CIA) задати інтервал можливих збитків. Це дозволяє отримати наближення до підходів типу FAIR чи ALE, не вдаючись до повного кількісного моделювання [20].

Наприклад: «високий вплив на доступність для цього сервісу» може відповідати діапазону втрат 10–50 тис. у.о. за інцидент. Тоді на наступному етапі дослідження можна розширити модель до фінансової.

Таким чином, якісні методи в нашій моделі використовуються на етапі:

– ідентифікації ризиків;

– первинного присвоєння рівнів ймовірності та впливу;

– формування шкал і порогів.

Кількісний елемент з’являється, коли:

– вербальні рівні перетворюються у числові бали;

– застосовується математична формула ризику;

– результати нормуються, ранжуються та, за можливості, пов’язуються з фінансовими показниками.

2.3.5. Приклад напівкількісної шкали

Для завершеності у моделі доцільно явно зафіксувати шкали, які будуть використовуватися в роботі.

Таблиця 2.2 – Приклад шкал для якісно-кількісної оцінки

Рівень	Опис ймовірності / впливу	Бал
L	Низький: малоймовірно / незначний вплив	1
M	Середній: можливий, але нечастий / помітний вплив	3
H	Високий: очікувано регулярно / суттєвий вплив	5
C	Критичний: майже неминучий / катастрофічний вплив	7

За такою схемою експерт виставляє, наприклад, $P = 5$ (H), $I_C = 7$ (C), $I_A = 3$ (M) тощо, після чого виконується розрахунок за формулою. Це і є типовим гібридним використанням якісних та кількісних методів, яке рекомендується багатьма сучасними підходами до кіберризиків і адаптоване в даній роботі до специфіки хмарних сервісів.

3. ПРАКТИЧНЕ ВПРОВАДЖЕННЯ РОЗРОБЛЕНОЇ МЕТОДИКИ

3.1 Опис платформи для впровадження методики

Для практичної перевірки та демонстрації розробленої методики оцінки кіберризиків у хмарних сервісах у даній роботі обрано публічну хмарну платформу Google Cloud Platform (GCP). Це один із провідних гіперскейл-провайдерів, який надає широкий спектр сервісів IaaS, PaaS та SaaS, а також розвинені механізми безпеки, моніторингу та керування відповідністю вимогам. Google Cloud позиціонується як платформа з багаторівневим (defense-in-depth) підходом до безпеки, де поєднуються фізичні, адміністративні та технічні контролі для захисту інфраструктури та даних клієнтів [31].

Використання Google Cloud як базової платформи дозволяє:

- змоделювати реальний сценарій роботи прикладного сервісу у публічній хмарі;
- продемонструвати, як розроблена модель оцінки ризиків застосовується до конкретних сервісів та конфігурацій;
- показати специфіку моделі спільної відповідальності (shared responsibility model) між провайдером та замовником у контексті ризик-менеджменту [32].

3.1.1. Загальна характеристика Google Cloud як платформи

Google Cloud є публічною хмарною платформою, що складається з набору сервісів для обчислень, зберігання даних, мережевої взаємодії, аналітики, штучного інтелекту та керування безпекою. В основі платформи лежить інфраструктура Google – глобальна мережа дата-центрів, магістральних каналів і систем розподілених обчислень, які також використовуються для власних сервісів Google (пошук, YouTube, Gmail тощо) [30].

Архітектура Google Cloud організована за ієрархією:

- Organization – верхній рівень (юридична/корпоративна сутність);
- Folders – логічні групи проектів (наприклад, за департаментами або середовищами: prod/test/dev);

– Projects – основна одиниця керування ресурсами, IAM-політиками, білінгом;

– Resources – конкретні сервіси: віртуальні машини, бази даних, сховища, функції тощо [34].

У контексті даної роботи особливе значення мають такі групи сервісів:

Обчислювальні сервіси:

Compute Engine – віртуальні машини (IaaS);

Google Kubernetes Engine (GKE) – керований Kubernetes-кластер (контейнеризація).

Сховища та бази даних:

Cloud Storage – об’єктне сховище для файлів, резервних копій та статичного контенту;

Cloud SQL – керована реляційна база даних (MySQL, PostgreSQL, SQL Server).

Мережа та захист периметра:

– Virtual Private Cloud (VPC) – віртуальна мережа з підмережами, правилами маршрутизації та firewall-політиками;

– Cloud Load Balancing – розподіл навантаження між екземплярами сервісів;

– Cloud Armor – захист від веб- і DDoS-атак на рівні периметра.

Ідентичність, доступ та ключі:

– Cloud IAM – керування ідентичностями та доступом до ресурсів;

– Cloud KMS – служба керування криптографічними ключами;

– підтримка hardware-based безпеки на рівні інфраструктури (HSM, secure boot тощо) [35].

Моніторинг, журналювання та аналіз безпеки:

– Cloud Logging та Cloud Monitoring – централізований збір логів і метрик;

– Security Command Center (SCC) – інтегрована платформа виявлення вразливостей, помилок конфігурації, підозрілої активності;

– інші сервіси для керування вразливостями та відповідністю вимогам [36].

На рис. 3.1 наведено інтерфейс консолі Google Cloud із вибраним проєктом, у межах якого розгорнуто тестовий веб-застосунок.

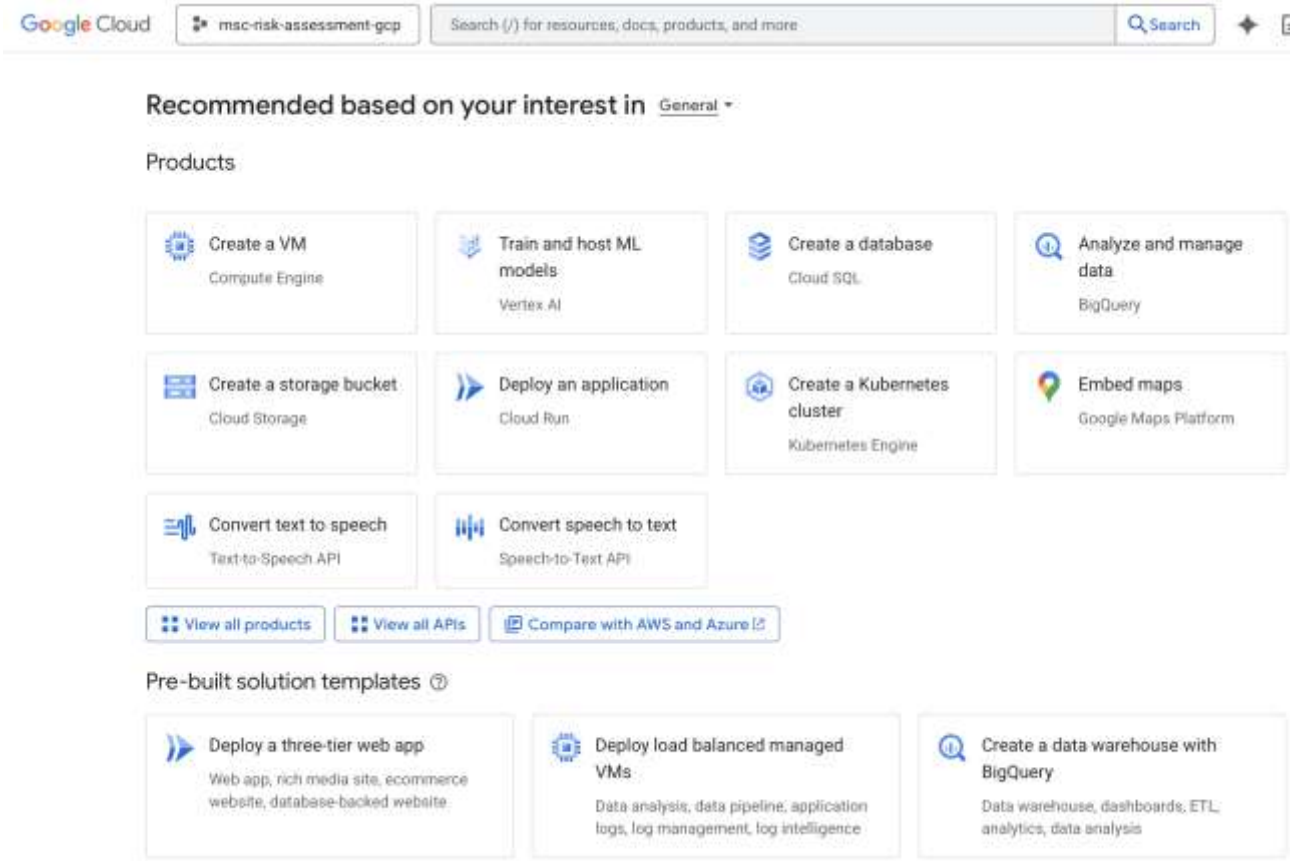

Рисунок 3.1 – Головна консоль Google Cloud із вибраним тестовим проєктом

Наявність цих сервісів дозволяє розглядати Google Cloud як повноцінне середовище для побудови та аналізу моделі ризиків, включно з технічними й організаційними аспектами безпеки.

