МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “АНАЛІЗ ТА ВДОСКОНАЛЕННЯ МЕТОДІВ ШИФРУВАННЯ ДАНИХ У ХМАРНИХ ОБЧИСЛЕННЯХ”

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

_____ Дмитро МИСНИК
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Дмитро МИСНИК
Ім’я, ПРІЗВИЩЕ

Керівник: Світлана ЛЕГОМІНОВА
Д.е.н., проф. Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
Д.т.н., проф. Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Миснику Дмитру Анатолійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Аналіз та вдосконалення методів шифрування даних у хмарних обчисленнях”,
керівник кваліфікаційної роботи ЛЕГОМІНОВА Світлана, д.е.н., проф.,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від 27.02.24 № 36.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *міжнародні стандарти, наукова та технічна література. методи та засоби шифрування даних, загрози та вразливості безпеки хмарних обчислень*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати проблематику шифрування даних у хмарних обчисленнях.
4.2. Дослідити основні методи шифрування даних у хмарних обчисленнях.
4.3. Вивчити інструменти та методи покращення шифрування даних у хмарних обчисленнях, розробити практичні рекомендації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз проблематики шифрування даних у хмарних обчисленнях	08.04.2024	
4.	Дослідження основних методів шифрування даних у хмарних обчисленнях.	22.04.2024	
5.	Вивчення інструментів та методів покращення шифрування даних у хмарних обчисленнях	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Дмитро МИСНИК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Мисник Д.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Аналіз та вдосконалення методів шифрування даних у хмарних обчисленнях"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач МИСНИК Дмитро у кваліфікаційній роботі проаналізував основну проблематику шифрування даних у хмарних обчисленнях, дослідив основні методи шифрування даних у хмарних обчисленнях, вивчив інструменти та методи покращення шифрування даних у хмарних обчисленнях, розробив практичні рекомендації за темою дослідження.

МИСНИК Дмитро показав розуміння проблеми шифрування та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на одній конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача МИСНИКА Дмитра на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Мисник Д.А. допускається до захисту роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти МИСНИКА Дмитра
на тему "АНАЛІЗ ТА ВДОСКОНАЛЕННЯ МЕТОДІВ ШИФРУВАННЯ ДАНИХ У ХМАРНИХ ОБЧИСЛЕННЯХ"

Актуальність.

Хмарні технології стрімко розвиваються, що призводить до зростання обсягу даних, які обробляються та зберігаються в хмарних сервісах, а також забезпечення їх конфіденційності, доступності та цілісності. Існуючі методи шифрування даних часто виявляються недостатньо ефективними або потребують значних обчислювальних ресурсів, що може впливати на продуктивність хмарних систем. Вдосконалення методів шифрування є важливим для забезпечення захисту персональних даних, а також для підвищення довіри користувачів до хмарних сервісів. Тому забезпечення хмари сучасними методами шифрування даних у хмарних обчисленнях є актуальною в сучасних умовах та підтверджує своєчасність наукових досліджень.

Позитивні сторони.

1. Автором детально проаналізлвано основні загрози та вразливості даних та методи захисту від загроз в хмарних середовищах.
2. Розглянуто основні методи симетричного та асиметричного шифрування, проведено їх порівняльну характеристику.
3. Розроблено рекомендації щодо вдосконалення методів шифрування даних.

Недоліки.

Робота суттєво виграла б, якщо б автор провів більше практичних досліджень та виклав їх результати в роботі.

Відзначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "відмінно", а здобувач МИСНИК Дмитро заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Галина ГАЙДУР ____
д.т.н., професор *підпис* Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена аналізу та вдосконаленню методів шифрування даних у хмарних обчисленнях. Робота складається зі вступу, трьох розділів, що містять 12 рисунків, висновків і списку використаних джерел із 48 найменувань. Загальний обсяг роботи становить 60 аркушів, з яких 8 аркушів займає перелік умовних скорочень та список використаних джерел.

Метою роботи є аналіз та вдосконалення методів шифрування даних у хмарних обчисленнях.

Об'єктом дослідження є методи шифрування даних у хмарних обчисленнях.

Предмет дослідження – особливості застосування методів шифрування даних.

Методи дослідження. Для вирішення поставленого вище наукового завдання в роботі були використані методи аналізу, порівняння, класифікації, системного підходу до вдосконалення методів шифрування даних .

Як результат у роботі проаналізовано особливості хмарних обчислень та їх вразливості, досліджено основні принципи методів шифрування даних; вивчено інструменти та методи вдосконалення методів шифрування даних, розроблено практичні рекомендації.

Галузь застосування. Розроблені рекомендації можуть бути використані при плануванні та реалізації покращення методів шифрування даних в контексті хмарних обчислень.

Ключові слова: ХМАРНІ ОБЧИСЛЕННЯ, МЕТОДИ ШИФРУВАННЯ ДАНИХ, ЗАГРОЗИ ТА ВРАЗЛИВОСТІ ДАНИХ, ВДОСКОНАЛЕННЯ МЕТОДІВ ШИФРУВАННЯ ДАНИХ.

ABSTRACT

The qualification work is devoted to the analysis and improvement of data encryption methods in cloud computing. The work consists of an introduction, three chapters containing ?? figures, conclusions and the list of references containing ?? items. The total volume of the work is ?? pages, of which ?? pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to analyse and improve data encryption methods in cloud computing.

The object the study is data encryption methods in cloud computing.

The subject of the study is the peculiarities of using data encryption methods.

Research methods. To solve the above scientific task, the methods of analysis, comparison, classification, and a systematic approach to improving data encryption methods were used in the work..

As a result, the paper analyses the features of cloud computing and its vulnerabilities, investigates the basic principles of data encryption methods; examines tools and methods for improving data encryption methods, and develops practical recommendations.

Field of application. The developed approaches can be used in the planning and implementation the improvement of data encryption methods in the context of cloud computing.

Keywords: CLOUD COMPUTING, DATA ENCRYPTION METHODS, DATA THREATS AND VULNERABILITIES, IMPROVEMENT OF DATA ENCRYPTION METHODS..

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

Якщо в КР певний термін, скорочення чи позначення повторюється менше трьох разів, його у перелік не включають, а його розшифрування наводять у тексті при першому згадуванні. Перелік друкується двома колонками, в яких ліворуч за абеткою наводять позначення чи терміни, праворуч - їх детальне розшифрування (тлумачення).

SaaS	Програмне забезпечення як сервіс
PaaS	Платформа як сервіс
IaaS	Інфраструктура як сервіс
UCaaS	Об'єднані комунікації як сервіс
IoT	Інтернет речей
CASB	Брокер безпеки доступу до хмарних сервісів
DES	Стандарт шифрування даних
IDEA	International Data Encryption Algorithm
AES	Advanced Encryption Standard
ZTM	Моделі з нульовою довірою
NGFW	Розгортання брандмауерів нового покоління
MFA	Багатофакторна автентифікація
IAM	Управління ідентифікацією та доступом
KMS	Автоматизовані системи управління ключами
QKD	Квантовий розподіл ключів

ВСТУП

Актуальність теми. Стрімкий, перманентний розвиток технологій та поява нових загроз кібербезпеки створюють необхідність вдосконалення методів шифрування даних. З огляду на те, що хмарні обчислення відкривають нові можливості для зберігання і обробки великих обсягів даних, їх безпека стає об'єктом зростаючої загрози з боку кіберзлочинців. Аналіз і запропоновані покращення існуючих методів шифрування є необхідними складовими забезпечення безпеки даних.

Отже, дослідження методів шифрування даних у хмарних обчисленнях є актуальним науковим завданням.

Мета роботи полягає у аналізі та вдосконаленні методів шифрування даних у хмарних обчисленнях.

Об'єкт дослідження – методи шифрування даних у хмарних обчисленнях.

Предмет дослідження – особливості застосування методів шифрування даних.

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

1. Проаналізувати проблематику шифрування даних у хмарних обчисленнях.

2. Дослідити основні методи шифрування даних у хмарних обчисленнях.

3. Вивчити інструменти та методи покращення шифрування даних у хмарних обчисленнях, розробити практичні рекомендації.

Методи дослідження. Для вирішення поставленого вище наукового завдання в роботі були використані методи аналізу, порівняння, класифікації, системного підходу до вдосконалення методів шифрування даних.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір методів шифрування даних у хмарних обчисленнях, що надасть належний захист від кіберзагроз. Викладення результатів цього дослідження сприятиме вдосконаленню методів шифрування, що в свою чергу призведе до покращення безпеки даних.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

Розділ 1 ПРОБЛЕМАТИКА ШИФРУВАННЯ ДАНИХ У ХМАРНИХ ОБЧИСЛЕННЯ

1.1 Сутність хмарних обчислень та їх роль в цифровому середовищі

Сучасний цифровий світ зазнає невпинних змін, що призводить до стрімкого розвитку технологій. Серед них важливе місце посідають хмарні обчислення, які стали великою інновацією зі значним впливом не тільки на сервіси в мережі Інтернет, але й на весь ринок інформаційних технологій.

В результаті прогресу в різних існуючих обчислювальних моделях, користувачам відкриваються нові можливості для швидкого та ефективного використання обчислювальних систем без необхідності власного обладнання. Вони можуть безперешкодно підключатися до хмарної обчислювальної системи, де вони легко зможуть виконати свої запити з мінімальним залученням третіх сторін [1].

