Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: «Механізм оцінювання ефективності захисту персональних даних в хмарних середовищах»

Виконавець: студентка IV курсу, групи КБ-43

_____ **Анастасія РАМУЛЬ**
(підпис) (ім'я, прізвище)

	Підпис	**Ім'я ПРІЗВИЩЕ**
Керівник		Сергій ДАКОВ
Нормоконтроль		Олександр ТОРОШАНКО

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
29 листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студентці **КБ-43** **Рамуль Анастасії Дмитрівні**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Механізм оцінювання ефективності захисту персональних даних в хмарних середовищах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Хмарні обчислення, зберігання персональних даних, моделі загроз, стандарти безпеки, критерії оцінки ефективності захисту.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з основами хмарних обчислень , моделями розгортання хмарних сервісів, ідентифікувати типові ризики та вразливості персональних даних у таких середовищах , розробити механізм оцінювання ефективності захисту даних з урахуванням обраних метрик.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблено механізм оцінювання ефективності захисту персональних даних у хмарних середовищах.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видав _____ Сергій ДАКОВ
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Анастасія РАМУЛЬ
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 22.01.2025	*виконано*
2	Аналіз літератури	23.01.2025 – 11.02.2025	*виконано*
3	Обґрунтування вибору рішення	12.02.2025 – 15.02.2025	*виконано*
4	Формування критеріїв та метрик оцінювання безпеки в хмарних середовищах	16.02.2025 – 04.03.2025	*виконано*
5	Розробка механізму оцінювання з урахуванням MCDA та AHP	05.03.2025 – 21.03.2025	*виконано*
6	Реалізація десктоп-додатку для проведення оцінювання	22.03.2025 – 08.04.2025	*виконано*
7	Тестування системи на прикладі AWS, Azure, GCP та формування рекомендацій	09.04.2025 – 10.05.2025	*виконано*
8	Оформлення пояснювальної записки	11.05.2025 – 27.05.2025	*виконано*
9	Підготовка до захисту	28.05.2025 – 13.06.2025	*виконано*

Завдання видав _____ Сергій ДАКОВ
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Анастасія РАМУЛЬ
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 56 сторінок , включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки та список джерел. Крім того, робота містить 2 додатки із загальною кількістю сторінок 14. У пояснювальній записці кваліфікаційної роботи міститься11 рисунків і 2 таблиці.

Метою роботи є підвищення ефективності захисту персональних даних у хмарних середовищах шляхом розробки та впровадження механізму їх оцінювання.

Для досягнення зазначеної мети поставлено наступні завдання:

– Аналіз існуючих методів захисту персональних даних у хмарних середовищах і виявлення їх слабких місць;

– Розробка концепції механізму оцінювання ефективності захисту персональних даних;

– Реалізація запропонованого механізму на практиці та перевірка його дієвості ;

– Формулювання практичних рекомендацій щодо покращення захисту персональних даних.

Об’єктом дослідження є процес оцінювання ефективності захисту персональних даних у хмарних середовищах.

Предметом дослідження є методи оцінювання ефективності захисту персональних даних у хмарних середовищах.

Практична цінність роботи полягає у створенні механізму, що дозволяє хмарним провайдерам або користувачам проводити об’єктивну оцінку рівня безпеки персональних даних з можливістю візуалізації та генерації рекомендацій на основі результатів.

Ключові слова: хмарні обчислення, персональні дані, захист інформації, інформаційна безпека, хмарний провайдер, механізм оцінювання.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AHP	–	Analytic Hierarchy Process — метод аналітичної ієрархії
AWS	–	Amazon Web Services — хмарна платформа Amazon
GDPR	–	General Data Protection Regulation — Загальний регламент захисту даних (ЄС)
GCP	–	Google Cloud Platform — хмарна платформа Google
IaaS	–	Infrastructure as a Service — інфраструктура як послуга
ISO/IEC 27001	–	Міжнародний стандарт управління інформаційною безпекою
MCDA	–	Multi-Criteria Decision Analysis — багатокритеріальний аналіз
MFA	–	Multi-Factor Authentication — багатофакторна автентифікація
NIST	–	National Institute of Standards and Technology — Національний інститут стандартів і технологій (США)
PaaS	–	Platform as a Service — платформа як послуга
SaaS	–	Software as a Service — програмне забезпечення як послуга
ТЗІ	–	Технічний захист інформації

ВСТУП

Стрімкий розвиток інформаційних технологій та широке використання хмарних обчислень кардинально змінили спосіб зберігання та обробки персональних даних. Хмарні середовища пропонують масштабованість, гнучкість та ефективність, але водночас створюють низку проблем, пов'язаних із безпекою та захистом даних. Безпека персональних даних, що зберігаються в хмарі, стає центральним питанням для користувачів, організацій та регуляторів, особливо в контексті жорстких вимог міжнародних стандартів та національних законів про захист даних.

Незважаючи на наявність численних технічних рішень для захисту - таких як шифрування, аутентифікація, сегментація мережі та контроль доступу - бракує чітких та об'єктивних методологій для оцінки ефективності цих заходів у контексті хмарних платформ. Існує потреба у розробці системного підходу до вимірювання та порівняння рівня захисту, що враховує не тільки технічні параметри, але й організаційні та регуляторні аспекти.

Аналіз існуючої наукової літератури та матеріалів міжнародних конференцій (IEEE, ACM, ENISA та ін.) показує, що більшість досліджень присвячено окремим аспектам безпеки хмарних технологій, таким як вибір алгоритмів шифрування або моделей управління ідентифікацією.Значно менше уваги приділяється розробкам, що дозволяють кількісно оцінити ефективність впроваджених заходів, а також інтегрувати цю оцінку у внутрішні процеси безпеки хмарного провайдера. Це створює прогалину в знаннях, на заповнення якої спрямована дана робота.

Актуальність теми полягає саме в цій прогалині: розробці практично застосовного механізму оцінювання ефективності захисту персональних даних, який дозволяє організаціям не лише провести внутрішній аудит безпеки, а й приймати обґрунтовані рішення щодо вдосконалення захисту у хмарному середовищі.

Метою кваліфікаційної роботи є підвищення ефективності захисту персональних даних у хмарних середовищах шляхом розробки та впровадження механізму їх оцінювання, що дозволить виявити слабкі місця та запропонувати рекомендації щодо їх покращення.

Основні завдання:

– Аналіз існуючих методів захисту персональних даних у хмарних середовищах і виявлення їх слабких місць;

– Розробка концепції механізму оцінювання ефективності захисту персональних даних;

– Реалізація запропонованого механізму на практиці та перевірка його дієвості ;

– Формулювання практичних рекомендацій щодо покращення захисту персональних даних.

Об'єкт дослідження:

Процес оцінювання ефективності захисту персональних даних у хмарних середовищах.

Предмет дослідження:

Методи оцінювання ефективності захисту персональних даних у хмарних середовищах.

Практична новизна. Розроблений механізм пропонує структурований і практичний підхід до оцінки заходів захисту, включаючи кількісну шкалу для вимірювання ефективності. На відміну від існуючих описових моделей, тут пропонується інтегрована модель оцінки, яка об'єднує технічні, організаційні та регуляторні аспекти безпеки. Механізм може бути застосований в реальних умовах IT-відділами, аудиторами та організаціями, що підлягають контролю з боку регуляторних органів.

Сфера застосування. Отримані результати можуть бути використані організаціями, що використовують хмарні платформи для внутрішнього аудиту та планування безпеки. механізм був протестований шляхом застосування на реальній платформі.

РОЗДІЛ 1
АНАЛІЗ СТАНУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ХМАРНИХ СЕРЕДОВИЩАХ

1.1. Особливості хмарних обчислень та класифікація хмарних моделей

Хмарні технології - це системи, які дозволяють віддалено обробляти та зберігати дані, пропонуючи обчислювальні ресурси та потужності користувачам у вигляді інтернет-сервісів [1]. Ці технології забезпечують повсюдний і зручний мережевий доступ до спільного набору обчислювальних та інформаційних ресурсів, таких як мережі передачі даних, сервери, бази даних, додатки і сервіси, які можуть бути швидко надані і вилучені на вимогу користувача, при цьому операційні витрати і запити до постачальника послуг мінімальні .

Концепція хмарних обчислень виникла ще в 1960-х роках, коли Джон Маккарті запропонував, що в майбутньому комп'ютерна обробка даних буде здійснюватися за допомогою загальнодоступних утиліт. Сьогодні під хмарними обчисленнями зазвичай розуміють надання обчислювальних ресурсів і потужностей користувачам у вигляді інтернет-сервісів. Ці ресурси надаються в «чистому» вигляді, тобто користувачі можуть навіть не знати, які комп'ютери обробляють їхні запити або які операційні системи використовуються [2].

Хмарні обчислення мають кілька важливих характеристик, які вирізняють їх як трансформаційну парадигму в сфері інформаційних технологій. Нижче наведені ключові особливості.

Самообслуговування на вимогу дозволяє користувачам самостійно обирати і використовувати різноманітні обчислювальні можливості і ресурси (наприклад, мережеві сховища, бази даних, обчислювальні потужності і розподіл пам'яті). Більше того, користувачі мають можливість динамічно змінювати свій набір ресурсів, не потребуючи явної згоди постачальника послуг.

Висока еластичність та гнучкість сервісів забезпечується архітектурою хмарних обчислень, яка дозволяє безперешкодно коригувати обчислювальні ресурси у відповідь на мінливі запити користувачів. У випадках підвищеного навантаження на сервіси розподіл ресурсів може бути оперативно збільшений, тоді як у періоди зниження попиту непотрібні ресурси можуть бути ефективно дерозподілені. Ця можливість позбавляє організації необхідності витрачати час і фінансові ресурси на придбання та налаштування додаткового обладнання та програмного забезпечення, яке в майбутньому може рідко знадобитися.

Інтеграція ресурсів хмарного провайдера дозволяє об’єднувати обчислювальні ресурси в єдине ціле, полегшуючи динамічний перерозподіл як фізичних, так і віртуальних ресурсів між кінцевими користувачами. Використовуючи сучасні технології віртуалізації, хмарні провайдери можуть легко нарощувати потужності та замінювати несправне обладнання без шкоди для продуктивності та надійності [1].

Облік споживання ресурсів та модель оплати за фактом використання передбачає, що користувачі оплачують тільки ті послуги, якими вони користуються, включаючи такі показники, як обсяги передачі даних, використання пропускної здатності та обсяги зберігання даних. Такий підхід сприяє економічній ефективності для користувачів.

Використання передових технологій у центрах обробки даних, якими керують провайдери хмарних послуг, зазвичай використовують більш передові та інноваційні технології, ніж традиційні центри обробки даних, які пропонують послуги оренди серверів, або ті, що управляються внутрішніми силами організацій. Ці технології дозволяють автоматизовано оптимізувати використання ресурсів, значно зменшуючи операційні витрати та витрати на обслуговування порівняно зі звичайними дата-центрами [3].

Високий рівень доступності досягається завдяки розподіленій інфраструктурі дата-центрів, розташованих у різних регіонах. Такий підхід забезпечує користувачам постійний і стабільний доступ до сервісів незалежно від їх географічного розташування.

Відмовостійкість реалізується за рахунок багаторівневого резервування. Кожен центр обробки даних має незалежне джерело живлення та мережеве підключення. Безперервний моніторинг стану кожного центру обробки даних дозволяє автоматично перенаправляти запити на альтернативні центри в разі збою, а також реплікувати дані між різними місцями, що гарантує безперебійну роботу навіть під час виходу з ладу всього центру обробки даних [4].

Незважаючи на численні переваги, які надають хмарні технології, існує кілька обмежень:

Залежність від підключення до Інтернету зумовлює, що ефективна робота хмарних сервісів залежить від надійного підключення до Інтернету. Однак ця залежність є менш проблематичною в сучасному суспільстві, оскільки доступ до Інтернету стає все більш повсюдним.

Зростаюча вразливість до кіберзагроз становить значний виклик, особливо з огляду на те, що хмарні системи є основними цілями для різних форм атак. Несанкціонований доступ залишається критичною проблемою, що дозволяє зловмисникам використовувати конфіденційну інформацію та порушувати цілісність системи. Крім того, значний ризик становлять розподілені атаки на відмову в обслуговуванні (DDoS), здатні перевантажити хмарні ресурси і, таким чином, поставити під загрозу як доступність даних, так і загальну безпеку [3].Хмарні обчислення можна систематично розділити на кілька категорій: публічні хмари, приватні хмари, гібридні хмари та хмари спільнот. Ретельне вивчення відмінностей між цими різними типами хмар дозволяє виявити важливі характеристики та наслідки для їх використання [2].

Приватна хмара - це інфраструктура, призначена виключно для використання однією організацією. Це означає, що вона може обслуговувати декількох споживачів, наприклад, різні підрозділи організації, а також потенційно її клієнтів і підрядників.

Управління приватною хмарою може покладатися на саму організацію, третю сторону або комбінацію обох. Важливо, що ця інфраструктура може

фізично перебувати в межах юридичної юрисдикції організації, а може бути розташована за її межами.

На противагу цьому, публічна хмара характеризується доступністю для широкого використання широким загалом. Право власності, управління та експлуатації може належати комерційним підприємствам, науковим установам, державним органам або їхнім комбінаціям. Публічні хмари перебувають під юрисдикцією відповідних постачальників послуг.

Ця модель, як правило, передбачає оренду програмного забезпечення, інфраструктури або платформ хмарних обчислень на основі принципу «програмне забезпечення як послуга» (SaaS), «інфраструктура як послуга» (IaaS) або «платформа як послуга» (PaaS).

Гібридна хмарна архітектура являє собою інтеграцію двох або більше окремих хмарних інфраструктур - приватних, публічних або громадських - при цьому кожна з них зберігає свої індивідуальні характеристики.