3.1.2. Модель безпеки та спільної відповідальності в Google Cloud

Безпека в Google Cloud реалізується за принципом «захисту в глибину»: на рівні фізичних дата-центрів, мережі, віртуалізації, сервісів керування ідентичністю та доступом, а також на рівні інструментів моніторингу й аудиту [37].

Ключовою концепцією є модель спільної відповідальності:

– Google відповідає за безпеку хмарної інфраструктури (фізична безпека дата-центрів, мережа, гіпервізор, базовий рівень сервісів);

– клієнт відповідає за безпеку того, що розгортається в хмарі: конфігурації сервісів, управління обліковими записами та ролями, шифрування даних, політики доступу, захист прикладного коду тощо.

Google Cloud офіційно документує розподіл ролей і обов'язків у рамках цієї моделі для різних сервісів та сценаріїв (Compute Engine, GKE, Cloud SQL, Kubernetes тощо), що є важливим вхідним елементом для побудови моделі ризиків: частина ризиків пов'язана з провайдером, частина – з помилками клієнта [38].

Для допомоги замовникам Google пропонує Security Foundations / Enterprise Foundations Blueprint – рекомендації та еталонні архітектури для побудови безпечної «посадкової зони» в Google Cloud: організаційна структура, базові мережеві сегменти, IAM-політики, журнали, моніторинг та основні контролі безпеки. Ці матеріали, по суті, є шаблоном безпечної архітектури, на базі якого у даній роботі формується приклад для оцінки ризиків.

3.1.3. Опис прикладного проєкту: веб-застосунок у хмарі Google Cloud

Для практичної апробації розробленої методики в роботі розглядається прикладний сценарій розгортання трирівневого веб-застосунку у Google Cloud, який обробляє персональні та конфіденційні дані клієнтів (наприклад, систему управління заявками чи CRM для невеликої компанії). Цей приклад дозволяє врахувати типові для хмарних сервісів активи, загрози та вразливості.

Структуру віртуальної мережі VPC, що реалізує поділ на публічні та приватні підмережі для веб-рівня та рівня даних, показано на рисунку 3.2.

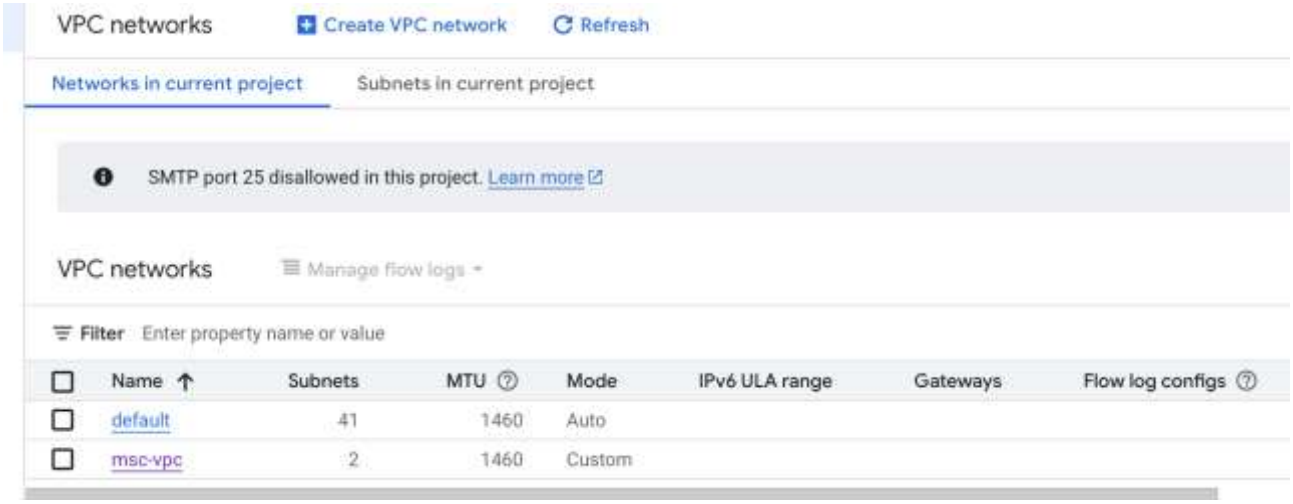

Рисунок 3.2 – Структура VPC-мережі з публічною та приватною підмережами.

На рисунку 3.3 продемонстровано інстанс бази даних Cloud SQL, який зберігає конфіденційні дані користувачів.

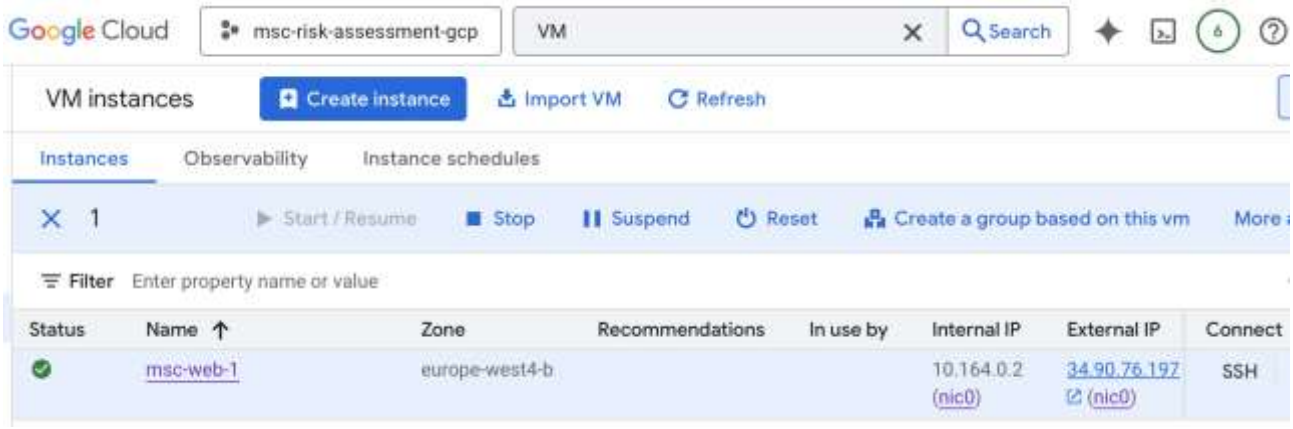

Рисунок 3.3 – Список VM-інстансів з msc-web-1 у Compute Engine

Для зберігання статичних файлів застосунку використовується сервіс Cloud Storage, приклад конфігурації бакету наведено на рисунку 3.4.

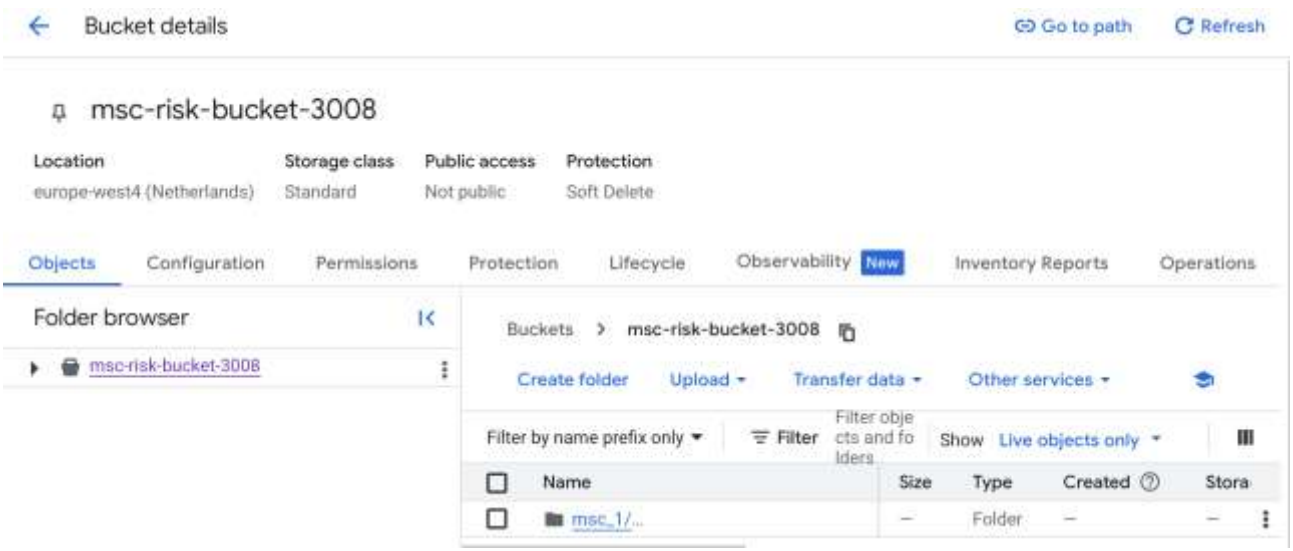

Рисунок 3.4 – Список бакетів з msc-risk-bucket

Архітектура проєкту (логічний рівень). Умовно архітектуру можна подати у вигляді таких компонентів.

1. Мережевий рівень (VPC):

– створюється Virtual Private Cloud (VPC) з поділом на публічну та приватну підмережі;

– у публічній підмережі розташовується балансувальник навантаження (Cloud Load Balancing), який приймає HTTPS-з'єднання з Інтернету;

– у приватних підмережах розміщуються екземпляри веб- та застосункових серверів (Compute Engineабо вузли GKE), а також база даних (Cloud SQL);

– на рівні VPC налаштовуються правила firewall, маршрути, VPN/Cloud Interconnect за потреби (наприклад, для інтеграції з локальним дата-центром).