Стандарт NIST SP 800-145 був опублікований восени 2010 року. З того часу середовище хмарних обчислень зазнало зростання технічної зрілості, проте визначення NIST зберегло своє визнання у всьому світі. NIST SP 800-145 дає визначення хмарних обчислень одним реченням: "модель для забезпечення універсального, зручного мережевого доступу на вимогу до спільного сховища конфігурованих обчислювальних ресурсів (наприклад, мереж, серверів, сховищ, додатків і сервісів), які можуть бути швидко надані і звільнені з мінімальними зусиллями з управління або взаємодії з постачальниками послуг". Визначення NIST характеризує важливі аспекти хмарних обчислень і покликане слугувати засобом для широкого порівняння хмарних сервісів і стратегій розгортання, а також забезпечити базову основу для обговорення від того, що таке хмарні обчислення, до того, як найкраще використовувати хмарні обчислення [2].

Хмарні обчислення мають величезний потенціал для надання різноманітних публічних послуг в залежності від однієї обраної моделі хмари з чотирьох. Кожна модель забезпечує абсолютно новий рівень універсальності та

потужності. Чотири основні моделі надання хмарних сервісів – це SaaS, UCaaS, PaaS та IaaS.

Програмне забезпечення як сервіс (SaaS) перетворює процес використання програм на простіший і зручніший. Користувачі отримують можливість працювати з додатками безпосередньо через свої пристрої, що робить доступ до них максимально зручним та гнучким. За допомогою веб-інтерфейсу або API можна легко отримати доступ до необхідних інструментів, працюючи в будь-якому місці з доступом до Інтернету.

Важливою перевагою SaaS є відсутність потреби в управлінні та контролі над інфраструктурою. Користувачі можуть зосередитися на використанні програм і не турбуватися про такі частини, як мережа, сервери чи зберігання даних. Це звільняє їх від необхідності вкладати час та ресурси у підтримку інфраструктури, дозволяючи зосередитися на власних задачах. Водночас користувачі можуть налаштовувати деякі параметри додатків для відповідності власним потребам, що надає певний рівень контролю і персоналізації [3].

Платформа як сервіс (PaaS) відкриває користувачам можливість розгортання їхніх програм на хмарній інфраструктурі без необхідності управління базовими компонентами. Вони можуть розгортати створені або придбані додатки, використовуючи мови програмування, бібліотеки, сервіси та інструменти, які надаються провайдером.

Користувачі не мають прямого контролю над мережею, серверами, операційними системами або сховищами, але вони можуть керувати розгорнутими додатками і, можливо, налаштовувати параметри конфігурації середовища, у якому вони працюють. Це дає їм значний рівень гнучкості та контролю над власними програмами, необхідними для їхньої роботи, при цьому звільняючи від складних завдань з управління інфраструктурою.

Інфраструктура як сервіс (IaaS) надає користувачам можливість отримати доступ до обчислювальних ресурсів, таких як обробка, зберігання та мережі, безпосередньо через хмарні ресурси. Вони можуть розгортати та запускати будь-яке програмне забезпечення, включаючи операційні системи та додатки, на цих

ресурсах. Хоча користувачі не мають прямого контролю над базовою інфраструктурою, вони зберігають контроль над операційними системами, сховищем та розгорнутими додатками [4].

Умови сучасної кризи сприяють зростанню популярності об'єднаних комунікацій як сервісу (UCaaS), що забезпечує неперервний зв'язок та віддалену співпрацю через хмарну мережу. Ця модель не лише забезпечує безпеку та надійність, але й дозволяє віддаленим працівникам працювати в безпечному, віртуалізованому середовищі. У зв'язку з ростом роботи з дому, об'єднані комунікації стають ключовим інструментом для збереження зв'язку між командами, незалежно від їх місцезнаходження. Платформа UCaaS дозволяє не лише спілкуватися та співпрацювати через телефонні та відеодзвінки, але й обмінюватися файлами та ресурсами через хмарне середовище для оптимізації робочих процесів [5].

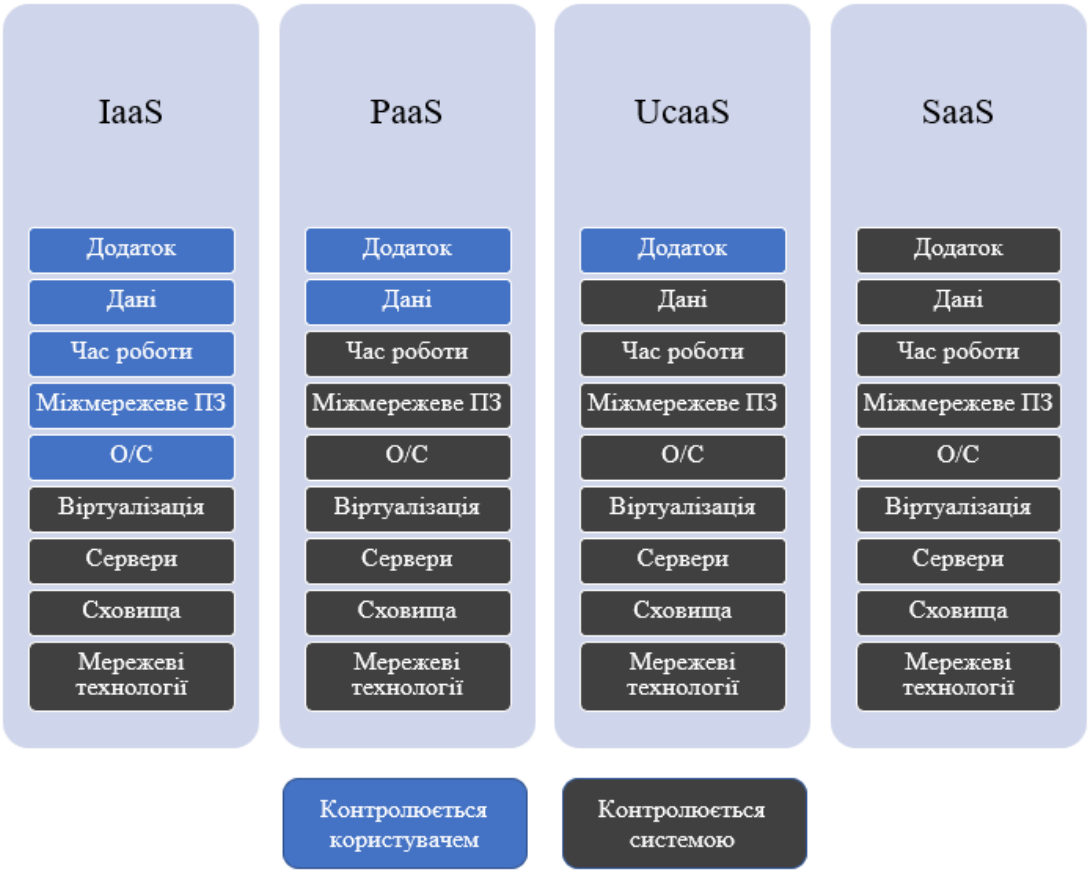

Рис. 1.1. Ключова відмінність між сервісними моделями хмарних обчислень

Модель розгортання хмари – це "конфігурація" певних параметрів хмарного середовища, таких як розмір сховища, доступність та власність. Існує чотири основні моделі розгортання хмар, які суттєво відрізняються між собою: публічна, приватна, гібридна та спільнотна. Існують також не настільки поширені системи організації на основі веб-технологій, такі як віртуальна приватна, міжхмарна та інші.

Приватна хмара, також відома як внутрішня або корпоративна модель, є моделлю розгортання, де хмарна інфраструктура належить конкретній організації. Ця організація має повний контроль над системою та керує нею централізовано. В той же час, третя сторона, така як провайдер, може надавати серверні ресурси для приватної хмари.

Більшість компаній вважають за краще тримати обладнання у своєму локальному центрі обробки даних, оскільки це дозволяє внутрішній команді максимально контролювати та керувати всією інфраструктурою. Такий підхід дозволяє забезпечити високий рівень безпеки та конфіденційності, оскільки дані зберігаються та обробляються всередині власної мережі компанії. Приватна хмара може бути особливо корисною для організацій з високими вимогами до захисту даних або з обмеженим доступом до публічних хмарних сервісів.

Публічна хмара – це добре відома модель хмарних сервісів, популярна для веб-додатків, обміну файлами та неконфіденційного зберігання даних. Вона рекомендується для розробки програмного забезпечення та спільних проєктів. У цій моделі провайдер володіє та управляє усім обладнанням, необхідним для роботи публічної хмари, зберігаючи пристрої у великих центрах обробки даних [6].

Публічна хмара грає важливу роль у розробці та тестуванні, оскільки вона забезпечує доступне та легко налаштовуване віртуальне середовище. Розробники часто використовують її для розробки та тестування своїх програм, оскільки вона є недорогою, швидко розгортається та ідеально підходить для тестування. Інфраструктура публічної хмари забезпечує зручне середовище для

виконання цих завдань, сприяючи швидкому розвитку та впровадженню програмних рішень.

Гібридна хмара поєднує в собі публічні та приватні хмари, забезпечуючи безперешкодний обмін даними та додатками між ними і їх взаємодію. Це ідеальне рішення для організацій, які потребують використання обох платформ, залежно від специфіки діяльності та масштабів.

Гібридна хмара часто розгортається як приватна хмара, яка потім розширюється для інтеграції з одним або кількома публічними хмарними сервісами. Гібридна модель дозволяє компаніям максимально використовувати переваги обох типів хмарних рішень, забезпечуючи гнучкість та ефективність використання ресурсів відповідно до їх потреб та вимог [7].

Під час розгляду різних моделей розгортання хмарних інфраструктур стає очевидним, що кожна з них має свої унікальні переваги та використання, які впливають на вибір організації при впровадженні та використанні хмарних середовищ. Для кращого розуміння, порівняємо ці моделі за декількома ключовими критеріями в таблиці 1.1.

Таблиця 1.1.