Ці інфраструктури пов'язані між собою за допомогою стандартизованих або приватних технологій передачі даних, що полегшує періодичне використання ресурсів публічної хмари для балансування робочих навантажень. У цій моделі критичні програми та конфіденційні дані надійно зберігаються в приватній хмарі, що належить організації, тоді як у публічному сегменті розміщуються додаткові програми, особливо ті, що є складними, рідко використовуються або потребують регулярних оновлень.

Нарешті, хмара спільноти призначена для використання певною групою споживачів з організацій, які мають спільні цілі, такі як безпека, дотримання політик та вимог до відповідності. Цей тип хмари може перебувати у колективному володінні, управлінні та експлуатації однієї або декількох організацій, спільнот або сторонніх організацій, а також може існувати в межах або за межами юрисдикції своїх власників [5].

Для кращого розуміння відмінностей між типами хмарних моделей у таблиці 1.1 наведено їх порівняльну характеристику за ключовими критеріями.

Таблиця 1.1

Порівняльна характеристика моделей хмарних обчислень

Критерій	**Приватна хмара**	**Публічна хмара**	**Гібридна хмара**	**Хмара спільноти**
Доступність	Для однієї організації	Для широкого загалу	Поєднання приватної та публічної	Група організацій з подібними потребами
Управління	Власне або стороннє	Провайдер	Частково власне, частково провайдером	Колективне або стороннє
Безпека	Високий контроль	Залежить від провайдера	Високий контроль над критичними даними	Орієнтація на спільні вимоги
Гнучкість	Обмежена	Висока	Висока	Середня
Приклади	Фінанси, держустанови	Пошта, офісні сервіси	Великі корпорації з критичною інфраструктурою	Освіта, наука, державні коаліції

1.2. Визначення персональних даних та вимоги до їх захисту

Персональні дані визначаються як будь-яка інформація чи сукупність інформації, що прямо чи опосередковано стосується фізичної особи, яка ідентифікована або може бути конкретно ідентифікована. Ця категорія охоплює широкий спектр ідентифікаторів, які дозволяють розрізняти людей.

Поширеними прикладами персональних даних є повні імена, дати народження, стать, ідентифікаційні номери (наприклад, національний ідентифікаційний номер або номер паспорта), адреси електронної пошти, номери

телефонів, фізичні адреси та цифрові ідентифікатори, такі як IP-адреси. Захист цих даних є не просто регуляторною вимогою, а важливим аспектом забезпечення особистої конфіденційності та довіри в цифровій взаємодії .

Обробка персональних даних підлягає суворому правовому захисту. Зокрема, дані не можуть оброблятися необґрунтовано або без достатніх підстав. Однією з найважливіших підстав для законної обробки персональних даних є отримання прямої згоди від особи, чиї дані збираються, яку називають суб'єктом персональних даних. Така згода, як правило, запитується під час заповнення онлайн-форм або коли особи користуються послугами, які вимагають їхню особисту інформацію. Ця законодавча база підкреслює важливість прозорості та дотримання прав людини при обробці даних.

У Законі України “Про хмарні послуги” зазначено , що обробка персональних даних у сфері хмарних сервісів та дата-центрів вимагає суворого дотримання вимог, встановлених Законом України «Про захист персональних даних». Цей закон визначає конкретні обов'язки та відповідальність організацій, які обробляють персональні дані, забезпечуючи належні гарантії під час обробки даних у хмарних середовищах [6].

Використання хмарних рішень для зберігання даних пропонує безліч переваг, але водночас створює потенційні проблеми з регуляторними вимогами та дотриманням нормативних норм, особливо коли йдеться про конфіденційні персональні дані.

Щоб забезпечити надійне зберігання та обробку критично важливих корпоративних даних у хмарних середовищах, організації повинні дотримуватися кількох основних вимог.

Рішення для зберігання даних повинні бути розроблені з урахуванням надмірності, забезпечуючи не лише резервне копіювання даних, але й їх розподіл між різними об'єктами та пристроями. Такий багатогранний підхід допомагає зменшити ризики, пов'язані з втратою даних через такі обставини, як стихійні лиха, людські помилки або механічні збої. Організації повинні регулярно

тестувати свої процеси резервного копіювання та відновлення, щоб забезпечити швидке і точне відновлення даних у разі потреби.

Дані повинні бути легкодоступними для уповноваженого персоналу, коли це потрібно. Важливо розрізняти різні типи даних, наприклад, виробничі дані, які активно використовуються в бізнес-операціях, та архівні дані, які зберігаються для довгострокового зберігання. Ідеальне рішення для хмарного зберігання забезпечує стратегічний баланс між швидким отриманням даних та економічною ефективністю, дозволяючи організаціям оптимізувати свої витрати, зберігаючи при цьому високий рівень доступності.

На рисунку 1.1 зображено життєвий цикл персональних даних, що охоплює ключові етапи: від збору та зберігання до використання, передачі, архівації та знищення. Кожен із цих етапів вимагає впровадження відповідних заходів захисту відповідно до чинного законодавства.

Рисунок 1.1 – Життєвий цикл персональних даних

Комплексні заходи безпеки є обов'язковими для захисту персональних даних. Дані повинні бути зашифровані в стані спокою (під час зберігання) та в дорозі (під час передачі), щоб унеможливити доступ до них несанкціонованих осіб. Крім того, слід впровадити надійні механізми контролю доступу, щоб регулювати, хто може переглядати або змінювати конфіденційну інформацію, повторюючи захист, наявний у традиційних локальних системах зберігання даних.

Організації можуть використовувати такі функції, як одноразовий запис з багаторазовим зчитуванням (WORM) для блокування даних, що робить їх захищеними від несанкціонованого доступу після першого запису. Крім того, інтеграція рішень для аудиторського контролю, таких як AWS CloudTrail, підвищує здатність організації підтримувати відповідність та контролювати доступ до персональних даних, забезпечуючи необхідну прозорість та підзвітність [8].

Важливими положеннями щодо організації захисту персональних даних є вимоги статті 24 Закону “Про захист персональних даних”, згідно з якою:

Фізичні особи та організації, які збирають, управляють та обробляють персональні дані, мають юридичний та етичний обов'язок забезпечувати їх захист від випадкової втрати, знищення або незаконної обробки, включаючи несанкціонований доступ. Цей обов'язок поширюється на всіх власників, розпорядників персональних даних та будь-яких третіх осіб, залучених до їх обробки.

Для посилення підзвітності та нагляду органи державної влади, органи місцевого самоврядування та приватні суб'єкти, які обробляють персональні дані, зобов'язані створити спеціальний структурний підрозділ або призначити відповідальну особу, до повноважень якої належить безпосередньо захист персональних даних. Така структура забезпечує відповідність процедур обробки персональних даних вимогам законодавства.

Крім того, інформація про визначений підрозділ або відповідальну особу має бути повідомлена Уповноваженому Верховної Ради України з прав людини,

що сприятиме підвищенню рівня обізнаності громадськості та прозорості у сфері захисту персональних даних.

На визначений підрозділ або відповідальну особу покладаються найважливіші обов'язки, зокрема:

Забезпечення постійного навчання, консультування та підтримки власників або розпорядників даних щодо дотримання законодавства про захист персональних даних, таким чином сприяючи формуванню культури обізнаності та відповідальності в організації.

Координація та співпраця з Уповноваженим Верховної Ради України з прав людини та призначеними ним представниками для вирішення будь-яких питань або порушень, пов'язаних із законодавством про захист персональних даних, забезпечення швидкого вжиття коригувальних заходів у разі необхідності.

Крім того, окремі фахівці, включаючи ліцензованих підприємців, медичних працівників, адвокатів та нотаріусів, несуть особисту відповідальність за захист персональних даних, з якими вони працюють. Вони повинні гарантувати, що їхня практика відповідає встановленим законодавчим вимогам, активно використовуючи найкращі практики захисту даних. Таке колективне зобов'язання щодо захисту персональних даних не лише забезпечує дотримання законодавства, а й зміцнює довіру громадськості до управління персональними даними в умовах зростаючої цифровізації [7].

1.3. Поточні загрози та вразливості хмарних середовищ

Хмарна атака - це кібератака, спрямована на платформи хмарних сервісів, що охоплює різні аспекти, такі як обчислювальні сервіси, рішення для зберігання даних і програмні додатки. Такі атаки можуть призвести до серйозних наслідків, включаючи витік даних, втрату даних, несанкціонований доступ до конфіденційної інформації та перебої в роботі сервісів. Оскільки організації та приватні особи все більше покладаються на хмарні обчислення для зберігання та

обробки даних, відповідно розширюється коло потенційних цілей для кіберзловмисників[12].

Хоча хмарні сервіси пропонують численні переваги, включаючи гнучкість, масштабованість та економічну ефективність, вони водночас створюють значні вразливості та загрози для безпеки.

Рисунок 1.2 – Класифікація загроз у хмарних обчисленнях

Найбільше занепокоєння викликають питання конфіденційності, цілісності та доступності даних, які є ключовими у захисті конфіденційної інформації[10].

Несанкціонований доступ до даних виникає через вразливість користувачів і їхніх даних до кібератак, адже хмарні сервіси доступні через мережі. Хакери можуть використовувати вразливості програмного забезпечення або компрометувати облікові записи для отримання несанкціонованого доступу до даних. Особливо ризикують сервіси без багатофакторної автентифікації (MFA) та контролю доступу на основі ролей (RBAC).

Витік або втрата даних є результатом централізації зберігання та обробки інформації, притаманної хмарним середовищам, що збільшує відповідні ризики. Навіть за наявності надійних внутрішніх заходів безпеки відповідальність за захист даних частково перекладається на хмарного провайдера. Недостатня

практика шифрування або збої в протоколах безпеки провайдера можуть призвести до несанкціонованого розкриття критично важливих даних.

Атаки на інфраструктуру відбуваються, коли зловмисники націлюються на інфраструктуру хмарних сервісів, застосовуючи, наприклад, розподілені атаки на відмову в обслуговуванні (DDoS), які ставлять під загрозу їхню доступність. Хоча багато хмарних провайдерів розширюють заходи захисту від таких загроз, складні або скоординовані атаки все одно можуть порушити роботу сервісів.

Неправильні налаштування конфігурації — це, зокрема, надання публічного доступу до конфіденційних даних або неправильно налаштовані дозволи, що створюють значні вразливості. Такі проблеми часто виникають через людські помилки або недостатню обізнаність щодо найкращих практик безпеки. Зокрема, поширеними прикладами таких помилок конфігурації є випадки незахищених відкритих баз даних або файлових сховищ.

Внутрішні загрози пов’язані з діями співробітників або партнерів, які можуть навмисно чи ненавмисно порушити цілісність даних або сприяти несанкціонованому доступу. Хмарні платформи, що характеризуються високим рівнем інтеграції та різноманітним доступом користувачів, особливо вразливі до внутрішніх загроз, що ускладнює заходи контролю доступу.

Юридичні та регуляторні ризики виникають у зв’язку з вимогами на кшталт Загального регламенту про захист даних (GDPR), які суворо регламентують обробку інформації. Коли дані розміщуються в хмарі, можуть виникнути юрисдикційні складнощі, особливо якщо дані знаходяться в країнах з менш суворим законодавством про конфіденційність.

Перенесення критично важливих даних і додатків організації в хмару вимагає ретельного вивчення різних внутрішніх вразливостей, відмінних характеристик хмарних середовищ, встановлених засобів контролю безпеки і сучасних хмарних пропозицій[11].

Захоплення сеансу відбувається, коли зловмисники використовують слабкі місця у вебдодатках або сервісах для отримання несанкціонованого доступу, що

може призвести до шкідливих дій, таких як видалення даних користувача або розповсюдження спаму в мережі.

Уразливість виходу з віртуальної машини дозволяє зловмиснику виконати код на віртуальній машині, що дозволяє несанкціоновано взаємодіяти з гіпервізором та отримати доступ до операційної системи хоста, а також до інших віртуальних машин. Ефективне виявлення шкідливої активності на рівні віртуальної машини має вирішальне значення для профілактики.

Застарілі криптографічні практики, зокрема використання слабкого або відсутнього шифрування, роблять дані вразливими до розшифрування неавторизованими суб'єктами. Користувачам життєво важливо забезпечити належне шифрування даних, використовувати безпечні методи зберігання ключів і застосовувати надійні алгоритми шифрування.

Несанкціонований доступ до інтерфейсів керування, які дозволяють користувачам адмініструвати сервіси за потреби. Несанкціонований доступ може надати зловмисникам повний контроль як над обліковими записами користувачів, так і над додатками.

Вразливості інтернет-протоколів пов’язані з недосконалістю механізмів автентифікації, що виходять за рамки базових протоколів, робить мережі вразливими до ін'єкції шкідливого трафіку. Крім того, такі протоколи, як Internet Protocol (IP), User Datagram Protocol (UDP) і Transmission Control Protocol (TCP), вразливі до різних атак на відмову в обслуговуванні, включаючи перехоплення сеансів.

Ризики відновлення даних зумовлені динамічною природою хмарних обчислень, яка дозволяє розподіляти та перерозподіляти ресурси між користувачами, що може призвести до таких ризиків, як крадіжка або витік даних. Організації часто залучають сторонніх постачальників для надання послуг з відновлення даних, тому дуже важливо ретельно оцінити стан безпеки цих зовнішніх постачальників.

Проблеми з виставленням рахунків виникають через складні системи обліку для виставлення рахунків і розподілу послуг у хмарних обчисленнях, що

створює додаткові вразливості, які організації повинні усунути, щоб захиститися від потенційної експлуатації.

Отже, розвиток хмарних технологій вимагає всебічного розуміння їхніх вразливостей і впровадження надійних засобів захисту конфіденційних даних у цій сфері, що набуває дедалі більшого поширення.