2. Прикладний рівень:

– веб-застосунок розгортається або на групі керованих інстансів Compute Engine, або в кластері GKE (контейнеризована архітектура);

– статичний контент (зображення, документи) зберігається в Cloud Storage;

– застосунок використовує Cloud SQL як основну реляційну базу даних.

3. Рівень даних та криптографії:

– дані в базі та в об’єктному сховищі шифруються з використанням ключів, керованих через Cloud KMS (Customer-Managed Encryption Keys – CMEK, за потреби);

– політики шифрування «даних у стані спокою» та «даних у транзиті» (TLS) налаштовуються згідно з вимогами до конфіденційності.

4. Управління доступом та ідентичністю:

– доступ до ресурсів регулюється через Cloud IAM з використанням принципу «найменших привілеїв» (least privilege);

– для сервісних акаунтів застосунку та компонентів (VM/Pod) задаються окремі ролі з мінімально необхідним набором прав;

– адміністраторські доступи захищаються за допомогою багатофакторної автентифікації та журналювання дій.

5. Моніторинг, журнали та безпека:

– всі журнали (доступу, системні, мережеві, аудиту IAM) збираються у Cloud Logging і візуалізуються через Cloud Monitoring;

– Security Command Center використовується для виявлення хибних налаштувань (misconfigurations), вразливих образів контейнерів, проблем із правами доступу, а також для централізованого управління попередженнями;

– для захисту публічного периметра (веб-інтерфейсу) застосовується Cloud Armor з правилами щодо захисту від DDoS та типових веб-атак.

Інформаційні потоки. У рамках проєкту виділяються такі основні потоки даних:

– зовнішній трафік користувачів → балансувальник навантаження → фронтенд/бекенд-застосунок;

– запити застосунку → база даних Cloud SQL (читання/запис персональних даних);

– завантаження/зберігання файлів → Cloud Storage;

– службові журнали та метрики → Cloud Logging / Cloud Monitoring / Security Command Center.

Ці потоки є базою для подальшої ідентифікації активів, загроз (наприклад, SQL-ін’єкції, компрометація облікових даних, DDoS, неправильна

конфігурація IAM, витік резервних копій) та для побудови матриць ризику у розділі 3.2.

3.2. Тестування методики на реальних та симуляційних даних

3.2.1. Мета та підхід до тестування методики

Мета тестування – перевірити, чи дозволяє розроблена методика:

- коректно ранжувати ризики для реальної/реалістичної хмарної архітектури;
- відображати специфіку хмарних сервісів (multi-tenancy, модель спільної відповідальності, розподілена інфраструктура);
- адекватно реагувати на зміну вхідних параметрів (ваги, ймовірності, впливи) – тобто бути чутливою до змін конфігурацій та впроваджених засобів безпеки;
- надавати результати, придатні для прийняття управлінських рішень (пріоритезація заходів, вибір контролів, коригування SLA).

Оскільки повний доступ до статистики інцидентів великих хмарних провайдерів, як правило, обмежений, в роботі використовується змішаний підхід:

- структурні та конфігураційні дані – максимально реальні (архітектура з підрозділу 3.1, типові налаштування Google Cloud, логічні потоки даних);
- ймовірності та впливи – переважно симуляційні, але обґрунтовані експертно: базуються на типових сценаріях загроз для хмарних сервісів, наявності/відсутності контролів (IAM, WAF, KMS, SCC), важливості активів, вимогах до CIA.

3.2.2. Формування вхідних даних для прикладу Google Cloud

На основі архітектури з підрозділу 3.1 формуються вихідні множини даних для тестування:

1. Перелік активів (з прив’язкою до CIA-критеріїв)

A1 – База даних Cloud SQL з персональними даними клієнтів:

– конфіденційність – дуже висока;

– цілісність – висока;

– доступність – висока (критична для бізнес-процесів).

A2 – Веб-/аплікейшн-сервери (Compute Engine / GKE):

– доступність – висока;

– цілісність коду/конфігурацій – середня/висока;

– конфіденційність – низька/середня (якщо чутливі дані не зберігаються локально).

A3 – Об’єктне сховище Cloud Storage (документи, вкладення, експорт):

– конфіденційність – висока (можливі чутливі файли);

– цілісність – середня;

– доступність – середня/висока.

A4 – IAM та облікові записи адміністраторів/сервісів:

– Критичний вплив на всі аспекти (C/I/A) у разі компрометації.

A5 – Мережева інфраструктура (VPC, firewall-правила, Cloud Armor):

– основний вплив – на доступність (DDoS, сегментація) та частково на конфіденційність (ізоляція сегментів).

2. Перелік типових загроз та сценаріїв (на основі 2.1, 2.2 та 3.1):

– T1: Компрометація облікових даних адміністратора/сервісного акаунта (через фішинг/витік);

– T2: Неправильна конфігурація Cloud Storage (публічний доступ до приватних бакетів);

– T3: DDoS-атака на публічний веб-інтерфейс (обхід/відсутність належних правил Cloud Armor);

– T4: SQL-ін’єкція або інша вразливість застосунку → несанкціонований доступ до Cloud SQL;

– T5: Внутрішній порушник (insider) на стороні клієнта або провайдера, який має розширені права.

3. Шкали та ваги, узгоджені в 2.2–2.3:

– бальна шкала для ймовірності та впливів:

– 1 – низький; 3 – середній; 5 – високий (за потреби можна додати 7 – критичний).

Ваги для CIA (припустимо, що в цьому кейсі конфіденційність трохи важливіша за доступність):

$$w_C = 0.5, w_I = 0.25, w_I = 0.25;$$

$$w_C + w_I + w_I = 1.$$

Ці параметри повністю узгоджуються з логікою, викладеною в 2.2 (формула) та 2.3 (гібридний підхід та шкали).

3.2.3. Побудова сценаріїв ризику та призначення оцінок

Для тестування потрібно зафіксувати конкретні сценарії ризику “актив + загроза” і призначити їм оцінки:

1. Сценарій S1: Витік даних із Cloud SQL через компрометацію привілейованого акаунта (T1 + A1/A4).

Передумови: відсутність MFA, недостатній моніторинг аномальної активності, фішинг.

– Експертна оцінка:

– ймовірність: (P = 3) (середня; можливий, але не щоденний сценарій);

– вплив на C: (I_C = 5) (витік великого обсягу персональних даних);

– вплив на I: (I_I = 3) (можливі модифікації записів);

– вплив на A: (I_A = 2) (порушення доступності не є основним наслідком, але можливі короткочасні збої при розслідуванні).

2. Сценарій S2: Публічний доступ до приватного бакету Cloud Storage (T2 + A3).

Передумови: помилкова IAM-політика, відсутність контролів SCC та періодичного аудиту конфігурацій.

Оцінка:

– $P = 4$ (вище середнього, типовий misconfiguration-ризик у хмарі);

– $I_C = 4$ (витік конфіденційних документів, але, можливо, менш чутливих, ніж основна БД);

– $I_I = 2$ (ризик зміни файлів нижчий);

– $I_A = 1$ (доступність майже не страждає).

3. Сценарій S3: DDoS-атака на веб-фронтенд (T3 + A2/A5).

Передумови: часткове або некоректне налаштування Cloud Armor, недостатня масштабованість.

Оцінка:

– $P = 4$ (доволі ймовірно для публічного сервісу);

– $I_C = 1$ (конфіденційність безпосередньо не порушується);

– $I_I = 1$ (дані не змінюються);

– $I_A = 1$ (можлива тривала недоступність сервісу).

4. Сценарій S4: Експлуатація вразливості застосунку (SQL-ін’єкція) з доступом до БД (T4 + A1/A2).

Передумови: уразливий код, недостатнє тестування безпеки, відсутність WAF-правил.

Оцінка:

– $P = 3$ (за умови типового рівня безпеки середньої організації);

– $I_C = 5$ (безпосередній доступ до чутливих даних);

– $I_I = 4$ (можливі масові модифікації/видалення записів);

– $I_A = 2$ (сервіс може частково працювати, навіть при витоку).

5. Сценарій S5: Внутрішній порушник з розширеними правами (T5 + A1–A4).

Передумови: відсутність розподілу обов’язків, неформалізовані процеси ревізії доступів, слабкий контроль дій адміністраторів.

Оцінка:

– $P = 2$ (низько-середня ймовірність, але не нульова);

– $I_C = 5$ (потенційно повний витік даних);

– $I_I = 5$ (масштабна модифікація/видалення);

– $I_A = 4$ (можливе свідоме виведення системи з ладу).

Ці оцінки – симуляційні, але узгоджені з типовими шаблонами загроз для публічних хмар і логікою критеріїв з 2.1.

3.2.4. Застосування гібридної моделі до сценаріїв

Далі для кожного сценарію застосовується формула з підрозділу 2.2:

$$I_{total} = w_C \cdot I_C + w_I \cdot I_I + w_A \cdot I_A,$$

$$R = P \cdot I_{total}.$$

Підставимо обрані ваги $w_C = 0.5$, $w_I = 0.25$, $w_A = 0.25$.