Порівняльна характеристика моделей розгортання хмар [8]

Характеристика	Публічна	Приватна	Гібридна
Легкість у налаштуванні	Дуже легко налаштувати, провайдер виконує більшу частину роботи	Дуже важко налаштувати, оскільки команда в орагнізації сама створює систему з нуля	Дуже важко налаштувати через взаємопов'язані системи
Легкість у використанні	Дуже проста у використанні	Складна і вимагає наявності окремої штатної команди	Важко використовувати, якщо система не була налаштована належним чином
Контроль над даними	Низький, провайдер має повний контроль	Дуже високий, оскільки організація є власником системи	Дуже високий (при правильному налаштуванні)
Безпека та конфіденційність	Дуже низька, не підходить для конфіденційних даних	Дуже висока, ідеально підходить для зберігання даних організації	Дуже висока, якщо дані зберігаються в приватній хмарі

Характеристика	Публічна	Приватна	Гібридна
Хто може використовувати	Будь-хто може отримати доступ	Обмежений доступ, можуть отримати доступ тільки люди з певним дозволом	Середній рівень доступності

Вибір моделі розгортання хмарних сервісів залежить від конкретних потреб, вимог і стратегії бізнесу кожної організації. Однак важливо пам'ятати, що незалежно від обраної моделі, успішна інтеграція та ефективне використання хмарних технологій може значно підвищити продуктивність, гнучкість та конкурентоспроможність організації в сучасному цифровому середовищі [9].

Хмарні обчислення стали не тільки невід'ємною складовою цифрового середовища, а й стратегічно важливим інструментом для багатьох компаній та організацій. Хмара забезпечує більшу гнучкість і надійність, підвищує продуктивність і ефективність, а також допомагає знизити витрати на IT. Вона також сприяє інноваціям, дозволяючи організаціям швидше виходити на ринок і включати в свої стратегії використання штучного інтелекту і машинного навчання [10].

1.2 Основні загрози та вразливості даних у хмарних сервісах

Останнім часом кількість кібератак зростає. Наслідки кібератак у хмарі дуже серйозні. Провайдери хмарних сервісів не можуть гарантувати, що запит на послугу є справжнім і не є наслідком кібератаки. Таким чином, провайдери хмарних послуг повинні не лише мати можливість виявляти та запобігати кібератакам на сервіси, розгорнуті в їхніх хмарах, але й встановлювати чіткі інструкції щодо вирішення конфліктних ситуацій, які виникають внаслідок таких атак. Таким чином, очевидно, що деякі проблеми, пов'язані з захистом безпеки, конфіденційності та надійності хмарних сервісів, виходять за рамки технологічних рішень.

Необхідно визначити можливі хмарні загрози, щоб впровадити кращі механізми безпеки для захисту хмарних обчислювальних середовищ. Загроза –

це потенційна причина інциденту, який може завдати шкоди системі або організації. Вразливість – це слабке місце в ресурсі або системі, яке використовується загрозою. Агент загрози реалізує загрозу, використовуючи одну або більше вразливостей. Розглянемо детальніше різні види загроз [11].

Найпоширенішою загрозою безперечно є втрата даних. Втрата даних може виникнути з різних причин, включаючи стихійні лиха, такі як повені, землетруси, а також людські помилки, наприклад, випадкове видалення файлів адміністратором хмари, відмову жорсткого диска або відключення електроенергії, а також зараження шкідливим програмним забезпеченням. Щоб уникнути таких втрат, ефективною стратегією є регулярне резервне копіювання даних.

Ще одними з найчастіших загроз є DoS- та DDoS-атаки. DoS-атака, або «атака на відмову в обслуговуванні», має на меті перешкодити користувачам отримати доступ до своїх даних або додатків, і зазвичай здійснюється лише з одного джерела. Це відповідно впливає на те, що атаку відносно легко послабити. У порівнянні, DDoS-атака, або «розподілена атака на відмову в обслуговуванні», використовує кілька систем для атаки на хмарний сервіс. Зловмисник, керуючи мережею "зомбі", створює ботнет, який надсилає фальшивий трафік до цільового сервісу. Це призводить до перевантаження і недоступності ресурсів в хмарі для легітимних користувачів, що може спричинити серйозні проблеми з доступом до даних і додатків [12].

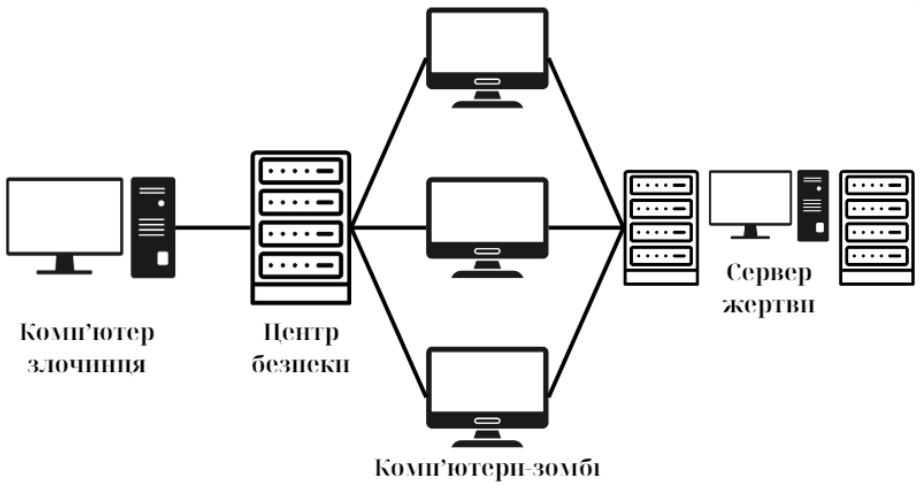

Рис. 1.2. Схема DDoS-атаки

Зловживання та недобросовісне використання хмарних технологій становлять серйозну загрозу для безпеки і конфіденційності даних. Хмарні провайдери пропонують користувачам різноманітні послуги, включаючи безкоштовні обмежені пробні періоди, які можуть бути використані зловмисниками для несанкціонованого доступу до хмарних сервісів. Це може призвести до зламування паролів, запуску потенційних точок атаки та виконання зловмисних команд.

Кіберзлочинці можуть використовувати слабкі системи реєстрації та обмежені можливості виявлення шахрайства провайдерів хмар. Деякі зловмисники вдаються до використання додатків з багатим контентом, таких як флеш-файли, для того, щоб приховати свій шкідливий код і використовувати браузери користувачів для встановлення шкідливого програмного забезпечення [13].

До розповсюджених вразливостей можна віднести також незахищені кінцеві пристрої. Протягом останніх кількох років Інтернет речей (IoT) став популярним, проте зростання цієї технології супроводжується збільшенням загроз безпеці незахищених пристроїв. Пристрої IoT вимагають значної автоматизації для їх встановлення, конфігурації та усунення помилок. Однак, навіть одна помилка може бути посиленою через використання автоматизованих інструментів управління IoT, що породжує мільйони нових векторів атак. Мережа відіграє критичну роль у функціонуванні IoT, тому всі пристрої мають бути обладнані надійними засобами мережевого захисту. Крім того, необхідно проводити регулярні аудити для перевірки налаштування та управління пристроями IoT, щоб переконатися, що вони знаходяться в найбільш безпечному стані.

Недостатньо захищена криптографія є однією з найбільших вразливостей безпеки даних. Зловмисники мають здатність розкрити будь-який криптографічний механізм або алгоритм. Неодноразово виявлялося, що у

реалізації криптографічних алгоритмів можна знайти критичні недоліки, які роблять навіть найміцніше шифрування вразливим або навіть анулюють його ефективність. Порушення безпеки може виникнути через помилки у виробництві програмного забезпечення, слабкість в алгоритмах або недоліки у реалізації [14].

Людський фактор так само відносять до серйозних вразливостей системі безпеки – інсайдери можуть бути колишніми або незадоволеними співробітниками, системними адміністраторами або партнерами компанії, які мають доступ до конфіденційної інформації та можуть використовувати її для нанесення шкоди. [15]

Звісно, наведені характеристики загроз та вразливостей не є вичерпними. Кожного дня з'являються нові загрози порушенню безпеки даних в хмарному середовищі. На рисунку 3 наведена класифікація взаємопов'язаних загроз та вразливостей