1.4. Огляд існуючих рішень і підходів до забезпечення безпеки даних у хмарі

Безпека та конфіденційність хмарних сховищ є першочерговим завданням, особливо для організацій, які обробляють конфіденційну інформацію, таку як корпоративні дані, фінансова інформація, наприклад, дані кредитних карток, та конфіденційні медичні записи. Внутрішні ризики, пов'язані з віртуальним зберіганням даних, вимагають ретельної оцінки потенційного несанкціонованого доступу фізичних або юридичних осіб, які не мають дозволу на перегляд такої конфіденційної інформації. Така пильність необхідна для запобігання порушенням, які можуть призвести до значних фінансових та репутаційних збитків[15].

Оскільки кіберзагрози продовжують розвиватися і створювати значні виклики, абоненти хмарних сервісів все частіше надають пріоритет захисту своїх даних [13]. Вони вимагають гарантій, що їхня інформація захищена від несанкціонованого доступу та кібератак за допомогою найновіших та найефективніших доступних заходів безпеки. Отже, організації повинні впроваджувати комплексну, багаторівневу стратегію безпеки та конфіденційності, яка охоплює різні аспекти захисту даних.

Ця система безпеки повинна включати кілька важливих компонентів, таких як надійний захист кінцевих точок для захисту пристроїв, за допомогою яких користувачі отримують доступ до хмарних сервісів. Крім того, ефективна фільтрація контенту та електронної пошти може допомогти заблокувати шкідливий контент ще до того, як він потрапить до користувачів, тим самим

знижуючи ризик фішингових атак і проникнення шкідливого програмного забезпечення. Крім того, організації повинні проводити постійний аналіз загроз для виявлення потенційних вразливостей і проактивного реагування на нові загрози.

Разом із цими заходами безпеки організації повинні розробити комплексну політику конфіденційності, яка чітко пояснює, як оброблятимуться, зберігатимуться та захищатимуться дані. Така прозорість не тільки допомагає побудувати довіру з користувачами, але й забезпечує дотримання відповідних норм і стандартів захисту даних, ще більше зміцнюючи прихильність організації до захисту конфіденційних даних у хмарі.

У цьому розділі наведено огляд різних рішень і підходів, спрямованих на посилення захисту даних і досягнення оптимального рівня безпеки та конфіденційності даних у хмарних сховищах.

Тенденція ігнорувати підказки щодо оновлення системи - чи то операційної системи, чи то браузера, чи то поштового клієнта - є поширеною поведінкою, яка підриває комп'ютерну безпеку. Такі оновлення часто містять важливі вдосконалення, покликані захистити пристрої від новітніх вірусів і шкідливих програм.

У контексті хмарного зберігання даних дуже важливо, щоб організації, відповідальні за обслуговування серверів, брали на себе зобов'язання регулярно оновлювати системи безпеки. Такий підхід зменшує занепокоєння щодо потенційного нагляду за необхідними оновленнями з боку окремих користувачів, гарантуючи, що протоколи безпеки провайдерів хмарних послуг залишаються актуальними та надійними.

Постачальники хмарних послуг розгортають брандмауери як основний компонент своєї стратегії захисту даних. Брандмауери функціонують аналогічно до фізичних бар'єрів, захищаючи конфіденційні дані від несанкціонованого доступу. Ці захисні заходи, які можуть бути як апаратними, так і програмними, реалізують низку заздалегідь визначених правил, що регулюють весь мережевий трафік.

Основна мета цих правил - відфільтрувати потенційно шкідливі взаємодії, тим самим посилюючи безпеку даних, що зберігаються в хмарній інфраструктурі, і ускладнюючи спроби хакерів впровадити в систему шкідливе програмне забезпечення або віруси.

Двофакторна автентифікація (2FA) значно підвищує безпеку, вимагаючи дві різні форми ідентифікації для доступу до вебсайту. Наприклад, при вході на банківський портал користувачі повинні спочатку ввести свої облікові дані, а потім код, надісланий електронною поштою або SMS. Цей додатковий крок перевірки створює потужний бар'єр проти несанкціонованого доступу до електронної пошти, особистої інформації та фінансових даних, тим самим посилюючи безпеку облікового запису.

Традиційні комбінації імені користувача та пароля часто є недостатніми для захисту облікових записів користувачів від кіберзагроз; скомпрометовані облікові дані залишаються одним з найпоширеніших векторів несанкціонованого доступу до бізнес-даних та додатків в Інтернеті. Отримавши облікові дані користувача, хакери можуть проникнути на різні хмарні платформи, що є невід'ємною частиною діяльності організації.

Впровадження багатофакторної автентифікації (MFA) забезпечує надійний механізм захисту, гарантуючи, що тільки авторизований персонал може отримати доступ до критично важливих хмарних додатків і даних, як на місці, так і за його межами. MFA широко визнана як один з найефективніших заходів безпеки для захисту хмарних ресурсів.

Доступ до корпоративних даних повинен бути обмежений лише уповноваженими адміністраторами, а не широким колом користувачів. Такі обмеження підвищують безпеку даних, розміщених у хмарних середовищах.

Хоча різні хмарні додатки призначені для сприяння співпраці між клієнтами, безкоштовні пробні версії та відкритий доступ можуть ненавмисно зробити ці сервіси вразливими для зловмисників. Вектори атак можуть включати атаки типу «відмова в обслуговуванні» (DoS), фішингові кампанії, цифрове

шахрайство з кліками та крадіжку контенту, що може бути полегшено через скомпрометовані точки доступу.

Управління адміністративними привілеями в середовищі хмарних обчислень вимагає консервативного підходу, коли адміністративні облікові записи надаються виключно для виконання основних завдань. Вкрай важливо, щоб усі адміністративні облікові записи були ретельно інвентаризовані за допомогою автоматизованих методик, гарантуючи, що кожна особа, якій надано адміністративний доступ до ноутбуків, настільних комп'ютерів і серверів, має належні повноваження від вищого керівництва[14].

Забезпечення безпеки даних нерозривно пов'язане з існуванням конкретної письмової політики безпеки у постачальника хмарних послуг. За відсутності такої політики цілісність хмарного середовища ставиться під сумнів, оскільки провайдер не продемонстрував формалізованого підходу до безпеки даних. Організації, які не мають структурованої стратегії безпеки, вважаються ненадійними, коли йдеться про обробку конфіденційної корпоративної або клієнтської інформації.

Створення надійних стратегій безпеки має важливе значення для формування ефективної системи захисту даних, перетворюючи безпеку з простої концептуальної ідеї на проактивну основу для захисту конфіденційної інформації.

Коли необхідно знищити дані, це має бути зроблено безпечно, щоб зменшити ризики витоку даних. Небезпечне знищення даних залишає їх вразливими для отримання несанкціонованими особами. Наприклад, зберігання засекреченої та конфіденційної інформації в хмарі створює значні ризики, якщо постачальник послуг не виконує належним чином знищення даних із застарілого обладнання.

Основна функція послуги з видалення даних полягає в повному знищенні конфіденційних або критично важливих даних за допомогою стороннього або власного програмного забезпечення.

Співпраця з постачальниками хмарних послуг, які пропонують комплексні рішення для резервного копіювання даних, є дуже важливою. Покладання лише на один сервер для зберігання даних створює значні ризики; якщо цей сервер вийде з ладу, доступ до критично важливих даних може бути втрачено. Тому доцільно зберігати вторинну резервну копію важливої інформації на зовнішніх жорстких дисках. Така практика слугує додатковим рівнем захисту, убезпечуючи від потенційних збоїв або порушень безпеки, пов'язаних із хмарними сервісами.

Сучасні системи баз даних здатні шифрувати дані в стані спокою, гарантуючи, що розшифровка відбувається виключно за допомогою авторизованих додатків і підтверджених облікових даних користувача. Крім того, організації можуть використовувати шифрувальні пристрої, які полегшують шифрування даних під час передачі з приватної мережі, а потім розшифровують їх після доступу до них довірених користувачів. Вибір методу шифрування вимагає сумісності не лише з можливостями програми, що використовується, але й з можливостями постачальника хмарних послуг.

Шифрування резервних копій даних у хмарній інфраструктурі є обов'язковим для забезпечення цілісності та безпеки даних; незашифровані резервні копії роблять зусилля з шифрування неефективними. Якщо резервні копії даних не захищені належним чином за допомогою шифрування, вони стають вразливими до несанкціонованого доступу зловмисників.

Припущення, що заходи безпеки даних можуть бути ефективними без забезпечення шифрування резервних копій, є фундаментально хибним. Підсилення безпеки, яке залишається неперевіреним, стає неефективним.

Ця концепція шифрування гарантує, що результати алгебраїчних операцій, виконаних над зашифрованим текстом, відповідають результатам еквівалентних операцій, проведених над відкритим текстом, тим самим усуваючи необхідність розшифровки в процесі обчислень. Як показано на рисунку 1.3, динаміка роботи гомоморфного шифрування в хмарних інфраструктурах стає очевидною: власник даних захищає дані і передає їх на хмарний сервер за допомогою гомоморфного шифрування.

Авторизовані користувачі можуть згодом розшифрувати зашифрований текст за допомогою своїх приватних ключів. Якщо користувач бажає виконати певні операції над зашифрованим текстом, йому потрібно лише передати відповідні функції хмарному серверу, який обробляє зашифровані операції без розшифрування і згодом повертає зашифрований результат користувачеві.

Рисунок 1.3 – Гомоморфне шифрування

Система ієрархічного шифрування на основі набору атрибутів (HASBE) працює під наглядом доменного органу, ефективно поєднуючи принципи шифрування на основі набору атрибутів (ASBE) з ієрархічним шифруванням на основі ідентифікаційних даних (HIBE). Ця структура передбачає п'ять різних ролей учасників: власник даних, користувач, орган управління доменом, батьківський і довірений орган, а також постачальник хмарних послуг.

На відміну від традиційного шифрування на основі ідентичності, яке покладається на унікальну ідентичність, шифрування на основі атрибутів (ABE) використовує набір атрибутів. Доступ до зашифрованого контенту надається виключно користувачам, чиї набори атрибутів узгоджуються з відповідною політикою доступу. У контексті додатків для спільного використання даних шифрування на основі атрибутів пропонує складні механізми контролю доступу

до зашифрованих файлів, дозволяючи власнику даних вибірково визначати, хто може отримати доступ до захищеної інформації.

MA-ABE було розроблено для вирішення проблем, пов'язаних з єдиним централізованим органом у традиційних схемах ABE. Рисунок 1.4 ілюструє управління декількома атрибутами різними органами влади. MA-ABE має кілька переваг над традиційними схемами ABE - наприклад, системи MA-ABE можуть обробляти більшу кількість атрибутів і є більш відмовостійкими, ніж ті, що залежать від одного органу. Схеми MA-ABE також можуть підвищити рівень конфіденційності, оскільки жоден орган не має повного знання всіх атрибутів, пов'язаних з користувачем.

Рисунок 1.4 – Шифрування на основі атрибутів з декількома центрами сертифікації

У прагненні захистити конфіденційні дані в ненадійних хмарних середовищах було запропоновано нове рішення для шифрування баз даних у пам'яті. Це рішення включає в себе синхронізатор, який слугує посередником між власниками даних та клієнтами. Щоб успішно розшифрувати зашифровані дані, якими поділився власник, клієнт повинен отримати ключ від синхронізатора. Синхронізатор відіграє вирішальну роль у відстеженні як пов'язаних спільних даних, так і відповідних криптографічних ключів.

Щоб забезпечити надійний захист від кіберзагроз, хмарним провайдерам рекомендується залучати сторонні організації з безпеки для проведення регулярних оцінок своїх серверів і програмного забезпечення.

Ці незалежні оцінки є життєво важливими для виявлення вразливостей для хакерів, кіберзлочинців та нових шкідливих програм і вірусів. Таке проактивне тестування підвищує ймовірність того, що хмарні провайдери володіють необхідними засобами захисту даних клієнтів від несанкціонованого доступу.

Основоположний принцип хмарних обчислень ґрунтується на технології віртуалізації, яка сприяла появі багатокористувацьких хмарних середовищ. У багатокористувацьких конфігураціях програмне забезпечення часто розгортається на спільних фізичних хостах, що потенційно призводить до вразливостей для окремих користувачів, таких як ризик канальних атак.

У цьому контексті ефективною є стратегія управління доступом для багатьох користувачів, яка наголошує на суворій ізоляції даних для підприємств, що працюють у хмарних інфраструктурах.

Впровадження гібридного рішення для забезпечення безпеки підвищує секретність і цілісність даних у хмарних обчисленнях. Цей підхід інтегрує складні методології обміну ключами та автентифікації, тим самим зміцнюючи зв'язок користувача з провайдером хмарних послуг. Серед цих механізмів алгоритм відкритих ключів RSA слугує безпечним методом розподілу криптографічних ключів між користувачами та провайдерами.

Надлишковість у зберіганні даних, особливо щодо ультрарезервованих даних, вирішує критичну проблему доступності даних під час апаратних збоїв або перебоїв в електропостачанні. Можливість відновлення даних під час стихійних лих або значних системних збоїв у провайдерів хмарних послуг має першорядне значення. Найбільші світові хмарні провайдери впроваджують стратегії резервування, які передбачають багаторазове дублювання даних у різних центрах обробки даних.

Ключові стратегії управління стосуються методологій, що застосовуються для нагляду за ключами шифрування. Численні провайдери хмарних сервісів

наразі пропонують рішення для управління ключами, багато з яких інтегровані в ширші екосистеми хмарних сервісів. Однак значне занепокоєння, пов'язане з цими пропозиціями, викликає передача управління даними третім особам.

Альтернативний підхід, який зберігає контроль над ключами шифрування в межах організації, чи то за допомогою спеціальних рішень для управління ключами, чи то за допомогою шифрувальних пристроїв, може сприяти кращому зменшенню ризиків.

