МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ **МОДЕЛІ Й ТЕХНОЛОГІЇ ХМАРНОЇ БЕЗПЕКИ** ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Євгенія ЗАВГОРОДНЯ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД-42

Євгенія ЗАВГОРОДНЯ
Ім’я, ПРІЗВИЩЕ

Керівник: Тетяна МУЖАНОВА
к. держ. упр., доцент Ім’я, ПРІЗВИЩЕ

Рецензент:
Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Завгородній Євгенії Ярославівні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Моделі й технології хмарної безпеки ”,
керівник кваліфікаційної роботи МУЖАНОВА Тетяна, к. держ. упр., доцент,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “20” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека, проблеми безпеки в хмарних середовищах, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити теоретичні основи хмарної безпеки.
4.2. Проаналізувати сучасні технології забезпечення безпеки в хмарних середовищах.
4.3. Розробити рекомендації та вивчити перспективи розвитку технологій хмарної безпеки.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Дослідження теоретичних основ хмарної безпеки.	08.04.2025	
4.	Аналіз сучасних технологій забезпечення безпеки в хмарних середовищах.	22.04.2025	
5.	Розробка рекомендацій та вивчення перспектив розвитку технологій хмарної безпеки.	08.05.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2025	
7.	Оформлення роботи.	22.05.2025	
8.	Оформлення презентації.	03.06.2025	
9.	Отримання рецензії на роботу.	03.06.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувачка вищої освіти _____ Євгенія ЗАВГОРОДНЯ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна Мужанова
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувачка Завгородня Є.Я. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Моделі й технології хмарної безпеки"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка ЗАВГОРОДНЯ Євгенія у кваліфікаційній роботі дослідила теоретичні основи хмарної безпеки, проаналізувала сучасні технології забезпечення безпеки в хмарних середовищах, розробила рекомендації та вивчила перспективи розвитку технологій хмарної безпеки.

ЗАВГОРОДНЯ Євгенія показала розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довела володіння методами наукового дослідження, проявила себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки ЗАВГОРОДНЬОЇ Євгенії на оцінку "відмінно" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Завгородня Є.Я. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти ЗАВГОРОДНЬОЇ Євгенії
на тему “Моделі й технології хмарної безпеки”

Актуальність. У світі, де хмарні технології стають основою цифрової трансформації, питання їх безпеки набуває критичного значення. Швидке зростання популярності хмарних обчислень супроводжується зростанням загроз та вразливостей, які можуть призвести до витоку даних, фінансових втрат і порушення конфіденційності. Крім того, міжнародні стандарти та нормативні вимоги до хмарної безпеки постійно вдосконалюються, що вимагає адаптації організацій до нових умов.

Враховуючи ці аспекти, дослідження моделей та технологій хмарної безпеки є актуальним науковим завданням, яке сприятиме розробці ефективних методів захисту даних та інформаційних систем у хмарних середовищах.

Позитивні сторони.

1. У роботі досліджено сучасні моделі та технології хмарної безпеки, зокрема механізми автентифікації, управління доступом, шифрування та моніторинг загроз.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Авторка опрацювала значну джерельну базу: близько 50 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо вдосконалення механізмів хмарної безпеки та розглянуто перспективи використання штучного інтелекту для виявлення загроз у хмарних середовищах.

Недоліки.

Доцільно було б глибше проаналізувати питання регулювання хмарної безпеки на рівні міжнародних організацій, а також розглянути практичні кейси впровадження технологій безпеки в реальних компаніях.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувачка ЗАВГОРОДНЯ Євгенія заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____

підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню моделей та технологій хмарної безпеки. Робота складається зі вступу, трьох розділів, що містять 9 рисунків та 9 таблиць, висновків і списку використаних джерел із 49 найменувань. Загальний обсяг роботи становить 77 аркушів, з яких 6 аркушів займає список використаних джерел.

Метою роботи є дослідження моделей і технологій забезпечення безпеки в хмарних обчисленнях та розробка рекомендацій щодо підвищення рівня захисту даних у хмарних середовищах.

Об'єктом дослідження є методи та підходи забезпечення безпеки в хмарних обчисленнях.

Предмет дослідження – особливості застосування сучасних моделей і технологій забезпечення хмарної безпеки.

Методи дослідження. Для вирішення поставленого наукового завдання використано методи аналізу та синтезу, порівняння, моделювання, системного підходу, оцінки ризиків, а також методи експертної оцінки технологій хмарної безпеки.

Як результат у роботі досліджено теоретичні основи хмарної безпеки, проаналізовано сучасні технології забезпечення безпеки в хмарних середовищах, розроблено рекомендації та вивчено перспективи розвитку технологій хмарної безпеки.

Галузь застосування. Розроблені підходи можуть бути використані для підвищення рівня безпеки корпоративних інформаційних систем, що працюють у хмарному середовищі, а також у процесі впровадження політик інформаційної безпеки відповідно до міжнародних стандартів.

Ключові слова: ХМАРНА БЕЗПЕКА, МОДЕЛІ ТА ТЕХНОЛОГІЇ ХМАРНОЇ БЕЗПЕКИ, УПРАВЛІННЯ ДОСТУПОМ, ШИФРУВАННЯ ДАНИХ, ЗАХИСТ ІНФОРМАЦІЇ, МОНІТОРИНГ КІБЕРЗАГРОЗ.

ABSTRACT

The qualification work is devoted to the study of cloud security models and technologies. The work consists of an introduction, three chapters containing 9 figures and 9 tables, conclusions and the list of references containing 49 items. The total volume of the work is 77 pages, of which 6 pages are occupied by the list of references.

The purpose of the study is to investigate models and technologies for ensuring security in cloud computing and to develop recommendations for improving the level of data protection in cloud environments.

The object the study is the methods and approaches to ensuring security in cloud computing.

The subject of the study is the peculiarities of applying modern models and technologies for cloud security.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, modelling, systematic approach, risk assessment, as well as methods of expert evaluation of cloud security technologies were used.

As a result, the work investigates the theoretical foundations of cloud security, analyses modern security technologies in cloud environments, develops recommendations and studies the prospects for the development of cloud security technologies.

Field of application. The developed approaches can be used to improve the security of corporate information systems operating in the cloud environment, as well as in the process of implementing information security policies in accordance with international standards.

Keywords: CLOUD SECURITY, MODELS AND TECHNOLOGIES OF CLOUD SECURITY, ACCESS CONTROL, DATA ENCRYPTION, INFORMATION PROTECTION, CYBER THREAT MONITORING.

ЗМІСТ

ВСТУП ……..... 9

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ХМАРНОЇ БЕЗПЕКИ……. 11

1.1 Сутність та основні характеристики хмарних обчислень……. 11

1.2 Загрози та вразливості хмарних середовищ……..……..…….. 18

1.3 Нормативно-правові вимоги до хмарної безпеки……... 24

Висновки до розділу 1 29

РОЗДІЛ 2 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ХМАРНИХ СЕРЕДОВИЩАХ…… 31

2.1 Механізми автентифікації та управління доступом у хмарних середовищах…… 32

2.2 Використання Zero Trust підходу в хмарній безпеці……..... 38

2.3 Захист від кібератак та методи виявлення загроз у хмарних сервісах… 43

Висновки до розділу 2 49

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ХМАРНОЇ БЕЗПЕКИ……..… 50

3.1 Перспективи розвитку технологій шифрування та конфіденційних обчислень…… 50

3.2 Використання штучного інтелекту та машинного навчання для підвищення безпеки хмарних платформ…… 58

3.3 Рекомендації щодо покращення політик безпеки у хмарних сервісах.. 65

Висновки до розділу 3 68

ВИСНОВКИ …… 70

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ …… 72

ВСТУП

Актуальність теми. У світі, де компанії, державні установи та окремі користувачі активно використовують хмарні технології, питання забезпечення їхньої безпеки набуває критичного значення. Зростання популярності хмарних обчислень супроводжується збільшенням кількості кіберзагроз, які можуть призвести до витоку конфіденційної інформації, фінансових втрат та порушення цілісності даних. Розвиток технологій штучного інтелекту, інтернету речей (IoT) та великих даних (Big Data) створює нові виклики для захисту інформації в хмарних середовищах. Впровадження ефективних моделей і технологій безпеки є ключовим завданням для організацій, які використовують хмарні сервіси.

З огляду на зазначене, дослідження моделей і технологій хмарної безпеки є актуальним науковим завданням, яке сприятиме розробці ефективних методів захисту даних у хмарних обчисленнях.

Мета роботи полягає у дослідженні моделей і технологій забезпечення безпеки в хмарних обчисленнях та розробці рекомендацій щодо підвищення рівня захисту даних у хмарних середовищах.

Об'єкт дослідження – методи та підходи забезпечення безпеки в хмарних обчисленнях.

Предмет дослідження – особливості застосування сучасних моделей і технологій забезпечення хмарної безпеки.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити теоретичні основи хмарної безпеки.

2. Проаналізувати сучасні технології забезпечення безпеки в хмарних середовищах.

3. Розробити рекомендації та вивчити перспективи розвитку технологій хмарної безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використано методи аналізу та синтезу, порівняння, моделювання, системного підходу, оцінки ризиків, а також методи експертної

оцінки технологій хмарної безпеки.

Практичне значення одержаних результатів. Застосування напрацьованих моделей і технологій хмарної безпеки дозволить здійснити обґрунтований вибір методів і інструментів для забезпечення захисту даних у хмарних середовищах. Результати дослідження можуть бути використані для впровадження ефективних механізмів управління доступом, шифрування інформації та моніторингу загроз, що сприятиме підвищенню рівня безпеки корпоративних інформаційних систем. Запропоновані підходи також можуть бути застосовані в розробці політик хмарної безпеки відповідно до міжнародних стандартів та нормативних вимог, що забезпечить надійний захист даних з урахуванням можливостей і ресурсів організації.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ХМАРНОЇ БЕЗПЕКИ

Хмарні обчислення стали важливою складовою IT-інфраструктури підприємств, державних установ і приватних користувачів. Вони забезпечують масштабованість, гнучкість та ефективність використання ресурсів, дозволяючи організаціям оптимізувати витрати на обчислювальні потужності та зберігання даних. Однак стрімке поширення хмарних технологій супроводжується зростанням ризиків, пов’язаних із забезпеченням безпеки даних, контролем доступу та захистом від кіберзагроз.

Однією з ключових проблем хмарної безпеки є відсутність фізичного контролю над даними, оскільки вони можуть зберігатися на серверах у різних юрисдикціях та передаватися між дата-центрами. Це створює додаткові виклики у сфері дотримання нормативних вимог, зокрема міжнародних стандартів та національного законодавства.

Розвиток технологій кіберзахисту дозволяє впроваджувати новітні методи управління безпекою в хмарних середовищах. До них належать механізми багатофакторної автентифікації, шифрування даних, розмежування доступу, використання моделей Zero Trust та адаптивного моніторингу загроз.

1.1. Сутність та основні характеристики хмарних обчислень

Хмарні обчислення (Cloud Computing) — це модель надання обчислювальних ресурсів, яка забезпечує доступ до спільних ресурсів, таких як сервери, сховища, бази даних, програмне забезпечення та мережі, через інтернет. Основна ідея хмарних обчислень полягає у можливості використання обчислювальних потужностей як послуги без необхідності володіння фізичним обладнанням.

Концепція хмарних обчислень ґрунтується на принципах віртуалізації, розподіленої обробки даних та автоматизованого керування ресурсами. Користувачі можуть отримувати обчислювальні потужності на вимогу,

масштабувати їх відповідно до потреб і оплачувати лише використані ресурси, що робить цю модель економічно вигідною.

Сутність хмарних обчислень полягає у моделі надання IT-послуг, яка передбачає використання спільних ресурсів провайдерів, доступних користувачам через мережу Інтернет. Завдяки цьому організації можуть значно зменшити витрати на підтримку локальної IT-інфраструктури, зосереджуючись на розвитку власних бізнес-процесів. Хмарні технології забезпечують користувачам високу гнучкість, масштабованість та надійність, що є ключовими факторами їхньої популярності.

Однією з основних характеристик хмарних обчислень є можливість самообслуговування на вимогу, що дозволяє користувачам самостійно замовляти, конфігурувати та використовувати необхідні обчислювальні ресурси без необхідності втручання з боку провайдера. Такий підхід мінімізує часові витрати на розгортання інфраструктури, забезпечуючи оперативний доступ до необхідних потужностей. Важливим аспектом є також широкий мережевий доступ, що передбачає можливість використання хмарних сервісів з будь-якого пристрою, який має підключення до Інтернету. Це забезпечує гнучкість роботи та спрощує взаємодію між користувачами і системами [1].

Хмарні обчислення базуються на принципі об’єднання ресурсів, що передбачає багатокористувацьку архітектуру. Провайдери використовують моделі мультиоренди (multi-tenancy) (рис. 1.1), коли один фізичний сервер або кластер серверів одночасно обслуговує декілька незалежних користувачів, розподіляючи ресурси таким чином, щоб забезпечити максимальну ефективність та продуктивність. Це дозволяє значно зменшити вартість послуг для кінцевих споживачів, оскільки ресурси використовуються оптимально.

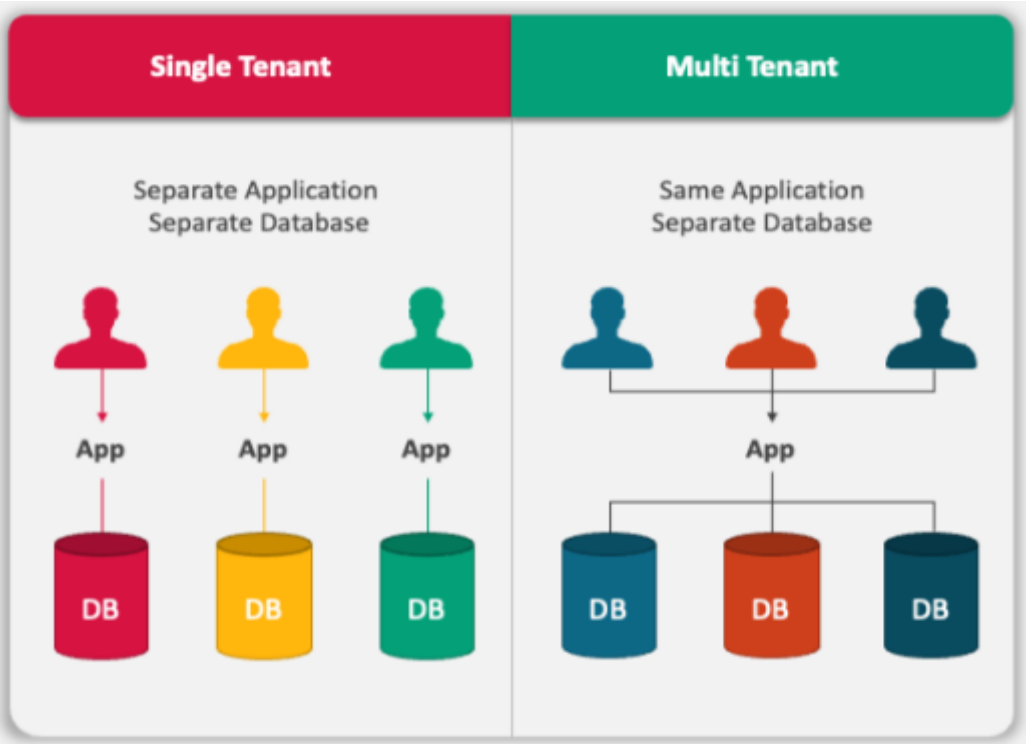

Рис. 1.1. Модель мультиоренди (multi-tenancy)

Ще однією важливою характеристикою є еластичність та масштабованість, що дозволяє користувачам у режимі реального часу збільшувати або зменшувати обсяги використовуваних ресурсів відповідно до поточних потреб. Така можливість особливо актуальна для підприємств, які працюють у динамічному середовищі та потребують гнучкого управління IT-інфраструктурою. Висока адаптивність хмарних обчислень дозволяє швидко реагувати на зміну навантаження, що забезпечує стабільність та безперервність бізнес-процесів [2].

Оскільки хмарні обчислення функціонують на основі моделей сервісного надання послуг, розрізняють три основні підходи до їхньої реалізації. Їх порівняння вказано у таблиці 1.1.

Інфраструктура як послуга (Infrastructure as a Service, IaaS) передбачає надання користувачам доступу до віртуальних серверів, дискових сховищ, мережевих ресурсів та інших базових компонентів, що дозволяє їм самостійно конфігурувати і керувати власним середовищем. Ця модель надає користувачам великий контроль над своїми ресурсами, що дає змогу оптимізувати інфраструктуру під специфічні вимоги проекту, забезпечуючи високу ступінь кастомізації.

Таблиця 1.1.