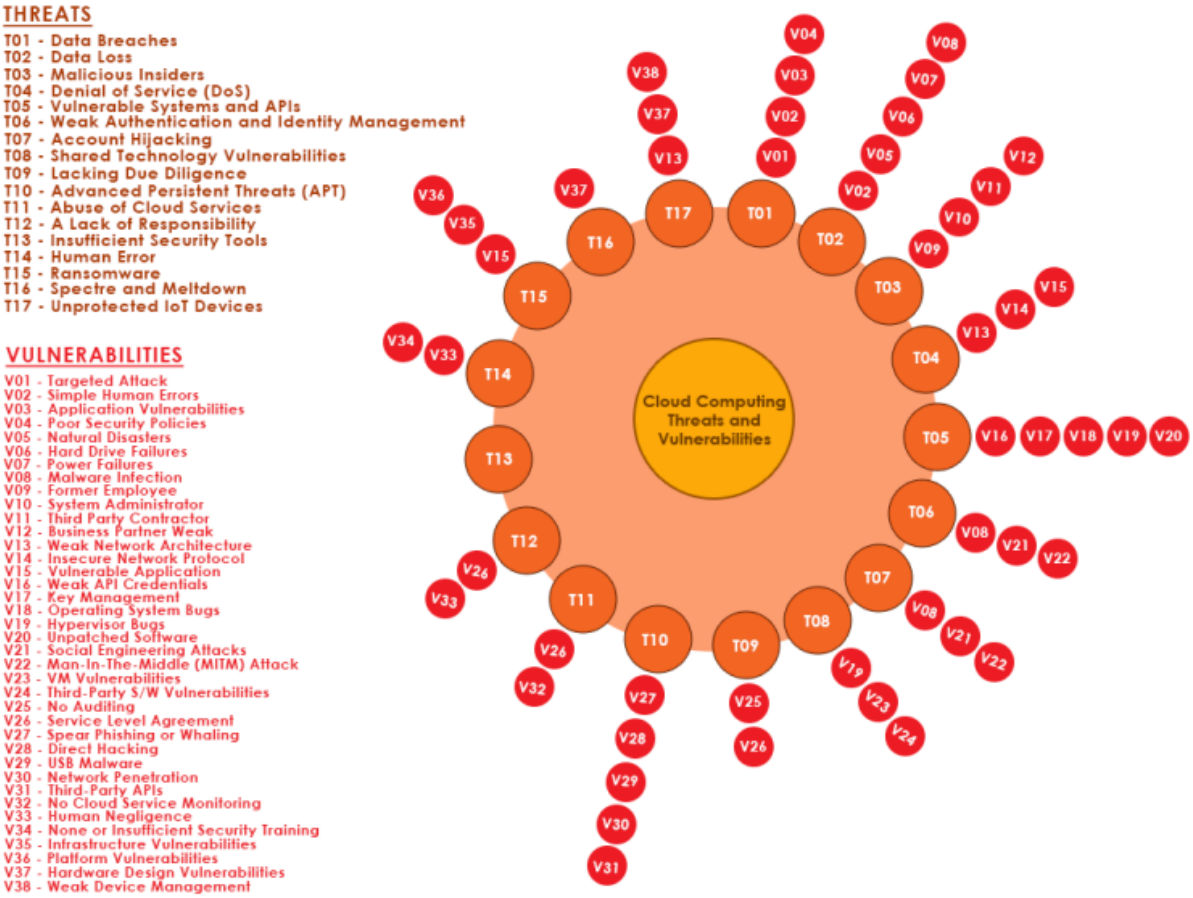

Рис. 1.3. Повна класифікація загроз та вразливостей у хмарних обчисленнях [16]

Таким чином, основні загрози та вразливості даних у хмарних сервісах вимагають постійного уваги та вдосконалення заходів безпеки. Важливо визнати, що загрози постійно змінюються, тому необхідно підтримувати високий рівень обізнаності та готовності до впровадження новітніх заходів захисту.

1.3 Кращі практики застосування методів шифрування у хмарних обчисленнях

Управління безпекою в хмарному середовищі націлене на забезпечення захисту систем та даних від потенційних загроз, вразливостей і порушень. Це включає впровадження та керування різними заходами безпеки, такими як шифрування даних, контроль доступу, виявлення загроз та реагування на інциденти. Такий всебічний підхід забезпечує, що всі складові хмарної інфраструктури організації будуть захищені – від даних, які вона зберігає, до послуг, які вона надає.

Хмарне шифрування - це процес перетворення даних з початкового формату звичайного тексту в нечитабельний формат, наприклад, зашифрований текст, перед передачею та зберіганням у хмарі. Як і будь-яка інша форма шифрування даних, хмарне шифрування робить інформацію нерозбірливою і, отже, марною без ключів шифрування. Це стосується навіть тих випадків, коли дані втрачено, викрадено або надано доступ до них неавторизованому користувачеві. Шифрування вважається одним з найефективніших компонентів стратегії кібербезпеки організації [17].

Термін "шифрування хмарного сховища" часто використовується для опису шифрування даних, що зберігаються у хмарному дата-центрі на диску – дані у стані спокою. Це важлива частина забезпечення безпеки, але не єдиний вид шифрування, який може бути застосований. Необхідно шифрувати дані як у стані спокою, так і в русі. Ці дані передаються в хмару або з неї, або між різними місцями у хмарі. Використання протоколів шифрування, таких як IPsec, під час

передачі даних по мережі, допомагає забезпечити їх конфіденційність та цілісність. Залежно від типу даних варто розглядати можливість використання шифрування на рівні додатків. Наприклад, багато систем керування базами даних пропонують можливість шифрувати дані на рівні додатків, окремо від шифрування на рівні сховища. Також з'являються нові технології, які також можуть убезпечити вразливість даних під час їх активного використання. Дані у активному стані зазвичай гірше захищені, ніж дані у стані спокою, так як зазвичай механізми захисту даних, що використовуються у стані спокою, автоматично відключаються перед початком роботи з ними [18].

Для кращого захисту хмарного середовища необхідно мати чітке розуміння вимог до безпеки елементів системи та рівень захисту, який необхідний системі для безперервного функціонування. На Рис. 1.4. зображена модель забезпечення безпеки, яка показує, що вимоги безпеки повинні бути розглянуті на ранній стадії, перш ніж переміщати конфіденційні дані організації в хмарне середовище.

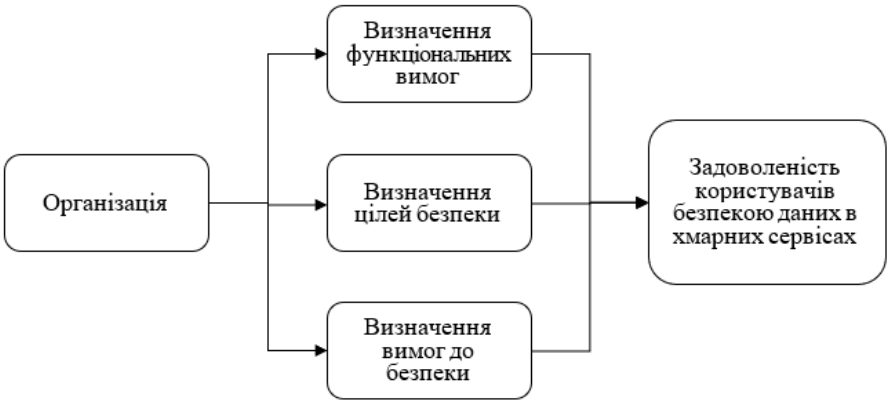

Рис. 1.4. Рамкова модель забезпечення безпеки у хмарі [19]

При оцінці різних функцій шифрування, які пропонують постачальники хмарних послуг, слід звернути увагу на обмеження доступу до інтерфейсу сервісу лише для автентифікованого та уповноваженого персоналу. Постачальник повинен надати функції автентифікації та ідентифікації, такі як ім'я користувача, пароль, клієнтські сертифікати протоколу TLS, двофакторну

автентифікацію та об'єднання ідентифікаційних даних з поточним постачальником ідентифікаційних даних підприємства. Необхідно також забезпечити можливість обмеження доступу до виділеної корпоративної, лінійної або громадської мережі.

Щоб уникнути ризику потрапляння ключів шифрування в чужі руки, дуже важливо уникати постачальників з ненадійними методами автентифікації. Якщо цього не зробити, системи компанії стануть вразливими перед кіберзлочинцями, які можуть намагатися викрасти дані, змінити інформацію або здійснити атаки різних типів [20].

Також ефективною практикою є збереження повної видимості та контролю. Організація, яка використовує хмарне шифрування, повинна мати змогу переглядати та контролювати свої дані. Надійний постачальник послуг запропонує рішення для хмарного шифрування з повною видимістю завантажених даних і списком користувачів, які мають до них доступ. Активний моніторинг дозволяє виявляти зміни в безпеці та конфігурації в екосистемі підприємства.

Крім того, забезпечення вдосконаленого фізичного захисту активів даних також є важливим для довгострокового контролю над видимістю та безпекою корпоративних даних. Провайдер хмарного шифрування також повинен забезпечувати повне та безповоротне видалення даних перед повторним наданням ресурсів, виведенням з експлуатації або утилізацією, щоб запобігти випадковому потраплянню даних до чужих рук [21].

Використання брокера безпеки доступу до хмарних сервісів (CASB) розглядається як надійний механізм захисту, що діє як зв'язок між внутрішньою інфраструктурою організації та хмарним середовищем. CASB виконує ряд важливих функцій, серед яких забезпечення прозорості використання хмарних сервісів, захист даних і виявлення загроз. Наприклад, за допомогою CASB компанії можуть контролювати доступ до хмарних ресурсів, забезпечувати виконання політик безпеки та виявляти підозрілу активність в режимі реального часу. Відсутність CASB підвищує ризик несанкціонованого доступу, порушення

вимог нормативного законодавства та можливість витоку даних у хмарному середовищі [22].

Програми навчання та підвищення обізнаності серед працівників є ключовими практиками для забезпечення кібербезпеки в організаціях. Людські помилки продовжують бути серйозною загрозою, тому освіта та свідомість персоналу стають надзвичайно важливими. Проведення регулярних навчальних програм гарантує, що співробітники залишаються інформованими про останні загрози безпеки, навчаються безпечному користуванню Інтернетом та дотриманню політики безпеки компанії. Такі тренінги можуть включати у себе вивчення того, як визнавати фішингові електронні листи або як захищати особисті робочі пристрої. Відсутність цієї підготовки може призвести до ненавмисного розкриття конфіденційних даних або створення точок доступу для кіберзлочинців [23].

Висновки до розділу 1

Хмарні обчислення відіграють ключову роль у цифровому середовищі, надаючи різноманітні можливості та переваги для користувачів і компаній. Вони забезпечують доступ до потужних обчислювальних ресурсів, що дозволяє виконувати складні завдання та обробку даних, масштабування ресурсів згідно з потребами користувачів, зручність та ефективність роботи з даними та програмами, а також знижують витрати на IT-інфраструктуру.

Однак, разом із зростанням використання хмарних сервісів збільшується й ризик безпеки даних у цих сервісах. Зловмисники вивчають та використовують потенційні вразливості хмарних сервісів, що надає їм можливість доступу до конфіденційної інформації організації.

Отже, шифрування хмарних даних є простим, але дієвим методом захисту конфіденційності у разі можливого злому. Навіть якщо зловмисники отримають доступ до даних, вони не зможуть прочитати вміст зашифрованих файлів.