У сучасних хмарних середовищах жорсткі диски є основним носієм інформації. Отже, надійність жорстких дисків є невід'ємною частиною функціонування хмарних рішень для зберігання даних. Дослідження виявили, що на частоту помилок несуттєво впливають фактори навколишнього середовища, такі як температура або частота використання, а скоріше демонструють сильні кластерні характеристики, що підкреслює важливість показників надійності в управлінні інфраструктурою хмарних сховищ.

Стратегічне застосування методологій приховування даних у середовищах хмарних обчислень створює значний потенціал для збереження конфіденційності даних. Концепція захисту баз даних через приховування даних поєднує автентичні дані з оманливими візуальними уявленнями, щоб приховати реальний обсяг даних.

Такі методи дозволяють авторизованим користувачам без особливих зусиль відрізнити фіктивні дані від справжніх. Збільшуючи загальний обсяг автентичної інформації, ці стратегії приховування даних одночасно підвищують безпеку чутливих персональних даних.

Ефективність хмарних середовищ у безпечному управлінні даними, чутливими до часу, залежить від створення та підтримки формального процесу контролю змін. Відсутність структурованого підходу під час планових оновлень може прискорити збої в роботі серверів, що призведе до перебоїв у наданні послуг і недоступності критично важливих даних. Отже, хмарні архітектури, в яких відсутня надійна система управління змінами, підривають їхню надійність для зберігання інформації, чутливої до часу.

Ранжований пошук за ключовими словами являє собою вдосконалену систему для організації зворотного зв'язку на основі відповідних параметрів, таких як частота ключових слів, що розширює її застосування і задовольняє нагальну потребу в захисті конфіденційності в контексті хмарних обчислень. Цей метод будує пошуковий індекс на основі частоти слів з використанням косинуса схожості, тим самим підвищуючи точність результатів пошуку за допомогою моделі векторного простору.

Технології штучного інтелекту (ШІ) все частіше використовуються постачальниками хмарних послуг для посилення заходів захисту даних. Інтеграція ШІ є особливо важливою у світлі проблем, пов'язаних з підбором кваліфікованого персоналу для забезпечення безпеки.

Використовуючи штучний інтелект, хмарні провайдери можуть автоматизувати початкову оцінку безпеки, тим самим зменшуючи навантаження на людський нагляд. Ці інструменти штучного інтелекту використовують складні алгоритми, призначені для виявлення та ідентифікації потенційних вразливостей безпеки, тим самим посилюючи захист даних.

Висновки за розділом 1

У першому розділі проаналізовано особливості хмарних обчислень, класифікації, регуляторні вимоги щодо захисту персональних даних та пов'язані з ними загрози.

Хмарні обчислення - це IT-модель, яка дозволяє гнучко, масштабовано та економічно ефективно використовувати ресурси, пропонуючи такі переваги, як самообслуговування, масштабованість та висока доступність. Однак вона також несе в собі ризики, такі як залежність від підключення до Інтернету та вразливість до кіберзагроз.

У розділі підкреслюється необхідність дотримання законодавства, зокрема Закону України «Про захист персональних даних», і наголошується на впровадженні технічних та організаційних заходів, таких як шифрування даних,

резервне копіювання, контроль доступу та аудит для забезпечення безпеки даних.

Отже, ефективний захист персональних даних у хмарних середовищах вимагає балансу між технологічними інноваціями та дотриманням правових норм і стандартів безпеки.

РОЗДІЛ 2
РОЗРОБКА МЕХАНІЗМУ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Визначення критеріїв та показників оцінки безпеки у хмарному середовищі

Для оцінки ефективності захисту персональних даних у хмарних середовищах необхідно враховувати як національну, так і міжнародну нормативну базу. В Україні основоположним нормативним документом є НД ТЗІ 2.5-004-99, що встановлює критерії оцінки захищеності інформації в комп'ютерних системах [16], які можуть бути частково адаптовані для застосування в хмарній інфраструктурі.

На міжнародному рівні кілька ключових стандартів заслуговують на увагу. Зокрема, ISO/IEC 27017 пропонує рекомендації щодо безпеки хмарних сервісів. Крім того, NIST SP 800-144 описує пов'язані з хмарними обчисленнями ризики та заходи захисту. Крім того, CSA Cloud Controls Matrix (CCM) являє собою стандартну матрицю контролю, призначену для систематичного структурування та оцінки стану безпеки хмарних середовищ.

Принципи, викладені в цих регламентах і стандартах, забезпечують надійну основу для оцінки хмарних сервісів. Як результат, з'явилося кілька ключових критеріїв, які полегшують ретельну оцінку того, наскільки ефективно ці сервіси можуть безпечно обробляти персональні дані. Використовуючи ці оціночні стандарти, організації можуть приймати більш обґрунтовані рішення щодо придатності постачальника хмарних послуг для захисту конфіденційної інформації та забезпечення приватності осіб.

На рисунку 2.1 представлено основні критерії, що формуються на основі вітчизняних та міжнародних стандартів і застосовуються для комплексного оцінювання безпеки хмарних середовищ.

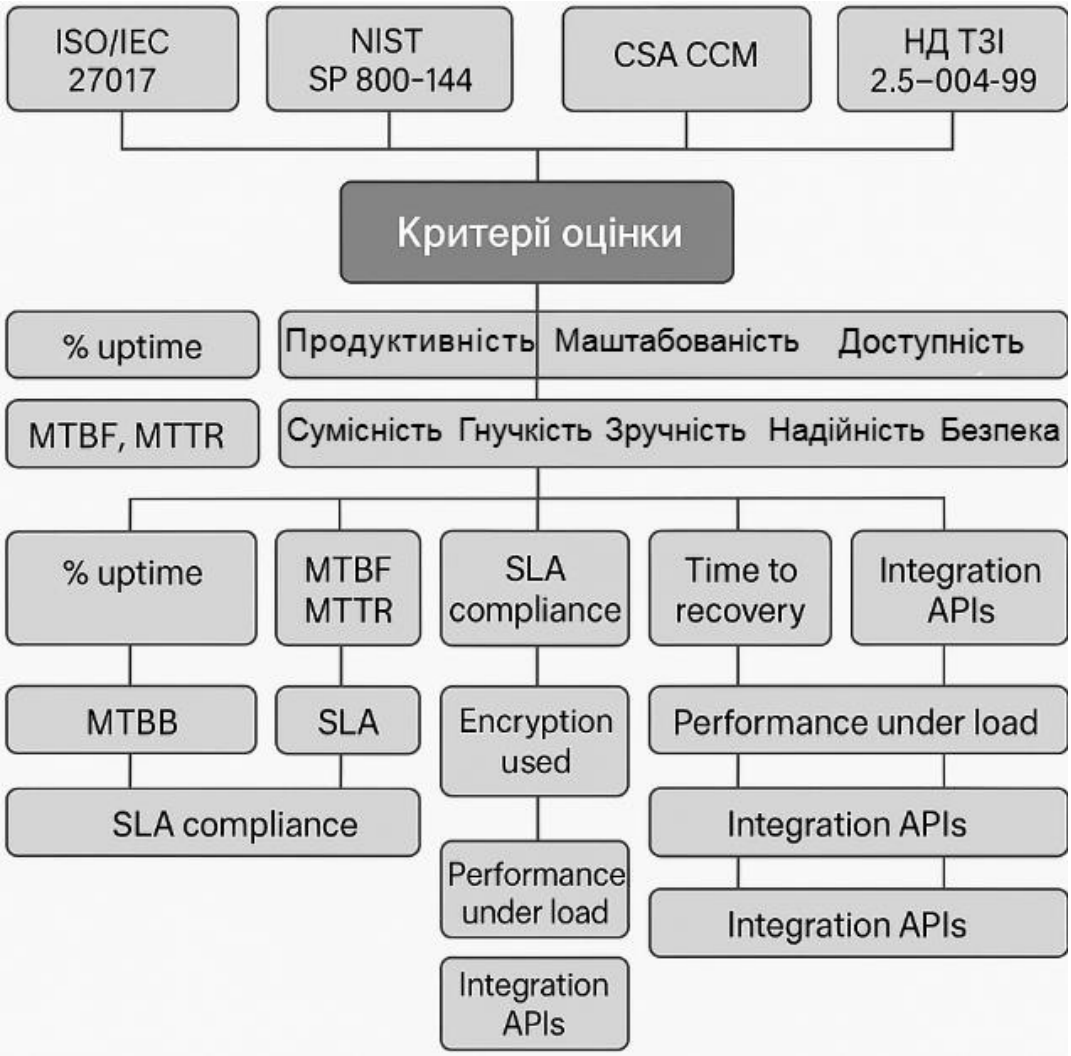

Рисунок 2.1 – Класифікація критеріїв оцінки безпеки хмарних сервісів

Доступність є ключовим критерієм у визначенні якості хмарних сервісів. Він кількісно визначає здатність послуги залишатися доступною для користувачів протягом заздалегідь визначеного часу. Для організацій цей показник має вирішальне значення, оскільки перебої в роботі сервісу можуть суттєво порушити операційну діяльність та організаційні процеси. Доступність зазвичай виражається у відсотках від операційного часу, враховуючи як заплановані, так і незаплановані простої [17]. Досягнення високого рівня доступності є фундаментальною передумовою для безперебійної роботи організаційних служб.

Надійність оцінює здатність хмарного сервісу виконувати свої функції без збоїв протягом тривалих періодів часу. Це охоплює стабільність системи за

стандартних умов експлуатації, а також здатність сервісу швидко відновлюватися після збоїв. У секторах, де безперервність роботи є життєво важливою, наприклад, в інформаційних послугах, цей критерій є незамінним. Для оцінки надійності зазвичай використовують такі показники, як середній час напрацювання на відмову (MTBF) та середній час відновлення (MTTR).

Безпека є, мабуть, найбільш важливим критерієм для оцінки якості хмарних сервісів, особливо в організаціях, де конфіденційність і цілісність даних мають першорядне значення. Оцінка безпеки передбачає комплексний аналіз захисту хмарного сервісу від внутрішніх і зовнішніх загроз, його здатності перешкоджати несанкціонованому доступу до даних і його відповідності визнаним міжнародним стандартам безпеки (наприклад, ISO/IEC 27001) [18]. Цей вимір безпеки також охоплює впровадження захисних заходів, таких як шифрування, багатофакторна автентифікація та надійні механізми контролю доступу.

Продуктивність хмарних сервісів є критично важливим фактором, що визначає швидкість та ефективність їхньої роботи за різних рівнів навантаження. Цей критерій охоплює різні показники, включаючи час відгуку сервісу, час обробки запитів і здатність сервісу підтримувати стабільну функціональність в умовах збільшення кількості користувачів або обсягів даних. В організаційному контексті важливість продуктивності підкреслюється, зокрема, у зв'язку з оперативною обробкою критично важливих даних і швидким доступом до інформаційних ресурсів.

Масштабованість, за визначенням хмарних обчислень, означає здатність хмарного сервісу задовольняти зростаючі вимоги до навантаження або обсягу даних, зберігаючи при цьому продуктивність і ефективність. Здатність хмарних сервісів швидко збільшувати свої ресурси у відповідь на підвищену активність користувачів або зростаючі потреби в обробці даних є незамінною для організацій, особливо в періоди, що характеризуються підвищеною операційною інтенсивністю. Оцінка масштабованості передбачає оцінку здатності хмарної інфраструктури надавати додаткові ресурси відповідно до мінливих вимог.

Зручність використання стосується зручності, пов'язаної з адмініструванням та управлінням хмарними сервісами. Сюди входить можливість швидкого налаштування, моніторингу в режимі реального часу, оновлення та відстеження стану сервісу. Ефективне управління послугами має першорядне значення для організацій, оскільки воно сприяє своєчасному реагуванню на потенційні проблеми та збої в роботі системи. Оцінка керованості охоплює доступ до аналітичних інструментів, які дозволяють відстежувати стан системи та прогнозувати тенденції продуктивності [19].

Сумісність оцінює ступінь, до якого хмарні сервіси можуть легко інтегруватися з існуючими організаційними системами і технологіями. Аналіз цього критерію передбачає оцінку здатності сервісів ефективно працювати в різних операційних системах і конфігураціях програмного та апаратного забезпечення. Висока сумісність має вирішальне значення для зменшення потенційних додаткових витрат, пов'язаних з адаптацією або вдосконаленням вже існуючих рішень.

Гнучкість - це здатність хмарного сервісу пристосовуватися до мінливих вимог організації. Оцінка цього критерію включає здатність сервісів змінювати конфігурацію, функціональність або розподіл ресурсів без значних технічних обмежень. Для організацій, особливо в таких контекстах, як військові операції або оперативне планування, швидка адаптивність хмарних сервісів до мінливих потреб має першорядне значення.

Комплексна оцінка якості хмарних сервісів, що мають відношення до інформаційної інфраструктури організації, вимагає застосування надійного набору критеріїв, які охоплюють різні аспекти продуктивності сервісу. Ці критерії враховують технічні, безпекові, операційні та економічні фактори, які мають вирішальне значення для надійності та ефективності хмарних рішень, особливо в світлі специфічних операційних вимог організації.

2.2. Вибір метрик для оцінювання рівня ефективності захисту

Оцінка якості хмарних сервісів за допомогою показників надійності, продуктивності та безпеки дає важливе уявлення про їхню операційну ефективність та можливості. Хоча стандартизовані показники полегшують кількісну оцінку, необхідно визнати обмеження, пов'язані з універсальними показниками, і ризики, притаманні виключно кількісним оцінкам. Враховуючи як аргументовані, так і контраргументовані точки зору, зацікавлені сторони можуть брати участь у збалансованій методології оцінки хмарних сервісів. Цей подвійний підхід охоплює не лише кількісні показники, але й якісні аспекти, забезпечуючи таким чином цілісну оцінку якості послуг[20].