Відмінності між моделями IaaS, PaaS та SaaS

Характеристика	IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)	SaaS (Software as a Service)
Опис	Надає інфраструктурні ресурси (сервери, сховища, мережі) у вигляді віртуалізованих сервісів	Надає платформу для розробки, тестування та розгортання додатків	Надає готові програмні рішення, доступні через Інтернет
Цільова аудиторія	Адміністратори, розробники, підприємства, які хочуть контролювати IT-інфраструктуру	Розробники, компанії, які створюють власні додатки	Кінцеві користувачі, які працюють із готовими сервісами
Контроль користувача	Користувач контролює ОС, віртуальні машини, сховище та мережеві налаштування	Користувач контролює лише додатки, дані та середовище розробки	Мінімальний контроль – користувач отримує готовий сервіс
Приклади сервісів	Amazon EC2, Google Compute Engine, Microsoft Azure Virtual Machines	Google App Engine, Microsoft Azure App Services, AWS Elastic Beanstalk	Google Workspace (Docs, Gmail), Microsoft 365, Dropbox
Переваги	Гнучкість у налаштуванні ресурсів, економія на фізичній інфраструктурі	Прискорює розробку ПЗ, усуває потребу в адміністрування серверів	Легка доступність, немає потреби в технічному обслуговуванні
Недоліки	Потребує адміністрування та налаштування, складність управління	Менший контроль над середовищем, обмежена гнучкість	Обмежена можливість кастомізації, залежність від провайдера

Використання IaaS дозволяє компаніям знизити витрати на придбання фізичного обладнання та утримання власних дата-центрів, оскільки всі ресурси, такі як сервери, мережі, сховища, розміщуються в хмарі і доступні за запитом. Вона також дозволяє масштабувати ресурси в залежності від потреб бізнесу, швидко збільшуючи чи зменшуючи потужності на основі змін в навантаженні чи попиті.

Незважаючи на високий рівень гнучкості, IaaS вимагає значних технічних знань та кваліфікації для належного адміністрування. Користувачі повинні мати навички в налаштуванні віртуальних машин, управлінні мережами та системами безпеки, а також у забезпеченні збереження даних та їхньої доступності. Відповідальність за налаштування, оновлення та підтримку інфраструктури лягає на кінцевого користувача, що може бути як перевагою, так і недоліком для тих, хто не має достатньої експертизи у цих питаннях [3].

Інфраструктура як послуга є оптимальним рішенням для великих підприємств, які потребують повного контролю над інфраструктурою, або для компаній, що мають специфічні вимоги до конфігурації своїх систем. Завдяки IaaS бізнеси можуть оперативно реагувати на зміни, спрощуючи процеси управління інфраструктурою та мінімізуючи час на впровадження нових технологій.

Платформа як послуга (Platform as a Service, PaaS) забезпечує користувачам середовище для розробки, тестування та розгортання додатків без необхідності адміністрування інфраструктури. Вона пропонує повністю керовану платформу, яка включає не тільки середовище для написання коду, але й підтримує інтеграцію з різними сервісами, такими як бази даних, сховища для зберігання даних, а також інструменти для аналізу та моніторингу продуктивності. Ця модель значно спрощує процес створення програмного забезпечення, оскільки розробники можуть використовувати попередньо налаштовані сервери, бази даних та інші сервіси, що дозволяє їм зосередитись виключно на розробці та реалізації функціональності додатка.

Оскільки адміністрування та підтримка інфраструктури лягають на постачальника послуги, компанії та розробники мають можливість зменшити витрати на технічну підтримку та інфраструктурні ресурси. Такий підхід є оптимальним для компаній, які зосереджені на розробці інноваційних рішень та прагнуть мінімізувати витрати на підтримку IT-інфраструктури, звільняючи ресурси для творчості, інновацій та швидкої адаптації до змінюваних умов ринку. Крім того, PaaS дозволяє легко масштабувати додатки, що важливо в умовах швидкого зростання користувацької бази або змін в обсягах даних [4].

Ця модель платформи також є перевагою для стартапів та малих бізнесів, які не мають великої IT-інфраструктури, але прагнуть запускати продуктивні рішення без необхідності інвестувати в значні технічні ресурси. Крім того, PaaS підтримує високий рівень автоматизації, що значно зменшує час на розробку та тестування програмного забезпечення, дозволяючи команді швидше реагувати на зміни вимог і створювати більш ефективні та надійні продукти.

Програмне забезпечення як послуга (Software as a Service, SaaS) надає користувачам готові програмні рішення, доступні через Інтернет. Це одна з найбільш популярних та розповсюджених моделей хмарних технологій, яка забезпечує доступ до різноманітних додатків і сервісів без необхідності встановлення їх на локальні пристрої. Користувачі отримують можливість працювати з програмами через веб-браузер, що значно спрощує процес інтеграції та використання таких рішень.

До популярних сервісів SaaS можна віднести хмарні системи управління підприємствами (ERP), електронну пошту, сервіси зберігання даних (наприклад, Google Drive, Dropbox), офісні пакети (як-от Microsoft 365 чи Google Workspace), а також спеціалізовані програми для управління проектами, фінансами та комунікацією. SaaS дозволяє компаніям і користувачам отримувати необхідні функціональні можливості без необхідності інвестувати в розробку, встановлення або оновлення програмного забезпечення [5].

Однією з головних переваг SaaS є значне зменшення витрат на закупівлю та обслуговування програмного забезпечення, оскільки користувачі не повинні

платити за ліцензії чи витрачати ресурси на інсталяцію та технічне обслуговування програм. Усі ці аспекти беруть на себе постачальники послуг, що забезпечує безперервну доступність оновлень і підтримки. Крім того, SaaS дає можливість для гнучкого доступу до програм з будь-якого пристрою, підключеного до Інтернету, що особливо корисно для мобільних користувачів та віддалених команд [6].

Завдяки своїй простоті у використанні, швидкому запуску та доступу до програмних рішень через Інтернет, SaaS стає оптимальним вибором для малого та середнього бізнесу, а також для стартапів, які хочуть зменшити витрати на IT-інфраструктуру та максимально зосередитись на своєму основному бізнесі.

На рисунку 1.2. зображено відмінність між моделями IaaS, PaaS та SaaS.

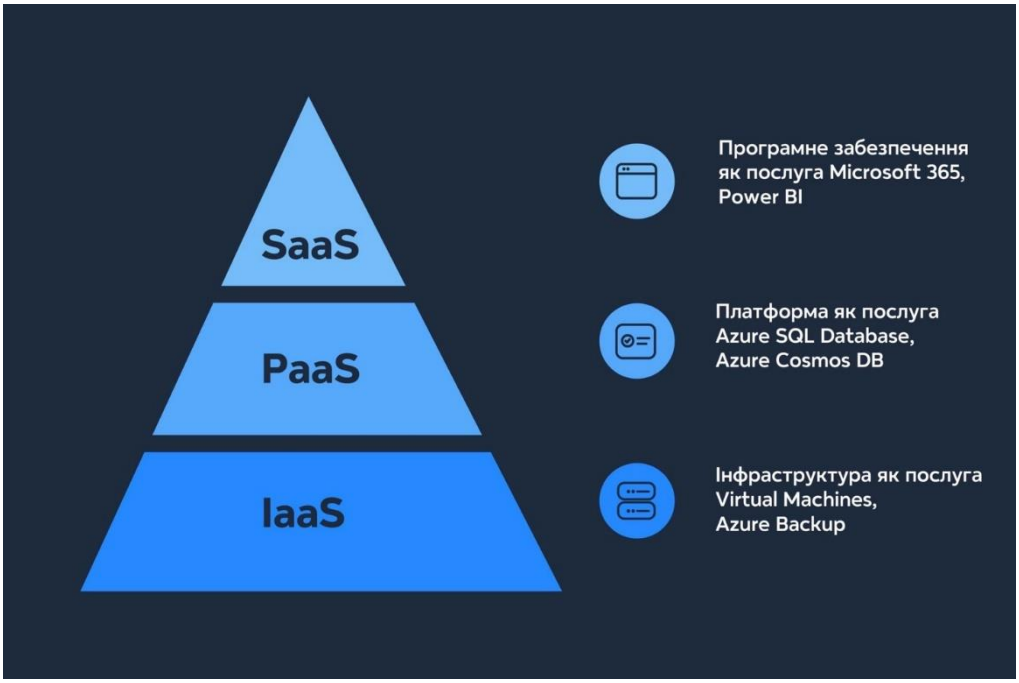

Рис. 1.2. Співвідношення моделей IaaS, PaaS та SaaS

Залежно від рівня доступності та контролю над ресурсами, хмарні обчислення можуть бути реалізовані у вигляді приватних, публічних, гібридних або мультихмарних середовищ. Приватна хмара забезпечує використання ресурсів лише однією організацією, що надає високий рівень безпеки та контролю, але водночас потребує значних витрат на розгортання та адміністрування. Публічні хмари є найбільш поширеним варіантом, оскільки забезпечують широкий доступ до ресурсів, які надаються провайдерами на

умовах підписки або за моделлю оплати за використання. Гібридні хмари поєднують переваги приватних та публічних моделей, дозволяючи організаціям гнучко керувати своїми даними та обчислювальними ресурсами.

В останні роки зростає популярність мультихмарних середовищ, які передбачають використання кількох незалежних хмарних платформ для оптимізації продуктивності, надійності та безпеки. Такий підхід дозволяє організаціям уникати залежності від одного провайдера, розподіляючи навантаження між різними платформами [7].

Хмарні обчислення є однією з ключових технологій цифрової трансформації, яка надає широкі можливості для оптимізації бізнес-процесів, зменшення витрат та підвищення гнучкості використання IT-ресурсів. Однак, поряд із численними перевагами, ця технологія створює нові виклики у сфері інформаційної безпеки, що вимагає розробки ефективних механізмів захисту даних, управління доступом та контролю за дотриманням нормативних вимог.

1.2. Загрози та вразливості хмарних середовищ

Загрози та вразливості хмарних середовищ є важливим аспектом у контексті забезпечення інформаційної безпеки. Хмарні технології, незважаючи на свою популярність і численні переваги, створюють нові виклики для підприємств і організацій у питаннях захисту даних, доступу до сервісів і управління інформаційними потоками. Враховуючи, що хмара надає доступ до критично важливих даних і ресурсів через Інтернет, її захист потребує спеціальних підходів і рішень для забезпечення конфіденційності, цілісності та доступності інформації. Загрози та вразливості хмарних середовищ можуть виникати на різних рівнях, від фізичної інфраструктури до застосунків, що працюють на хмарних платформах. Модель загроз для хмарних середовищ вказана на рис. 1.3.

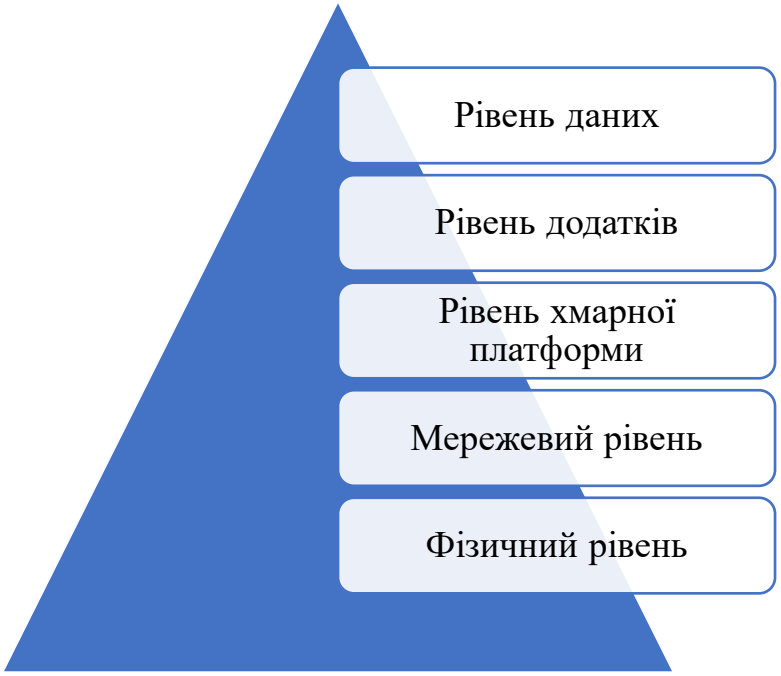

Рис. 1.3. Модель загроз для хмарних середовищ

Однією з основних загроз для хмарних середовищ є небезпека несанкціонованого доступу до даних. В умовах хмарних обчислень дані часто зберігаються на віддалених серверах, що знаходяться в дата-центрах, керованих постачальниками хмарних послуг. Це створює ризик доступу зловмисників до інформації через мережу Інтернет. Оскільки провайдери хмарних послуг є сторонами, які забезпечують фізичну та програмну інфраструктуру, вони можуть мати доступ до даних користувачів, що підвищує ризик витоку конфіденційної інформації. У разі неправильного налаштування доступу, неправильних налаштувань безпеки або слабких паролів, зловмисники можуть здобути доступ до даних або систем у хмарі [8].

Іншою серйозною загрозою є загроза витоку даних, яка може статися через недостатній контроль над тим, хто має доступ до чутливої інформації. Зловмисники можуть використовувати вразливості в хмарних сервісах для перехоплення даних або отримання несанкціонованого доступу до баз даних, особливо у разі використання ненадійних або застарілих методів шифрування. Після отримання доступу до даних зловмисники можуть красти, змінювати або публікувати інформацію, що може завдати значної шкоди як окремим користувачам, так і цілим організаціям.

Вразливості хмарних середовищ часто виникають через помилки у конфігураціях або через недотримання кращих практик з налаштування безпеки. Недостатня увага до налаштувань доступу, дефолтні паролі, неправильне налаштування мережевого доступу або відсутність шифрування на етапах передачі даних можуть стати основою для проникнення в систему (табл. 1.2). Враховуючи, що хмарні середовища зазвичай обслуговують велику кількість користувачів, відсутність централізованого контролю за налаштуваннями безпеки може призвести до збільшення кількості вразливих точок, через які можна здійснити атаку.

Таблиця 1.2.

Вразливості хмарних середовищ та їхні джерела

Вразливість	Джерело проблеми
Неправильні налаштування доступу	Помилки в конфігураціях доступу, використання слабких паролів
Використання дефолтних паролів	Неадекватна зміна паролів за замовчуванням у системах або на серверах
Невірне налаштування мережевого доступу	Відкриті порти, неправильна конфігурація міжсистемної безпеки
Відсутність шифрування даних	Шифрування не застосовується під час передачі або зберігання даних
Вразливості в сторонніх додатках	Недосконала безпека інтегрованих сторонніх програм або бібліотек
Відсутність централізованого контролю за безпекою	Розрізненість налаштувань безпеки у різних частинах хмарної інфраструктури

Також важливим аспектом є проблема захисту від атак на віддалене управління хмарними інфраструктурами. Платформи, які надають інтерфейси для адміністрування хмарної інфраструктури, можуть стати об'єктом атак з боку зловмисників, які намагаються здобути контроль над хмарною інфраструктурою. Уразливості в цих інтерфейсах або вразливі точки доступу до адміністративних панелей можуть дозволити злочинцям змінити налаштування хмарного

середовища або здійснити атаку на системи. Наприклад, використання неавторизованих методів доступу до інтерфейсів управління або експлуатація уразливостей в API (інтерфейсах програмування додатків) може призвести до серйозних наслідків.

Ще однією загрозою є атаки типу «відмова в обслуговуванні" (DDoS - Distributed Denial of Service). Хмарні сервіси можуть бути ціллю для масованих атак, спрямованих на їх паралізацію. Атаки DDoS можуть бути використані для створення значного навантаження на сервери, через що сервіси стають недоступними для легітимних користувачів. Оскільки хмарні середовища часто мають динамічний характер (збільшення або зменшення ресурсів залежно від потреб), ці атаки можуть бути більш ефективними, якщо сервіси не мають належного захисту або резервних механізмів від таких загроз [9].

Хмарні середовища можуть також зазнати атак через вразливості в сторонніх додатках, які інтегруються з хмарними платформами. У разі, якщо організація використовує сторонні програми або додатки для роботи в хмарі, уразливості в цих додатках можуть стати "вікном" для проникнення в основну інфраструктуру хмарної платформи. Це особливо стосується випадків, коли додатки не оновлюються регулярно або мають неперевірену безпеку. В такому випадку зловмисники можуть скористатися недоліками в сторонніх додатках для здійснення атак на хмарну платформу.

Іншою проблемою є загроза витоку даних через спільне використання ресурсів у хмарі (мультиорендність). У випадку, якщо кілька користувачів або організацій використовують одні й ті ж фізичні сервери або сховища даних, існує ризик того, що один орендар може отримати доступ до даних іншого. Це може статися через уразливості в механізмах розділення даних між різними користувачами або через помилки у налаштуваннях. Хоча провайдери хмарних послуг зазвичай забезпечують заходи безпеки для поділу даних, ця проблема залишається важливою, особливо для організацій, що обробляють конфіденційну інформацію [10].