Експертна оцінка фокусується на шифруванні - як важливої та успішної стратегії організації для надійного захисту даних в хмарних середовищах.

Кращі практики застосування методів шифрування у хмарних обчисленнях включають в себе використання потужних шифрувальних алгоритмів, захист ключів шифрування та комбінуванні різноманітних методів для захисту даних у спокої та в русі. Дотримання цих практик допомагає забезпечити конфіденційність та цілісність даних у хмарних обчисленнях, зменшуючи ризик їхнього несанкціонованого доступу та витоку.

Глибоке розуміння методів безпеки та їх використання може в кінцевому підсумку вирішально вплинути на рівень захисту корпоративної мережі, роблячи її непривабливою для кібератак.

Розділ 2 АНАЛІЗ МЕТОДІВ ШИФРУВАННЯ ДАНИХ У ХМАРНИХ ОБЧИСЛЕННЯХ

2.1 Принцип симетричного шифрування даних

Інформаційна безпека – важливий компонент операційної структури підприємства, який охоплює складні процеси регулювання потоків інформації та капіталу. Надійна інформаційна безпека дозволяє безперешкодно обмінюватися ресурсами та оптимізувати робочі процеси. Забезпечення безпеки цих систем надзвичайно важливе, оскільки будь-яке порушення може призвести до серйозних наслідків для підприємства.

Забезпечення безпеки інформації тісно пов'язане з використанням алгоритмів шифрування та дешифрування, особливо коли дані передаються через незахищені канали зв'язку. Шифрування, процес кодування даних, діє як ефективний бар'єр проти несанкціонованого доступу, забезпечуючи цілісність та конфіденційність інформації. Розшифрування, навпаки, є зворотним процесом, що дозволяє розшифрувати зашифровані дані за умови санкціонованого доступу.

Незважаючи на спільну мету – захист даних, різні алгоритми шифрування відрізняються за ефективністю через різноманітні фактори, такі як характеристики файлів та технологічне середовище. Алгоритми розділяються на три основні категорії: симетричні алгоритми шифрування, асиметричні алгоритми шифрування та геш-алгоритми.

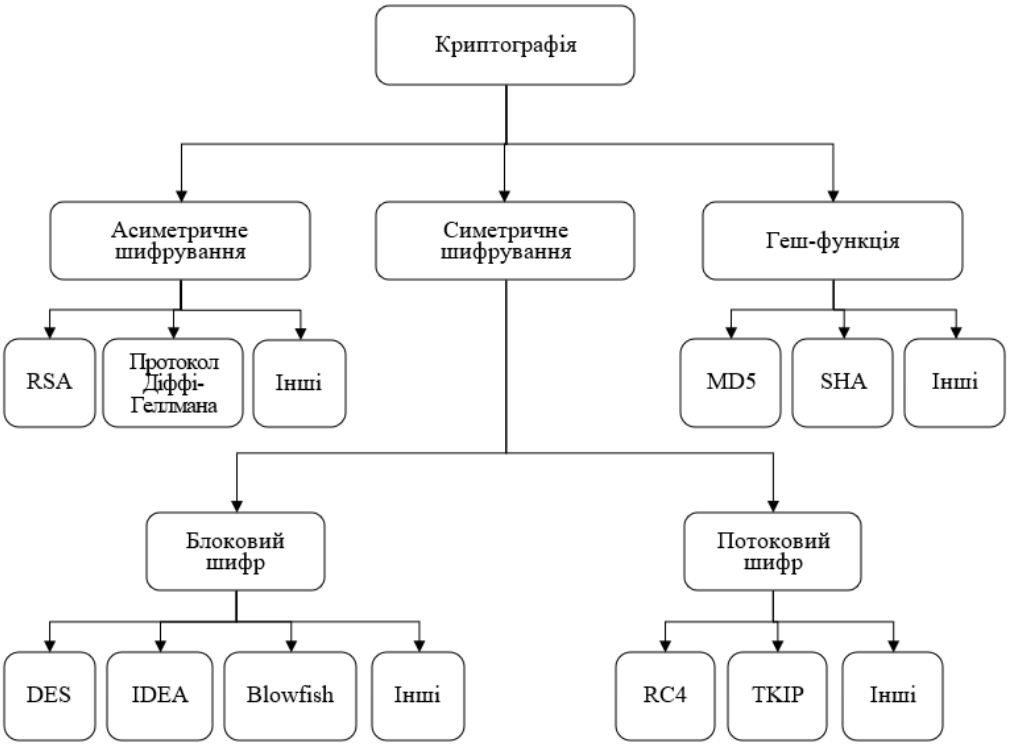

Рис. 2.1. Базова класифікація шифрів в криптографії [24]

Симетрична криптографія поділяється на дві ключові категорії: блокові шифри та потокові шифри. До цієї категорії належать різні алгоритми, такі як Blowfish, DES, AES, IDEA та інші. Кожен алгоритм використовує свій унікальний підхід до шифрування і дешифрування, обробляючи дані блоками фіксованого розміру і вимагаючи певного розміру ключа. Блоковий шифр працює, розбиваючи відкриті текстові повідомлення на блоки фіксованого розміру та шифруючи їх, утворюючи відповідні блоки зашифрованого тексту. Натомість, потокові шифри шифрують відкриті текстові повідомлення за допомогою безперервно генерованого потоку ключів, забезпечуючи більш динамічний підхід до шифрування [25].

Для кращого розуміння алгоритму шифрування та принципу його роботи розглядаються основні компоненти симетричного шифрування, які формують його основу. Відкритий текст представляє собою початкові дані, які призначені для передачі конкретному отримувачу і використовуються як вхідні дані для процесу шифрування. Алгоритм шифрування складається з низки операцій, які

застосовуються до відкритого тексту з використанням спеціального ключа, що призводить до створення зашифрованого тексту. Секретний ключ є важливим значенням, яке використовується для перетворення відкритого тексту в зашифрований, і залишається конфіденційним як для процесу шифрування, так і для розшифрування. Зашифрований текст – це результат шифрування вихідного відкритого тексту за допомогою визначеного алгоритму, який суттєво відрізняється від оригінального тексту і використовується для передачі даних. Алгоритм дешифрування – це послідовність операцій, які застосовуються до зашифрованого тексту з використанням того самого секретного ключа для отримання початкового відкритого тексту, тобто процес, що відновлює зашифровані дані у їхню первісну форму [26].

Симетричне шифрування використовує один і той самий ключ для як шифрування, так і розшифрування даних. Зберігання цього ключа в безпечності є критично важливим для забезпечення конфіденційності даних. Крім того, зміна ключа час від часу може запобігти вразливостям у випадку, якщо ключ буде вкрадено.

Ефективність будь-якої криптографічної системи залежить від того, як ключі передаються між сторонами, які беруть участь у комунікації. Цей процес, відомий як розподіл ключів, забезпечує безпечний обмін ключами між сторонами, які забезпечують, що вони залишаються конфіденційними. Розподіл ключів може відбуватися різними способами:

1. сторона А може обрати ключ і фізично доставити його Б;
2. посередник, наприклад, довірена третя сторона В, може вибрати ключ і фізично доставити його А і Б;
3. якщо А і Б раніше і нещодавно використовували ключ, одна сторона може передати новий ключ іншій стороні, зашифрований за допомогою старого ключа;
4. якщо А і Б мають зашифроване з'єднання з третьою стороною В, то С може передати ключ по зашифрованому зв'язку між А і Б.

Варіанти 1 і 2 підходять для сценаріїв з ручним обміном ключами, таких як шифрування за каналом зв'язку, де кожен пристрій шифрування зв'язується виключно зі своєю парою. Однак для наскрізного шифрування в мережі ручна передача ключів стає складним процесом. У розподілених системах окремим хостам або пристроям з часом може знадобитися зв'язок з багатьма іншими об'єктами, що вимагає динамічного надання ключів для кожного пристрою. Ця проблема є особливо складною в розподілених системах з великою площею, де підтримка безпечного розподілу ключів стає першочерговим завданням [27]. Розглянемо детальніше процеси алгоритмів симетричного шифрування.

Стандарт шифрування даних (DES) – це криптографічний метод, який грав важливу роль у забезпеченні безпеки даних. DES є блоковим шифром, що працює з блоками даних по 64 біти кожен. Для зашифрування та розшифрування використовується один і той же алгоритм і ключ, що має довжину 56 біт. Однак, DES, на жаль, виявився вразливим до різноманітних атак, що призвело до зниження його популярності.

DES ґрунтується на двох основних принципах криптографії: підстановці та транспозиції. Він складається з 16 етапів, які називаються раундами. Процес шифрування включає три основні етапи. Спочатку відкритий текст, який складається з 64 біт, проходить через початкову перестановку для отримання перетвореного вхідного тексту. Потім відбувається 16 раундів, кожен з яких включає в себе функції підстановки та транспозиції. У кінці останнього раунду отримуємо 64-бітний зашифрований текст, який отримується як функція від вихідного відкритого тексту та ключа [26].