У сфері оцінки послуг дослідники та практики використовують різноманітні методи та метрики для оцінки надійності, продуктивності та безпеки. Вибір цих методологій залежить від різних факторів, включаючи конкретну модель хмарного сервісу - інфраструктура як послуга (IaaS), платформа як послуга (PaaS) або програмне забезпечення як послуга (SaaS) - характер додатку або послуги, що розміщується, а також очікування і потреби кінцевих користувачів.

Оцінювання хмарних сервісів базується на низці стратегій, які охоплюють як технічні, так і організаційні аспекти (див. рис. 2.2).

В першу чергу слід критично оцінити угоди про рівень обслуговування (SLA), щоб забезпечити їхню чіткість, здійсненність і послідовне дотримання. Для цього використовують загальні метрики SLA, такі як час безвідмовної роботи, час відгуку і загальна доступність.

Також важливо впроваджувати тестування продуктивності за допомогою різноманітних інструментів і методологій, які імітують реальні сценарії використання, виявляючи потенційні вузькі місця або проблеми в інфраструктурі. Такі тести можуть охоплювати навантажувальне тестування, стрес-тестування, тестування масштабованості та тестування на витривалість.

Рисунок 2.2 — Стратегії оцінки хмарних сервісів.

Оцінка безпеки здійснюється шляхом тестування на проникнення, сканування вразливостей та інших методів, що допомагають виявити потенційні вразливості і оцінити ефективність протоколів безпеки.

Значущим джерелом інформації є опитування задоволеності клієнтів, що надають прямі відгуки користувачів про надійність, продуктивність та безпеку сервісів.

Порівняльний аналіз різних постачальників хмарних послуг дозволяє виявити найкращі практики та встановити стандарти якості, використовуючи стандартні галузеві інструменти бенчмаркінгу для порівняння результатів.

Безперервний моніторинг та аналітика допомагають виявляти тенденції, нові проблеми і можливості для вдосконалення, використовуючи різні

інструменти моніторингу та аналітичні платформи для збору та аналізу відповідних даних.

Оцінка сертифікації та дотримання вимог передбачає вивчення незалежних аудитів і сертифікатів, які підтверджують відповідність провайдера галузевим стандартам і правилам щодо безпеки, конфіденційності та якості послуг. Це допомагає дослідникам оцінити зобов'язання провайдера надавати високоякісні послуги.

Отже, при систематичній оцінці хмарних сервісів щодо надійності, продуктивності та безпеки важливо враховувати такі ключові фактори, як час безвідмовної роботи, історичні простої, угоди про рівень обслуговування, затримки, пропускна здатність, тестування навантаження, сертифікати безпеки, механізми шифрування, заходи контролю доступу, стратегії управління вразливостями та можливості реагування на інциденти[21]. Комплексний аналіз цих аспектів забезпечить осіб, які приймають рішення, необхідною інформацією для вибору постачальника хмарних послуг, який найкраще відповідає цілям і вимогам їхньої організації.

2.3. Опис запропонованого механізму оцінювання

Запропонований механізм оцінювання має на меті оцінити ефективність захисту персональних даних у хмарних середовищах, використовуючи комплексну систему аналізу безпеки, яка охоплює як міжнародні, так і національні стандарти. Цей механізм має важливе значення для забезпечення надійного захисту персональних даних, оскільки організації все більше покладаються на хмарні сервіси.

Підхід побудований як систематичний, поетапний аналіз, що фокусується на кількох критично важливих критеріях оцінки. Використання чітко визначених метрик оцінки полегшує як кількісне, так і якісне вимірювання ефективності безпеки. Загальна концепція відображає методи оцінювання, які зазвичай використовуються в системах управління ризиками, аудитах інформаційної

безпеки та стандартах оцінки відповідності, забезпечуючи тим самим надійну основу для вимірювання.

Цей механізм оцінювання за своєю суттю є гібридною, поєднуючи принципи багатокритеріального аналізу рішень (MCDA) та методу аналізу ієрархій (AHP). Інтеграція цих підходів дає дві значні переваги:

По-перше, ієрархічне структурування критеріїв: використання можливостей ієрархічного структурування AHP дозволяє логічно організувати фактори оцінки, такі як безпека і надійність. Така ієрархічна структура сприяє чіткому визначенню важливості кожного критерію у контексті загальної оцінки.

По-друге, зважування та порівняльний аналіз: завдяки застосуванню принципів MCDA механізм включає систему присвоєння ваг різним критеріям на основі пріоритетів, встановлених організацією. Це дає змогу проводити всебічне кількісне порівняння альтернатив, що в підсумку спрощує розрахунок сукупного показника ефективності захисту[22].

Етапи оцінювання:

1. Визначення критеріїв оцінювання: На першому етапі визначаються відповідні критерії оцінювання, які можуть включати такі аспекти, як доступність, надійність, безпека, продуктивність, масштабованість, зручність використання, інтероперабельність та гнучкість. Кожен критерій відіграє важливу роль у створенні повної картини стану безпеки хмарного сервісу.

2. Оцінка кожного критерію: Кожен визначений критерій оцінюється за заздалегідь визначеною шкалою, наприклад, від 1 до 5 або від 1 до 10, на основі емпіричних даних, зібраних з відповідного хмарного сервісу. Цей процес оцінювання є дуже важливим, оскільки він безпосередньо впливає на результати оцінки[23].

3. Розподіл вагових коефіцієнтів: Після підрахунку балів наступний крок передбачає присвоєння ваг кожному критерію, що відображає конкретні пріоритети організації. Таке зважування гарантує, що більш важливим факторам буде приділено більше уваги в загальній оцінці безпеки, таким чином роблячи результати більш узгодженими з цілями організації.

4. Розрахунок загального індексу безпеки за формулою зваженої суми:

$$S = \sum_{i=1}^{n} w_i \cdot x_i \quad . \tag{2.1}$$

де w_i— вага критерію;

x_i— оцінка критерію.

Ця формула дозволяє комплексно інтегрувати всі індивідуальні оцінки в єдиний показник загальної безпеки[24].

5. Інтерпретація результатів: На останньому етапі відбувається інтерпретація отриманого індексу безпеки. Розраховане значення порівнюється із заздалегідь визначеними пороговими рівнями, які поділяють ефективність безпеки на три окремі рівні: низький, середній та високий:

- Оцінка від 4,5 до 5,0 означає високий рівень безпеки.
- Оцінка від 3,5 до 4,4 означає середній (прийнятний) рівень безпеки.
- Оцінка нижче 3,5 означає низький рівень, який потребує покращення.

Приклад реалізації оцінювання з конкретними критеріями, метриками, вагами й балами наведено в Таблиці 2.1 у Додатку А.

Таким чином, запропонований механізм оцінювання забезпечує системний підхід до аналізу хмарних сервісів, акцентуючи увагу на ключових вимогах безпеки. В кінцевому підсумку він дає чіткий, практичний формат для прийняття обґрунтованих рішень щодо захисту персональних даних у хмарних середовищах.

2.4. Інтеграція механізму оцінювання у процеси безпеки хмарного провайдера

Запропонована механізм оцінювання, який синергетично інтегрує багатокритеріальний аналіз рішень (MCDA) з ієрархічним аналізом (AHP), забезпечує комплексну основу для вдосконалення системи управління інформаційною безпекою (СУІБ) постачальників хмарних послуг.

Ця інтеграція допомагає не лише стандартизувати та структурувати оцінку безпеки, але й обґрунтувати необхідність постійного вдосконалення практик безпеки протягом усього життєвого циклу хмарних сервісів.

Постачальники хмарних послуг можуть використовувати цей механізм на щоквартальній або щорічній основі для проведення вичерпної оцінки свого стану безпеки для різних пропозицій послуг. Висновки, отримані в результаті таких оцінок, відіграють ключову роль у формуванні інвестиційних стратегій, що стосуються передових технологій безпеки, включаючи системи запобігання втраті даних (DLP), рішення для управління інформацією та подіями безпеки (SIEM) і брандмауери для вебдодатків (WAF)[27].

Крім того, механізм полегшує порівняльний аналіз рівнів безпеки різних послуг, географічних регіонів і демографічних характеристик клієнтів, що дозволяє більш ефективно приймати рішення про розподіл ресурсів.

Інтегруючи механізм оцінювання в регулярні цикли внутрішнього аудиту безпеки, організації можуть систематично документувати як прогрес, так і регрес у ключових показниках безпеки. Така інтеграція підвищує прозорість звітності для зовнішніх аудиторів, органів сертифікації, таких як ISO/IEC 27001, і клієнтів, які вимагають демонстрації відповідності стандартам, таким як SOC 2 і GDPR[25].

Встановлення чітких порогових значень для критичних критеріїв, таких як забезпечення доступності системи на рівні або вище 99,9%, дозволяє автоматизувати оповіщення та коригувальні заходи, коли такі порогові значення не досягаються, тим самим підвищуючи загальну операційну стійкість.

Механізм виявляється особливо цінним в сфері управління інцидентами, дозволяючи організаціям проводити оцінку як до, так і після кіберінцидентів.

Аналізуючи коливання ключових показників ефективності, таких як зниження надійності або збільшення середнього часу відновлення (MTTR), провайдери можуть ефективно виявляти критичні вразливості своєї інфраструктури. Цей підхід, заснований на даних, розширює можливості оцінки

ризиків, дозволяючи сформулювати більш точну і оперативну матрицю ризиків, яка відображає умови безпеки в реальному часі.

Механізм дозволяє автоматизувати збір показників за допомогою різних платформ моніторингу, таких як Prometheus, CloudWatch, Zabbix і Azure Monitor. Ця можливість гарантує, що оцінки безпеки ґрунтуються на об'єктивних даних у режимі реального часу, що підвищує надійність оцінок.

Крім того, інтеграція з системами бази даних управління конфігурацією (CMDB) враховує динамічні зміни, що відбуваються в IT-інфраструктурі, надаючи контекстні дані, які збагачують оцінку безпеки.

Спираючись на інформацію, отриману в результаті оцінювання, організації можуть розробити обґрунтовані вимоги до безпеки, які визначатимуть оновлення політик і внутрішніх стандартів.

Ці висновки також можуть слугувати критеріями для складання контрактних угод з клієнтами, зокрема, угод про рівень обслуговування, які можуть передбачати гарантовані пороги обслуговування, включаючи доступність, масштабованість і продуктивність, таким чином встановлюючи чіткі очікування для зацікавлених сторін[26].

Результати оцінювання надають безцінні тематичні дослідження, які можуть слугувати ключовими навчальними ресурсами як для команд безпеки, так і для команд DevOps. Представляючи реальні приклади того, як різні рішення і дії вплинули на результати безпеки, ці тематичні дослідження значно збагачують розуміння командою критичної ролі, яку заходи безпеки відіграють в операційному успіху.

Такий проактивний і практичний підхід до навчання не лише розширює набір навичок, але й сприяє формуванню міцної культури, орієнтованої на безпеку, і почуття відповідальності серед усіх співробітників організації, що в кінцевому підсумку сприяє створенню більш безпечного операційного середовища (див. рис. 2.3).

Рисунок 2.3 - Цикл інтеграції механізму оцінювання безпеки.

Застосовуючи цей комплексний механізм, постачальники хмарних послуг можуть забезпечити постійне вдосконалення своїх практик безпеки, тим самим підвищуючи довіру та надійність серед своїх клієнтів.

Висновки за розділом 2

У цьому розділі описано механізм оцінювання ефективності захисту персональних даних у хмарних середовищах. Цей механізм інтегрує багатокритеріальний аналіз (MCDA) з процесом аналітичної ієрархії (AHP), що дозволяє провести комплексну та структуровану оцінку різних факторів, які впливають на рівень безпеки. Підхід ґрунтується на нормативних вимогах України (НД ТЗІ 2.5-004-99), а також міжнародних стандартах (включаючи ISO/IEC 27017, NIST SP 800-144 та CSA CCM), що забезпечує відповідність сучасним практикам інформаційної безпеки.

Визначено та обґрунтовано вісім основних критеріїв оцінки якості хмарних сервісів щодо безпеки персональних даних: доступність, надійність, безпека, продуктивність, масштабованість, зручність використання, сумісність та гнучкість. На основі цих критеріїв розроблено ієрархічну модель для кількісної оцінки загального рівня безпеки.

Запропоновано алгоритм реалізації механізму оцінювання, який включає збір метрик, визначення вагових коефіцієнтів, нормалізацію показників та розрахунок загального індексу ефективності. Крім того, було досліджено способи інтеграції запропонованого механізму у внутрішні процеси провайдера хмарних послуг, що полегшує його практичне застосування для моніторингу, аналізу ризиків та прийняття управлінських рішень щодо захисту персональних даних.

Таким чином, запропонована механізм оцінювання слугує універсальним інструментом, що забезпечує об'єктивну, структуровану та адаптивну оцінку рівня безпеки персональних даних у хмарному середовищі.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕХАНІЗМУ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ХМАРНОМУ СЕРЕДОВИЩІ

3.1. Вибір об’єкта оцінювання та постановка задачі

Об’єктом оцінювання обрано сервісну інфраструктуру хмарного постачальника, зокрема — віртуалізовані середовища, у яких зберігаються або обробляються персональні дані користувачів. У рамках дипломної роботи модельна оцінка проводиться на прикладі трьох найбільш поширених хмарних провайдерів: Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP).

Кожен із цих провайдерів пропонує власний набір сервісів, інструментів безпеки, політик конфіденційності та угод про рівень обслуговування (SLA), які впливають на загальний рівень захищеності персональних даних. Саме їхня різноспрямована архітектура, політики захисту та моделі доступу створюють оптимальні умови для порівняльного оцінювання з використанням єдиного механізму.