Проблема законодавчого та нормативного забезпечення є ще однією важливою загрозою для хмарних середовищ. Хмарні послуги часто надаються провайдерами, які мають інфраструктуру в різних країнах або навіть на різних континентах. Це створює проблеми у плані дотримання національних законів щодо захисту персональних даних або іншої чутливої інформації. Наприклад, зберігання даних в країнах, де рівень захисту інформації є низьким або не відповідає міжнародним стандартам, може призвести до порушення законодавства, що впливає на репутацію організацій і може призвести до штрафів та санкцій. Потенційні проблеми нормативно-правового забезпечення, пов'язані з хмарними послугами та захистом персональних даних показані в таблиці 1.3.

Таблиця 1.3.

Потенційні проблеми нормативно-правового забезпечення, пов'язані з хмарними послугами та захистом персональних даних

Проблема	Опис	Приклад країни / регіону	Можливі наслідки
Міжнародне розташування інфраструктури	Хмарні сервіси часто мають сервери в різних країнах, що створює труднощі для дотримання національних законів.	США, ЄС, Китай, Індія	Труднощі з контролем за дотриманням законів, різні вимоги до захисту інформації.
Низький рівень захисту персональних даних	Зберігання даних в країнах з низьким рівнем захисту персональних даних може порушити законодавство.	країни, що розвиваються, де рівень захисту слабший	Порушення законів щодо захисту персональних даних, штрафи, санкції.

Продовження табл. 1.3.

Неузгодженість стандартів захисту даних	Відсутність єдиних стандартів щодо захисту персональних даних між країнами та міжнародними організаціями.	Різні країни, що не мають спільних стандартів	Ризик втрати даних або порушення приватності, негативний вплив на репутацію організації.
Штрафи та санкції	Порушення національних та міжнародних законів щодо зберігання та обробки даних може призвести до штрафів.	ЄС (GDPR), США (CCPA)	Великий фінансовий штраф, судові розгляди, відновлення репутації організації.

Загроза зловживання правами доступу також є важливою проблемою для хмарних середовищ. Логічне управління доступом є важливим для забезпечення безпеки, оскільки дозволяє контролювати, хто може отримувати доступ до яких ресурсів в хмарі. Неправильне або неналежне адміністрування прав доступу може призвести до того, що несанкціоновані особи отримають доступ до критично важливої інформації. Оскільки в хмарі використовується мультиорендність і спільні ресурси, контроль за доступом стає ще більш важливим, оскільки помилка в налаштуваннях прав може призвести до серйозних наслідків для кількох організацій одночасно.

Загрози та вразливості хмарних середовищ потребують комплексного підходу до їх виявлення та управління. Використання сучасних методів захисту, таких як багаторівнева аутентифікація, шифрування, моніторинг та аудит, допомагає знижувати ризики і забезпечувати надійність хмарних платформ. Багаторівнева аутентифікація, зокрема, є важливою для запобігання несанкціонованому доступу, оскільки вона вимагає від користувачів додаткових підтверджень особистості, що ускладнює злом акаунтів. Шифрування забезпечує конфіденційність даних, як під час їх зберігання, так і під час передачі через

мережу, що робить їх менш уразливими до атак [11].

Моніторинг і аудит є критично важливими для виявлення підозрілих активностей та швидкого реагування на інциденти. Регулярний моніторинг хмарних систем дозволяє оперативно виявляти порушення безпеки або ненавмисні помилки, які можуть спричинити витік або пошкодження даних. Аудит дозволяє аналізувати лог-файли та інші дані для виявлення слабких місць в інфраструктурі або процесах.

Однак, щоб гарантувати максимальний рівень безпеки, організації повинні постійно оновлювати свої стратегії захисту, враховуючи нові загрози та вразливості, що виникають у сфері хмарних технологій. Системи безпеки мають бути гнучкими та адаптивними до змін у технологічному середовищі, нових типів атак і вразливостей, що з’являються з часом. Постійне навчання та підвищення кваліфікації персоналу також є важливим компонентом стратегії захисту, оскільки людський фактор часто стає причиною порушень безпеки. Регулярне оновлення та вдосконалення політик безпеки допомагає організаціям мінімізувати ризики і підтримувати надійність своїх хмарних платформ.

1.3. Нормативно-правові вимоги до хмарної безпеки

Нормативно-правові вимоги до хмарної безпеки є важливим аспектом правового регулювання в сучасному світі інформаційних технологій, зокрема в умовах інтенсивного розвитку хмарних технологій. Хмара, як концепція обробки і зберігання даних, передбачає передачу та обробку величезних обсягів інформації, що може включати персональні дані, корпоративну інформацію, а також інші чутливі дані, що вимагає забезпечення високого рівня безпеки. У зв'язку з цим питання нормативно-правового регулювання, що стосується хмарної безпеки, набувають особливої актуальності, оскільки вони визначають основи для захисту інформації, прав користувачів та відповідальності в разі порушення безпеки.

Однією з головних проблем при обробці та зберіганні даних в хмарах є їхнє

місцезнаходження. Оскільки хмарні сервіси зазвичай мають розподілену інфраструктуру, дані можуть зберігатися на серверах, розташованих у різних юрисдикціях, що ускладнює застосування національних стандартів безпеки. Це створює виклики для розробки єдиних міжнародних нормативних актів, що дозволяють узгодити вимоги безпеки з різними правовими системами та підходами до захисту даних.

У зв'язку з цими викликами виникає необхідність гармонізації правових норм, що регулюють обробку даних у хмарних середовищах, з міжнародними стандартами безпеки. Одним із найбільш значущих документів у цій сфері є Загальний регламент захисту даних Європейського Союзу (GDPR), що визначає основні вимоги щодо обробки персональних даних у межах ЄС та для організацій, що обробляють дані громадян Європейського Союзу. GDPR вперше встановив єдині вимоги до обробки персональних даних, що застосовуються до всіх організацій, незалежно від того, в якій країні вони зареєстровані. Це регулювання охоплює всі аспекти обробки даних, включаючи питання зберігання, передачі, використання та знищення даних у хмарних середовищах. Основні принципи GDPR щодо хмарної безпеки показані в таблиці 1.4.

Таблиця 1.4

Основні принципи GDPR та їх застосування до хмарної безпеки

Принцип GDPR	Опис принципу	Застосування в хмарній безпеці
Принцип прозорості	Потрібно інформувати користувачів про обробку їх даних	Постачальники послуг повинні повідомляти, як, де і з якою метою обробляються дані
Принцип мінімізації даних	Збір і обробка тільки необхідних даних	Постачальники повинні обробляти лише ті дані, які необхідні для виконання цілей
Принцип забезпечення безпеки	Забезпечення належного захисту даних	Використання шифрування, багатофакторної аутентифікації та систем моніторингу

Згідно з GDPR, постачальники хмарних послуг повинні відповідати низці вимог щодо забезпечення безпеки обробки персональних даних. Однією з основних вимог є надання користувачам прозорої інформації про те, як їхні дані обробляються. Організації повинні інформувати користувачів про мету збору даних, способи їх обробки, а також про можливі ризики для безпеки даних, які можуть виникнути при обробці. Зокрема, якщо дані зберігаються або обробляються поза межами ЄС, це має бути чітко зазначено, оскільки це може впливати на рівень захисту даних у залежності від юрисдикції [12].

Окрім прозорості, регламент передбачає принципи мінімізації даних, які вимагають, щоб постачальники хмарних послуг обробляли лише ті дані, які необхідні для виконання визначених цілей. Згідно з цим принципом, збір даних має бути обмежений, а самі дані не можуть зберігатися довше, ніж це необхідно для досягнення поставлених цілей. Цей принцип стає особливо важливим у випадках, коли обробка даних стосується чутливих категорій інформації, таких як медичні дані чи фінансові записи [13].

Іншим важливим фактором є принцип забезпечення безпеки, який передбачає застосування відповідних технічних і організаційних заходів для захисту даних від несанкціонованого доступу, змін або знищення. Це охоплює використання методів шифрування для захисту даних під час передачі та зберігання, застосування багатофакторної аутентифікації для доступу до систем, а також впровадження систем моніторингу та аудиту для виявлення можливих загроз. Кожен постачальник хмарних послуг зобов'язаний також забезпечити можливість відновлення даних у випадку їх втрати або пошкодження, що є важливим аспектом забезпечення безперервності бізнес-процесів. Цикл управління безпекою даних у хмарах представлений на рисунку 1.4.

Рис. 1.4 Цикл управління безпекою даних у хмарах

Не менш важливим є питання юридичної відповідальності в разі порушення вимог щодо безпеки даних. Відповідно до GDPR, в разі порушення безпеки даних, постачальник послуг зобов'язаний повідомити користувачів та наглядові органи протягом 72 годин після виявлення інциденту. Це передбачає відповідальність за втрату даних або несанкціонований доступ до них, а також передбачає фінансові штрафи за невиконання вимог регламенту. Санкції можуть бути дуже значними, що є стимулом для постачальників хмарних послуг забезпечувати належний рівень безпеки своїх систем [14].

ISO/IEC 27001 є ще одним важливим міжнародним стандартом, що визначає вимоги до управління інформаційною безпекою в організаціях, які надають хмарні послуги. Стандарт містить комплекс вимог до побудови системи управління інформаційною безпекою (СУІБ), що включає в себе ідентифікацію та оцінку ризиків, розробку політик безпеки, а також постійний моніторинг і удосконалення заходів безпеки. Дотримання вимог ISO/IEC 27001 дозволяє хмарним постачальникам послуг довести свою відповідність міжнародним стандартам безпеки і підвищити довіру своїх клієнтів.

Основні вимоги для хмарних постачальників відповідно до стандарту ISO/IEC 27001 показані у таблиці 1.5.

Таблиця 1.5

Основні вимоги для хмарних постачальників за стандартом ISO/IEC 27001

Вимога стандарту ISO/IEC 27001	Опис вимоги
Оцінка ризиків	Визначення та оцінка потенційних ризиків для інформаційної безпеки в хмарних середовищах
Впровадження політик безпеки	Розробка внутрішніх політик для захисту інформації та управління безпекою
Моніторинг і аудит	Постійний моніторинг систем і проведення аудиту безпеки для виявлення загроз
Удосконалення систем безпеки	Оновлення та удосконалення заходів безпеки на основі виявлених уразливостей
Управління доступом	Обмеження доступу до критичної інформації за допомогою методів аутентифікації та авторизації

Рис. 1.5 ілюструє взаємозв'язок між основними міжнародними нормативними документами, що регулюють питання хмарної безпеки, зокрема GDPR, ISO/IEC 27001 і ISO/IEC 27018.

Рис. 1.5 Міжнародні нормативні документи з безпеки хмарних технологій

Варто зазначити, що окрім загальних нормативних актів і стандартів безпеки, існують також специфічні вимоги для певних галузей, що особливо чутливі до питання безпеки даних. Наприклад, у сфері охорони здоров'я існують особливі вимоги до захисту медичних записів, у тому числі щодо їх зберігання у

хмарах. Законодавство, яке регулює захист медичних даних, вимагає застосування посиленого захисту, зокрема шифрування даних та забезпечення їх цілісності.

Подібні вимоги також можуть бути актуальними для фінансового сектору, де обробка та зберігання даних клієнтів вимагає особливих заходів безпеки, таких як використання криптографічних засобів для захисту фінансових транзакцій. У багатьох країнах існують закони, які вимагають застосування таких технологій для забезпечення безпеки фінансових даних, а також для запобігання шахрайству і фінансовим злочинам [15].

Важливою частиною правового регулювання хмарної безпеки є питання юрисдикції, оскільки дані, що зберігаються на хмарних серверах, можуть переміщуватися через міжнародні кордони. Це створює проблеми для застосування місцевих норм безпеки, оскільки різні країни можуть мати різні вимоги до захисту даних. Зокрема, деякі країни можуть не мати таких же суворих вимог до захисту даних, як країни ЄС, що може вплинути на рівень безпеки в хмарі.

Нормативно-правові вимоги до хмарної безпеки є важливим елементом забезпечення належного рівня захисту даних у хмарних сервісах. Вони визначають права і обов'язки постачальників послуг та користувачів, а також гарантують захист від несанкціонованого доступу та порушень безпеки. Успішне впровадження таких вимог дозволяє створити надійну правову основу для розвитку хмарних технологій і забезпечення їхньої безпеки в глобальному масштабі.

Висновки до розділу 1

У розділі розглянуто ключові аспекти, що стосуються хмарних технологій, їхніх характеристик, загроз та вразливостей, а також нормативно-правових вимог, які регулюють безпеку в хмарних середовищах.

Досліджено сутність хмарних обчислень як технології, що дозволяє ефективно використовувати ресурси обчислювальних систем через Інтернет.

Охарактеризовано основні типи хмарних сервісів (IaaS, PaaS, SaaS), які пропонують різні рівні доступу до ресурсів та послуг, розглянуто переваги хмарних технологій, серед яких масштабованість, гнучкість, економічність і можливість доступу до високоякісних ресурсів без значних капіталовкладень.

Аналіз основних загроз і вразливостей, характерних для хмарних середовищ, показав, що хмара, завдяки своїй дистрибутивній природі, стикається з численними ризиками, такими як несанкціонований доступ, втрата даних, порушення конфіденційності та цілісності даних, а також можливі збої в роботі інфраструктури. Важливим є забезпечення високого рівня безпеки для запобігання таких загроз через використання надійних методів шифрування, моніторингу та управління доступом.

Проаналізовано нормативно-правові вимоги до хмарної безпеки, зокрема основні документи, які регулюють захист даних у хмарних середовищах. Акцентовано увагу на положеннях міжнародних нормативних документів, таких як GDPR, ISO/IEC 27001, та їх застосуванні для забезпечення безпеки даних, що зберігаються в хмарах. Окрім цього, було розглянуто важливість відповідності локальним вимогам в різних юрисдикціях, а також необхідність забезпечення конфіденційності та доступності даних при використанні хмарних технологій.

Теоретичні основи хмарної безпеки є комплексною і багатоаспектною темою, яка охоплює як технологічні, так і правові аспекти. Важливим завданням є розробка та впровадження ефективних стратегій захисту даних в хмарних середовищах, враховуючи постійно зростаючі загрози та вимоги до правового регулювання. Успішне забезпечення безпеки в хмарах потребує інтеграції технічних заходів безпеки з відповідними нормативно-правовими актами та стандартами, що створюють основу для надійного та ефективного використання хмарних технологій.

Розділ 2 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ХМАРНИХ СЕРЕДОВИЩАХ

Хмарні технології стали фундаментом для обробки, зберігання та управління даними. Вони забезпечують гнучкість, масштабованість та економічну ефективність для бізнесу будь-якого рівня. Проте, разом із поширенням хмарних сервісів, зростає і необхідність у надійному захисті даних, що передаються, обробляються або зберігаються у віддалених середовищах. Аналіз сучасних технологій забезпечення безпеки в хмарних середовищах охоплює широкий спектр рішень і методів, які спрямовані на виявлення, запобігання та реагування на кіберзагрози.

Однією з найважливіших технологій є шифрування даних — як у стані спокою, так і під час передачі. Сучасні хмарні провайдери застосовують передові криптографічні алгоритми, зокрема AES-256 для зберігання даних і TLS 1.3 для їх передачі мережею. Це гарантує, що навіть у разі несанкціонованого доступу дані залишаться нерозшифрованими і непридатними для використання. Окрім цього, зростає популярність концепції «нульового довіри» (Zero Trust Security), яка базується на принципі постійної перевірки автентичності користувачів і пристроїв незалежно від їх розташування в мережі. Це передбачає багатофакторну автентифікацію (MFA), мікросегментацію мережі, контроль привілеїв і поведінкову аналітику [16].

Ще одним важливим напрямом є застосування засобів виявлення загроз (Threat Detection) та засобів управління подіями інформаційної безпеки (SIEM). Завдяки інтеграції машинного навчання та штучного інтелекту, сучасні системи можуть у реальному часі виявляти аномалії у поведінці користувачів, шкідливі дії або підозрілі патерни. Такі технології дозволяють запобігати атакам ще на ранніх етапах, знижуючи ризики витоку конфіденційної інформації.

Окрему роль відіграє управління ідентифікацією та доступом (IAM). У великих хмарних середовищах необхідно мати точний контроль над тим, хто має доступ до яких ресурсів. Технології IAM забезпечують створення політик

доступу, аудит дій користувачів, автоматичне відкликання прав у разі зміни ролі користувача чи його звільнення. Розширення цієї концепції в контексті хмари призвело до появи рішень Cloud Identity Governance.

Зростання популярності контейнерних технологій, таких як Docker та Kubernetes, викликало необхідність впровадження нових методів безпеки. Це зокрема безпека на рівні контейнерів, сканування образів на наявність вразливостей, контроль над мережевими політиками контейнерів, а також застосування технологій безпечної інтеграції та доставки (DevSecOps). Забезпечення безпеки має бути інтегрованим у весь життєвий цикл розробки програмного забезпечення — від кодування до розгортання.

Варто також згадати про важливість відповідності стандартам і регуляторним вимогам (наприклад, GDPR, ISO/IEC 27001, HIPAA), адже хмарні середовища часто обслуговують користувачів з різних юрисдикцій. Провайдери хмарних послуг повинні гарантувати прозорість, контроль над обробкою персональних даних, а також можливість незалежного аудиту [17].