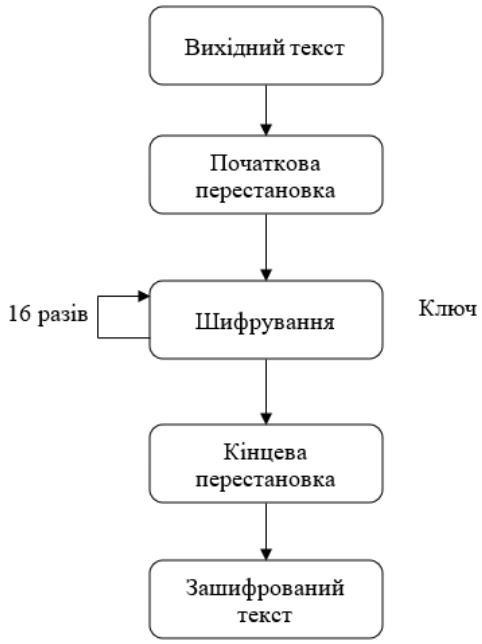

Рис. 2.2. Узагальнена схема шифрування алгоритму DES

Щоб розшифрувати дані, зашифровані за допомогою DES, процес розшифрування змінює послідовність кроків, застосованих під час шифрування. Як правило, для розшифрування використовується той самий алгоритм, що і для шифрування, з ключовою відмінністю, яка полягає у зворотному порядку застосування підключів. Кожен раунд розшифрування змінює відповідний раунд шифрування на протилежний. Зрештою, фінальна перестановка ефективно скасовує початкову перестановку шифрування, що призводить до відновлення початкового значення даних. Цей послідовний процес реверсування гарантує, що зашифровані дані будуть успішно розшифровані, відновлюючи їх до початкового вигляду.

International Data Encryption Algorithm (IDEA) – це надійна система блокового шифрування, що призначена для роботи з 64-бітними блоками даних та використовує 128-бітний ключ для своїх криптографічних операцій [28]. У процесі шифрування, кожен 64-бітний блок даних розбивається на чотири рівні підблоків довжиною по 16 бітів кожен, які проходять через вісім циклів, кожен з яких включає унікальні перетворення.

Кожен цикл IDEA використовує шість різних ключів, отриманих з початкового 128-бітного ключа. Вихідні дані з кожного раунду служать вхідними даними для наступного, створюючи послідовний ефект, що поліпшує зашифрований результат. Однак у восьмому циклі алгоритм відхиляється від цього патерну. Ця фаза, зазвичай арифметичних операцій, використовує чотири додаткові ключі, відмінні від попередніх. Остаточний ключ шифру генерується після завершення цієї фази.

Важливо відзначити, що IDEA використовує в цілому 52 ключі для управління різними операціями та перетвореннями. Ця складна система управління ключами підкреслює спрямованість IDEA на надійні методи шифрування, забезпечуючи високий рівень захисту конфіденційних даних [29].

Blowfish – це симетричний шифр з 64-бітним блоком та змінною довжиною ключа. Створений Брюсом Шнайером у 1993 році як алгоритм загального призначення, він прагнув стати швидкою, ефективною та безкоштовною альтернативою застарілим DES та IDEA. Одним з головних переваг Blowfish є його висока швидкодія порівняно з DES та IDEA, а також доступність для всіх користувачів без патентів чи обмежень. Проте через невеликий розмір блоку, який вважається небезпечним, він не зміг повністю витіснити DES із застосування.

Цей процес передбачає кілька етапів. Початковий ключ шифрування проходить трансформацію через алгоритм розширення ключа, щоб створити серію підключів. Потім відбувається початкова перестановка вхідного тексту, яка стає основою для подальших операцій. Блок даних розбивається на дві половини, що дозволяє їх паралельну обробку. Наступним етапом є проходження блоку через 16 раундів шифрування, кожен з яких включає в себе послідовність складних криптографічних операцій. У кінці виконується фінальна перестановка, яка синтезує результати шифрування і формує готовий зашифрований текст [30].

Стандарт Advanced Encryption Standard (AES) є основним алгоритмом блочного шифрування, який прийшов на зміну алгоритмам DES і Triple DES. Він

шифрує і розшифровує 128-бітний блок даних. Було визначено, що Advanced Encryption Standard наразі є найкращим симетричним алгоритмом шифрування для мережевої безпеки. Теоретично вважається, що його неможливо зламати, оскільки комбінації ключів величезні. Залежно від обраного розміру ключа – 128 біт, 196 біт або 256 біт – AES виконує 10, 12 або 14 раундів шифрування відповідно.

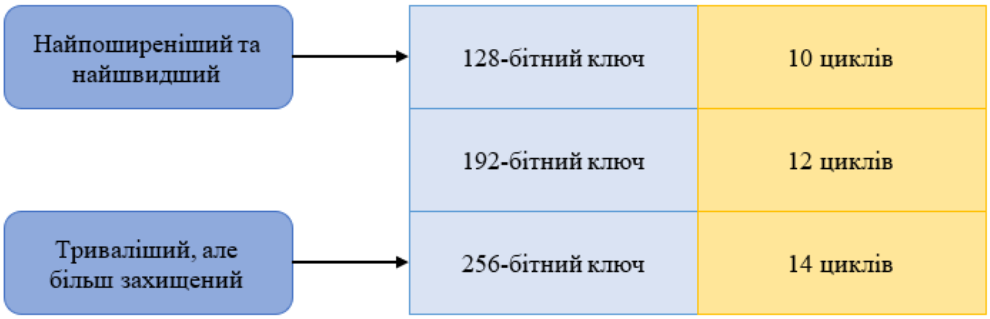

Рис. 2.3. Визначення довжини ключа AES

Кожен цикл шифрування складається з чотирьох основних операцій: заміна байтів, зсув рядків, перемішування стовпців і додавання ключа раунду. Слід зазначити, що операція перемішування стовпців виключена з останнього циклу. Під час шифрування в кожному раунді використовуються окремі ключі циклів, згенеровані з заданого ключа шифру, що підвищує безпеку.

Дані, призначені для шифрування, розбиваються на блоки, кожен з яких представляється у вигляді масиву даних. Такий структурований підхід полегшує застосування AES до різних типів даних і забезпечує ефективний процес шифрування.

Процес розшифрування – це процес шифрування, який виконується у зворотному порядку. Дані, які передаються як зашифрований вміст, розшифровуються до оригінального вмісту за допомогою ключа AES [31].

Таким чином, ми розглянули основні базові алгоритми симетричного шифрування. Для узагальнення складемо порівняльну таблицю.

Таблиця 2.1

Порівняльна характеристика криптографічних алгоритмів [32]

Назва алгоритму	Розмір ключа (біт)	Унікальність алгоритму	До яких атак вразливий
DES	56	16 раундів, зсув вліво, структура Файстеля, підстановка 32-бітної заміни	Брутфорс, лінійний та диференціальний криптоаналіз
IDEA	128	8,5 раундів, мережева структура Файстеля	Слабкий ключ
Blowfish	32-448	16 раундів, ключ-незалежний S-бокс, структура Файстеля	Слабкий ключ, диференціальна атака другого порядку
AES	128, 192, 256	10, 12 абл 14 раундів, мережа замін-перестановок	Атака сторонніми каналами, відомий відкритий текст
RC-6	128, 192, 256	20 циклів, Мережа Файстеля	Відомий відкритий текст

Отже, проаналізувавши порівнявши алгоритми, можемо зробити висновок, що кожен з них має свої унікальні характеристики, які впливають на його безпеку та ефективність. В основному, всі розглянуті алгоритми належать до структур Файстеля або мереж замін-перестановок, що прямо вказує на їхню складність та стійкість до криптоаналізу. В залежності від специфічних вимог безпеки, наявних ресурсів та потенційних загроз. організації, які потребують захист свого хмарного середовища, можуть обрати будь-який з наведених алгоритмів, інших наявних, або комбінації з декількох.

2.2 Основи асиметричного шифрування даних у хмарних обчислення

Асиметричне шифрування, також відоме як криптографія з відкритим ключем, відрізняється від традиційного симетричного підходу, оскільки використовує два ключі: публічний (відкритий) та приватний (закритий). Ця технологія дозволяє створювати захищені канали комунікації та здійснювати безпечний обмін даними навіть у відкритих мережах, таких як хмарні обчислення.

Публічний ключ є загальнодоступним і використовується будь-якими користувачами для надсилання повідомлень відправнику. Приватний ключ залишається конфіденційним і відомий лише відправнику. Повідомлення, зашифроване публічним ключем, може бути розшифроване тільки за допомогою відповідного приватного ключа, що зберігається у відправника. Так само, повідомлення, зашифроване приватним ключем, може бути розкодоване з використанням публічного ключа. Відкритий ключ не потребує особливих заходів безпеки, оскільки він доступний широкому загалу та може передаватися відкритими каналами зв'язку в мережі Інтернет. Така система забезпечує безпечний обмін даними між користувачами, незважаючи на відкритий характер публічного ключа. Найпоширенішими алгоритмами асиметричного шифрування є RSA та протокол Діффі-Геллмана.