Таким чином, об’єкт оцінювання є репрезентативним, а результати його аналізу — релевантними для широкого кола організацій, які стоять перед вибором або аудитом хмарного середовища.

У рамках постановки задачі передбачається створити прикладну реалізацію механізму оцінювання, яка дозволить:

- Нормалізувати та структурувати набір критеріїв оцінки ефективності захисту персональних даних у хмарі;

- Інтегрувати механізм зважування цих критеріїв відповідно до важливості для конкретної організації;

- Надати інструмент для введення балів, які користувач може задавати згідно з наявною інформацією про хмарного провайдера;

- Здійснити розрахунок зведеного індексу безпеки, що агрегує всі оцінки у єдину величину;

- Реалізувати можливість візуального представлення результатів для зручності аналізу та порівняння альтернатив;

- Провести тестове оцінювання обраних платформ, щоб перевірити працездатність розробленого підходу на практиці.

Реалізація цих задач дозволить оцінити придатність хмарного середовища до зберігання персональних даних не лише з технічної точки зору, але й у контексті управлінської підтримки прийняття рішень, з урахуванням нормативних вимог, ризиків та пріоритетів конкретної організації.

3.2. Розробка вебдодатку для реалізації механізму оцінювання

З метою практичного впровадження механізму багатокритеріального оцінювання, описаного у попередньому розділі, було розроблено програмне забезпечення, яке реалізує послідовну логіку вибору хмарного провайдера, введення оцінок, обчислення інтегрального показника безпеки та візуалізації результатів. Такий підхід дозволяє користувачу самостійно враховувати внутрішні вимоги до захисту даних, застосовуючи адаптивну модель оцінювання.

Програмний модуль реалізовано мовою C++/CLI з використанням бібліотек Windows Forms у середовищі розробки Microsoft Visual Studio 2022. Вибір даного стеку технологій зумовлений необхідністю створення десктопного додатку з інтерактивним інтерфейсом, простим управлінням файлами та можливістю візуалізації даних.

На рисунку 3.1 зображено блок-схему основного алгоритму взаємодії користувача з додатком. Схема демонструє послідовність дій — від вибору провайдера до формування звіту.

Рисунок 3.1 – Алгоритм оцінювання рівня захищеності персональних даних у хмарній інфраструктурі

Інтерфейс реалізовано у вигляді Windows Forms-додатку. Основними елементами графічного інтерфейсу користувача є таблиця з критеріями та оцінками, набір кнопок для запуску функцій, область для побудови діаграм, а також поле для виводу інтерпретації результату.

Кожна функція пов’язана з відповідним методом, що обробляє дані на основі введених користувачем значень. Це дозволяє уникнути дублювання логіки та забезпечити послідовну обробку даних.

На рисунку 3.2 показано вікно програми після відкриття вкладки для провайдера AWS. У таблиці зображено назви критеріїв, їхні описи та ваги.

Користувач вводить оцінки вручну у відповідне поле, після чого натискає кнопку «Розрахувати».

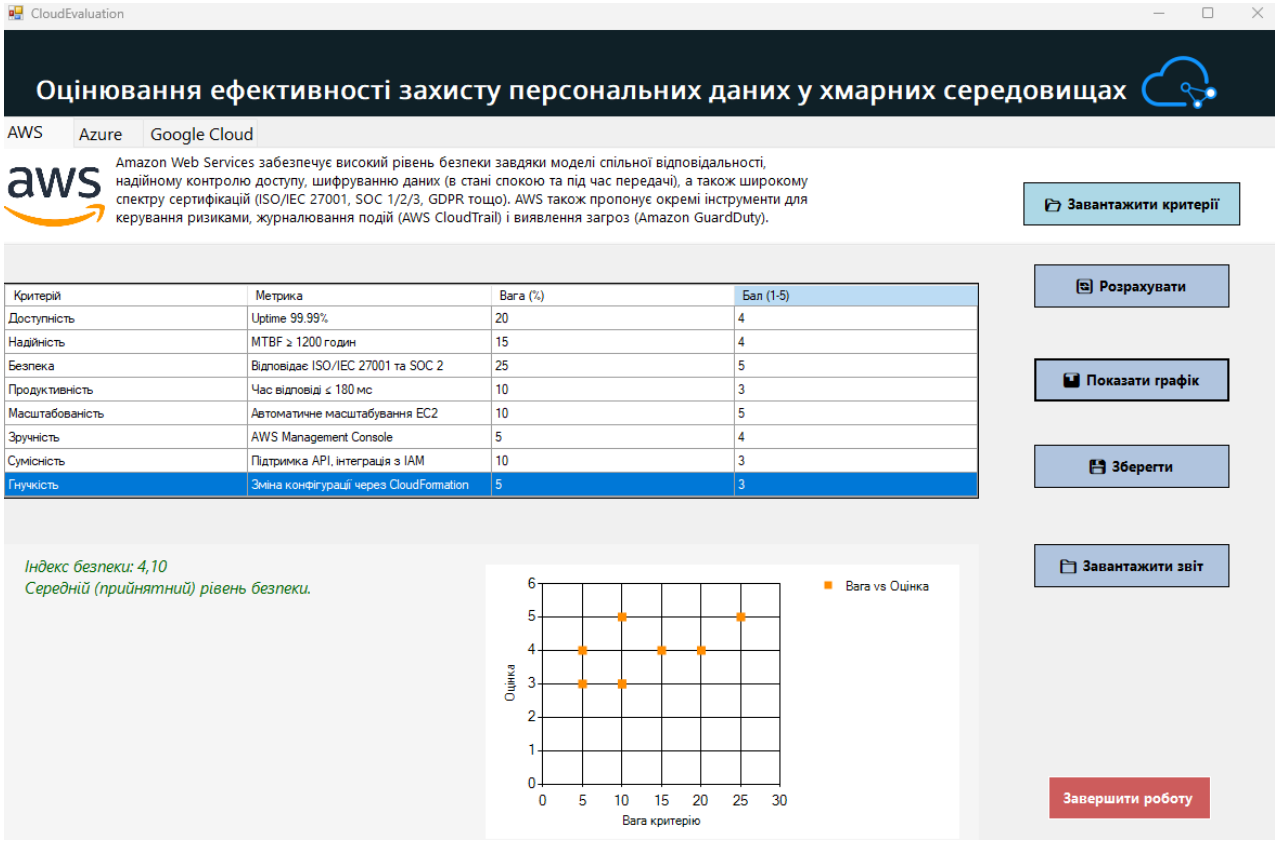

Рисунок 3.2 – Інтерфейс програми (вкладка AWS)

Після завершення обчислень додаток автоматично формує два текстові звіти. Перший — last_provider.txt — містить розгорнуту інформацію щодо останнього провайдера, який було оцінено. Другий звіт — providers_summary.txt — акумулює результати оцінювання кількох провайдерів, що дає змогу здійснювати їх подальше порівняння.

Також реалізовано можливість побудови графіка «Вага – Оцінка», що допомагає виявити критично недооцінені або переоцінені аспекти безпеки з точки зору користувача.

Розроблене програмне забезпечення виконує повний цикл багатокритеріального оцінювання ефективності захисту персональних даних у хмарних середовищах. Інтерфейс орієнтований на зручність користувача та

забезпечує повну автономію роботи без потреби у підключенні до зовнішніх серверів.

3.3. Інтеграція критеріїв і метрик у функціональність додатку

Інтеграція критеріїв та метрик у функціональність розробленого додатку є фундаментальним етапом реалізації багатокритеріального механізму оцінювання ефективності захисту персональних даних у хмарному середовищі. На цьому етапі забезпечується поєднання теоретичних засад (розроблених у розділі 2) з практичною реалізацією (розділ 3.2), шляхом впровадження повноцінної системи обробки оцінювальних даних.

Кожен критерій у системі пов'язаний із відповідними метриками, що відображають конкретні аспекти якості хмарних послуг (наприклад: Uptime, MTBF, ISO/IEC 27001 compliance, response time тощо). Такі метрики задають об'єктивну основу для оцінювання, що дозволяє уникнути суб’єктивізму й гарантує порівнюваність результатів між провайдерами.

Технічна реалізація інтеграції включає кілька етапів. Насамперед, здійснюється структуризація вхідних даних: кожен критерій подається у вигляді окремого текстового файлу, що містить три ключові параметри — назву критерію, опис або пояснення відповідної метрики, а також ваговий коефіцієнт.

Після завантаження даних вони відображаються у графічному інтерфейсі у вигляді таблиці, де користувач має можливість ввести власні оцінки, керуючись аналізом змісту метрики або наявними даними конкретного хмарного провайдера.

Далі здійснюється обчислення агрегованого індексу захищеності шляхом застосування формули зваженої середньої. Такий підхід дозволяє врахувати як рівень реалізації кожного аспекту безпеки, так і його значущість у загальній системі. Для забезпечення точності результатів реалізовано перевірку коректності введених даних: проводиться контроль на наявність порожніх

оцінок, перевищення допустимого діапазону, а також виявлення нульових або відсутніх вагових коефіцієнтів.

Завершальним етапом є виведення результатів та їх візуалізація. Отримані результати інтеграції зберігаються у текстових файлах і супроводжуються графічним відображенням співвідношення ваг та оцінок, що дозволяє візуально визначити сильні та слабкі сторони безпеки кожного провайдера.

Інтеграція побудована на засадах методів MCDA (Multicriteria Decision Analysis) та AHP (Analytic Hierarchy Process). Метод MCDA забезпечує гнучку адаптацію до організаційних пріоритетів шляхом можливості ручного коригування вагових коефіцієнтів критеріїв. У свою чергу, метод AHP дозволяє ієрархічно структурувати критерії та метрики, що дає змогу відобразити логічний зв’язок між окремими показниками безпеки та загальним рівнем захисту.

Реалізована інтеграція не лише автоматизує обчислення, а й виконує роль аналітичного модуля, що може бути адаптований під специфічні потреби організацій, регуляторів або аудиторів, які займаються безпекою даних у хмарному середовищі.

3.4. Проведення тестового оцінювання та аналіз результатів

Для підтвердження працездатності створеного механізму багатокритеріального оцінювання було проведено тестове оцінювання рівня захисту персональних даних.Головна мета — перевірити, наскільки інструмент дозволяє адаптивно оцінити рівень захисту відповідно до індивідуальних потреб конкретної організації.

Оцінювання проводиться шляхом проставлення значень за кожним із критеріїв, визначених у розділі 2.1, які вже були інтегровані в інтерфейс додатку (див. розділ 3.3). Користувач самостійно присвоює оцінки в діапазоні від 1 до 5, орієнтуючись на власні внутрішні вимоги до безпеки, значущість кожного

аспекту для конкретної інфраструктури, а також результати внутрішніх аудитів або технічну документацію, надану провайдером.

Цей підхід дозволяє організаціям не просто оцінити, наскільки добре забезпечено захист у хмарному середовищі, а й адаптувати аналіз під свої бізнес-процеси, галузеві вимоги або регуляторні обмеження.

У додатку передбачено можливість завантажити файл з критеріями для обраного провайдера (наприклад, AWS, Azure, GCP), після чого користувач вводить відповідні оцінки.

На Рисунку 3.3 наведено фрагмент інтерфейсу оцінювання, де відображено таблицю з критеріями, їх вагами та введеними значеннями.

Критерій	Метрика	Вага (%)	Бал (1-5)
Доступність	Uptime 99.95%	15	5
Надійність	MTBF ≥ 1100 годин	20	4
Безпека	Відповідає ISO/IEC 27001 та GDPR	25	5
Продуктивність	Час відповіді ≤ 190 мс	10	5
Масштабованість	Автоматичне масштабування Azure VM	5	5
Зручність	Azure Portal	5	4
Сумісність	Підтримка API, інтеграція з Azure AD	10	3
Гнучкість	Зміна конфігурації через ARM шаблони	10	4

Рисунок 3.3 – Інтерфейс введення оцінок користувачем

Після того, як користувач заповнить таблицю, ввівши необхідні дані, система автоматично розрахує інтегральний показник ефективності безпеки. Цей показник слугує комплексною оцінкою ефективності безпеки на основі оцінених критеріїв. Після цього розрахунку система генерує візуальне представлення у вигляді графіка. Цей графік призначений для того, щоб допомогти користувачам швидко визначити, які критерії отримали найнижчі бали, виділяючи ті з них, які мають значну важливість у загальній оцінці безпеки.

У цьому контексті на Рисунку 3.4 показано приклад графіка, отриманого за результатами оцінювання, що дозволяє користувачам легко інтерпретувати та аналізувати свої показники ефективності безпеки. Візуальне відображення не лише демонструє індивідуальні оцінки, але й підкреслює сфери, які можуть

потребувати подальшої уваги або вдосконалення, що дозволяє користувачам приймати обґрунтовані рішення на основі представлених даних.