У підсумку, ефективне забезпечення безпеки в хмарних середовищах потребує комплексного підходу: поєднання технічних засобів, політик, навчання персоналу та постійного моніторингу. Оскільки загрози постійно еволюціонують, компаніям потрібно інвестувати в інноваційні рішення і співпрацювати з надійними хмарними провайдерами, аби гарантувати безпеку своїх даних і бізнес-процесів.

2.1 Механізми автентифікації та управління доступом у хмарних середовищах

Багатофакторна автентифікація (MFA) є ключовим елементом сучасної стратегії кібербезпеки в хмарних середовищах. Вона забезпечує додатковий рівень захисту, вимагаючи від користувачів підтвердження своєї особи за допомогою двох або більше факторів. Це значно зменшує ризик несанкціонованого доступу, навіть якщо зловмисник отримав пароль

користувача.

Основні методи автентифікації охоплюють(рис. 2.1):

- Одноразові паролі (OTP): генеруються додатками, такими як Google Authenticator або Authy, і мають обмежений час дії.
- Фізичні токени: пристрої, як-от YubiKey, які забезпечують високий рівень безпеки.
- Біометричні дані: використання відбитків пальців, розпізнавання обличчя або сканування райдужної оболонки ока.
- SMS-коди: хоча менш безпечні через можливість перехоплення, все ще використовуються як додатковий фактор.

Рис. 2.1. Основні методи автентифікації

Впровадження MFA повинно бути комплексним і охоплювати всі критичні системи та облікові записи, особливо адміністративні. Згідно з дослідженням Palo Alto Networks, багато хмарних облікових записів мають серйозні вразливості через відсутність належних заходів безпеки, включаючи MFA [18].

Важливо впроваджувати адаптивну MFA, яка враховує контекстні фактори, такі як місцезнаходження користувача, пристрій, з якого здійснюється вхід, та поведінкові патерни. Це дозволяє зменшити кількість запитів на додаткову автентифікацію для звичних дій, водночас посилюючи захист у випадках підозрілої активності.

Навчання користувачів є невід'ємною частиною ефективного

впровадження MFA. Співробітники повинні розуміти важливість багатофакторної автентифікації, вміти розпізнавати фішингові атаки та знати, як правильно використовувати засоби автентифікації.

Регулярний моніторинг і аудит MFA-систем допомагає виявляти та реагувати на підозрілу активність. Це включає аналіз журналів входу, виявлення невдалих спроб автентифікації та незвичних входів. Також важливо мати плани на випадок відмови MFA, наприклад, використання резервних кодів або альтернативних методів автентифікації.

Впровадження багатофакторної автентифікації в хмарних середовищах є критично важливим для забезпечення безпеки даних та систем. Це вимагає комплексного підходу, який включає вибір відповідних методів автентифікації, адаптивні механізми, навчання користувачів та постійний моніторинг.

Управління ідентифікацією та доступом (IAM) є критично важливим компонентом забезпечення безпеки в хмарних середовищах [19]. Зі зростанням використання хмарних технологій, організації стикаються з необхідністю ефективного контролю над тим, хто має доступ до яких ресурсів і на яких умовах. IAM дозволяє централізовано управляти ідентифікацією користувачів, контролювати їх доступ до ресурсів, забезпечувати відповідність політикам безпеки та знижувати ризики несанкціонованого доступу.

Однією з ключових практик в IAM є впровадження принципу найменших привілеїв (PoLP), який передбачає надання користувачам лише тих прав доступу, які необхідні для виконання їхніх обов'язків. Це зменшує ймовірність зловживання правами доступу та обмежує потенційні наслідки у разі компрометації облікового запису. Для реалізації цього принципу рекомендується використовувати рольову модель доступу (RBAC), де права доступу призначаються не окремим користувачам, а ролям, які відповідають певним функціональним обов'язкам [20].

Важливою частиною IAM є автоматизація процесів надання та відкликання доступу. Використання автоматизованих систем управління життєвим циклом ідентифікацій (Identity Lifecycle Management) дозволяє забезпечити своєчасне

оновлення прав доступу відповідно до змін у статусі користувача, наприклад, при зміні посади або звільненні. Це мінімізує ризик залишення активних облікових записів з надмірними правами доступу.

В умовах багатохмарного середовища особливу увагу слід приділяти централізації управління ідентифікацією. Використання єдиного постачальника ідентифікацій (Identity Provider, IdP) дозволяє забезпечити узгодженість політик безпеки, спростити управління доступом та покращити видимість активності користувачів [21]. Крім того, інтеграція з системами єдиного входу (Single Sign-On, SSO) підвищує зручність для користувачів та зменшує кількість облікових записів, які потрібно управляти.

Моніторинг та аудит дій користувачів є невід'ємною частиною ефективного IAM. Збір та аналіз журналів доступу дозволяє виявляти аномальні або підозрілі дії, що можуть свідчити про спроби несанкціонованого доступу або внутрішні загрози. Використання аналітичних інструментів та систем виявлення загроз допомагає своєчасно реагувати на інциденти безпеки.

Також важливо враховувати специфіку управління доступом для нефізичних ідентифікацій, таких як облікові записи служб, API-ключі та токени доступу. Ці ідентифікації часто мають широкі права доступу і можуть бути використані зловмисниками у разі компрометації [22]. Рекомендується застосовувати принцип найменших привілеїв, регулярно перевіряти та відкликати невикористовувані облікові записи, а також використовувати спеціалізовані інструменти для управління доступом у хмарній інфраструктурі.

IAM повинен бути гнучким та адаптивним, здатним швидко реагувати на зміни в організаційній структурі, технологічному середовищі та загрозах безпеці. Впровадження політик умовного доступу (Conditional Access), які враховують контекстні фактори, такі як місцезнаходження користувача, тип пристрою або рівень ризику, дозволяє забезпечити більш точний контроль над доступом до ресурсів.

Ефективне управління ідентифікацією та доступом в хмарних середовищах вимагає комплексного підходу, який поєднує технологічні рішення, політики

безпеки, навчання персоналу та постійний моніторинг [23]. Це дозволяє забезпечити захист критичних ресурсів, зменшити ризики несанкціонованого доступу та відповідати вимогам нормативних актів і стандартів безпеки. Основні компоненти IAM та їх переваги наведені в табл. 2.1.

Таблиця 2.1

Основні компоненти IAM

Компонент IAM	Опис	Переваги
Принцип найменших привілеїв (PoLP)	Надання мінімально необхідних прав доступу	Зменшує ризик зловживань та витоку даних
Рольова модель доступу (RBAC)	Призначення доступу на основі ролей	Централізація, зручне управління
Автоматизація IAM	Управління життєвим циклом доступу	Зниження людських помилок, вчасне відкликання прав
Централізоване управління	Єдиний постачальник ідентифікацій (IdP) та SSO	Зменшення складності, підвищення прозорості
Моніторинг та аудит	Запис дій користувачів та аналіз журналів	Виявлення інцидентів, швидке реагування
Управління нефізичними ідентифікаторами	Контроль облікових записів служб, API-ключів, токенів	Захист автоматизованого доступу до хмарних ресурсів
Умовний доступ (Conditional Access)	Контекстні політики доступу (локація, пристрій, ризик)	Гнучкість, динамічне реагування на зміну середовища користувача

Принцип найменших привілеїв (Least Privilege Access) є фундаментальним підходом до забезпечення безпеки в хмарних середовищах. Він передбачає надання користувачам, процесам і системам лише тих прав доступу, які необхідні для виконання їхніх конкретних завдань [24]. Цей підхід мінімізує ризик несанкціонованого доступу та зловживання привілеями, що особливо актуально в умовах зростаючої кількості кіберзагроз.

Одним із ключових аспектів реалізації принципу найменших привілеїв є проведення регулярних аудитів привілеїв. Це дозволяє виявити надмірні або

застарілі права доступу та своєчасно їх відкликати. Згідно з рекомендаціями експертів, важливо також розмежовувати облікові записи адміністратора та стандартного користувача, щоб обмежити можливості для несанкціонованих змін у системі.

Для ефективного управління привілеями рекомендується використовувати модель рольового доступу (RBAC), яка дозволяє призначати права доступу на основі ролей, а не індивідуально для кожного користувача [25]. Це спрощує адміністрування та забезпечує більшу прозорість у розподілі прав.

Ще одним важливим елементом є впровадження тимчасових привілеїв доступу (Just-In-Time Access). Це означає, що користувачі отримують необхідні права лише на час виконання конкретного завдання, після чого ці права автоматично відкликаються. Такий підхід зменшує ризик зловживання привілеями та підвищує загальний рівень безпеки.

Важливо також впроваджувати системи управління привілейованим доступом (PAM), які дозволяють контролювати та моніторити доступ до критичних ресурсів. Ці системи забезпечують централізоване управління привілеями, автоматизують процеси надання та відкликання доступу, а також ведуть детальний журнал дій користувачів.

У хмарних середовищах особливу увагу слід приділяти управлінню доступом до облікових записів служб, API-ключів та токенів доступу. Ці ідентифікатори часто мають широкі права доступу і можуть бути використані зловмисниками у разі компрометації [26]. Рекомендується застосовувати принцип найменших привілеїв, регулярно перевіряти та відкликати невикористовувані облікові записи, а також використовувати спеціалізовані інструменти для управління правами доступу в хмарній інфраструктурі.

Важливо впроваджувати політики умовного доступу (Conditional Access), які враховують контекстні фактори, такі як місцезнаходження користувача, тип пристрою або рівень ризику. Це дозволяє забезпечити більш точний контроль над доступом до ресурсів та підвищити загальний рівень безпеки.

Основні аспекти наведено на рис. 2.2.

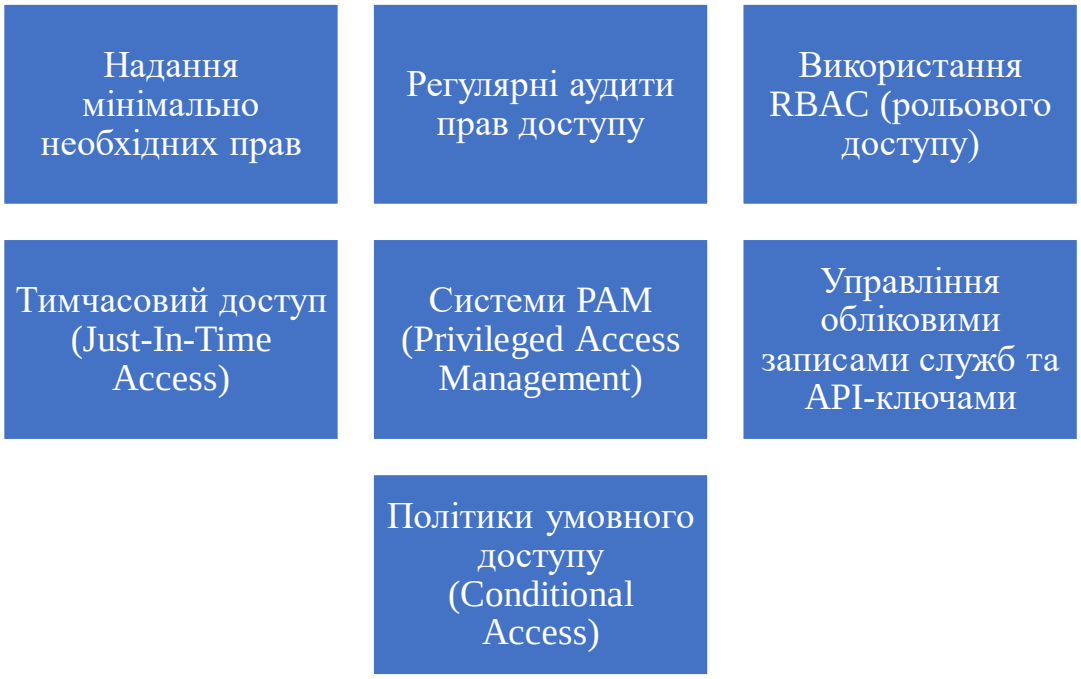

Рис. 2.2. Перелік ключових аспектів принципу найменших привілеїв

Впровадження принципу найменших привілеїв в хмарних середовищах є критично важливим для забезпечення безпеки даних та систем. Це вимагає комплексного підходу, який включає регулярні аудити привілеїв, використання моделей рольового доступу, впровадження тимчасових привілеїв, систем управління привілейованим доступом, а також політик умовного доступу. Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу та забезпечити високий рівень захисту в хмарних середовищах [27].

2.2 Використання Zero Trust підходу в хмарній безпеці

Концепція Zero Trust (ZT) ґрунтується на принципі «нікому не довіряй, перевіряй усіх», що є суттєвою відмінністю від традиційних моделей безпеки, які передбачають існування «надійного» периметру. У хмарному середовищі, де ресурси розподілені, а кордони мережі розмиті, Zero Trust стає особливо актуальним. Один із ключових аспектів його реалізації – це постійна верифікація користувачів та пристроїв, незалежно від їхнього розташування. На відміну від класичних підходів, де доступ часто надається на основі IP-адреси або знаходження всередині корпоративної мережі, ZT вимагає багатофакторної

аутентифікації (MFA), аналізу контексту (наприклад, час, геолокація, тип пристрою) та постійного моніторингу поведінки [28]. Це дозволяє мінімізувати ризики, пов’язані з витоком облікових даних або компрометацією пристроїв.

Важливим елементом Zero Trust у хмарі є сегментація мережі на основі мікросегментів. На відміну від традиційних широких мережевих зон, мікросегментація дозволяє ізолювати окремі робочі навантаження, сервіси або навіть процеси, обмежуючи можливість горизонтального пересування зловмисників. Наприклад, якщо хакер отримає доступ до одного віртуального сервера, він не зможе автоматично поширитися на інші ресурси через жорсткі правила міжсегментного доступу. Для реалізації цього підходу використовуються програмно-визначені мережі (SDN), брокери безпечного доступу (SAB) та політики, засновані на атрибутах (ABAC) [29].

Іншим критичним компонентом є шифрування даних як під час передачі, так і під час зберігання. У моделі Zero Trust будь-який трафік між сервісами, користувачами або компонентами хмарної інфраструктури має бути зашифрований, навіть якщо він передається всередині «надійної» мережі. Це особливо важливо в умовах публічних хмар, де фізичний контроль над інфраструктурою відсутній. Використання протоколів TLS, IPSec, а також технологій контейнерного шифрування (наприклад, AWS KMS або Azure Key Vault) дозволяє забезпечити конфіденційність і цілісність даних [30].

Крім того, Zero Trust передбачає автоматизований аналіз ризиків і адаптивний контроль доступу. Системи, такі як SIEM (Security Information and Event Management) разом із машинним навчанням, дозволяють виявляти аномалії в реальному часі – наприклад, незвичайні спроби доступу або підозрілу активність користувачів. На основі цих даних політики доступу можуть динамічно змінюватися, наприклад, вимагати додаткового підтвердження або повністю блокувати сесію. Таким чином, навіть якщо зловмисник отримає доступ до системи, його можливості будуть обмежені.

Основні компоненти Zero Trust зібрані у табл. 2.2

Таблиця 2.2

Основні компоненти Zero Trust

Компонент	Опис	Приклади технологій/інструментів
Багатофакторна аутентифікація (MFA)	Постійна верифікація користувачів через кілька факторів (пароль, SMS, біометрія).	Google Authenticator, Microsoft Authenticator, YubiKey
Мікросегментація мережі	Розділення мережі на ізольовані сегменти для запобігання горизонтальному пересуванню.	VMware NSX, Cisco ACI, AWS Security Groups
Шифрування даних	Захист даних під час передачі та зберігання.	TLS, IPSec, AWS KMS, Azure Key Vault
Адаптивний контроль доступу	Динамічне змінення рівня доступу на основі аналізу ризиків.	Okta, Azure AD Conditional Access, Palo Alto Prisma
Автоматизований моніторинг (SIEM)	Аналіз логів і подій безпеки в реальному часі.	Splunk, IBM QRadar, Microsoft Sentinel

Реалізація Zero Trust у хмарних середовищах вимагає інтеграції різних технологій і підходів, серед яких центральне місце займає ідентифікація та управління доступом (IAM). У контексті хмарної безпеки IAM-системи повинні забезпечувати не лише традиційну аутентифікацію, але й підтримувати принцип найменших привілеїв (PoLP), коли користувач або сервіс отримує лише ті права, які необхідні для виконання поточних задач. Наприклад, у AWS це реалізується через IAM-ролі та політики, які детально визначають, хто, до чого і за яких умов може отримати доступ [31].

Важливим аспектом є інтеграція Zero Trust з DevOps-процесами (DevSecOps). У сучасних хмарних середовищах інфраструктура часто розгортається за допомогою IaC (Infrastructure as Code), і будь-які помилки в конфігураціях можуть призвести до порушень безпеки. Тому політики Zero Trust повинні впроваджуватися вже на етапі розробки, наприклад, через сканування

шаблонів Terraform або CloudFormation на відповідність стандартам CIS Benchmark [32]. Крім того, використання сервісів типу AWS GuardDuty або Azure Security Center дозволяє автоматично виявляти невідповідності в реальному часі.