Приклад розрахунку для S1 (витік з Cloud SQL):

$$P = 3;\ I_C = 5;\ I_I = 3;\ I_A = 2.$$

Зведений вплив:

$$I_{I_{total}} = 0.5 \cdot 5 + 0.25 \cdot 3 + 0.25 \cdot 2 = 2.5 + 0.75 + 0.5 = 3.75.$$

Ризик:

$$R_{S1} = 3 \cdot 3.75 = 11.25.$$

Аналогічно виконуємо розрахунки для інших сценаріїв.

Для компактного представлення результати доцільно оформити у вигляді таблиці. Приклад результатів приведено в таблиці 3.1.

Таблиця 3.1 – Результати розрахунку ризиків для прикладу Google Cloud (симуляційні дані)

Сценарій	P	I_C	I_I	I_A	I_{total}	$R = P\ I_{total}$	Рівень ризику*
S1 – витік з Cloud SQL (компрометація акаунта)	3	5	3	2	3.75	11.25	Високий
S2 – публічний бакет Cloud Storage	4	4	2	1	3.00	12.00	Високий
S3 – DDoS на веб-фронтенд	4	1	1	5	2.00	8.00	Середній
S4 – SQL-ін’єкція в застосунку	3	5	4	2	4.00	12.00	Високий
S5 – внутрішній порушник	2	5	5	4	4.75	9.50	Середньо-високий

*Рівні можна задати, наприклад:

- 0–5 – низький;
- 5–10 – середній;

– 10–15 – високий.

Пояснення. Найвищі значення (R) отримали S2 та S4 (по 12.0) – це витік через публічний бакет і SQL-ін’єкція, тобто сценарії, пов’язані з компрометацією конфіденційності через помилки конфігурації або вразливість застосунку. Це узгоджується з тим, що ми задали вищу вагу для конфіденційності $w_C = 0.5$.

Сценарій S1 (витік через привілейований акаунт) також належить до високих ризиків 11.25, хоча має дещо нижчу ймовірність, ніж S2, але дуже високий вплив на C.

Сценарій S3 (DDoS) має помірно високий ризик 8.0, оскільки при високій ймовірності вплив сконцентрований на доступності, яка в даному налаштуванні трохи менш «вагома», ніж конфіденційність.

Сценарій S5 (insider) дає $R = 9.5$: порівняно невисока ймовірність (2), але дуже великий вплив за всіма трьома компонентами (особливо на C та I), тому підсумковий ризик вищий, ніж у багатьох “середніх” загроз.

Таким чином, методика дає логічну і зрозумілу картину пріоритезації: на перший план виходять сценарії витоку даних (особливо через конфігураційні помилки та вразливості коду), далі – внутрішній порушник і DDoS.

3.2.5. Аналіз результатів та перевірка адекватності методики

1. Ранжування ризиків відповідає експертним очікуванням:

– витоки чутливих даних (S1, S2, S4) отримали найвищі бали – саме це зазвичай і є найкритичнішим для веб-сервісів з персональними даними;

– DDoS-атака S3 при поточних вагових коефіцієнтах не перекриває за значимістю ризики витоку, але залишається в зоні середньо-високого ризику;

– внутрішній порушник S5 хоч і малоймовірний, але через величезні потенційні наслідки також потрапляє в зону підвищеної уваги.

2. Методика чутлива до зміни ваг та параметрів.

Якщо, наприклад, для того ж самого кейсу організація вважає доступність критичнішою (наприклад, онлайн-платежі в реальному часі), можна змінити ваги, наприклад:

$$w_C = 0.3, w_I = 0.2, w_A = 0.5.$$

У такому разі перерахунок покаже суттєве зростання значення R для S3 (DDoS), що змістить його у топ-ризики. Тобто модель гнучко адаптується до пріоритетів бізнесу, що було однією з вимог у 2.2.

3. Методика дозволяє моделювати "до/після" впровадження контролів.

Наприклад, якщо для S2 впровадити:

- автоматизований аудит конфігурацій (Security Command Center),
- обов'язкові шаблони створення бакетів,
- додаткове навчання адміністраторів,

це зменшить ймовірність помилкової конфігурації. Можна змінити P для S2 з 4 до 2.

Було: $R_{S2} = 12.0$.

Стало: $R_{S2} = 2 \cdot 3{,}0 = 6.0$.

Таким чином, ризик переходить із «високого» в «середній» рівень. Аналогічно можна моделювати вплив MFA, посилення IAM, WAF, шифрування, сегментації тощо на інші сценарії. Це демонструє здатність методики підтримувати прийняття рішень щодо вибору та ефективності заходів безпеки.

3.3. Аналіз отриманих результатів та оцінка ефективності запропонованої методики

У підрозділі 3.2 розроблена методика була апробована на прикладі трирівневого веб-застосунку в Google Cloud з використанням симуляційних, але реалістичних даних. У даному підпункті проведемо системний аналіз отриманих результатів та оцінимо ефективність методики з позицій:

- відповідності очікуванням та пріоритетам безпеки;
- чутливості до зміни параметрів (ваг, ймовірностей, контролів);
- придатності для практичного використання у хмарному середовищі;

– обмежень та напрямів удосконалення.

3.3.1. Узагальнення результатів тестування

На основі формули $R = P(\ w_C \cdot I_C + w_I \cdot I_I + w_A \cdot I_A\ )$ та обраних ваг $w_C = 0.5, w_I = 0.25, w_A = 0.25$ було розраховано значення ризику для п'яти ключових сценаріїв (S1–S5), характерних для хмарного прикладу в Google Cloud:

– S1 – витік даних з Cloud SQL через компрометацію привілейованого акаунта → $R_{S1} = 11.25$;

– S2 – помилковий публічний доступ до приватного бакету Cloud Storage → $R_{S2} = 12.0$;

– S3 – DDoS-атака на веб-фронтенд → $R_{S3} = 8.0$;

– S4 – SQL-ін'єкція в застосунку з доступом до БД → $R_{S4} = 12.0$;

– S5 – внутрішній порушник з розширеними правами → $R_{S5} = 9.5$.

За заданою шкалою (умовно: 0–5 – низький, 5–10 – середній, 10–15 – високий) до високих ризиків віднесено S1, S2, S4; до середніх/середньо-високих – S3 і S5.

Вже на цьому рівні видно ключову властивість методики: вона концентрує увагу на ризиках, пов'язаних з витоком та несанкціонованим доступом до даних, що повністю відповідає вибраному профілю ваг (конфіденційність як найважливіший критерій).

3.3.2. Відповідність очікуванням та пріоритетам безпеки

Якщо зіставити ранжування ризиків з інтуїтивними та професійними очікуваннями для веб-сервісу з персональними даними у публічній хмарі, отримаємо:

– найвищий рівень ризику мають: витік через публічний бакет (S2); SQL-ін'єкція з доступом до БД (S4); витік через компрометацію привілейованого акаунта (S1).

Це три різні технічні вектори, але всі вони ведуть до головного наслідку – масової компрометації конфіденційних даних. Саме такі сценарії зазвичай є

найкритичнішими для організацій (особливо з урахуванням регуляторних штрафів і репутаційних наслідків). Той факт, що модель «підняла» їх у верхню частину рейтингу, говорить про адекватне відображення пріоритетів безпеки.

DDoS (S3) отримав середній рівень ризику: висока ймовірність, але вплив зосереджений на доступності, яка у вибраній конфігурації важлива, але не важливіша за конфіденційність. Це логічно для сценарію, де сервіс працює з персональними даними: тимчасовий простій менш критичний, ніж їх витік.

Insider (S5) показує високий вплив (особливо по C та I) при нижчій ймовірності → результат у зоні «середньо-високого» ризику. Це також відповідає реальній практиці: внутрішні зловмисники трапляються рідше, але їхні дії можуть бути руйнівними.

Таким чином, розроблена методика не суперечить здоровому глузду й експертному досвіду, а навпаки – формалізує їх у вигляді числових значень і чітких пріоритетів. Важливо, що це досягнуто без «жорсткого підганяння» під результат: формула та шкали були задані загально (ще в розділі 2), а кейс і сценарії – типові для хмари.

3.3.3. Чутливість моделі до змін параметрів та контролів

1. Чутливість до ваг (бізнес-пріоритетів).

У 3.2 розглядався варіант зміни ваг у бік доступності, наприклад:

$$w_C = 0.3, w_I = 0.2, w_A = 0.5.$$

У цьому випадку:

- ризик DDoS S3 відчутно зростає, бо високий I_A отримує більшу вагу;
- ризики витоку ($S1$, $S2$, $S4$) знижують свої бали відносно S3, але залишаються суттєвими;
- структура пріоритезації змінюється: DDoS може вийти в лідери, якщо бізнес-кейс – критичні онлайн-транзакції, де кожна хвилина простою дорога.

Це демонструє, що модель:

- адаптивна до різних типів сервісів (даноцентричні vs сервісоцентричні);

– дозволяє явно «прив’язати» ризик до апетиту до ризику й бізнес-моделі організації, а не нав’язує універсальну картину.