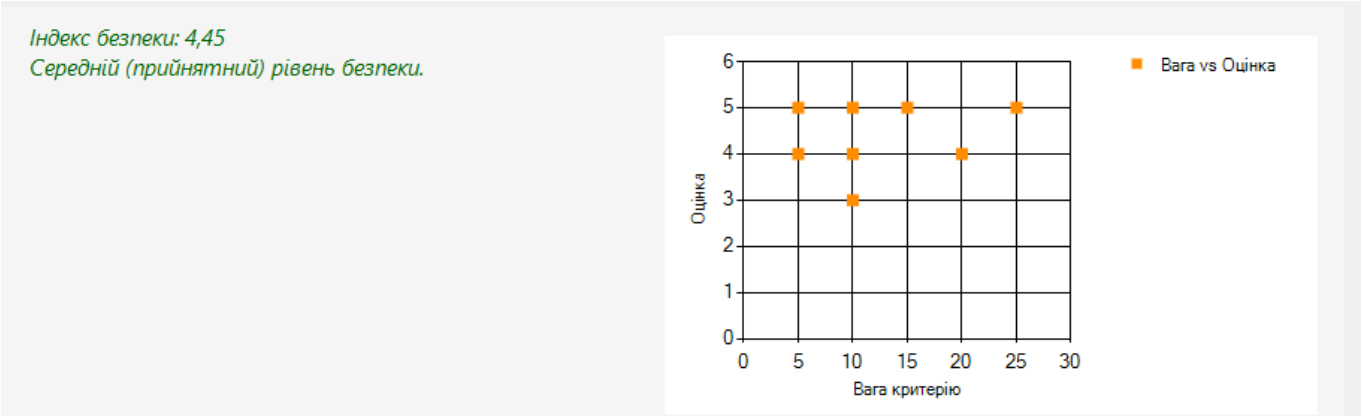

Рисунок 3.4 – Графік «Вага – Оцінка» для аналізу слабких місць

За результатами тестового оцінювання користувач отримує інтегральний бал за шкалою від 1 до 5, що інтерпретується як низький, середній або високий рівень захисту. Окрім цього, надаються текстові рекомендації, сформовані на основі виявлених слабких місць, зокрема у випадках низьких оцінок за критеріями з високим пріоритетом. Також генерується звіт у вигляді файлу, який можна використати для внутрішнього аудиту або для подальшого порівняння результатів у майбутньому.

Крім того, підтримується агреговане порівняння результатів різних провайдерів у файлі providers_summary.txt, що дозволяє обґрунтувати вибір оптимальної хмарної платформи.

Тестове оцінювання підтвердило здатність системи адаптуватися до специфічних умов організації, враховувати її потреби та надавати візуалізований, об’єктивний аналіз ефективності захисту персональних даних. Цей підхід забезпечує гнучкість у використанні механізму для компаній із різним рівнем цифрової зрілості. Така адаптивність гарантує, що всі організації, незалежно від того, чи вони тільки починають свій шлях цифрової трансформації, чи вже добре просунулися, можуть використовувати механізм для ефективного зміцнення своїх систем захисту даних.

3.5. Рекомендації щодо покращення захисту персональних даних на основі аналізу

На основі отриманих результатів тестового оцінювання, проведеного з використанням розробленого механізму, було сформовано перелік практичних рекомендацій для підвищення рівня захисту персональних даних у хмарному середовищі.

Ці рекомендації розроблені з урахуванням виявлених слабких місць, а також з урахуванням вагової значущості критеріїв безпеки, які організація вважає пріоритетними. Вони можуть бути використані як частина внутрішньої політики безпеки, або інтегровані до планів відповідності вимогам регуляторів (зокрема, GDPR, ISO/IEC 27001, SOC 2 тощо).

На поточному етапі рекомендовано звернути увагу на такі аспекти:

1)Регулярно використовувати механізм оцінювання для моніторингу стану захисту, принаймні щоквартально або після внесення змін до хмарної інфраструктури.

2)Актуалізувати критерії оцінки згідно зі зміною бізнес-процесів, загрозової моделі або появи нових регуляторних вимог.

3)Впровадити системи логування та звітності (audit logging) з подальшим аналізом журналів доступу до персональних даних.

4)Зміцнити контроль доступу через чітке визначення ролей користувачів, застосування принципу найменших привілеїв (PoLP) та впровадження багатофакторної автентифікації (MFA).

5)Підвищувати рівень обізнаності персоналу шляхом внутрішнього навчання та тренінгів щодо безпечної роботи в хмарних середовищах.

6)Автоматизувати політики виявлення аномалій, інтегруючи механізми штучного інтелекту для виявлення нетипової поведінки при роботі з персональними даними.

7)Періодично проводити аудит відповідності стандартам захисту даних із залученням сторонніх експертів або сертифікованих аудиторів.

8)Забезпечити резервне копіювання та зашифроване зберігання персональних даних, а також розробити та протестувати план відновлення після інцидентів (Disaster Recovery Plan).

9) Оцінювати надійність провайдерів на основі зібраної статистики (історія збоїв, наявність сертифікатів, відповідь на інциденти), використовуючи метрики з додатку.

Застосування вищезазначених рекомендацій дозволить не лише підвищити рівень захисту персональних даних, але й формалізувати процес управління безпекою в організації, що особливо важливо в умовах масштабованих та динамічних хмарних середовищ.

Висновки за розділом 3

У третьому розділі було здійснено практичну реалізацію розробленого механізму оцінювання ефективності захисту персональних даних у хмарному середовищі. Основну увагу приділено розробці вебдодатку, який об’єднує теоретичні засади багатокритеріального аналізу з реальними потребами організацій щодо управління безпекою даних.

Було виконано інтеграцію критеріїв і метрик безпеки у функціональність додатку, що дозволяє адаптувати процес оцінювання до конкретних вимог користувача. Завдяки реалізації моделі зваженої оцінки додаток надає кількісну інтерпретацію рівня захисту, а також візуальні інструменти аналізу слабких місць.

Тестове оцінювання продемонструвало можливості інструменту в контексті практичного застосування. Це підтвердило ефективність запропонованого підходу для використання в реальних умовах, зокрема в рамках внутрішнього аудиту або планування заходів інформаційної безпеки.

Запропоновані рекомендації, сформовані на основі результатів аналізу, можуть стати основою для побудови політик захисту даних у хмарі та сприяти підвищенню загального рівня кіберстійкості організації.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було досягнуто поставлену мету — підвищення ефективності захисту персональних даних у хмарних середовищах шляхом створення механізму їх об'єктивного оцінювання з урахуванням технічних, організаційних та регуляторних аспектів безпеки.

Основні результати проведеного дослідження:

1. Проведено аналіз сучасного стану захисту персональних даних у хмарних середовищах, розглянуто архітектуру хмарних обчислень, типи хмар, а також виявлено основні загрози та вразливості, притаманні хмарним платформам. Було також вивчено чинне законодавство України та міжнародні стандарти щодо захисту персональних даних.

2. Розроблено універсальний механізм оцінювання, заснований на методах багатокритеріального аналізу (MCDA) з використанням зваженої моделі. Механізм дозволяє обчислювати інтегральний індекс рівня захисту з урахуванням вагової значущості критеріїв.

3. Створено програмну реалізацію запропонованого механізму у вигляді вебдодатку з можливістю завантаження власних наборів критеріїв, введення оцінок користувачем, автоматичного обчислення показників ефективності, візуалізації результатів та генерації текстових звітів.

4. На основі результатів оцінювання сформовано практичні рекомендації щодо підвищення рівня захисту персональних даних. Вони включають технічні та організаційні заходи з акцентом на регулярний аудит, автоматизацію політик безпеки, посилення контролю доступу та обізнаності персоналу.

Таким чином, виконана робота має як теоретичну, так і практичну цінність, і може бути основою для подальших досліджень у сфері оцінювання безпеки інформаційних систем та розробки інструментів підтримки прийняття рішень у кібербезпеці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Зінченко О. В. Хмарні технології / О. В. Зінченко, С. В. Прокопов, С. О. Сєрих, В. В. Василенко, М. Ю. Березівський // Хмарні технології. – 2020. – С. 51–57.

2. Шемшур В. М. Хмарні технології / В. М. Шемшур, Б. С. Безпоясний [Електронний ресурс]. – Режим доступу: http://library.ippro.com.ua/attachments/article/.pdf – С. 4–8.

3. Батаєв С. В. Аналіз принципів роботи, переваг та викликів у використанні хмарних технологій в умовах сьогодення / С. В. Батаєв, О. С. Мельник // Вчені записки. – 2024. – № 3202431. – С. 40–43.

4. Яхно В. М. Аналіз ефективності хмарних обчислень для розподілених обчислювальних систем / В. М. Яхно, Н. В. Чупринка // Ukrainian Journal of Computing Innovations. – 2024. – № 2. – С. 15–18.

5. Кривенко П. О. Алгоритмічно-програмний метод планування та динамічного виділення ресурсів для хмарних обчислень / П. О. Кривенко. – 2020. – С. 8–11.

6. Закон України «Про хмарні послуги» [Електронний ресурс] // Верховна Рада України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення: 05.05.2025).

7. Закон України «Про захист персональних даних» [Електронний ресурс] // Верховна Рада України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 05.05.2025).

8. Скриньковський Р., Сопільник Р., Малашко О., Віконський В., Ковалів М., Процюк Т., Заяць Р. Принципи правового регулювання використання хмарних технологій для обробки персональних даних // Traektoriâ Nauki = Path of Science. – 2020. – Т. 6, № 7. – С. 2022–2029. DOI: 10.22178/pos.60-7.

9. Головацький Н. Т. Питання захисту персональних даних при використанні хмарних технологій // Аналітично-порівняльне правознавство. – 2024. – № 5. – С. 460–465.

10. Білобровко О. О. Засоби захисту даних у хмарних сервісах : дис. ... д-ра техн. наук / О. О. Білобровко. – Тернопіль : Західноукраїнський національний університет, 2023. – С. 9–11.

11. Soares L. F. B. Secure user authentication in cloud computing management interfaces / L. F. B. Soares // Proc. of the IEEE 32nd Int. Performance Computing and Communications Conf. (IPCCC), Dec. 6–8, 2013, San Diego, CA. – 2013. – P. 1–2.

12. Єсіна М. В., Онопрієнко В. В., Толок А. В. Моделі загроз хмарних послуг // Радіотехніка. – 2023. – № 212. – С. 36–41.

13. Oliveira D., Squicciarini A., Lin D. Cloud security baselines // In: Cloud computing security. – CRC Press, 2020. – P. 31–44.

14. Lin D., Squicciarini A. Data protection models for service provisioning in the cloud // Proc. of the 15th ACM Symp. on Access Control Models and Technologies. – 2010. – P. 183–192.

15. Akhtar N., Kerim B., Perwej Y., Tiwari A., Praveen S. A comprehensive overview of privacy and data security for cloud storage // Int. Journal of Scientific Research in Science, Engineering and Technology. – 2021. – Vol. 8, No. 3. – P. 131–138.

16. ТЗІ 2.5-004-99. Технічний захист інформації. Порядок створення комплексної системи захисту інформації. – Київ : Держкомзв’язку України, 1999.

17. ISO/IEC 27017:2015. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services. – Geneva : International Organization for Standardization, 2015.

18. Jansen W., Grance T. Guidelines on Security and Privacy in Public Cloud Computing (NIST SP 800-144). – Gaithersburg : National Institute of Standards and Technology, 2011.

19. Cloud Security Alliance. Cloud Controls Matrix (CCM) v4.0. – Cloud Security Alliance, 2021. [Електронний ресурс]. – Режим доступу: https://cloudsecurityalliance.org/

20. Nikitina L., Dzheniuk N., Borysova L. Експертна система для оцінки ризиків хмарних сервісів // Системи управління, навігації та зв'язку. Збірник наукових праць. – 2024. – № 1(75). – С. 146–151.

21. Фукс О., Пташинський М. Я., Марікуца У. Дослідження методів оцінювання якості хмарних сервісів, включаючи метрики надійності, продуктивності та безпеки // Herald of Khmelnytskyi National University. Technical sciences. – 2024. – № 335(3(1)). – С. 335–341.

22. Андрощук О., Голобородько М., Кондратенко Ю., Литовченко Г. Критерії та рекомендації з оцінювання якості хмарних сервісів для інформаційної інфраструктури // Сучасні інформаційні технології у сфері безпеки та оборони. – 2024. – № 51(3). – С. 60–70.

23. Назаренко Д. М. Дослідження методів захисту у хмарних системах. – 2023.

24. Іванченко І., Педченко Є. Структурна модель системи оцінювання кібербезпеки хмарних сервісів об'єктів інформаційної інфраструктури // Кібербезпека: освіта, наука, техніка. – 2024. – № 1(25). – С. 505–515.

25. Stergiou C., Psannis K. E., Kim B. G., Gupta B. Secure integration of IoT and cloud computing // Future Generation Computer Systems. – 2018. – Vol. 78. – P. 964–975.

26. Vehent J. Securing DevOps: security in the cloud. – Simon and Schuster, 2018.

27. Зарічук О. Г. Безпека в хмарних обчисленнях: методи забезпечення приватності та інтеграції в сучасних додатках // Управління розвитком. – 2024. – № 23(1). – С. 45.