Окрему увагу приділяють захисту API, які є основою взаємодії між хмарними сервісами. У моделі Zero Trust кожен API-виклик має бути авторизований, а параметри запиту – перевірені на предмет ін'єкцій або несанкціонованого доступу. Для цього використовуються API-шлюзи з підтримкою OAuth 2.0, OpenID Connect та інших стандартів, а також механізми rate limiting для запобігання DDoS-атакам [33].

Також варто враховувати специфіку мультихмарних і гібридних середовищ, де дані та сервіси розподілені між різними платформами (наприклад, AWS, Azure і локальним дата-центром). У таких умовах Zero Trust вимагає єдиної точки контролю доступу, яка може бути реалізована за допомогою рішень типу Google BeyondCorp або VMware SASE. Ці технології поєднують VPN, SD-WAN і ZT-принципи в єдину архітектуру, забезпечуючи безпеку незалежно від місця розташування ресурсів.

Одним із найбільших викликів Zero Trust у хмарній безпеці є баланс між захистом і зручністю. Наприклад, постійні запити на підтвердження доступу можуть знизити продуктивність роботи співробітників, особливо в великих організаціях. Для вирішення цієї проблеми використовуються методи адаптивної аутентифікації, коли рівень строгості перевірок залежить від оцінки ризику. Наприклад, якщо користувач підключається зі знайомого пристрою через корпоративну мережу, система може запросити лише пароль, але при спробі доступу з нової країни – вимагати MFA або навіть підтвердження від керівника.

Іншим викликом є сумісність із існуючими системами, особливо в організаціях, які поступово переходять від традиційної інфраструктури до хмари. Наприклад, legacy-додатки, які не підтримують сучасні протоколи аутентифікації, можуть вимагати додаткових проксі-рішень або модифікації коду. У таких випадках допомагають технології типу Identity-Aware Proxy (IAP), які дозволяють «обгорнути» старі системи в ZT-архітектуру без повної їхньої переробки.

Також важливим аспектом є відповідність регуляторним вимогам, таким як GDPR, HIPAA або PCI DSS. Zero Trust допомагає виконувати багато з цих вимог (наприклад, шифрування даних або журналювання подій), але може вимагати додаткових налаштувань для аудиту та звітності [34]. Наприклад, у Azure Active Directory можна налаштувати детальні логи доступу, які потім аналізуються в Sentinel для виявлення порушень.

У майбутньому розвиток Zero Trust у хмарній безпеці буде тісно пов'язаний із впровадженням штучного інтелекту для прогнозування загроз, а також із появою квантово-стійкого шифрування, яке стане актуальним із розвитком квантових обчислень. Вже зараз компанії, такі як Google і Microsoft, інвестують у дослідження в цій галузі, що свідчить про довгострокову перспективу Zero Trust як основи кібербезпеки.

У загальному вигляді складові Zero Trust зображені на рис. 2.3.

Рис. 2.3 Архітектура Zero Trust у хмарному середовищі

2.3 Захист від кібератак та методи виявлення загроз у хмарних сервісах

Системи виявлення (IDS) та запобігання (IPS) вторгненням є ключовими компонентами забезпечення безпеки в хмарних середовищах. Вони дозволяють виявляти та реагувати на потенційні загрози в режимі реального часу, забезпечуючи захист від широкого спектра кібератак.

У хмарних середовищах IDS/IPS системи можуть бути реалізовані як віртуальні пристрої або як хмарні сервіси, інтегровані з інфраструктурою постачальника хмарних послуг. Наприклад, Google Cloud пропонує Cloud IDS, який забезпечує виявлення мережевих загроз, таких як шкідливе програмне забезпечення, шпигунські програми та атаки командного та контрольного типу.

Однією з переваг хмарних IDS/IPS є їхня здатність масштабуватися відповідно до потреб організації. Це дозволяє ефективно обробляти змінні обсяги трафіку та забезпечувати постійний захист навіть при зростанні навантаження [35].

Проте, впровадження IDS/IPS у хмарних середовищах пов'язане з низкою викликів. Серед них — складність моніторингу трафіку в багатокористувацьких та гібридних хмарних архітектурах, а також обмеження, пов'язані з шифруванням трафіку. Для подолання цих викликів рекомендується використовувати хмарні IDS/IPS рішення, оптимізовані для конкретної інфраструктури, такі як AWS GuardDuty або Azure Security Center.

Крім того, важливо інтегрувати IDS/IPS з системами управління інформацією та подіями безпеки (SIEM) для покращення аналізу загроз та автоматизації реагування на інциденти [36]. Це дозволяє отримувати більш повну картину безпеки та швидше реагувати на потенційні загрози.

Загалом, ефективне використання IDS/IPS у хмарних середовищах вимагає комплексного підходу, що включає вибір відповідних рішень, налаштування політик безпеки та інтеграцію з іншими інструментами кібербезпеки. Це

дозволяє забезпечити надійний захист даних і систем в умовах сучасних кіберзагроз.

Одним із ключових підходів до виявлення та реагування на загрози є використання систем аналізу поведінки користувачів та подій безпеки, зокрема UEBA (User and Entity Behavior Analytics) та SIEM (Security Information and Event Management) [37].

UEBA — це технологія, яка використовує машинне навчання та алгоритми аналізу поведінки для виявлення аномалій у діях користувачів та інших об'єктів в мережі. Вона дозволяє створювати базові профілі нормальної поведінки та виявляти відхилення, які можуть свідчити про потенційні загрози, такі як компрометація облікових записів або внутрішні атаки.

SIEM, у свою чергу, є системою, що збирає, аналізує та корелює дані з різних джерел, таких як журнали подій, мережевий трафік та інші, для виявлення та реагування на інциденти безпеки в режимі реального часу. Вона забезпечує централізоване управління інформацією про безпеку та допомагає організаціям дотримуватися нормативних вимог.

Інтеграція UEBA та SIEM дозволяє підвищити ефективність виявлення загроз у хмарних середовищах. UEBA доповнює SIEM, надаючи можливість глибшого аналізу поведінки користувачів та виявлення складних атак, які можуть залишатися непоміченими традиційними методами.

У хмарних середовищах, де обсяг даних та кількість користувачів постійно зростає, використання UEBA та SIEM стає особливо актуальним. Вони дозволяють виявляти аномалії, такі як незвичні спроби входу в систему, нетипові дії з файлами або підозрілі переміщення даних, що може свідчити про потенційні загрози.

UEBA та SIEM сприяють автоматизації процесів реагування на інциденти, зменшуючи час, необхідний для виявлення та усунення загроз. Це особливо важливо в умовах хмарних середовищ, де швидкість реагування є критичним фактором для забезпечення безпеки.

Впровадження UEBA та SIEM у хмарних середовищах є ефективним

підходом до забезпечення безпеки, який дозволяє організаціям виявляти та реагувати на загрози в режимі реального часу, забезпечуючи захист даних та систем від потенційних атак [38].

Штучний інтелект та автоматизація стали важливими інструментами для забезпечення кіберзахисту в умовах сучасних загроз, особливо в контексті застосування Zero Trust підходу в хмарній безпеці. Zero Trust передбачає принцип, за якого жоден користувач або пристрій не вважається довіреним за умовчанням, навіть якщо він знаходиться всередині корпоративної мережі. Для ефективного впровадження цього підходу в хмарній безпеці необхідно використовувати новітні технології, що допомагають здійснювати постійний моніторинг, верифікацію та контролювання доступу до ресурсів в реальному часі. Оскільки хмарні середовища є складними та динамічними, їх захист потребує постійної адаптації та автоматизації процесів безпеки. У цьому контексті штучний інтелект (ШІ) та автоматизація відіграють ключову роль у досягненні високого рівня безпеки, ефективності та надійності.

Одним із основних завдань застосування ШІ в Zero Trust безпеці є постійна ідентифікація та верифікація користувачів і пристроїв. Завдяки алгоритмам машинного навчання можна розробляти системи, які здатні здійснювати динамічну оцінку довіри до кожного користувача та пристрою, враховуючи такі фактори, як історія доступу, поведінка в мережі, рівень ризику та інші параметри. Це дозволяє знижувати ймовірність внутрішніх загроз, коли зловмисник може отримати доступ до системи, використовуючи законні облікові дані. ШІ дозволяє ефективно виявляти аномальні дії, порушення політик безпеки та інші підозрілі активності в режимі реального часу.

Одним із основних компонентів використання ШІ у Zero Trust є впровадження адаптивних політик доступу. Це політики, які автоматично коригуються залежно від змін у поведінці користувачів або пристроїв. Наприклад, якщо пристрій підключається до хмарної інфраструктури з незвичного місця або в незвичний час, система ШІ може ініціювати додаткові перевірки та вимагати додаткову автентифікацію, перш ніж дозволити доступ до

ресурсів. Такі адаптивні політики забезпечують гнучкість в управлінні безпекою, зменшуючи навантаження на користувачів та адміністративний персонал.

Один з важливих аспектів автоматизації в Zero Trust підході — це використання технологій оркестрації та автоматичних реакцій на загрози. Завдяки автоматизації можна оперативно реагувати на потенційні загрози без необхідності втручання людини. Наприклад, при виявленні підозрілого доступу система може автоматично обмежити доступ до певних ресурсів або навіть заблокувати певний користувацький акаунт, якщо виявлено аномальні дії. Автоматизація цих процесів дозволяє мінімізувати час реагування на загрози та скоротити ймовірність успішної атаки.

Ще одним важливим аспектом є використання ШІ для виявлення та аналізу великих обсягів даних, що генеруються в хмарних середовищах. Хмари містять величезну кількість інформації, що постійно змінюється, що ускладнює ручне управління безпекою. Алгоритми ШІ, зокрема, глибинне навчання, здатні аналізувати та обробляти ці дані на високій швидкості, виявляючи навіть найменші ознаки можливих загроз. Це дозволяє вчасно виявити й усунути потенційні вразливості, перш ніж вони можуть бути використані зловмисниками.

Автоматизація в Zero Trust безпеці дозволяє зменшити людський фактор у процесах управління безпекою. Часто саме через людську недбалість або помилки у налаштуваннях системи безпеки виникають уразливості. Використання автоматизованих систем дозволяє знизити кількість таких помилок, оскільки алгоритми не схильні до того ж ступеня впливу, що й люди. Це дозволяє зробити процеси більш стабільними та передбачуваними, що в умовах швидко змінюваних кіберзагроз є критично важливим [39].

Іншим напрямом застосування ШІ є виявлення та протидія загрозам через аналіз мережевого трафіку. Завдяки алгоритмам ШІ можна автоматично виявляти аномалії в трафіку, які можуть свідчити про спроби атаки або витік інформації. Такі інструменти здатні виявляти навіть нові типи атак, яких не було в базах даних зразків загроз, шляхом аналізу поведінки трафіку, що дозволяє швидко ідентифікувати шкідливі дії без необхідності людського втручання.

Застосування автоматизації в Zero Trust підході також допомагає у процесі регулювання доступу до ресурсів на основі контексту, який включає в себе як відомості про користувача, так і про стан системи в момент запиту доступу. Це означає, що доступ до конкретних ресурсів може бути дозволений або обмежений залежно від поточної ситуації, а також з урахуванням багатьох параметрів, таких як місце знаходження користувача, час доби, рівень загрози, наявність вразливостей у пристрої тощо. Всі ці параметри можуть бути автоматично оцінені ШІ та використані для ухвалення рішення про доступ.

Також варто зазначити, що штучний інтелект та автоматизація дозволяють ефективно підтримувати і впроваджувати політики безпеки на масштабах великих організацій або підприємств, де чисельність користувачів та пристроїв може бути надзвичайно великою. В умовах Zero Trust підходу це дозволяє здійснювати централізоване управління політиками безпеки, забезпечуючи ефективний контроль за всіма користувачами та пристроями, що підключаються до хмарної інфраструктури.

Використання ШІ та автоматизації в кіберзахисті, зокрема в Zero Trust підході, має значні переваги, однак також виникають і певні виклики. Наприклад, ШІ потребує великих обсягів даних для ефективного навчання і адаптації до нових загроз. Крім того, важливим аспектом є прозорість роботи алгоритмів, оскільки в деяких випадках складність моделей ШІ може ускладнити їх інтерпретацію та оцінку ефективності. Також існує ризик потенційних вразливостей в самих системах ШІ, які можуть бути використані зловмисниками для обходу заходів безпеки.

Для забезпечення ефективної роботи таких систем необхідно також постійно оновлювати алгоритми та адаптувати їх до нових загроз, що може бути складним завданням у швидко змінюваному середовищі кібербезпеки. Однак, попри ці труднощі, впровадження штучного інтелекту та автоматизації в Zero Trust підхід у хмарній безпеці залишається важливим кроком на шляху до підвищення рівня захищеності та ефективності кіберзахисту.

Щоб підсумувати основні аспекти застосування ШІ та автоматизації в Zero

Trust підході, наведемо таблицю 2.3, що відображає ключові елементи цього процесу.

Таблиця 2.3

Основні аспекти застосування ШІ та автоматизації в Zero Trust підході в хмарній безпеці

Аспект	Опис
Ідентифікація та верифікація	Використання алгоритмів ШІ для постійної ідентифікації та верифікації користувачів і пристроїв у реальному часі.
Адаптивні політики доступу	Автоматичне коригування політик доступу залежно від поведінки користувачів або пристроїв.
Оркестрація та автоматичні реакції	Використання автоматизації для оперативного реагування на загрози без участі людини.
Аналіз великих даних	Застосування ШІ для обробки великих обсягів даних та виявлення потенційних загроз.
Зменшення людського фактора	Автоматизація процесів для зниження ймовірності помилок, спричинених людським фактором.
Аналіз мережевого трафіку	Використання ШІ для виявлення аномалій в мережевому трафіку, які можуть свідчити про загрози.
Контекстний доступ	Автоматичне визначення доступу до ресурсів на основі параметрів користувача та системи.
Масштабування	ШІ дозволяє ефективно підтримувати безпеку на масштабах великих організацій або підприємств.
Виклики та ризики	Необхідність постійного оновлення моделей ШІ та врахування їхніх вразливостей.

Висновки до розділу 2

У результаті проведеного аналізу сучасних технологій забезпечення безпеки в хмарних середовищах було розглянуто ключові компоненти, які формують ефективну систему кіберзахисту. Зокрема, досліджено механізми автентифікації та управління доступом, що забезпечують контрольоване і

безпечне підключення користувачів до хмарних ресурсів, із застосуванням багатофакторної автентифікації, ролей та політик доступу.

Особливу увагу приділено впровадженню Zero Trust підходу як сучасної концепції захисту, яка базується на принципі постійної перевірки кожного елемента у системі незалежно від його місцезнаходження. У межах цього підходу розглянуто роль штучного інтелекту та автоматизації як засобів забезпечення безперервного моніторингу, адаптивного управління ризиками та оперативного реагування на інциденти.

Також проаналізовано методи захисту від кібератак і сучасні технології виявлення загроз, включаючи поведінковий аналіз, виявлення аномалій, системи виявлення вторгнень (IDS) та механізми попередження атак.

Отже, комплексне застосування зазначених технологій дозволяє істотно підвищити рівень безпеки хмарних сервісів, забезпечити стійкість до загроз та зменшити ймовірність несанкціонованого доступу або компрометації даних.

Розділ 3 РЕКОМЕНДАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ХМАРНОЇ БЕЗПЕКИ

Технології хмарної безпеки продовжують еволюціонувати у відповідь на зростаючу складність кіберзагроз, масштабування хмарних інфраструктур та потребу в безпечному доступі до ресурсів із будь-якої точки світу. На основі проведеного аналізу можна стверджувати, що подальший розвиток у цій сфері має бути спрямований на зміцнення механізмів автентифікації, впровадження адаптивних моделей доступу, ширше використання Zero Trust підходу, а також активне застосування штучного інтелекту для автоматизації процесів моніторингу, виявлення загроз і реагування на інциденти. З урахуванням сучасних тенденцій особливого значення набувають питання прозорості, масштабованості, відповідності нормативним вимогам і підвищення довіри до хмарних сервісів.

3.1 Перспективи розвитку технологій шифрування та конфіденційних обчислень

Технології шифрування та конфіденційних обчислень (Confidential Computing) розвиваються стрімкими темпами, пропонуючи нові методи захисту інформації під час її передачі, зберігання та обробки.

Стрімкий прогрес у галузі квантових обчислень створює серйозні виклики для сучасних криптографічних систем, оскільки квантові комп’ютери здатні ламати традиційні алгоритми шифрування, такі як RSA та ECC (Elliptic Curve Cryptography), за рахунок ефективних квантових алгоритмів, зокрема алгоритму Шора [40]. Це може призвести до масштабних порушень безпеки в цифровій інфраструктурі, включаючи фінансові операції, захищені комунікації та хмарні сховища даних. У зв’язку з цим одним із найважливіших напрямків розвитку сучасної криптографії є розробка та впровадження квантово-стійких алгоритмів шифрування, які зможуть протистояти атакам з використанням квантових

обчислювальних систем.