2. Чутливість до впровадження контролів.

У 3.2 розглянуто приклад зниження P для S2 (помилкова конфігурація бакету) з 4 до 2 після впровадження:

– автоматизованих перевірок конфігурацій (SCC, політики);

– шаблонів створення сховищ;

– тренінгу адміністраторів.

Фактично:

– було: $R_{S2} = 12.0$ (високий);

– стало: $R_{S2} = 6.0$ (середній).

Це досить показовий результат:

– модель кількісно демонструє ефект від контролів;

– одночасно не змінює структуру впливу CIA – конфіденційність для S2 так само критична, але ймовірність інциденту падає;

– керівництво може використати цю дельту $12 \rightarrow 6$ як аргумент для інвестування в конкретні засоби (SCC, політики, навчання).

Аналогічні сценарії можна змоделювати для MFA, посилення IAM, WAF, сегментації мережі тощо – методика однаково працює, бо «точка впливу» комплаєнс- та технічних заходів у моделі – зміна P та/або (I_C, I_I, I_A).

Висновок по чутливості:

Методика не є «жорсткою» або інертною – вона:

– реагує на зміну ваг (пріоритетів безпеки);

– демонструє ефект від впровадження/посилення контролів;

– зберігає внутрішню логіку (ризики не «стрибають» хаотично).

Це ознаки адекватної та керованої моделі ризику.

3.3.4. Практична придатність для хмарного середовища

З точки зору практики роботи з хмарою (на прикладі Google Cloud), методика показала кілька важливих переваг:

1. Урахування специфіки хмарних сервісів.

При виставленні (P, I_C, I_I, I_A) для S1–S5 фактично враховувалися:

– multi-tenancy та ризики ізоляції;

– помилки конфігурацій (public bucket, неправильні IAM-ролі);

– особливості моделі спільної відповідальності (що робить S2 та S4 дуже актуальними, бо це «помилки клієнта»);

– наявність/відсутність стандартних сервісів безпеки (SCC, Cloud Armor, IAM, KMS).

Тобто модель не є абстрактною – вона «прив'язана» до конкретних особливостей Google Cloud та типових архітектур.

2. Можливість інтеграції у процеси ISMS.

Оскільки:

– критерії (2.1) узгоджені з CIA та стандартною логікою ISO/IEC 27005;

– формула ризику проста й прозора;

– результати можуть бути представлені як матриця ризиків, – методику можна відносно легко інтегрувати у наявні процеси управління ризиками (реєстр ризиків, плани обробки, регулярний перегляд).

3. Придатність для навчання та розширення.

Той самий кейс у Google Cloud може бути використаний:

– для навчальних лабораторних робіт (студентам пропонується виставити свої P, I, порахувати R, порівняти з «еталоном»);

– для розширення (додавання нових сценаріїв: компрометація API-ключів, помилки в CI/CD, міжхмарні інтеграції);

– для порівняння різних хмар (Google Cloud vs AWS vs Azure) при схожих архітектурах.

Отже, методика реально можна застосувати в організації, яка використовує публічну хмару, і масштабувати на інші платформи.

3.3.5. Обмеження методики та напрями удосконалення

Попри позитивні результати, методика має низку об'єктивних обмежень:

1. Суб’єктивність експертних оцінок. Значення (P, I_C, I_I, I_A) базуються на експертному судженні. Якщо:

– експертів мало;

– відсутні спільно погоджені шкали;

– не проводиться калібрування оцінок – виникає ризик суб’єктивних перекосів.

Це частково знімається:

– формалізацією описів рівнів (що таке «низький», «середній», «високий»);

– груповим обговоренням;

– періодичною ревізією оцінок у світлі нових інцидентів.

2. Обмежений набір сценаріїв та один кейс. У тестуванні розглядалося 5 типових сценаріїв для однієї архітектури. У реальній організації:

– сценаріїв буде більше (десятки/сотні);

– з’являться міжсервісні та міжхмарні залежності;

– потрібна автоматизація збору інформації (інтеграція з SCC, SIEM, CMDB).

Подальший розвиток методики може включати:

– розширення бібліотеки типових сценаріїв для різних сервісів (GKE, BigQuery, Pub/Sub тощо);

– часткову автоматизацію формування початкових (P, I) за станом конфігурацій.

3. Відсутність прямої прив’язки до фінансових показників. Поточна реалізація обмежується бальними шкалами (1–5), без прямого перетворення в грошові показники. Для управлінських рішень іноді потрібні саме:

– очікувані річні збитки;

– розподіли можливих втрат.

Подальший розвиток – інтеграція елементів FAIR/ALE: задання для кожного рівня впливу інтервалу можливих фінансових втрат і використання результатів моделі як основи для такого перерахунку.

Отже, за результатами тестування на кейсі Google Cloud і аналізу в цьому підпункті можна сформулювати такі висновки.

1. Методика коректно відображає пріоритети безпеки для веб-застосунку в публічній хмарі: найвищі бали отримують ризики витоку конфіденційних даних, нижчі – сценарії, що впливають переважно на доступність.

2. Гібридний характер моделі (якісно-кількісний) забезпечує баланс між формальністю й практичною застосовністю: з одного боку, використовуються експертні шкали, з іншого – числові результати дозволяють ранжувати ризики, моделювати «до/після» від впровадження контролів і змінювати ваги залежно від бізнес-контексту.

3. Модель є чутливою до змін параметрів, що свідчить про її керованість: зміна ваг та впровадження заходів безпеки (MFA, SCC, WAF тощо) приводять до передбачуваних і логічних змін у значеннях ризиків.

4. Методика є практично придатною для хмарних середовищ, оскільки безпосередньо враховує специфіку Google Cloud (VPC, IAM, KMS, SCC, Cloud Storage, Cloud SQL) і може бути перенесена на інші платформи з мінімальною адаптацією.

5. Основні обмеження пов’язані з суб’єктивністю експертних оцінок, обмеженим набором сценаріїв і відсутністю прямої фінансової інтерпретації, що відкриває напрямки для подальших досліджень і розширення роботи.

У цілому запропоновану методику можна вважати ефективною та доцільною для використання як у дослідницькому контексті, так і як основа для побудови практичної системи оцінки кіберризиків у хмарних сервісах на рівні організації.

ВИСНОВКИ

В кваліфікаційній роботі розв’язано актуальну задачу підвищення ефективності методики оцінки кіберризиків в хмарних сервісах. При цьому отримано наступні результати.

1. У роботі узагальнено сучасний стан кіберризиків у хмарних сервісах: показано, що поєднання мультиорендності, розподіленої інфраструктури, моделі спільної відповідальності та людського фактора формує специфічний профіль загроз, який потребує окремих підходів до оцінки ризиків, відмінних від традиційних дата-центрів.

2. Запропоновано системний набір критеріїв оцінки кіберризиків у хмарних сервісах, що включає ймовірність реалізації загрози, вплив на конфіденційність, цілісність і доступність інформаційних активів, хмарні особливості та організаційні чинники. Це дозволило формалізувати вимоги до оцінки ризику саме в контексті хмарних технологій.

3. Розроблено гібридну модель оцінки кіберризиків, у якій інтегральний показник ризику обчислюється як добуток ймовірності інциденту та зваженого впливу за складовими CIA. Модель поєднує якісні експертні оцінки з кількісними бальними шкалами та дає змогу гнучко налаштовувати ваги залежно від пріоритетів організації, що робить її сумісною з вимогами ISO/IEC 27005.

4. На базі тестового проєкту в Google Cloud Platform проведено практичне впровадження й тестування методики: сформовано перелік активів і типових сценаріїв загроз, виконано розрахунок ризиків для реалістичної архітектури веб-застосунку, продемонстровано, що модель коректно ранжує ризики і чутливо реагує на зміну ваг та впровадження захисних заходів.

5. Показано, що запропонована методика є ефективною та придатною для практичного використання: вона забезпечує прозоре ранжування ризиків, підтримує моделювання ефекту від заходів безпеки та може бути інтегрована в процеси управління інформаційною безпекою організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cloud, H. (2011). The nist definition of cloud computing. National institute of science and technology, special publication, 800 (2011), 145. https://csrc.nist.gov/pubs/sp/800/145/final

2. CSA Security Guidance for Critical Areas of Focus in Cloud Computing. Режим доступу. https://cloudsecurityalliance.org/research/guidance

3. Catteddu, D. (2009, December). Cloud Computing: benefits, risks and recommendations for information security. In Iberic Web Application Security Conference. Berlin, Heidelberg: Springer Berlin Heidelberg. https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Computing%20Security%20Risk%20Assessment.pdf

4. Types Of Cloud Computing. Режим доступу. https://cloudiofy.com/types-of-cloud-computing/

5. Simmon, E. (2018). Evaluation of cloud computing services based on NIST SP 800-145. NIST Special Publication, 500 (322). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.500-322.pdf

6. Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. NIST special publication, 500 (2011), 292. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

7. What is ISO 27005? https://www.itgovernanceusa.com/cyber-security-solutions/iso27001/iso-27005

8 Assessing and Managing Information Security Risks. Режим доступу. https://www.k9security.io/assessing-and-managing-information-security-risks/

9. Top Risk Management Frameworks To Use. Режим доступу: https://www.splunk.com/en_us/blog/learn/risk-management-frameworks.html

10. Cayirci, E., Garaga, A., Santana, A., & Roudier, Y. (2014, December). A cloud adoption risk assessment model. In 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing (pp. 908-913). IEEE.