ДОДАТКИ

Додаток А

Таблиця 2.1

Приклад оцінювання хмарного сервісу за критеріями безпеки

Критерій	Метрика (приклад)	Оцінка (1–5)	Вага (%)	Бал з урахуванням ваги
Доступність	Uptime 99.9%	5	20%	1.00
Надійність	MTBF ≥ 1000 годин	4	15%	0.60
Безпека	Відповідає ISO/IEC 27001	4	25%	1.00
Продуктивність	Час відповіді ≤ 200 мс	3	10%	0.30
Масштабованість	Автоматичне масштабування	5	10%	0.50
Зручність	Наявність панелі адміністрування	4	5%	0.20
Сумісність	Підтримка API, інтеграція з AD	3	10%	0.30
Гнучкість	Можливість швидкої зміни конфігурації	4	5%	0.20
Загальний бал				**4.10**

Додаток Б

Лістинг програми

```
#pragma endregion

// ---------------------- Кнопка: Завантажити AWS ----------------------
private: System::Void button5_Click(System::Object^ sender, System::EventArgs^ e)
{
	label2->Text = "";
	chart1->Series->Clear();
	dataGridView1->Rows->Clear();
	currentProviderName = "AWS";

	String^ filePath =
"C:\Users\ramul\University\Diplom\Evaluation\criteria\aws.txt";

	try {
		array<String^>^ lines = System::IO::File::ReadAllLines(filePath,
System::Text::Encoding::UTF8);

		for each (String ^ line in lines) {
			array<String^>^ parts = line->Split(';');
			if (parts->Length == 3) {
				String^ name = parts[0];
				String^ description = parts[1];
				double weight;

				if (Double::TryParse(parts[2], weight)) {
					int rowIndex = dataGridView1->Rows->Add();
					dataGridView1->Rows[rowIndex]->Cells[0]->Value
```

```
= name;
                                    dataGridView1->Rows[rowIndex]->Cells[1]->Value
= description;
                                    dataGridView1->Rows[rowIndex]->Cells[2]->Value
= weight;
                                    dataGridView1->Rows[rowIndex]->Cells[3]->Value
= nullptr;
                                }
                            }
                        }

                MessageBox::Show(gcnew String(u8"Критерії AWS успішно
завантажені!"),
                        gcnew String(u8"Завантаження"), MessageBoxButtons::OK,
MessageBoxIcon::Information);
        }
        catch (Exception^ ex) {
                MessageBox::Show(gcnew String(u8"Помилка при завантаженні: ") +
ex->Message,
                        gcnew String(u8"Помилка"), MessageBoxButtons::OK,
MessageBoxIcon::Error);
        }
}

// ---------------------- Кнопка: Завантажити Azure ----------------------
private: System::Void button6_Click(System::Object^ sender, System::EventArgs^ e)
{
        label2->Text = "";
        chart1->Series->Clear();
        dataGridView1->Rows->Clear();
```

```
        currentProviderName = "Azure";

        String^ filePath =
"C:\Users\ramul\University\Diplom\Evaluation\criteria\azure.txt";

        try {
            array<String^>^ lines = System::IO::File::ReadAllLines(filePath,
System::Text::Encoding::UTF8);

            for each (String ^ line in lines) {
                array<String^>^ parts = line->Split(';');
                if (parts->Length == 3) {
                    String^ name = parts[0];
                    String^ description = parts[1];
                    double weight;

                    if (Double::TryParse(parts[2], weight)) {
                        int rowIndex = dataGridView1->Rows->Add();
                        dataGridView1->Rows[rowIndex]->Cells[0]->Value
= name;
                        dataGridView1->Rows[rowIndex]->Cells[1]->Value
= description;
                        dataGridView1->Rows[rowIndex]->Cells[2]->Value
= weight;
                    }
                }
            }

            MessageBox::Show(gcnew String(u8"Критерії Azure успішно
завантажено!"),
```

```
                gcnew String(u8"Завантаження"), MessageBoxButtons::OK,
MessageBoxIcon::Information);
        }
        catch (Exception^ ex) {
                MessageBox::Show(gcnew String(u8"Помилка завантаження: ") + ex-
>Message,
                gcnew String(u8"Помилка"), MessageBoxButtons::OK,
MessageBoxIcon::Error);
        }
}

// ---------------------- Кнопка: Завантажити Google Cloud ----------------------
private: System::Void button7_Click(System::Object^ sender, System::EventArgs^ e)
{
        label2->Text = "";
        chart1->Series->Clear();
        dataGridView1->Rows->Clear();
        currentProviderName = "Google Cloud";

        String^ filePath =
"C:\Users\ramul\University\Diplom\Evaluation\criteria\google_cloud.txt";

        try {
                array<String^>^ lines = System::IO::File::ReadAllLines(filePath,
System::Text::Encoding::UTF8);

                for each (String ^ line in lines) {
                        array<String^>^ parts = line->Split(';');
                        if (parts->Length == 3) {
                                String^ name = parts[0];
```

```
                String^ description = parts[1];
                double weight;

                if (Double::TryParse(parts[2], weight)) {
                    int rowIndex = dataGridView1->Rows->Add();
                    dataGridView1->Rows[rowIndex]->Cells[0]->Value
= name;
                    dataGridView1->Rows[rowIndex]->Cells[1]->Value
= description;
                    dataGridView1->Rows[rowIndex]->Cells[2]->Value
= weight;
                }
            }
        }

        MessageBox::Show(gcnew String(u8"Критерії Google Cloud успішно
завантажені!"),
            gcnew String(u8"Завантаження"), MessageBoxButtons::OK,
MessageBoxIcon::Information);
    }
    catch (Exception^ ex) {
        MessageBox::Show(gcnew String(u8"Помилка завантаження: ") + ex-
>Message,
            gcnew String(u8"Помилка"), MessageBoxButtons::OK,
MessageBoxIcon::Error);
    }
}

// ---------------------- Кнопка: Розрахувати ----------------------
private: System::Void button1_Click(System::Object^ sender, System::EventArgs^ e)
```

```
{
    double sumWeightedScores = 0.0;
    double totalWeight = 0.0;
    bool anyScoreEntered = false;

    for (int i = 0; i < dataGridView1->Rows->Count; i++) {
        if (dataGridView1->Rows[i]->IsNewRow) continue;

        String^ weightStr = dataGridView1->Rows[i]->Cells[2]->Value != nullptr ?
            dataGridView1->Rows[i]->Cells[2]->Value->ToString() : "";
        String^ scoreStr = dataGridView1->Rows[i]->Cells[3]->Value != nullptr ?
            dataGridView1->Rows[i]->Cells[3]->Value->ToString() : "";

        if (weightStr->Length == 0 || scoreStr->Length == 0) {
            continue;
        }

        double weight = 0;
        double score = 0;

        if (!Double::TryParse(weightStr, weight) || !Double::TryParse(scoreStr, score)) {
            MessageBox::Show(gcnew String(u8"Введено некоректні числові
значення."),
                gcnew String(u8"Помилка"), MessageBoxButtons::OK,
MessageBoxIcon::Error);
            return;
        }

        if (score < 0 || score > 5) {
            MessageBox::Show(gcnew String(u8"Оцінки мають бути в межах від 0 до
```

```
5."),
            gcnew String(u8"Помилка"), MessageBoxButtons::OK,
MessageBoxIcon::Warning);
        return;
    }

    sumWeightedScores += weight * score;
    totalWeight += weight;
    anyScoreEntered = true;
  }

  if (!anyScoreEntered) {
    MessageBox::Show(gcnew String(u8"Будь ласка, введіть оцінки."),
      gcnew String(u8"Увага"), MessageBoxButtons::OK,
MessageBoxIcon::Information);
    return;
  }

  if (totalWeight == 0) {
    MessageBox::Show(gcnew String(u8"Ваги не задані або дорівнюють нулю."),
      gcnew String(u8"Помилка"), MessageBoxButtons::OK,
MessageBoxIcon::Error);
    return;
  }

  double index = sumWeightedScores / totalWeight;
  String^ conclusion;

  if (index >= 4.5) {
    conclusion = gcnew String(u8"Високий рівень безпеки.");
```

```
    }
    else if (index >= 3.5) {
        conclusion = gcnew String(u8"Середній (прийнятний) рівень безпеки.");
    }
    else {
        conclusion = gcnew String(u8"Низький рівень безпеки. Потребує
покращення.");
    }

    label2->Text = gcnew String(u8"Індекс безпеки: ") + index.ToString("0.00") +
"\n" + conclusion;

    if (currentProviderName == nullptr || currentProviderName->Length == 0) {
        currentProviderName = gcnew String(u8"Невідомий провайдер");
    }

    if (evaluatedProviders == nullptr) {
        evaluatedProviders = gcnew
System::Collections::Generic::List<System::Tuple<System::String^, double>^>();
    }

    evaluatedProviders->Add(gcnew Tuple<String^, double>(currentProviderName,
index));

    String^ table = gcnew String(u8"Критерії:\n");
    int widthCriteria = 20;
    int widthMetric = 50;
    int widthWeight = 10;
    int widthScore = 10;
```

```
    table += dataGridView1->Columns[0]->HeaderText->PadRight(widthCriteria);
    table += dataGridView1->Columns[1]->HeaderText->PadRight(widthMetric);
    table += dataGridView1->Columns[2]->HeaderText->PadRight(widthWeight);
    table += dataGridView1->Columns[3]->HeaderText->PadRight(widthScore);
    table += "\n";

    for (int i = 0; i < dataGridView1->Rows->Count; i++) {
        if (dataGridView1->Rows[i]->IsNewRow) continue;

        String^ val0 = dataGridView1->Rows[i]->Cells[0]->Value != nullptr ?
            dataGridView1->Rows[i]->Cells[0]->Value->ToString() : "";
        table += val0->PadRight(widthCriteria);

        String^ val1 = dataGridView1->Rows[i]->Cells[1]->Value != nullptr ?
            dataGridView1->Rows[i]->Cells[1]->Value->ToString() : "";
        table += val1->PadRight(widthMetric);

        String^ val2 = "";
        if (dataGridView1->Rows[i]->Cells[2]->Value != nullptr) {
            double w;
            if (Double::TryParse(dataGridView1->Rows[i]->Cells[2]->Value-
>ToString(), w))
                val2 = w.ToString("0.00");
            else
                val2 = dataGridView1->Rows[i]->Cells[2]->Value->ToString();
        }
        table += val2->PadRight(widthWeight);

        String^ val3 = "";
        if (dataGridView1->Rows[i]->Cells[3]->Value != nullptr) {
```

```
            double s;
            if (Double::TryParse(dataGridView1->Rows[i]->Cells[3]->Value-
>ToString(), s))
                val3 = s.ToString("0.00");
            else
                val3 = dataGridView1->Rows[i]->Cells[3]->Value->ToString();
        }
        table += val3->PadRight(widthScore);
        table += "\n";
    }

    String^ result = gcnew String(u8"Провайдер: ") + currentProviderName +
        gcnew String(u8"\nІндекс безпеки: ") + index.ToString("0.00") +
        gcnew String(u8"\n") + conclusion + gcnew String(u8"\n");

    System::IO::File::WriteAllText("last_provider.txt", table + "\n" + result,
System::Text::Encoding::UTF8);
    System::IO::File::AppendAllText("providers_summary.txt", table + "\n" + result +
"\n----------------------------\n", System::Text::Encoding::UTF8);
}

// ---------------------- Кнопка: Зберегти ----------------------
private: System::Void button2_Click(System::Object^ sender, System::EventArgs^ e)
{
        try {
                String^ filePath = "last_provider.txt";

                if (System::IO::File::Exists(filePath)) {
                        String^ msg = gcnew String(u8"Дані успішно
збережено!\nФайл: ") + System::IO::Path::GetFullPath(filePath);
```

```
                MessageBox::Show(msg, gcnew String(u8"Інформація"),
MessageBoxButtons::OK, MessageBoxIcon::Information);
                System::Diagnostics::Process::Start("notepad.exe", filePath);
            }
            else {
                MessageBox::Show(gcnew String(u8"Файл збереження не
знайдено. Спочатку виконайте розрахунок."),
                    gcnew String(u8"Увага"), MessageBoxButtons::OK,
MessageBoxIcon::Warning);
            }
        }
        catch (Exception^ ex) {
            MessageBox::Show(gcnew String(u8"Помилка при перевірці файлу:
") + ex->Message,
                gcnew String(u8"Помилка"), MessageBoxButtons::OK,
MessageBoxIcon::Error);
        }
}

// ---------------------- Кнопка: Завантажити звіт ----------------------
private: System::Void button4_Click(System::Object^ sender, System::EventArgs^ e)
{
        try {
            String^ reportPath = "providers_summary.txt";

            if (System::IO::File::Exists(reportPath)) {
                System::Diagnostics::Process::Start("notepad.exe", reportPath);
            }
            else {
                MessageBox::Show("Файл звіту не знайдено.", "Увага",
```

```
MessageBoxButtons::OK, MessageBoxIcon::Information);
            }
        }
        catch (Exception^ ex) {
            MessageBox::Show("Помилка при відкритті звіту: " + ex->Message,
"Помилка", MessageBoxButtons::OK, MessageBoxIcon::Error);
        }
}

// ---------------------- Кнопка: Побудувати графік ----------------------
private: System::Void button3_Click(System::Object^ sender, System::EventArgs^ e)
{
        try {
            chart1->Series->Clear();
            chart1->ChartAreas->Clear();
            chart1->ChartAreas->Add("MainArea");

            auto series = gcnew
System::Windows::Forms::DataVisualization::Charting::Series(gcnew String(L"Вага
vs Оцінка"));
            series->ChartType =
System::Windows::Forms::DataVisualization::Charting::SeriesChartType::Point;
            series->MarkerSize = 8;
            series->Color = System::Drawing::Color::DarkOrange;

            for (int i = 0; i < dataGridView1->Rows->Count; i++) {
                if (dataGridView1->Rows[i]->IsNewRow) continue;

                String^ weightStr = dataGridView1->Rows[i]->Cells[2]->Value
!= nullptr ?
```

```
                dataGridView1->Rows[i]->Cells[2]->Value->ToString() :
"";
            String^ scoreStr = dataGridView1->Rows[i]->Cells[3]->Value !=
nullptr ?
                dataGridView1->Rows[i]->Cells[3]->Value->ToString() :
"";

            double weight, score;
            if (Double::TryParse(weightStr, weight) &&
Double::TryParse(scoreStr, score)) {
                series->Points->AddXY(weight, score);
            }
        }

        chart1->Series->Add(series);

        auto axisY = chart1->ChartAreas["MainArea"]->AxisY;
        axisY->Minimum = 0;
        axisY->Maximum = 6;
        axisY->Interval = 1;
        axisY->Title = gcnew String(L"Оцінка");

        chart1->ChartAreas["MainArea"]->AxisX->Title = gcnew
String(L"Вага критерію");
    }
    catch (Exception^ ex) {
        MessageBox::Show("Помилка при побудові графіка: " + ex-
>Message,
            "Помилка", MessageBoxButtons::OK, MessageBoxIcon::Error);
    }
```

```
}
// ---------------------- Кнопка: Завершити роботу ----------------------
private: System::Void button8_Click(System::Object^ sender, System::EventArgs^ e)
{
	this->Close();}
```