Національний інститут стандартів і технологій (NIST) вже кілька років проводить конкурс на визначення нових стандартів постквантової криптографії (Post-Quantum Cryptography, PQC). У 2022 році було обрано перші переможці, серед яких алгоритми на основі криптографії решіток (lattice-based cryptography), такі як CRYSTALS-Kyber для асиметричного шифрування та CRYSTALS-Dilithium для цифрових підписів. Ці алгоритми вважаються одними з найбільш перспективних, оскільки їх математична основа – задача найкоротшого вектора (Shortest Vector Problem, SVP) – є складною як для класичних, так і для квантових комп'ютерів [41]. Очікується, що впродовж наступних п'яти-десяти років ці стандарти будуть інтегровані в основні протоколи безпеки - TLS, PGP та VPN.

Однак перехід на постквантову криптографію пов'язаний із низкою технічних та організаційних труднощів. По-перше, багато сучасних систем використовують апаратне прискорення RSA та ECC, тоді як нові алгоритми можуть вимагати значно більших обчислювальних потужностей. По-друге, для забезпечення плавного переходу розробляються гібридні схеми шифрування, які поєднують класичні та квантово-стійкі методи. Наприклад, деякі VPN-провайди вже тестують рішення, де TLS-ключі формуються за допомогою як ECC, так і алгоритмів на основі решіток, що дозволяє забезпечити безпеку навіть у разі компрометації одного з підходів.

Окрім lattice-based криптографії, досліджуються й інші підходи, такі як [42]:

- Кодова криптографія (Code-based cryptography), що базується на складності декодування лінійних кодів (наприклад, алгоритм McEliece);
- Мультиваріантна криптографія (Multivariate cryptography), яка використовує системи нелінійних рівнянь;
- Хеш-базова криптографія (Hash-based cryptography), що застосовується переважно для цифрових підписів (наприклад, SPHINCS+).

Кожен з цих методів має свої переваги та недоліки, і їх подальший розвиток залежатиме від прогресу в квантових обчисленнях та криптоаналізі.

Окремо варто відзначити, що квантово-стійке шифрування стає особливо актуальним для хмарних технологій, де дані часто передаються між різними серверами та зберігаються в зашифрованому вигляді. Великі хмарні провайдери, такі як AWS, Google Cloud та Microsoft Azure, вже починають тестувати PQC-алгоритми у своїх інфраструктурах, щоб забезпечити захист клієнтських даних у довгостроковій перспективі [43].

Таким чином, розвиток квантово-стійкого шифрування є критично важливим етапом у забезпеченні кібербезпеки майбутнього, і його впровадження вимагатиме тісної співпраці між урядовими організаціями, науковими установами та IT-індустрією.

Сучасні хмарні технології стикаються з ключовою проблемою – необхідністю обробки чутливих даних у середовищі, де фізичний контроль над інфраструктурою належить третім сторонам. Традиційні методи шифрування захищають дані лише під час передачі (in transit) та зберігання (at rest), залишаючи їх вразливими під час безпосередньої обробки (in use). Саме для вирішення цієї проблеми була розроблена концепція конфіденційних обчислень – інноваційного підходу, який дозволяє виконувати операції з даними, залишаючи їх зашифрованими навіть у процесі обчислень.

Основним технічним механізмом реалізації конфіденційних обчислень є технологія Trusted Execution Environments (TEE). TEE створює ізольовані області виконання – так звані анклави (enclaves), – які захищені на апаратному рівні від несанкціонованого доступу, включаючи спроби зловмисників або навіть адміністраторів хмарної інфраструктури. Провідні виробники процесорів вже інтегрували підтримку TEE у свої чипи: Intel SGX (Software Guard Extensions) дозволяє створювати захищені анклави для критично важливих операцій, AMD SEV (Secure Encrypted Virtualization) забезпечує шифрування пам'яті віртуальних машин, а ARM TrustZone реалізує аналогічний функціонал для мобільних та вбудованих систем [44].

Важливим аспектом розвитку конфіденційних обчислень є їх інтеграція у хмарні сервіси великих провайдерів. Microsoft Azure пропонує рішення Azure

Confidential Computing, яке дозволяє запускати захищені віртуальні машини та контейнери. AWS реалізував схожу функціональність у своїй технології Nitro Enclaves, а Google Cloud розвиває власні рішення на базі Asylo Framework. Ці сервіси особливо актуальні для галузей з високими вимогами до конфіденційності, таких як фінансовий сектор, охорона здоров'я або державні установи.

Окрім апаратних рішень на базі TEE, існують і програмні підходи до реалізації конфіденційних обчислень. Гомоморфне шифрування (Homomorphic Encryption) дозволяє виконувати математичні операції над зашифрованими даними без необхідності їх розкриття. Хоча повністю гомоморфне шифрування залишається занадто ресурсомістким для масового використання, часткові та деякі варіанти напівгомоморфного шифрування вже знаходять практичне застосування. Технологія Secure Multi-Party Computation (SMPC) дає змогу декільком сторонам спільно обчислювати функції над своїми даними, не розкриваючи власних вхідних даних іншим учасникам. А методи Zero-Knowledge Proofs (ZKP) дозволяють довести істинність твердження без розкриття самої інформації, що є особливо цінним для систем автентифікації та блокчейн-технологій.

Перспективи розвитку конфіденційних обчислень включають кілька ключових напрямків. По-перше, це оптимізація продуктивності TEE-рішень, оскільки поточні реалізації часто мають обмеження щодо обсягів пам'яті та швидкодії. По-друге, важливим є розвиток стандартизації та інтероперабельності між різними платформами, що дозволить створювати кросплатформенні рішення. По-третє, особливу увагу приділяють інтеграції конфіденційних обчислень з технологіями машинного навчання, що відкриває нові можливості для аналізу чутливих даних без порушення їх конфіденційності. Вже сьогодні з'являються рішення, які дозволяють тренувати ML-моделі на зашифрованих даних або виконувати передбачення без доступу до оригінальної інформації.

Таким чином, конфіденційні обчислення представляють собою потужний інструмент для забезпечення безпеки даних у сучасних хмарних середовищах. Їх розвиток дозволить створити нову парадигму обробки інформації, де

конфіденційність і безпека будуть забезпечені на всіх етапах роботи з даними – від зберігання до обчислювальних операцій. Впровадження цих технологій вимагатиме подальших досліджень у галузі криптографії, оптимізації апаратного забезпечення та розробки нових програмних інструментів, але потенційні переваги для кібербезпеки роблять цей напрямок одним з найперспективніших у сучасній IT-індустрії.

Гомоморфне шифрування (HE) є однією з найперспективніших технологій у сфері конфіденційних обчислень, оскільки дозволяє виконувати математичні операції над зашифрованими даними без необхідності їх попереднього розшифрування. Ця унікальна властивість відкриває революційні можливості для обробки чутливої інформації в хмарних середовищах, де важливо забезпечити максимальний захист даних на всіх етапах роботи. Принципова відмінність HE від традиційних методів шифрування полягає в тому, що воно зберігає алгебраїчні властивості вихідних даних після їх зашифрування, дозволяючи проводити обчислення прямо над криптотекстом.

Історично концепція гомоморфного шифрування була вперше сформульована ще в 1978 році, але практична реалізація повністю гомоморфної схеми (Fully Homomorphic Encryption, FHE) стала можливою лише у 2009 році завдяки роботам Крейга Джентрі. Сучасні реалізації HE поділяються на три основні категорії: частково гомоморфні (PHE), що підтримують лише один тип операцій (наприклад, тільки додавання або тільки множення); деякою мірою гомоморфні (SHE), які дозволяють обмежену кількість операцій; та повністю гомоморфні (FHE), здатні виконувати довільні обчислення [45]. Кожен з цих типів знаходить своє застосування в залежності від конкретних вимог до безпеки та продуктивності.

Однією з найбільших перешкод для широкого впровадження гомоморфного шифрування залишається його значна обчислювальна складність. Повністю гомоморфні схеми можуть сповільнювати обчислення в десятки тисяч разів порівняно з роботою над відкритими даними. Для подолання цієї проблеми розробляються нові оптимізовані алгоритми, такі як CKKS (Cheon-Kim-Kim-

Song), який дозволяє ефективно працювати з дійсними числами, або BGV (Brakerski-Gentry-Vaikuntanathan), оптимізований для роботи з цілими значеннями. Паралельно ведуться роботи з апаратної оптимізації – використання GPU, FPGA та спеціалізованих процесорів для прискорення гомоморфних обчислень. Наприклад, компанія Intel розробляє спеціальні інструкції для своїх процесорів, які мають значно прискорити роботу з FHE [46].

Сфера практичного застосування гомоморфного шифрування постійно розширюється. У фінансовому секторі HE дозволяє проводити аналіз кредитоспроможності клієнтів без розкриття їх персональних даних банкам. В охороні здоров'я – обробляти медичні записи пацієнтів, зберігаючи їх конфіденційність. Особливо перспективним є поєднання HE з технологіями машинного навчання, що дозволяє тренувати моделі на зашифрованих даних або робити передбачення, не отримуючи доступу до оригінальної інформації. Вже існують робочі реалізації нейронних мереж, здатних працювати з гомоморфно зашифрованими вхідними даними.

Великі технологічні компанії активно інвестують у розвиток цієї технології. Microsoft Research розробила бібліотеку SEAL (Simple Encrypted Arithmetic Library), Google інтегрує підтримку HE у свої хмарні сервіси, а IBM пропонує інструменти для роботи з FHE у своїй платформі. Паралельно з'являються стартапи, які спеціалізуються на комерціалізації гомоморфного шифрування, пропонуючи рішення для різних галузей [47].

Перспективи розвитку гомоморфного шифрування включають кілька ключових напрямків. По-перше, це подальша оптимізація алгоритмів для зменшення накладних витрат на обчислення. По-друге – розробка стандартів і протоколів для забезпечення сумісності різних реалізацій. По-третє – створення зручних інструментів для розробників, які дозволять інтегрувати HE в існуючі системи без необхідності глибоких знань у криптографії. Важливим напрямком є також поєднання гомоморфного шифрування з іншими технологіями конфіденційних обчислень, такими як TEE або SMPC, для створення гібридних рішень з оптимальним балансом між продуктивністю та безпекою.

Незважаючи на технічні складності, гомоморфне шифрування має потенціал стати ключовою технологією для захисту даних у цифрову епоху. Його розвиток дозволить створити принципово нові моделі роботи з конфіденційною інформацією, де безпека даних забезпечується на фундаментальному математичному рівні. В міру подолання проблем з продуктивністю та зростання обчислювальних потужностей ми можемо очікувати все більш широкого впровадження HE в різних сферах – від хмарних обчислень до IoT пристроїв і блокчейн-технологій.

Сучасний розвиток технологій блокчейну та децентралізованих систем відкриває нові горизонти для застосування передових методів шифрування, створюючи принципово нові моделі захисту даних. Децентралізована природа блокчейну, поєднана з криптографічними технологіями нового покоління, формує основу для створення більш безпечних, прозорих і стійких до цензури інформаційних систем. Однією з ключових тенденцій у цьому напрямку є розвиток децентралізованих сховищ даних з end-to-end шифруванням. Такі системи, як IPFS (InterPlanetary File System) у поєднанні з протоколами типу Filecoin, дозволяють зберігати інформацію в розподіленій мережі, усуваючи недоліки централізованих хмарних сховищ – єдину точку відмови та потенційну можливість цензури. При цьому використання сучасних алгоритмів шифрування забезпечує конфіденційність даних, навіть коли вони зберігаються на вузлах, яким користувач не довіряє.

Особливий інтерес представляє інтеграція технологій нульового розголошення (Zero-Knowledge Proofs) у блокчейн-системи. ZKP-технології, такі як zk-SNARKs та zk-STARKs, вже знайшли широке застосування в криптовалютах (Zcash, Mina Protocol), дозволяючи підтверджувати достовірність транзакцій без розкриття їх вмісту. Це створює нову парадигму конфіденційності в публічних блокчейнах, де традиційно вся інформація є відкритою [48]. Розвиток цього напрямку призводить до появи "конфіденційних смарт-контрактів" – програм, які можуть виконуватися в децентралізованій мережі, обробляючи зашифровані дані без їх розкриття. Такі технології особливо

актуальні для фінансового сектору, де вимоги до конфіденційності поєднуються з необхідністю прозорості операцій.

Інноваційним напрямком є поєднання блокчейн-технологій з гомоморфним шифруванням та іншими методами конфіденційних обчислень. Такі гібридні системи дозволяють створювати децентралізовані платформи для аналізу чутливих даних, де інформація залишається зашифрованою на всіх етапах обробки. Наприклад, у сфері охорони здоров'я це дозволяє проводити дослідження на основі медичних записів пацієнтів без порушення їх конфіденційності. Децентралізовані організації (DAO) з використанням таких технологій можуть приймати колективні рішення на основі зашифрованих даних, що відкриває нові можливості для спільної роботи з конфіденційною інформацією.

Розвиток Web3 та метавсесвітів також стимулює вдосконалення методів шифрування в децентралізованих системах. Цифрові ідентичності, NFT-активи та віртуальна власність у метавсесвітах вимагають нових підходів до захисту даних, які б поєднували переваги блокчейну (незмінність, децентралізація) з потужними криптографічними механізмами. Виникають нові концепції, такі як самосуверенні ідентичності (Self-Sovereign Identity), де користувач повністю контролює свої персональні дані за допомогою криптографічних ключів, а процеси автентифікації будуються на основі ZKP.

Водночас розвиток цих технологій стикається з низкою викликів. Масштабованість блокчейн-систем залишається проблемою, особливо при використанні складних криптографічних схем, які вимагають значних обчислювальних ресурсів. Енергоефективність також є важливим фактором, оскільки багато сучасних методів (особливо повністю гомоморфне шифрування) мають високу обчислювальну складність. Крім того, залишаються відкритими питання регулювання та стандартизації, особливо у світлі зростаючих вимог до захисту даних (таких як GDPR).

Майбутній розвиток децентралізованих систем шифрування, ймовірно, буде спрямований на створення гібридних архітектур, які поєднують переваги

різних підходів. Наприклад, поєднання TEE для швидкої обробки даних із ZKP для підтвердження коректності обчислень може стати оптимальним рішенням для багатьох сценаріїв використання. Паралельно триває робота над підвищенням ефективності базових криптографічних примітивів, що дозволить масштабувати ці технології для масового застосування. Важливим напрямком є також розробка зручних інструментів для розробників, які б приховали складність базових криптографічних операцій і дозволили ширшому колу фахівців інтегрувати ці технології у свої рішення.

Технології шифрування та конфіденційних обчислень знаходяться на передовій кібербезпеки, і їх розвиток буде визначати майбутнє захисту даних у хмарних середовищах. Впровадження квантово-стійкої криптографії, вдосконалення TEE, поширення HE та інтеграція з блокчейном відкривають нові можливості для створення надійних і конфіденційних систем.

3.2 Використання штучного інтелекту та машинного навчання для підвищення безпеки хмарних платформ

Сучасні хмарні технології стають все більш складними та розподіленими, що зумовлює потребу в інноваційних підходах до забезпечення їх безпеки. Традиційні методи кіберзахисту, такі як сигнатурний аналіз або правила брандмауерів, вже не справляються з сучасними загрозами, особливо в умовах динамічних атак. Штучний інтелект та машинне навчання (МН) пропонують нові можливості для виявлення аномалій, прогнозування загроз і автоматизації реагування на інциденти. У цьому розділі розглядаються ключові аспекти застосування ШІ/МН для підвищення безпеки хмарних платформ, включаючи методи, технології та перспективні напрямки розвитку.

Сучасні системи захисту хмарних платформ дедалі частіше впроваджують методи штучного інтелекту та машинного навчання для протидії складним кіберзагрозам. Одним із найбільш перспективних напрямків є виявлення аномалій у мережевому трафіку та поведінці користувачів. Традиційні

сигнатурні методи, що базуються на заздалегідь визначених шаблонах атак, часто виявляються неефективними проти нових, невідомих загроз або витончених APT-атак. Машинне навчання, особливо підходи без нагляду, такі як алгоритми ізольованого лісу чи автоенкодери, дозволяють виявляти відхилення від нормальної поведінки, аналізуючи великі обсяги операційних даних у реальному часі. Наприклад, системи на основі LSTM-мереж здатні виявляти складні часові закономірності у логах доступу, що може свідчити про підготовку до атаки brute force або несанкціоноване переміщення даних. Великі хмарні провайдери вже активно інтегрують ці технології – Amazon GuardDuty використовує машинне навчання для аналізу потоків даних VPC Flow Logs, DNS-логів та подій AWS CloudTrail, автоматично виявляючи підозрілу активність, таку як незвичайні спроби доступу або комунікація з відомими шкідливими IP-адресами.