11. RISK MANAGEMENT STANDARDS. https://www.enisa.europa.eu/sites/default/files/publications/O.7.2-T2-Risk_Management_standards.pdf

12. Dempsey, K. L., Johnson, L. A., Scholl, M. A., Stine, K. M., Jones, A. C., Orebaugh, A., ... & Johnston, R. (2011). Information security continuous monitoring (ISCM) for federal information systems and organizations. Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication 800-137.pdf

13. Robyn Ferreira. Continuous Monitoring and Frameworks: A Web of Security Vigilance. Режим доступу: https://scytale.ai/resources/continuous-monitoring-and-frameworks-a-web-of-security-vigilance

14. Cloud Security Assessment Tools: How to Find the Right Fit. Режим доступу: https://cymulate.com/blog/cloud-security-assessment-tools

15. Cloud security and AI protection. https://cloud.google.com/security/products/security-command-center

16. Automating FAIR™. Режим доступу: https://safe.security/the-fair-standard/

17. Top 9 Cloud Compliance Tools in 2025. Режим доступу: https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-compliance-tools/

18. G. Gatti, J. M. J. Valero, M. Gil Pérez and C. Basile, "Holistic Cyber Risk Assessment in the Cloud Continuum: A Multi-Layer, Multi-Domain Approach," in *IEEE Access*, vol. 13, pp. 180593-180612, 2025, doi: 10.1109/ACCESS.2025.3622915

19. Annunziata, G., Sheykina, A., Palomba, F., De Lucia, A., Catolino, G., & Ferrucci, F. (2024, June). Security risk assessment on cloud: a systematic mapping study. In *Proceedings of the 28th international conference on evaluation and assessment in software engineering*, pp. 604-613.

20. Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information security risk assessment methods in cloud computing: Comprehensive review. *Journal of Computer Information Systems*, 1-28.

21. Sabri, A. Q., & Dahlan, H. B. M. (2025). Decision-Making Model for Risk Assessment in Cloud Computing Using the Enhanced Hierarchical Holographic Modeling. *Computers*, *14*(11), 491.

22. Kumari, N. S., & Vurukonda, N. (2024). Cyber Security Risk Assessment Framework for Cloud Customer and Service Provider. *International Journal of Advanced Computer Science & Applications*, *15*(12).

23. Zbořil, M. (2022). Risk Assessment Method of Cloud Environment. *Computing and Informatics*, *41*(5), 1186-1206.

24. Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. *IEEE Access*, *9*, 20717-20735.

25. AL-QTIEMAT, E. M. A. N., & AL-ODAT, Z. E. Y. A. D. (2024). Examining cloud security: identifying risks and the implemented mitigation strategies. *Journal of Theoretical and Applied Information Technology*, *102*(7).

26. ENISA – European Union Agency for Cybersecurity. (2022). *Risk management standards*. ENISA. https://www.enisa.europa.eu/publications/risk-management-standards

27. ENISA – European Union Agency for Cybersecurity. (2021). *Cloud security for healthcare services*. ENISA. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cloud%20Security%20for%20Healthcare%20Services.pdf

28. ENISA – European Union Agency for Cybersecurity. (2023). *Technical implementation guidance on cybersecurity risk management measures*. ENISA. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

29. Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. *Future Internet*, *14*(1), 11.

30. Amini, A., & Jamil, N. (2018, May). A comprehensive review of existing risk assessment models in cloud computing. In *Journal of Physics: Conference Series* (Vol. 1018, No. 1, p. 012004). IOP Publishing.

31. Albakri, S. H., Shanmugam, B., Samy, G. N., Idris, N. B., & Ahmed, A. (2014). Security risk assessment framework for cloud computing environments. *Security and Communication Networks*, *7*(11), 2114-2124.

32. Drissi, S., Chergui, M., & Khatar, Z. (2025). A Systematic Literature Review on Risk Assessment in Cloud Computing: Recent Research Advancements. *IEEE Access*. Doi: *10.1109/ACCESS.2025.3561123*

Додаток А.
Копії публікацій

ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
КАФЕДРА СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ
ГРОМАДСЬКА ОРГАНІАЦІЯ «КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

науково-практичний симпозіум

ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ: СИСТЕМИ ТА РІШЕННЯ (ТІР:СТ – 2025)

24 жовтня 2025 року
м. Тернопіль

ЗМІСТ

УДК 004.056

Наталія ЯЦКІВ, Аліна МИКОЛАЙСЬКА

Західноукраїнський національний університет

КЛАСИФІКАЦІЯ КІБЕРРИЗИКІВ У ХМАРНИХ СЕРВІСАХ

Вступ. Широке впровадження хмарних сервісів у бізнес-процеси, державне управління та повсякденну діяльність користувачів супроводжується зростанням кількості та складності кіберризиків. Модель спільної відповідальності провайдера та споживача, багатокористувацьке середовище, віртуалізація ресурсів, географічно розподілене зберігання даних і автоматизоване масштабування створюють якісно новий простір загроз, який не повністю покривається традиційними підходами до інформаційної безпеки.

У таких умовах особливої ваги набуває системна класифікація кіберризиків у хмарних сервісах, що дозволяє структурувати загрози, уразливості й наслідки інцидентів, узгодити підходи до оцінки ризиків і обґрунтувати вибір організаційних та технічних заходів захисту відповідно до стандартів ENISA, NIST, ISO/IEC 27001 [1].

Мета. Систематизувати та обґрунтувати класифікацію кіберризиків у хмарних сервісах як основу для подальшої розробки методики їх кількісної та якісної оцінки.

1. Підходи до класифікації кіберризиків у хмарних сервісах

Класифікація кіберризиків у хмарних сервісах може здійснюватися за різними критеріями: за джерелом походження (зовнішні/внутрішні), за природою (технічні, організаційні, правові), за об'єктом впливу (дані, сервіси, інфраструктура, користувачі), за етапами життєвого циклу послуг (планування, міграція, експлуатація, виведення з експлуатації). ENISA у своїх звітах пропонує ризик-орієнтовану класифікацію, яка базується на сценаріях інцидентів, типах активів і виявлених уразливостях, що дозволяє охопити як технологічні, так і організаційні аспекти [1].

NIST застосовує ризик-орієнтований підхід, що поєднує класифікацію ризиків з моделлю загроз та рекомендаціями щодо контролів, орієнтуючись на публічні хмарні середовища та модель спільної відповідальності [2].

У контексті хмарних сервісів доцільно будувати класифікацію кіберризиків у кількох взаємопов'язаних вимірах:

- за рівнем (організаційний, технологічний, бізнес-рівень);
- за доменом (безпека даних, безпека інфраструктури, ідентифікація та доступ, відповідність, безперервність бізнесу);
- за моделлю використання (SaaS, PaaS, IaaS) та розгортання.

Такий багатовимірний підхід дозволяє пов'язати виявлені ризики з конкретними сервісними моделями, відповідальністю сторін, нормативними вимогами та наборами контролів [3].

2. Організаційно-політичні ризики

До організаційно-політичних ризиків належать ризики, пов'язані з управлінням, контрактами, відповідністю і взаємовідносинами між провайдером та клієнтом. ENISA

виокремлює, зокрема, ризики: залежність від постачальника, втрата контролю над даними й процесами, виклики відповідності, репутаційні ризики через дії «сусідів» по хмарі, припинення надання сервісів або їх поглинання іншим провайдером, проблеми ланцюга постачання.

Залежність від постачальника проявляється у складності або неможливості міграції даних і сервісів до іншого провайдера через закриті формати даних, нестандартні API, відсутність процедур повернення або знищення даних. Це призводить до довготривалої залежності, підвищення витрат і ускладнює реагування на інциденти безпеки чи зміну політик провайдера. Ризик втрати контролю пов'язаний із передачею значної частини функцій управління IT-інфраструктурою зовнішній організації; у результаті замовник може не мати достатньої прозорості щодо реального стану безпеки, журналів доступу, механізмів резервного копіювання та відновлення [1].

Ризики відповідності стосуються невідповідності регуляторним вимогам (GDPR, національне законодавство, галузеві стандарти), особливо за умови розміщення даних у різних юрисдикціях та використання субпідрядників. Відсутність прозорості щодо місця зберігання та обробки даних, субобробників та сертифікацій провайдера ускладнює оцінку відповідності. Такі ризики класифікуються як бізнес-критичні, бо можуть призвести до значних штрафів та обмеження діяльності організації [2].

3. Технічні ризики інфраструктури та віртуалізації

Технічні ризики охоплюють уразливості інфраструктури, гіпервізора, механізмів ізоляції віртуальних машин, мережевої сегментації, засобів моніторингу й управління ресурсами. У хмарних середовищах особливо критичними є ризики порушення ізоляції між тенантами (наприклад, через уразливості гіпервізора), некоректної конфігурації мережевих політик, а також зловживання обчислювальними ресурсами для проведення атак (DDoS, brute force, «cryptojacking» тощо).