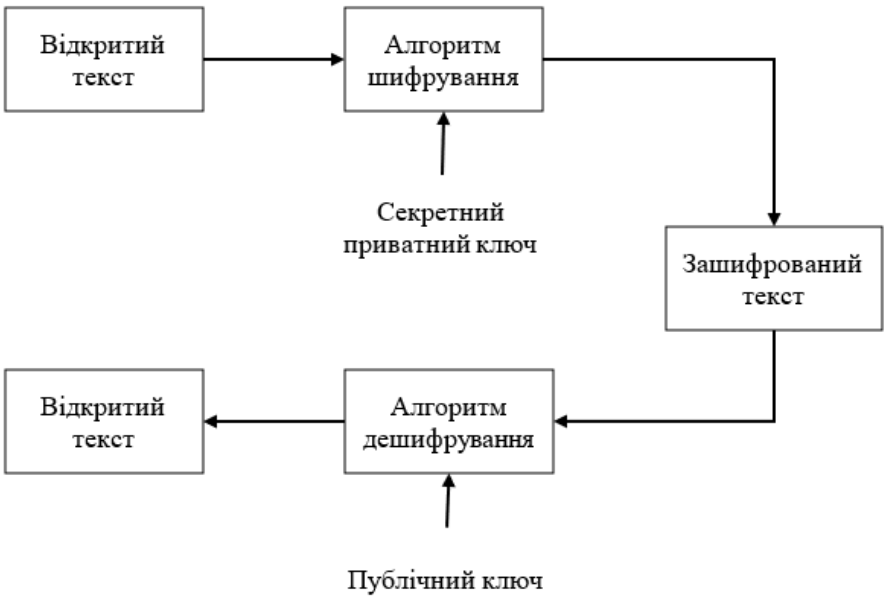

Рис. 2.4. Принцип асиметричного шифрування

RSA – відносно повільний алгоритм. Через це він не використовується для безпосереднього шифрування даних користувача. Частіше RSA використовується для передачі спільних ключів для криптографії з симетричним ключем, які потім використовуються для масового шифрування-розшифрування. В алгоритмі RSA під час генерації ключів для асиметричного шифрування,

вибираються два великих простих числа, які використовуються для створення модуля. Публічний ключ обирається таким чином, щоб він був взаємно простим з числом, що обчислюється на основі вибраних простих чисел. Шифрування виконується шляхом піднесення повідомлення до степеня, що відповідає публічному ключу, за модулем, тоді як розшифрування - це піднесення зашифрованого тексту до степеня, яка відповідає приватному ключу, з використанням того ж самого модуля. Безпека алгоритму ґрунтується на складності факторизації великих чисел, використовуваних для створення ключів, що ускладнює спроби несанкціонованого доступу до зашифрованих даних [33].

Протокол Діффі-Геллмана — це метод безпечного обміну ключами між сторонами через ненадійний канал зв'язку. Кожна сторона генерує випадкове приватне число і, на основі цього числа та загально відомих параметрів, обчислює відповідне публічне число. Публічні числа обмінюються між сторонами, і кожна сторона використовує публічне число іншої сторони разом зі своїм приватним числом для обчислення спільного секретного ключа. Цей спільний секретний ключ може бути використаний для подальшого шифрування та розшифрування повідомлень між сторонами. Оскільки обчислення спільного секретного ключа базується на публічних числах, які обмінюються між сторонами, і приватних числах, які залишаються секретними, протокол Діффі-Геллмана забезпечує безпеку обміну ключами, навіть якщо зловмисники перехоплять зв'язок [34].

2.3 Порівняльний аналіз розглянутих методів

Хмарні сервіси разом з технологіями та моделями розгортання несуть відповідальність за впровадження ризиків та вразливостей, пов'язаних з хмарними технологіями. У такому хмарному середовищі одним із ключових питань стає вибір методу шифрування даних, що забезпечить їхню конфіденційність та цілісність.

Алгоритми шифрування з використанням симетричного та асиметричного ключів виявляються дієвими при захисті конфіденційності даних, що передаються через різноманітні канали зв'язку. Серед них симетричні методи криптографії часто виходять переможцями завдяки їх простоті та ефективності, що забезпечується меншою вимогливістю до обчислювальних ресурсів та спрощеним процесом впровадження. Тим не менш, важливо враховувати, що обидва типи шифрування мають свої переваги та недоліки, і вибір між ними повинен здійснюватися з урахуванням конкретних потреб проекту та умов його впровадження. [35]

Розглянемо основні переваги і недоліки розглянутих в попередніх розділах методів. DES відомий як перший широко використовуваний алгоритм шифрування, що в значній мірі сприяло його популярності та розповсюдженню. Він відрізняється простою структурою та алгоритмом, що робить його дуже доступним для використання. Однак основною його недолікою є короткий ключ, що складається лише з 56 бітів. У порівнянні з сучасними алгоритмами, це може зробити DES вразливим до атак брутфорсу, особливо з урахуванням швидкого розвитку технологій. З плином часу та зростанням потужності обчислювальних засобів, DES стає більш вразливим до різних атак, що зменшує його ефективність в забезпеченні надійного криптографічного захисту

Переваги алгоритму Blowfish включають гнучкість ключа, оскільки він дозволяє використовувати ключі різної довжини, що забезпечує високий рівень безпеки та робить його універсальним у застосуванні. Крім того, у порівнянні з DES та IDEA, Blowfish пропонує значно швидший процес шифрування, що робить його ефективним у різних сценаріях застосування. Проте у алгоритму Blowfish також є свої недоліки. З урахуванням зростаючої потужності обчислювальних систем, короткий розмір ключа може зробити його вразливим до атак брутфорсу. Крім того, в порівнянні з іншими алгоритмами, такими як AES, Blowfish не має такого широкого спектру використання, що може обмежити його практичність у деяких областях застосування [36].

Переваги алгоритму AES включають високий рівень безпеки завдяки використанню ключів різної довжини (128, 192 або 256 біт), що забезпечує ефективний захист даних від несанкціонованого доступу та різних атак. Також важливою перевагою є ефективність алгоритму, оскільки AES має оптимальну швидкість та високу ефективність у виконанні криптографічних операцій. Це робить його ідеальним вибором для різноманітних застосувань, включаючи хмарні обчислення. Проте алгоритм має деякі недоліки. Обмеженість розміру блоку на рівні 128 біт може викликати деякі труднощі в обробці великих обсягів даних, особливо у випадку, коли вони потребують розбиття на менші частини. Також важливо враховувати вимоги до ресурсів, оскільки шифрування та розшифрування за допомогою AES може вимагати значних обчислювальних ресурсів, особливо при використанні довших ключів. це може бути проблемою в невеликих середовищах, де доступні ресурси обмежені. [37]

Алгоритм RSA відомий своєю високою криптографічною надійністю, оскільки його безпека базується на складності розкладання великих простих чисел. Це робить його ефективним в захисті від різних атак. Однією з ключових переваг RSA є можливість безпечного обміну ключами через відкриті канали зв'язку. Однак, процес генерації ключів та обробка великих чисел може вимагати значних обчислювальних ресурсів, що призводить до затримок у виконанні операцій, особливо при використанні довших ключів. Крім того, RSA має обмеження на розмір повідомлень, які можуть бути шифровані безпосередньо алгоритмом, що може ускладнювати обробку великих обсягів даних.

Протокол Діффі-Геллмана є ефективним методом безпечного обміну ключами, що дозволяє сторонам встановлювати спільний секретний ключ навіть у випадку, коли комунікація відбувається через ненадійний канал. Але необхідно пам'ятати про потенційні загрози безпеці, де зловмисники можуть перехоплювати та модифікувати обмінювані ключі, особливо якщо протокол не використовує додаткові заходи для підтвердження автентичності сторін.[38]

Підсумовуючи, для кращого аналізу та розуміння різниці між алгоритмами зберемо деякі характеристики в таблиці 2.2.

Таблиця 2.2.

Порівняння симетричного та асиметричного шифрування даних

Характеристика	Симетричне шифрування			Асиметричне шифрування	
	DES	BLOWFISH	AES	RSA	Діффі-Геллмана
Ключ, що використо-вується	Для шифрування та дешифрування використовується один і той самий ключ	Для шифрування та дешифрування використовується один і той самий ключ	Для шифрування та дешифрування використовується один і той самий ключ	Для шифрування та дешифрування використовуються різні ключ	Обмін ключами
Рівень шифрування	Високий	Високий	Високий	Високий	Високий
Швидкість	Швидкий	Швидкий	Швидкий	Швидкий	Повільний
Пропускна здатність	Нижча, ніж в AES	Дуже висока	Нижча, ніж в Blowfish	Низька	Нижча, ніж в RSA
Енерго-споживання	Вище, ніж в AES	Дуже низьке	Вище, ніж в Blowfish	Високе	Нижче, ніж в RSA
Можливість налаштування	Немає	Є	Немає	Є	Є
Які сторони захищені	І користувач, і провайдер	І користувач, і провайдер	І користувач, і провайдер	Тільки користувач	–

Отже, порівняльний аналіз симетричного та асиметричного шифрування в контексті хмарних обчислень демонструє, що кожен з цих методів має свої переваги та обмеження. Симетричне шифрування відзначається високою швидкістю обробки даних, проте вимагає безпечного обміну ключами. З іншого боку, асиметричне шифрування забезпечує більшу безпеку завдяки використанню двох ключів, але при цьому може бути менш ефективним в роботі з великими обсягами даних. При виборі методу шифрування у хмарних обчисленнях важливо враховувати специфіку проекту, його потреби у швидкості, безпеці та ресурсах. Розумне поєднання обох методів, або використання гібридних підходів, може бути оптимальним рішенням для забезпечення надійності та ефективності захисту даних у хмарному середовищі.

У перспективі, шифрування залишається важливою складовою для надійної та безпечної передачі даних. Різноманітні програмні засоби можуть використовувати як симетричні, так і асиметричні алгоритми шифрування для посилення захисту конфіденційності даних. Забезпечення високого рівня безпеки системи мінімізує ймовірність її компрометації. Майбутнє кібербезпеки залежить від ефективного використання таких шифрувальних алгоритмів, які ускладнюють або навіть роблять неможливими спроби несанкціонованого доступу до даних.

Висновки до розділу 2

Таким чином, симетричне шифрування даних виявляється важливою складовою сучасних криптографічних систем, забезпечуючи ефективний та безпечний обмін інформацією. Принцип симетричного шифрування базується на використанні одного ключа для як шифрування, так і розшифрування даних, що спрощує процес, але одночасно вимагає надійного збереження цього ключа від несанкціонованого доступу. Такий підхід забезпечує конфіденційність даних під час їх передачі через відкриті мережі, такі як Інтернет. Важливо також враховувати розмір ключа та використовуваний алгоритм шифрування для запобігання потенційним атакам і забезпечення високого рівня безпеки.