Окремий інтерес представляє застосування глибокого навчання для аналізу графових структур даних у хмарних середовищах. Графові нейронні мережі (GNN) дозволяють ефективно моделювати складні взаємозв'язки між різними об'єктами хмарної інфраструктури – віртуальними машинами, контейнерами, мікросервісами та користувачами. Це дає змогу виявляти складні багатоетапні атаки, які часто залишаються непоміченими традиційними системами моніторингу. Наприклад, аналізуючи шаблони комунікації між компонентами системи, GNN можуть ідентифікувати несанкціоновані зв'язки, які можуть свідчити про поширення шкідливого ПЗ або підготовку до атаки типу "схід на схід". При цьому сучасні реалізації таких систем демонструють здатність обробляти графи з мільйонами вершин і ребер, що робить їх практично застосовними для великих хмарних інфраструктур.

Сфера прогнозування кіберзагроз також отримує нові можливості завдяки машинному навчанню. Методи часових рядів, такі як Prophet або архітектури Temporal Fusion Transformer, дозволяють не тільки виявляти вже відбуваються атаки, але й передбачати потенційні загрози на основі історичних даних та зовнішніх індикаторів компрометації. Це особливо цінним для запобігання

DDoS-атакам, де навіть невеликий час попередження дозволяє вжити профілактичні заходи. Деякі хмарні провайдери вже тестують системи, здатні прогнозувати ймовірність атаки на конкретні клієнтські ресурси на основі аналізу глобальних тенденцій кіберзлочинності, геополітичних подій та активності в darknet.

Автоматизоване реагування на інциденти (SOAR) досягає нового рівня завдяки інтеграції з машинним навчанням. Сучасні системи вже здатні не тільки виявляти загрози, але й приймати рішення про оптимальний спосіб реагування, враховуючи контекст інциденту, критичність задіяних ресурсів та потенційний вплив на бізнес-процеси. Наприклад, при виявленні атаки на віртуальну машину система може автоматично визначити, чи варто її відразу вимкнути, ізолювати для подальшого аналізу чи просто обмежити мережевий трафік, ґрунтуючись на оцінці ризиків, зробленій ML-моделлю. Такі рішення вже реалізовані в продуктах типу Microsoft Azure Sentinel, де використовується поєднання машинного навчання для аналізу загроз і workflow-автоматизації для реагування.

Сучасні технології машинного навчання та штучного інтелекту пропонують потужні інструменти для захисту хмарних інфраструктур, причому різні алгоритми знаходять застосування у вирішенні конкретних задач кібербезпеки. Глибинні нейронні мережі демонструють особливу ефективність у виявленні складних багатоетапних атак, таких як APT (Advanced Persistent Threats), аналізуючи великі обсяги логів і виявляючи тонкі взаємозв'язки між подіями. Наприклад, архітектури Transformer, спочатку розроблені для обробки природної мови, успішно адаптуються для аналізу послідовностей подій безпеки, виявляючи довгострокові залежності, які зазвичай упускають традиційні системи. Графові нейронні мережі (GNN) знайшли своє застосування у моделюванні складних взаємозв'язків у хмарних середовищах, дозволяючи візуалізувати та аналізувати потоки даних між різними компонентами інфраструктури. Це особливо корисно для виявлення несанкціонованого переміщення даних або незвичайних шаблонів комунікації між мікросервісами, які можуть свідчити про компрометацію. Технології обробки природної мови

(NLP), такі як BERT або GPT, застосовуються для аналізу текстових логів і автоматичної класифікації подій безпеки, що значно підвищує ефективність обробки великих обсягів неструктурованих даних. Важливим напрямком є розвиток алгоритмів без нагляду, таких як автоенкодери або методи кластеризації, які дозволяють виявляти аномалії без попередньої розмітки даних, що критично важливо для виявлення раніше невідомих типів атак. При цьому постійно вдосконалюються методи інтерпретації результатів роботи ML-моделей, оскільки для прийняття рішень у сфері безпеки необхідно не тільки виявити аномалію, але й зрозуміти її природу та потенційні наслідки.

Таблиця 3.1

Застосування різних алгоритмів машинного навчання у хмарній безпеці

Алгоритм/ Технологія	Сфера застосування	Переваги	Недоліки
LSTM-мережі	Аналіз часових рядів (логи доступу, мережевий трафік)	Виявлення довгострокових залежностей у послідовностях подій	Висока обчислювальна складність для довгих послідовностей
Графові нейронні мережі	Моделювання взаємозв'язків у хмарній інфраструктурі	Ефективне виявлення складних багатоетапних атак	Вимагає якісного представлення даних у формі графа
Трансформери	Аналіз послідовностей подій безпеки	Здатність виявляти довгострокові залежності у великих наборах даних	Велика потреба в обчислювальних ресурсах
Автоенкодери	Виявлення аномалій без навчальної вибірки	Працює без попередньої розмітки даних	Може давати помилкові спрацьовування на рідкісні, але легальні події

Продовження табл. 3.1

Методи кластеризації	Групування подібних подій безпеки	Дозволяє виявляти нові типи загроз без попередніх знань	Складність інтерпретації результатів
NLP (BERT, GPT)	Аналіз текстових логів і автоматична класифікація подій	Ефективна обробка неструктурованих даних	Вимагає великих обсягів даних для навчання

Впровадження технологій штучного інтелекту в системи захисту хмарних середовищ стикається з низкою технічних та організаційних викликів, які потребують уваги розробників і кібербезпеківців.

Однією з ключових проблем є якість та репрезентативність даних, що використовуються для навчання моделей - недостатній обсяг маркованих даних про кіберзагрози, дисбаланс класів (коли нормальна активність значно перевищує кількість прикладів атак) і потенційні упередження в навчальних вибірках можуть суттєво знизити ефективність алгоритмів. Особливу складність становлять adversarial attacks, коли зловмисники спеціально модифікують вхідні дані для обходу систем захисту - наприклад, вносять мінімальні зміни в мережевий трафік, які непомітні для людини, але здатні обдурити ML-модель.

Проблема інтерпретованості результатів (Explainable AI) залишається актуальною для складних нейронних мереж, оскільки фахівцям з кібербезпеки необхідно розуміти логіку, за якою система класифікує подію як загрозу, особливо при прийнятті рішень про блокування ресурсів або ініціювання реагування.

Обмеження продуктивності та масштабованості ML-рішень також є суттєвим фактором, оскільки аналіз великих обсягів даних у реальному часі вимагає значних обчислювальних ресурсів, що може призвести до збільшення вартості хмарної інфраструктури. Важливим аспектом є відповідність вимогам регуляторних стандартів (таких як GDPR або PCI DSS), особливо коли мова йде про обробку персональних даних або фінансової інформації - використання ML-моделей для аналізу таких даних потребує додаткових механізмів захисту та аудиту.

Ключові аспекти інтеграції ШІ в хмарну безпеку зображені на рис. 3.1.

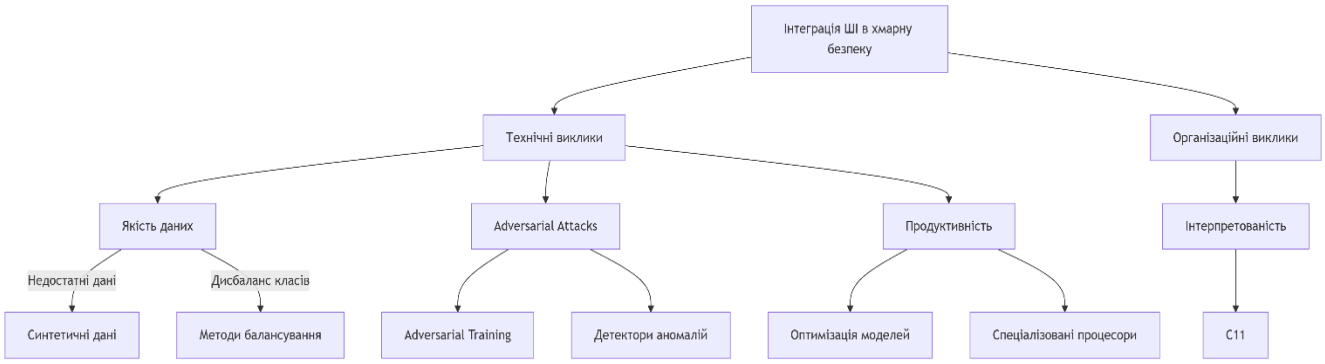

Рис. 3.1 Основні аспекти інтеграції ШІ в хмарну безпеку

Перспективи застосування штучного інтелекту та машинного навчання в хмарній безпеці охоплюють низку інноваційних напрямків, які кардинально змінять підходи до захисту даних у найближчі роки. Однією з найбільш перспективних технологій є Federated Learning, яка дозволяє навчати машинні моделі на децентралізованих даних без необхідності їх централізованого зберігання [49]. Цей підхід особливо актуальний для хмарних середовищ, оскільки дозволяє зберігати конфіденційність даних клієнтів – інформація залишається на пристроях користувачів, а на сервер передаються лише оновлення моделі. Великі технологічні компанії, такі як Google, вже активно використовують цей метод для покращення своїх сервісів, зберігаючи при цьому приватність користувачів.

Важливим напрямком розвитку є поєднання методів машинного навчання з технологіями конфіденційних обчислень, такими як гомоморфне шифрування або Trusted Execution Environments (TEE). Таке поєднання дозволить виконувати аналіз чутливих даних без їх розшифрування, що особливо важливо для таких сфер, як фінанси або охорона здоров'я. Наприклад, лікарня може використовувати хмарний сервіс для аналізу медичних записів пацієнтів, при цьому самі записи залишатимуться зашифрованими протягом усього процесу обробки. Це відкриває нові можливості для спільної роботи з даними без порушення вимог GDPR та інших нормативів щодо захисту персональної інформації.

Очікується значний прогрес у створенні автономних систем кіберзахисту, здатних самостійно виявляти, аналізувати та нейтралізовувати загрози в

реальному часі. Такі системи будуть поєднувати передові алгоритми глибокого навчання з технологіями автоматизованого реагування (SOAR), що дозволить значно скоротити час між виявленням атаки та її усуненням. Вже зараз з'являються перші комерційні рішення, які використовують reinforcement learning для адаптації до нових типів атак, постійно вдосконалюючи свої алгоритми без втручання людини.

Значний потенціал має інтеграція технологій обробки природної мови (NLP) в системи моніторингу безпеки. Сучасні трансформерні моделі, такі як GPT або BERT, можуть аналізувати великі обсяги текстових логів, автоматично класифікувати події та виявляти підозрілу активність, що значно підвищує ефективність аналізу безпеки в складних хмарних інфраструктурах. Це особливо актуально для великих підприємств, де щодня генеруються мільйони лог-записів, які неможливо ефективно обробляти вручну.

Розвиток explainable AI (XAI) стане ключовим фактором для подальшого впровадження машинного навчання в системи безпеки. Здатність пояснювати прийняті рішення критично важлива для кібербезпеки, де необхідно точно розуміти, на підставі яких ознак система класифікує подію як загрозу. Нові методи візуалізації та інтерпретації роботи складних нейронних мереж дозволять зробити алгоритми більш прозорими та надійними, що особливо важливо для застосування в регульованих галузях, таких як банківський сектор або державні установи.

Водночас залишаються відкритими питання щодо захисту самих систем машинного навчання від кібератак. Adversarial attacks, коли зловмисники спеціально модифікують вхідні дані для обману моделей, стають все більш поширеними. Розробка стійких алгоритмів, здатних протистояти таким атакам, вимагатиме глибокого розуміння як механізмів роботи ML-моделей, так і методів, які використовують кіберзлочинці. Це призведе до появи нових напрямів досліджень на стику машинного навчання та кібербезпеки, де спеціалістам доведеться одночасно розвивати як атакуючі, так і захисні методики.

Майбутнє хмарної безпеки безпосередньо пов'язане з подальшим вдосконаленням алгоритмів штучного інтелекту, збільшенням обчислювальних потужностей і розвитком нових парадигм обробки даних. Впровадження квантових обчислень може призвести до появи принципово нових методів криптографії та аналізу даних, тоді як прогрес у галузі нейроморфних чипів дозволить створювати більш ефективні системи реального часу для виявлення загроз. Усе це формує комплексний підхід до захисту хмарних інфраструктур, де штучний інтелект стає не просто інструментом, а ключовим компонентом архітектури безпеки, здатним адаптуватися до динамічного ландшафту кіберзагроз.

3.3 Рекомендації щодо покращення політик безпеки у хмарних сервісах

Сучасний етап розвитку хмарних технологій вимагає комплексного підходу до формування ефективних політик безпеки, які б враховували як технічні аспекти захисту даних, так і організаційні механізми управління ризиками. Першочерговим завданням є впровадження багаторівневої системи управління доступом, яка має ґрунтуватися на принципі найменших привілеїв (PoLP). Це передбачає ретельне визначення прав доступу для кожного користувача відповідно до його службових обов'язків, використання комбінації рольового (RBAC) та атрибутивного (ABAC) управління, а також обов'язкове застосування багатофакторної автентифікації для всіх критичних систем. Особливу увагу слід приділити регулярному аудиту прав доступу (щоквартальний) та впровадженню інструментів автоматизованого моніторингу змін у конфігураціях доступу. Для особливо критичних операцій, таких як доступ до адміністративних функцій, доцільно ввести додатковий рівень затвердження керівником підрозділу.

Не менш важливим напрямом є розробка комплексної політики керування даними, яка повинна включати чітку класифікацію даних за рівнями

конфіденційності, впровадження автоматизованих інструментів маркування даних та використання DLP-систем для запобігання витоку інформації. Обов'язковим елементом такої політики має стати застосування шифрування як для даних у спокої, так і під час передачі, а також розробка детальних процедур знищення даних після закінчення терміну їх зберігання. При цьому особливу увагу необхідно приділити захисту персональних даних з урахуванням вимог GDPR та інших нормативних актів, що особливо актуально для організацій, які працюють у міжнародному середовищі.

Для забезпечення оперативного виявлення та усунення загроз необхідно вдосконалювати процеси моніторингу та реагування на інциденти. Це передбачає впровадження сучасних SIEM-систем з повною інтеграцією з хмарними сервісами, налаштування автоматизованих сповіщень про підозрілу активність та розробку детальних playbooks реагування на різні типи інцидентів. Особливу ефективність демонструють регулярні навчальні імітації кібератак (щопівроку), які дозволяють не лише перевірити готовність персоналу до реальних загроз, але й виявити слабкі місця в системі захисту. Критично важливим є забезпечення цілодобового моніторингу критичних систем та створення спеціалізованого центру реагування на кіберінциденти (CSIRT) з чітко розподіленими ролями та обов'язками.

Надійність хмарних сервісів безпосередньо залежить від ефективності політик резервного копіювання та відновлення. Тут рекомендується дотримуватися правила 3-2-1 (три копії, два носії, одна поза майданчиком), регулярно тестувати процеси відновлення (щомісяця) та використовувати георозподілені сховища для резервних копій. Обов'язковими елементами таких політик мають стати шифрування резервних копій, суворий контроль доступу до них, а також розробка альтернативних сценаріїв відновлення роботи. Особливу увагу слід приділити мінімізації часу відновлення (RTO) та максимально допустимих втрат даних (RPO), що є критично важливими показниками для бізнес-безпеки.

Враховуючи, що людський фактор залишається одним з найслабкіших

ланок безпеки, необхідно ретельно проробляти програми підвищення обізнаності з кібербезпеки. Це передбачає проведення обов'язкових щоквартальних тренінгів, впровадження системи фішингових симуляцій та розробку персоналізованих навчальних програм для різних категорій співробітників. Особливу ефективність демонструє створення корпоративної культури кібербезпеки через системну роботу з внутрішніми комунікаціями та впровадження системи мотивації за виявлення потенційних загроз. Для керівників підрозділів доцільно проводити спеціалізовані тренінги з управління кіберризиками, які дозволять їм адекватно оцінювати загрози та приймати обґрунтовані рішення.

Для проактивного управління ризиками рекомендується впроваджувати автоматизовані інструменти оцінки ризиків, зокрема спеціалізовані SaaS-рішення, які дозволяють отримувати об'єктивну картину рівня безпеки. Важливим елементом є проведення щорічних комплексних аудитів безпеки, впровадження системи безперервного моніторингу вразливостей та інтеграція оцінки ризиків у процес прийняття управлінських рішень. Корисною практикою є використання бенчмаркінгу для порівняння з кращими практиками галузі, що дозволяє ідентифікувати напрями для вдосконалення.

Окремої уваги вимагає оптимізація політик роботи з третіми сторонами, оскільки багато хмарних рішень передбачають використання послуг вендорів. Тут необхідно розробляти детальні SLA з чіткими вимогами до безпеки, проводити попередній аудит безпеки постачальників та впроваджувати ефективні системи моніторингу дотримання вимог. Критично важливим є обмеження доступу третіх сторін до систем за принципом необхідності та розробка планів дій на випадок порушень з боку постачальників.