До цієї групи належать також ризики, пов'язані з неправильним управлінням ресурсами, помилками у налаштуванні систем балансування навантаження, механізмів авто-масштабування, резервного копіювання та реплікації. Неправильні параметри масштабування можуть призвести як до відмови сервісу, так і до неконтрольованого споживання ресурсів та витрат. ENISA виокремлює сценарії, пов'язані з виснаженням ресурсів, відмовою сервісів та збоями в ланцюгу постачання [4].

Суттєвою групою є ризики управління доступом до панелей адміністрування хмарної платформи, API та інтерфейсів управління. Компрометація цих інтерфейсів (наприклад, через фішинг, повторне використання паролів, відсутність багатофакторної автентифікації) дозволяє зловмиснику змінювати конфігурацію мережі, створювати нові ресурси, отримувати доступ до сховищ даних та журналів. Стандарти NIST та ISO/IEC 27017 наголошують на необхідності чітких політик керування доступом і сегментації адміністративних повноважень між провайдером і клієнтом [2].

4. Ризики безпеки даних та приватності

Ризики безпеки даних у хмарних сервісах пов'язані з конфіденційністю, цілісністю, доступністю та приватністю персональних даних. До них належать: несанкціонований доступ до даних через вразливості застосунків або інтерфейсів,

втрата чи пошкодження даних через помилки реплікації або резервного копіювання, витік даних унаслідок неправильно налаштованих сховищ (наприклад, публічні S3-бакети чи відкриті об'єктні сховища), недостатнє або некоректне шифрування даних «на спокої» та «в транзиті».

Окрему підгрупу становлять ризики приватності та захисту персональних даних, що регулюються стандартами ISO/IEC 27018 та національним/наднаціональним законодавством. До них відносять: незаконну обробку персональних даних, передачу даних у треті країни без належних гарантій, відсутність механізмів реалізації прав суб'єктів даних (право на забуття, переносимість тощо), а також недостатній контроль субобробників провайдера.

Класифікуючи ризики безпеки даних, доцільно розрізняти:

– ризики, пов'язані з конфігурацією (misconfiguration: відкриті сховища, надлишкові права доступу, відсутність шифрування);

– ризики, пов'язані з обробкою та зберіганням (неналежне резервування, недостовірне відновлення, незахищені журнали);

– ризики, пов'язані з життєвим циклом даних (неналежне видалення, повторне використання носіїв, неконтрольований доступ до «сміттєвих» копій).

Такий поділ дозволяє цілеспрямовано підбирати контролі: шифрування, токенізацію, DLP, контроль життєвого циклу даних, аудит доступу, а також вимоги до знищення і повернення даних після завершення контракту [2].

5. Ризики, пов'язані з відповідністю, аудитом і спільною відповідальністю

Хмарна безпека реалізується в рамках моделі спільної відповідальності, де частина контролів належить провайдеру, а частина – клієнту. Неправильне розуміння цієї моделі формує окрему категорію ризиків: організація вважає, що за безпеку повністю відповідає провайдер, і недооцінює власні завдання щодо налаштування сервісів, керування доступом, шифрування, моніторингу та реагування. ISO/IEC 27017 прямо орієнтований на уточнення розподілу повноважень та контролів між сторонами.

Ризики комплаєнсу та аудиту пов'язані з відсутністю або недостатністю доказової бази (логів, звітів, сертифікатів) для підтвердження відповідності регуляторним вимогам і внутрішнім політикам. Якщо провайдер не надає прозорих і стандартизованих механізмів аудиту (регулярні звіти, атестації за ISO/IEC 27001, 27017, SOC 2 тощо), це ускладнює управління ризиками та може призвести до санкцій з боку регуляторів або партнерів.

6. Ризики появи нових типів загроз та еволюції атак

Динамічний характер хмарних середовищ обумовлює появу нових класів загроз, у тому числі тих, що використовують специфічні можливості хмарної інфраструктури:

– «Cybercrime as a Service», коли хмарні ресурси використовуються як платформа для розгортання ботнетів, сервісів DDoS за запитом, ферм для майнінгу криптовалют;

– атаки на метадані і контрольні площини, спрямовані на отримання повного контролю над тенантським середовищем;

– атаки на ланцюги CI/CD та DevOps-процеси, характерні для хмарних

застосунків (контейнерні образи, інфраструктура як код);

– зловживання API, які відкривають доступ до управління ресурсами та даними [5].

Такі ризики важко повністю описати в рамках статичних класифікацій, тому сучасні підходи рекомендують поєднувати базову таксономію ризиків із моделями загроз, що постійно оновлюються. Це дозволяє враховувати появу нових векторів атак без повного перегляду структури класифікації.

Висновки. Класифікація кіберризиків у хмарних сервісах є важливою передумовою ефективної методики їх оцінки. Багатовимірний підхід (за рівнем, доменом, сервісною моделлю, життєвим циклом даних) дозволяє пов'язати конкретні ризики з відповідними контролями, відповідальністю сторін та нормативними вимогами.

Безпека даних і приватність у хмарі вимагають окремої, деталізованої класифікації ризиків. Поділ на ризики конфігурації, обробки, зберігання та життєвого циклу даних дозволяє точніше обирати засоби захисту.

Еволюція хмарних технологій породжує нові типи загроз, що доповнюють традиційні категорії ризиків. Практичне застосування запропонованих класифікацій створює основу для побудови формалізованих методик оцінки кіберризиків у хмарних сервісах, що, у свою чергу, дозволяє обґрунтовано обирати архітектурні рішення, моделі розгортання, інструменти моніторингу та реагування, а також оптимізувати витрати на забезпечення кібербезпеки в умовах зростаючої залежності від хмарних технологій.

Перелік використаних джерел.

1. Cloud Computing Risk Assessment. [Електронний ресурс].- Режим доступу: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

2. Jansen, W. A., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. . [Електронний ресурс].- Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

3. Cloud computing: benefits, risks and recommendations for information security. [Електронний ресурс].- Режим доступу: https://www.enisa.europa.eu/sites/default/files/all_files/ENISA%20-%20Cloud%20Computing%20-%20final.pdf

4. Cayirci, E., Garaga, A., Santana de Oliveira, A., & Roudier, Y. (2016). A risk assessment model for selecting cloud service providers. Journal of Cloud Computing, 5 (1), 14.

5. Marinos, L. (2016). ENISA Threat Taxonomy: A tool for structuring threat information. ENISA,Heraklion. [Електронний ресурс].- Режим доступу: https://www.um.es/documents/2096502/4937674/Enisa.pdf/2374a6a9-3c9d-422c-b5ad-b047a2fb8568




ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КІБЕРБЕЗПЕКИ
ГРОМАДСЬКА ОРГАНІАЦІЯ «КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму
"ЗАХИСТ'ІНФОРМАЦІЇ'2025"

28 листопада 2025
Тернопіль

УДК 004.056

Наталія ЯЦКІВ, Аліна МИКОЛАЙСЬКА

Західноукраїнський національний університет

МОДЕЛЬ ОЦІНКИ КІБЕРРИЗИКІВ У ХМАРНИХ СЕРВІСАХ

Вступ. Активне впровадження хмарних сервісів у бізнес–процеси організацій різних масштабів зумовлює різке зростання залежності активів від інфраструктури сторонніх провайдерів. Концентрація даних і обчислювальних ресурсів у хмарі, розподіленість компонентів, використання API та автоматизованих DevOps–процесів створюють специфічний профіль кіберризиків, що суттєво відрізняється від класичних IT–середовищ. Існуючі рамки управління ризиками (NIST SP 800–30/800–37, ISO/IEC 27005, ENISA Cloud Computing Risk Assessment, CSA Cloud Controls Matrix) задають загальні принципи і процеси, але потребують адаптації до контексту конкретних хмарних сервісів, моделей розгортання та розподілу відповідальності. Це обумовлює необхідність розробки спеціалізованої моделі оцінки ризиків, яка враховує особливості архітектури хмарних рішень, типів сервісів (IaaS/PaaS/SaaS), юридичних вимог, динаміки навантажень та можливостей безперервного моніторингу [1].

Мета. Розробити формалізовану модель оцінки ризиків у хмарних сервісах, що дозволяє системно і відтворювано визначати рівень кіберризику для різних сценаріїв використання хмари та обґрунтовувати вибір заходів захисту.

1. Методологічні засади побудови моделі

У якості методологічної основи моделі доцільно використати процесний підхід ISO/IEC 27005 до управління ризиками інформаційної безпеки (ідентифікація, аналіз, оцінка, обробка, моніторинг і перегляд ризиків) у поєднанні з NIST SP 800–30/800–37, що деталізують етапи оцінки ризику та вбудовують їх у життєвий цикл інформаційних систем. Для хмарного контексту додаються рекомендації ENISA щодо аналізу переваг і ризиків хмарних технологій та практики CSA Cloud Controls Matrix (CCM), яка надає структурований каталог контролів для IaaS, PaaS і SaaS [2].