Запропонований комплекс рекомендацій формує цілісний підхід до вдосконалення політик безпеки в хмарних сервісах. Їх системне впровадження дозволить організаціям не лише значно знизити ризики кіберзагроз і забезпечити дотримання нормативних вимог, але й підвищити стійкість бізнес-процесів, оптимізувати витрати на кібербезпеку та створити міцну основу для подальшого

вдосконалення системи захисту. Важливо розуміти, що в умовах швидкої еволюції кіберзагроз політики безпеки мають бути динамічними та регулярно оновлюватися, враховуючи зміни в технологіях, появу нових типів атак та трансформацію бізнес-процесів самої організації. Лише комплексний і гнучкий підхід до управління безпекою хмарних сервісів може гарантувати їх ефективність у довгостроковій перспективі.

Висновки до розділу 3

Проведено комплексний аналіз ключових напрямів розвитку технологій хмарної безпеки та розроблено практичні рекомендації щодо підвищення ефективності захисту хмарних середовищ. Отримані результати демонструють, що сучасний етап цифрової трансформації вимагає інноваційних підходів до забезпечення безпеки хмарних рішень.

Перспективи розвитку технологій шифрування вказують на необхідність широкого впровадження передових методів криптографічного захисту, зокрема гомоморфного шифрування та конфіденційних обчислень. Ці технології відкривають нові можливості для обробки даних без необхідності їх розшифрування, що особливо актуально для чутливих галузей, таких як фінанси, охорона здоров'я та державний сектор. Очікується, що розвиток квантово-стійких алгоритмів шифрування стане вирішальним фактором у забезпеченні довгострокової безпеки хмарних даних.

Дослідження потенціалу штучного інтелекту та машинного навчання підтвердило їх ключову роль у створенні проактивних систем захисту. Інтеграція AI/ML-рішень дозволяє не лише ефективно виявляти аномалії та потенційні загрози в режимі реального часу, але й прогнозувати можливі атаки на основі аналізу історичних даних. Особливо перспективним є поєднання технологій поведінкового аналізу з системами автоматизованого реагування, що значно підвищує стійкість хмарних інфраструктур до складних багатоетапних кібератак.

Розроблені рекомендації щодо покращення політик безпеки формують

цілісну методологію управління ризиками в хмарних середовищах. Запропонований підхід передбачає поєднання технічних заходів (багаторівневий контроль доступу, шифрування даних, SIEM-системи) з організаційними механізмами (політики керування даними, програми підвищення обізнаності, аудит постачальників). Особливу увагу приділено необхідності створення гнучких, адаптивних політик, здатних оперативно реагувати на зміни в ландшафті загроз.

Результати дослідження підтверджують, що подальший розвиток хмарної безпеки вимагатиме інтеграції трьох ключових компонентів: передових криптографічних рішень, інтелектуальних систем аналізу та комплексних організаційних політик. Реалізація запропонованих підходів дозволить створити стійкі, адаптивні системи захисту, здатні ефективно протистояти сучасним кіберзагрозам у динамічному хмарному середовищі. Майбутні дослідження в цій галузі доцільно зосередити на оптимізації взаємодії між запропонованими технологіями та розробці уніфікованих стандартів їх впровадження.

ВИСНОВКИ

У кваліфікаційній роботі проведено комплексне дослідження сучасних підходів до забезпечення безпеки в хмарних середовищах, проаналізовано ключові загрози та вразливості, а також розроблено практичні рекомендації щодо підвищення рівня захисту даних і сервісів у контексті динамічного розвитку хмарних технологій.

У першому розділі розглянуто теоретичні основи хмарної безпеки, зокрема сутність хмарних обчислень, їх архітектурні моделі (IaaS, PaaS, SaaS) та фундаментальні характеристики, такі як гнучкість, масштабованість та економічна ефективність. Особливу увагу приділено аналізу потенційних загроз безпеці, серед яких виділено атаки на віртуалізовану інфраструктуру, втрату або витік конфіденційних даних, несанкціонований доступ через слабкі ланки автентифікації, а також ризики, пов'язані з багатоорендністю хмарних середовищ. Крім того, було досліджено нормативно-правову базу, що регулює сферу хмарної безпеки, включаючи міжнародні стандарти (ISO 27001, NIST SP 800-53), європейські регламенти (GDPR) та галузеві вимоги, що дозволило визначити ключові критерії відповідності для забезпечення конфіденційності, цілісності та доступності даних.

Другий розділ присвячений глибокому аналізу сучасних технологій захисту хмарних середовищ. Детально досліджено механізми автентифікації та управління доступом, зокрема багатофакторну автентифікацію (MFA), єдиний вхід (SSO) та системи управління ідентичністю (IAM), які є критично важливими для запобігання несанкціонованому доступу. Окремий акцент зроблено на концепції Zero Trust, яка передбачає постійну верифікацію користувачів і пристроїв незалежно від їхнього розташування, що особливо актуально в умовах гібридних хмарних архітектур. Також проаналізовано сучасні методи захисту від кібератак, такі як системи виявлення та запобігання вторгненням (IDS/IPS), платформи моніторингу безпеки (SIEM) та автоматизовані засоби аналізу

поведінки, які дозволяють оперативно виявляти аномалії та реагувати на загрози в режимі реального часу.

У третьому розділі сформульовано рекомендації щодо вдосконалення хмарної безпеки та визначено перспективні напрями розвитку цієї сфери. Серед ключових пропозицій – активне впровадження передових технологій шифрування, зокрема гомоморфного шифрування та квантово-стійкої криптографії, що дозволяє захищати дані як під час передачі, так і під час обробки. Великий потенціал також пов’язаний із використанням штучного інтелекту та машинного навчання для прогнозування кібератак, аналізу шаблонів поведінки та автоматизації реагування на інциденти. Крім того, обґрунтовано необхідність регулярного оновлення політик безпеки, проведення комплексних аудитів, а також підвищення кіберграмотності користувачів через навчальні програми та тренінги.

Проведене дослідження підтвердило, що хмарна безпека є складною та багатоаспектною дисципліною, яка потребує інтеграції технічних, організаційних та правових заходів. Незважаючи на наявність ефективних рішень, такі фактори, як зростання складності кібератак, поява квантових обчислень та розвиток децентралізованих хмарних архітектур, постійно ставлять нові виклики. Тому подальший розвиток цієї галузі має ґрунтуватися на проактивних підходах, міжгалузевій співпраці та постійній адаптації до змін. Реалізація запропонованих заходів дозволить організаціям не лише захистити свої активи, але й забезпечити довгострокову стійкість хмарних рішень у цифрову епоху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Balani Z., Varol H. Cloud computing security challenges and threats. *2020 8th international symposium on digital forensics and security (ISDFS)*, Beirut, Lebanon, 1–2 June 2020. 2020. URL: https://doi.org/10.1109/isdfs49300.2020.9116266

2. Choo K.-K. R., Rana O. F., Rajarajan M. Cloud security engineering: theory, practice and future research. *IEEE transactions on cloud computing*. 2017. Vol. 5, no. 3. P. 372–374. URL: https://doi.org/10.1109/tcc.2016.2582278

3. Akinade, Afees & Ige, Adebimpe & Pub, Anfo. Cloud Security Challenges and Solutions: A Review of Current Best Practices. International Journal of Multidisciplinary Research and Growth Evaluation. 2024. № 06. P. 26-35. URL: https://www.researchgate.net/publication/387558426_Cloud_Security_Challenges_and_Solutions_A_Review_of_Current_Best_Practices

4. Cloud computing security: foundations and challenges. Taylor & Francis Group, 2020. 522 p.

5. Cloud computing security / J. Arshad et al. *International journal of grid and high performance computing*. 2012. Vol. 4, no. 1. P. 52–66. URL: https://doi.org/10.4018/jghpc.2012010104

6. Cloud security, privacy, and trust baselines. *Cloud computing security*. Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742, 2016. P. 45–58. URL: https://doi.org/10.1201/9781315372112-5

7. Cyber security threats and countermeasures in digital age. *Journal of applied science and education (JASE)*. 2024. Vol. 4, no. 1. P. 1–20. URL: https://doi.org/10.54060/a2zjournals.jase.42

8. Deep dive on popular security models and strategies of cloud computing / K. Venkatesh et al. *Privacy and security challenges in cloud computing*. Boca Raton, 2022. P. 147–170. URL: https://doi.org/10.1201/9781003219880-8

9. Ismail H. Cloud computing. a security analysis. GRIN Verlag GmbH, 2019.

10. Jin H., Dai W., Zou D. Theory and methodology of research on cloud security. *Science china information sciences*. 2016. Vol. 59, no. 5. URL: https://doi.org/10.1007/s11432-016-5549-1

11. Journal I. Cloud computing security. *Interantional journal of scientific research in engineering and management*. 2024. Vol. 08, no. 10. P. 1–7. URL: https://doi.org/10.55041/ijsrem38330 (

12. Research of cyber security technologies of cloud services iaas, paas and saas / T. Smirnova et al. *Cybersecurity: education, science, technique*. 2024. Vol. 4, no. 24. P. 6–27. URL: https://doi.org/10.28925/2663-4023.2024.24.627

13. Waghchaude M. K. G. A review on cloud computing security issues, applicable solutions and implementation. *Interantional journal of scientific research in engineering and management*. 2024. Vol. 08, no. 05. P. 1–5. URL: https://doi.org/10.55041/ijsrem32988

14. Bunkar R. K. Study on security model in cloud computing. *International journal of advanced research in computer science*. 2017. P. 841–844. URL: https://doi.org/10.26483/ijarcs.v8i7.4350

15. Junjie L. Key security technologies of cloud computing platforms. *Proceedings of international conference on soft computing techniques and engineering application*. New Delhi, 2013. P. 411–417. URL: https://doi.org/10.1007/978-81-322-1695-7_47

16. A cloud-based ehealth architecture for privacy preserving data integration / A. Dubovitskaya et al. *ICT systems security and privacy protection*. Cham, 2015. P. 585–598. URL: https://doi.org/10.1007/978-3-319-18467-8_39

17. Ahmed W. Trends and challenges in securing cloud computing environments: an overview of current techniques. *Premier journal of computer science*. 2024. URL: https://doi.org/10.70389/pjcs.100004

18. Akbarov A., Khomidov I. Cloud computing technologies and their digital security in the digital economy. *Economics and education*. 2023. Vol. 24, no. 1. P. 50–55. URL: https://doi.org/10.55439/eced/vol24_iss1/a6

19. Caven P., Camp L. J. Towards a more secure ecosystem: implications for cybersecurity labels and sboms. *SSRN electronic journal*. 2023. URL: https://doi.org/10.2139/ssrn.4527526

20. Cloud security key management / W. Jiang et al. *Cloud computing security*. 2020. P. 167–194. URL: https://doi.org/10.1201/9780429055126-16

21. Dai X. B., Wang Z. J., Zhang Y. Data security and privacy protection of cloud computing. *Advanced materials research*. 2013. Vol. 846-847. P. 1570–1573. URL: https://doi.org/10.4028/www.scientific.net/amr.846-847.1570

22. Data protection-data security-privacy. *Computers & security*. 1984. Vol. 3, no. 1. P. 57–58. URL: https://doi.org/10.1016/0167-4048(84)90031-2

23. Data security and data protection in cloud privacy systems / H. Kapoh et al. *Jurnal syntax admiration*. 2024. Vol. 5, no. 11. P. 4801–4809. URL: https://doi.org/10.46799/jsa.v5i11.1768

24. Data security and privacy protection / ed. by X. Chen, X. Huang, M. Yung. Singapore : Springer Nature Singapore, 2025. URL: https://doi.org/10.1007/978-981-97-8540-7

25. Dhankar S., Tiwari V. Cloud computing - issues and threat. *SSRN electronic journal*. 2019. URL: https://doi.org/10.2139/ssrn.3463179

26. Gadde R. Survey on cloud computing technologies and security threats. *SSRN electronic journal*. 2024. URL: https://doi.org/10.2139/ssrn.4906403

27. Gupta S. Cryptographic key management for data protection. *Cloud computing security*. 2020. P. 151–156. URL: https://doi.org/10.1201/9780429055126-14

28. Gupta, Brij B & Agrawal, Dharma & Yamaguchi, Shingo. Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. 2016. URL: https://doi.org/10.4018/978-1-5225-0105-3

29. Li R. Analysis of key technologies for data security protection based on cloud computing. *International journal of computer science and information technology*. 2024. Vol. 4, no. 1. P. 243–252. URL: https://doi.org/10.62051/ijcsit.v4n1.30

30. Li R. Analysis of key technologies for data security protection based on cloud computing. *International journal of computer science and information technology*. 2024. Vol. 4, no. 1. P. 243–252. URL: https://doi.org/10.62051/ijcsit.v4n1.30

31. Maleh Y. Enhancing e-learning security in cloud environments. *Cybersecurity management in education technologies*. New York, 2023. P. 171–210. URL: https://doi.org/10.1201/9781003369042-9

32. Moseley R. Web and network basics. *Advanced cybersecurity technologies*. Boca Raton, 2021. P. 5–24. URL: https://doi.org/10.1201/9781003096894-2

33. Security systems in cloud computing / H. Lalchhanhima et al. *Educational administration theory and practices*. 2024. URL: https://doi.org/10.53555/kuey.v30i5.5858

34. Security threat analysis in cloud computing / M. Iqbal Fadillah et al. *JATI (jurnal mahasiswa teknik informatika)*. 2024. Vol. 9, no. 1. P. 992–998. URL: https://doi.org/10.36040/jati.v9i1.12528

35. Strizhov M., Ray I. Multi-keyword similarity search over encrypted cloud data. *ICT systems security and privacy protection*. Berlin, Heidelberg, 2014. P. 52–65. URL: https://doi.org/10.1007/978-3-642-55415-5_5

36. An analysis on security issues and research challenges in cloud computing / U. Aijaz et al. *Journal of security in computer networks and distributed systems*. 2024. Vol. 1, no. 1. P. 37–44. URL: https://doi.org/10.46610/joscnds.2024.v01i01.005

37. Bespalova N. V. Cloud technology security. *Computational nanotechnology*. 2024. Vol. 11, no. 5. P. 124–132. URL: https://doi.org/10.33693/2313-223x-2024-11-5-124-132

38. Dave R. Cybersecurity in cloud computing environments: challenges and solutions. *Interantional journal of scientific research in engineering and management*. 2025. Vol. 09, no. 01. P. 1–9. URL: https://doi.org/10.55041/ijsrem40961

39. Lata M., Kumar V. Cyber security techniques in cloud environment: comparative analysis of public, private and hybrid cloud. *Edpacs*. 2025. P. 1–21. URL: https://doi.org/10.1080/07366981.2025.2449743

40. Li T., Yan L. SIEM based on big data analysis. *Cloud computing and security*. Cham, 2017. P. 167–175. URL: https://doi.org/10.1007/978-3-319-68505-2_15

41. Network attack prediction method based on threat intelligence / J. Wang et al. *Cloud computing and security*. Cham, 2018. P. 151–160. URL: https://doi.org/10.1007/978-3-030-00012-7_14

42. Network security analysis for cloud computing environment / L. Xie et al. *International journal of modeling, simulation, and scientific computing*. 2022. URL: https://doi.org/10.1142/s1793962322500544

43. Security issues and research challenges in cloud computing / B. B. Jagadale et al. *International journal of engineering and computer science*. 2024. Vol. 13, no. 05. P. 26158–26171. URL: https://doi.org/10.18535/ijecs/v13i05.4820

44. Security threat analysis in cloud computing / M. Iqbal Fadillah et al. *JATI (jurnal mahasiswa teknik informatika)*. 2024. Vol. 9, no. 1. P. 992–998. URL: https://doi.org/10.36040/jati.v9i1.12528

45. Singh U., Tiwari A., Sharma S. Data security in cloud computing. *International journal of engineering applied sciences and technology*. 2020. Vol. 04, no. 10. P. 170–173. URL: https://doi.org/10.33564/ijeast.2020.v04i10.033

46. Surveying and analyzing security, privacy and trust issues in cloud computing environments / D. Sun et al. *Procedia engineering*. 2011. Vol. 15. P. 2852–2856. URL: https://doi.org/10.1016/j.proeng.2011.08.537

47. Tn N. Exploring on cloud security landscapes:a comprehensive review. *Interantional journal of scientific research in engineering and management*. 2024. Vol. 08, no. 05. P. 1–5. URL: https://doi.org/10.55041/ijsrem34217

48. Vemula V. R. Recent advancements in cloud security using performance technologies and techniques. *2023 9th international conference on smart structures and systems (ICSSS)*, CHENNAI, India, 23–24 November 2023. 2023. URL: https://doi.org/10.1109/icsss58085.2023.10407744

49. Waizel G. A qualitative analysis of cloud adoption in the public and the private sectors from cyber security vendors' perspective. *Review of economic and business studies*. 2023. Vol. 16, no. 1. P. 19–37. URL: https://doi.org/10.47743/rebs-2023-1-0002