Ключовою концепцією моделі є представлення ризику як функції від трьох груп параметрів:

- характеристик активів (цінність, критичність, залежність від хмари);
- параметрів загроз і вразливостей (ймовірність виникнення інцидентів, рівень експозиції, ефективність існуючих контролів);
- контексту хмарної архітектури (тип сервісу, модель розгортання, модель спільної відповідальності, географія та юрисдикція розміщення даних).

Модель повинна забезпечити можливість як якісної (категорії «низький–середній–високий»), так і кількісної/напівкількісної (бальна шкала, інтегральний індекс) оцінки ризиків.

2. Структура моделі оцінки ризиків

Запропоновану модель доцільно будувати багаторівневою, виділяючи щонайменше три рівні.

Рівень бізнес–процесів – аналіз впливу відмови або компрометації хмарних сервісів на виконання ключових бізнес–функцій, фінансові показники, репутацію, відповідність нормативним вимогам.

Рівень хмарних сервісів – оцінка ризиків для конкретних сервісів (облікові записи, сховища, віртуальні машини, контейнерні платформи, бази даних, serverless–функції тощо).

Рівень технічної інфраструктури та контролів – урахування стану мережевих, криптографічних, ідентифікаційно–авторизаційних, моніторингових та інших засобів безпеки, у т.ч. специфічних для хмари (IAM–політики, security–групи, KMS, WAF, CASB).

Для кожного хмарного сервісу вводиться набір атрибутів: тип моделі (IaaS/PaaS/SaaS), модель розгортання (публічна, приватна, гібридна, multi–cloud), категорія даних (персональні, фінансові, комерційна таємниця), вимоги до конфіденційності, цілісності та доступності. На основі цих атрибутів формується профіль ризику сервісу, який визначає релевантний набір загроз (наприклад, витік даних через неправильно налаштоване сховище, атаки на API, компрометація облікових записів адміністратора, вразливості в ланцюгу постачання, збої провайдера).

3. Етапи процесу оцінки ризиків у моделі

1. Підготовка та визначення контексту. На цьому етапі визначаються межі оцінки (організаційний підрозділ, система, проєкт), перелік хмарних сервісів та провайдерів, регуляторні вимоги (GDPR, національне законодавство, галузеві стандарти), а також ролі й відповідальність сторін (клієнт, хмарний провайдер, інтегратор). Частина інформації може бути зібрана на основі опитувальника CSA CAIQ, що формалізує питання до провайдера [3].

2. Ідентифікація активів, загроз і вразливостей. Формується реєстр активів, пов'язаних із хмарою (дані, сервіси, облікові записи, ключі шифрування, журнали подій). Для кожної категорії активів визначаються можливі загрози (технічні, організаційні, юридичні) на основі ENISA–каталогів ризиків та типових сценаріїв атак на хмару. Вразливості класифікуються за джерелом: конфігураційні помилки, недоліки процесів, людський фактор, залежність від третьої сторони, слабкі або відсутні контролі.

3. Аналіз і розрахунок ризиків. Для кожного сценарію ризику оцінюється ймовірність реалізації P та величина впливу I на конфіденційність, цілісність та доступність, а також на юридичні та наслідки відповідності. На практиці модель може використовувати напівкількісний підхід:

$$R = P \cdot I \cdot W,$$

де W – ваговий коефіцієнт, що враховує критичність бізнес–процесу або особливі вимоги до даних (наприклад, персональні дані, дані платіжних карток). Значення P та I задаються на шкалі (наприклад, 1–5 або 1–10), а результат нормується до уніфікованої шкали ризику (низький, середній, високий, критичний). У більш складному варіанті можливе використання методів багатокритеріальної оптимізації або нечіткої логіки для точнішого урахування невизначеності [4].

4. Оцінка ефективності існуючих контролів. На цьому кроці ризики коригуються з урахуванням реалізованих заходів безпеки, зіставлених із доменами CSA CCM (ідентичність та доступ, шифрування, безпека віртуалізації, логування та моніторинг, управління змінами тощо). Для кожного контролю встановлюється рівень зрілості/ефективності, що дозволяє переходити від «вихідного» (інгерентного) ризику до «залишкового».

5. Пріоритизація та формування плану обробки ризиків. Ризики ранжуються за значенням інтегрального показника R, додатково враховується можливість їхнього агрегування на рівні бізнес–процесів і хмарних сервісів. Для пріоритетних ризиків визначаються сценарії обробки (зменшення, уникнення, передавання, прийняття) відповідно до ISO/IEC 27005 та ISO/IEC 27001, а також перелік рекомендованих технічних і організаційних заходів.

6. Безперервний моніторинг та перегляд оцінок. Оскільки хмарні середовища є високо динамічними, модель передбачає регулярне оновлення оцінок ризику на основі даних моніторингу (журнали доступу, події безпеки, результати сканування вразливостей, звіти провайдера). Інтеграція з SIEM/SOAR–системами та хмарними засобами моніторингу дозволяє автоматизувати частину розрахунків та оперативно реагувати на зміну профілю загроз.

4. Формалізація ризику та індекс хмарної безпеки

Для практичної реалізації моделі доцільно запровадити індекс хмарної безпеки для кожного сервісу або бізнес–процесу. Такий індекс може мати вигляд зваженої суми окремих компонентів ризику:

$$R_{cloud} = \sum_j w_j \cdot R_j,$$

де R_j – ризик за окремим сценарієм (наприклад, витік даних, відмова сервісу, порушення відповідності;

w_j – вагові коефіцієнти, що відображають пріоритети організації (наприклад, більша вага для ризиків, пов'язаних із персональними даними або безперервністю бізнесу).

Таке формулювання дозволяє агрегувати ризики з різних джерел та відображати їх у єдиному показнику, що зручно для представлення керівництву.

На основі значень R_{cloud} визначаються «діапазони дій»:

– зелений рівень – ризик прийнятний, достатньо підтримувати поточні контролі та здійснювати моніторинг;

– жовтий рівень – потрібна оптимізація конфігурацій і додаткові компенсуючі заходи;

– червоний рівень – необхідні невідкладні технічні та організаційні зміни, можлива зміна моделі використання хмари або провайдера.

5. Інтеграція моделі з нормативними рамками та практикою

Розроблювана модель повинна бути сумісною з існуючими стандартами та рамками, щоб її результати могли використовуватися в системах менеджменту інформаційної безпеки (ISMS) і звітності для аудиту. По–перше, вона має

підтримувати узгодження з ISO/IEC 27001/27002, ISO/IEC 27017 (контролі для хмарних сервісів) та ISO/IEC 27018 (захист персональних даних у хмарі). По–друге, показники та категорії ризику повинні легко відображатися на домени CSA CCM і опитувальники CAIQ, що спрощує оцінку постачальників та участь у програмах на кшталт CSA STAR [5].

Крім того, модель має враховувати підходи ENISA до оцінки ризиків у хмарі, де ризики ранжуються за ймовірністю й впливом та супроводжуються рекомендаціями щодо заходів безпеки для різних типів користувачів (малі/середні підприємства, великі організації, постачальники послуг). Це дозволяє забезпечити порівнюваність результатів оцінки з європейськими практиками та полегшує комунікацію з регуляторами й партнерами.

Висновки. Хмарні сервіси формують специфічний профіль кіберризиків, обумовлений мультитенантністю, розподіленою архітектурою, високим рівнем автоматизації та розподілом відповідальності між провайдером і клієнтом; тому використання лише загальних підходів до управління ризиками без спеціалізованої адаптації є недостатнім.

Розроблена модель оцінки ризиків у хмарних сервісах базується на міжнародно визнаних стандартах (ISO/IEC 27005, NIST SP 800–30/800–37) і рекомендаціях ENISA та CSA, але доповнюється багаторівневою структурою (бізнес–процеси – хмарні сервіси – технічні контролі) та механізмами формалізованого розрахунку інтегрального показника ризику.

Описаний процес оцінки ризиків (визначення контексту, ідентифікація активів, загроз і вразливостей, аналіз і розрахунок ризиків, урахування ефективності контролів, пріоритизація та безперервний моніторинг) забезпечує відтворюваність результатів, підтримує як якісний, так і напівкількісний аналіз і може бути інтегрований у існуючі ISMS–процеси.

Запровадження індексу хмарної безпеки та узгодження моделі з рамками ISO/IEC та ENISA дозволяє організаціям не лише оцінювати поточний рівень ризику, але й обґрунтовано приймати рішення щодо вибору/зміни хмарних провайдерів, оптимізації конфігурацій сервісів і планування заходів із підвищення кіберстійкості хмарної інфраструктури.

Перелік використаних джерел.

1. Force, Joint Task. "Risk management framework for information systems and organizations". NIST Special Publication 800 (2018): 37.

2. Cloud Computing Risk Assessment. [Електронний ресурс].- Режим доступу: https://www.enisa.europa.eu/publications/cloud–computing–risk–assessment

3. Cloud Controls Matrix and CAIQ v4. [Електронний ресурс].- Режим доступу: https://cloudsecurityalliance.org/artifacts/cloud–controls–matrix–v4

4. Information Security. NIST Special Publication 800–30. [Електронний ресурс].- Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800–30r1.pdf

5. Ali, T., Al–Khalidi, M., & Al–Zaidi, R. (2024). Information security risk assessment methods in cloud computing: Comprehensive review. Journal of Computer Information Systems, 1–28.