Натомість, асиметричне шифрування є важливою складовою безпеки даних у хмарних обчисленнях. Воно дозволяє безпечно обмінюватися ключами і зашифровувати дані, забезпечуючи конфіденційність і цілісність інформації, навіть коли спілкування відбувається через ненадійні канали. Цей метод шифрування використовується в різних сферах і завдяки його математичним основам та застосуванню сучасних криптографічних протоколів, асиметричне шифрування стає надійним і ефективним засобом захисту конфіденційної інформації в умовах хмарних обчислень.

РОЗДІЛ 3 ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ МЕТОДІВ ШИФРУВАННЯ ДАНИХ У ХМАРНИХ ОБЧИСЛЕННЯХ

3.1 Аналіз тенденцій розвитку шифрування в хмарних середовищах

На основі досліджень, проведених в перших двох розділах можна впевнено сказати, що забезпечення безпеки та конфіденційності даних в хмарних середовищах визначаються як одні з ключових проблем в сучасному цифровому світі. Шифрування, як технологія, яка дозволяє захищати інформацію від несанкціонованого доступу, стає невід'ємною складовою в будь-якій стратегії безпеки даних у хмарних середовищах.

Розуміння тенденцій розвитку шифрування в хмарних середовищах має величезне значення для розробки та впровадження ефективних стратегій захисту даних, що будуть відповідати вимогам безпеки, конфіденційності та регулятивних вимог.

Організації все частіше намагаються оптимізувати свої хмарні сервіси та посилити можливості аварійного відновлення. Це призводить до збільшення попиту на крос-платформенні рішення для шифрування. Мультихмарні сервіси шифрування розроблені з метою надання єдиних стандартів безпеки у різних хмарних середовищах, забезпечуючи захист даних незалежно від їх місцезнаходження. Це рішення змушує постачальників послуг з шифрування вдосконалювати свої продукти та впроваджувати інновації, щоб забезпечити сумісність з різними хмарними платформами.

Впровадження мультихмарних рішень для шифрування дозволяє організаціям ефективно зменшити ризики, пов'язані з залежністю від одного постачальника, тим самим підвищуючи стійкість до можливих витоків даних або системних збоїв. Крім того, ці рішення допомагають підприємствам відповідати нормативним вимогам та дотримуватися високих стандартів захисту даних у всіх хмарних середовищах. [39]

Ще однією зростаючою тенденцією є використання моделі з нульовою довірою (Zero Trust Model). Вона відзначається радикальним переглядом підходу організацій до кібербезпеки, де організація нічому не довіряє в мережі, навіть власним внутрішнім ресурсам. Вона використовує принцип "довіряй, але перевіряй", вимагаючи постійної аутентифікації та авторизації від користувачів для отримання доступу до будь-яких ресурсів. Це означає, що кожен запит на доступ повинен пройти перевірку, перед тим як буде надано дозвіл, незалежно від мережевого контексту чи місцезнаходження користувача.

З огляду на зростання загроз кібербезпеці, включаючи інсайдерські атаки та складні розподілені загрози, прийняття моделі з нульовою довірою стає все більш важливим. Шляхом розгляду кожної спроби доступу як потенційної загрози, незалежно від її походження в організації, ця модель дозволяє компаніям значно посилити свої системи безпеки.

Основні складові моделі нульової довіри включають мікросегментацію мережі, механізми аутентифікації, надійні методи шифрування даних та суворий контроль над привілейованим доступом. Впровадження цієї моделі передбачає зміну парадигми в тому, як організації розробляють і впроваджують свої стратегії безпеки. Вони повинні перейти від статичного захисту, орієнтованого на периметр, до більш динамічних, адаптивних підходів, які надають пріоритет стійкості до загроз та їх пом'якшенню [40].

У контексті посилення глобальних правил захисту даних, таких як GDPR, HIPAA та CCPA, зашифроване хмарне сховище перетворюється з необов'язкової опції на необхідну складову для відповідності нормативним вимогам. Зростаючий тиск з боку регуляторних органів змушує компанії акцентувати увагу на впровадженні передових рішень для шифрування з метою відповідності законодавчим вимогам та зменшення ризику значних фінансових штрафів. Відтак, постачальники послуг шифрування активно включають у свої рішення функції управління комплаєнсом, спрощуючи процес дотримання складних регуляторних норм.

За допомогою надійних технологій шифрування, компанії можуть забезпечити захист конфіденційних даних та дотриматись прав на приватність своїх клієнтів, що сприяє зміцненню довіри та лояльності. Більше того, рішення для шифрування, які мають інтегровані інструменти управління відповідністю, дозволяють організаціям більш ефективно реагувати на складні регуляторні вимоги, забезпечуючи виконання законодавства про захист даних без втрати операційної ефективності [41].

3.2 Рекомендації щодо подальшого вдосконалення методів шифрування даних

Методи шифрування даних виступають ключовим інструментом для захисту інформації від несанкціонованого доступу та забезпечення конфіденційності під час передачі та зберігання. І хоча сфера хмарного обчислення часто аналізується та реформується, питання захисту даних та надійності користувачів залишається невизначеним через зростаючі схеми кібератак, а також помилки хмарних систем зберігання даних. Необхідно розуміти основні завдання забезпечення захисту даних в хмарі та на виконанні яких завдань будується система захисту. Розглянемо ці основні завдання:

1. Цілісність – у хмарних обчисленнях під час передачі даних до хмарного сховища виникає ризик їхнього пошкодження або несанкціонованих маніпуляцій з ними. Оскільки інформація та обчислення делегуються на віддалені сервери, збереження цілісності даних стає вирішальним для забезпечення точності та надійності взаємодії. Для захисту даних від несанкціонованих змін і підтримки достовірності інформації необхідні механізми моніторингу та перевірки.

2. Доступність – доступність у хмарних обчисленнях означає безперешкодне отримання необхідних даних абонентами. Безперебійний доступ до ресурсів хмарних обчислень є життєво важливим для роботи організації,

оскільки персонал отримує безперервний доступ до даних і може забезпечити безперебійну роботу сервісів.

3. Безпека даних – підвищення безпеки хмарних обчислень передбачає впровадження надійних заходів, таких як шифрування, автентифікація та виявлення вторгнень для захисту збережених даних. Ці заходи знижують ризики несанкціонованого доступу, витоку даних і зловмисних дій, тим самим посилюючи загальний рівень безпеки хмарних середовищ.

4. Функціональна сумісність – сумісність означає здатність різних систем або процесів ефективно співпрацювати та безперешкодно обмінюватися даними. Безперешкодна інтеграція хмарних обчислювальних мереж дозволяє організаціям використовувати синергію та підвищувати ефективність. Однак закриті хмарні системи, яким бракує інтероперабельності, перешкоджають безперешкодному обміну інформацією, обмежуючи потенційну економію коштів та операційну ефективність [42].

Якщо ці всі завдання керівники організації та розробники безпекової політики розуміють, розроблені ними системи захисту будуть ефективно функціонувати.

Впровадження тенденцій розвитку шифрування, розглянутих в попередньому підрозділі, дозволить організаціям зменшити ризики порушення безпеки та витоку конфіденційної інформації, а також забезпечить відповідність з нормативними вимогами щодо захисту даних. Розглянемо детальніше процес впровадження моделі з нульовою довірою.

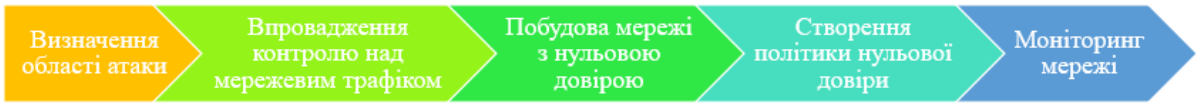

Рис. 3.1. Впровадження моделі з нульовою довірою

Область атаки - це сукупність усіх потенційних точок вразливості в системі, мережі або організації, які можуть бути використані зловмисниками для порушення безпеки. Вона охоплює різні елементи, такі як обладнання,

програмне забезпечення, додатки, мережева інфраструктура, облікові записи користувачів і сховища даних. Визначення області атаки передбачає виявлення та розуміння цих вразливих місць, щоб ефективно розставити пріоритети у забезпеченні безпеки.

Зосередившись на визначенні області атаки, організації можуть точно визначити критичні активи та зони підвищеного ризику, які потребують посиленого захисту. Такий цілеспрямований підхід дозволяє їм ефективно розподіляти ресурси, впроваджувати адаптовані політики безпеки і розгортати спеціалізовані інструменти для зниження ризиків і запобігання потенційним загрозам. У контексті стратегії безпеки з нульовою довірою визначення області атаки є основним кроком на шляху до створення комплексної системи безпеки. Визначивши найбільш важливі цифрові активи та визначивши їх пріоритетність, організації можуть проактивно зміцнити свій захист, зменшити ймовірність успішних кібератак і захистити свої цінні ресурси від потенційних порушень [43].

Впровадження контролю над мережевим трафіком передбачає регулювання потоку даних у вашій мережі на основі залежності, на яку покладається кожна система. Наприклад, багатьом системам може знадобитися доступ до бази даних, що містить важливу інформацію про клієнтів, продукти чи послуги. У цьому випадку запити не просто надсилаються в систему, а проходять через базу даних, яка містить конфіденційні дані та складну архітектуру. Розуміючи ці нюанси та залежності, організації можуть приймати обґрунтовані рішення щодо впровадження та розміщення засобів мережевого контролю. Такий стратегічний підхід дозволяє їм розгортати механізми, які ефективно керують потоками даних у мережі, гарантуючи, що конфіденційна інформація залишається захищеною та неушкодженою. Розуміння тонкощів потоку мережевого трафіку дає організаціям можливість адаптувати свої заходи безпеки для усунення конкретних вразливостей і ефективного зниження потенційних ризиків.

Архітектура мережі з нульовою довірою передбачає розробку системи безпеки, пристосованої до унікальних вимог захисту поверхні атаки вашої організації. Одним з ключових компонентів багатьох архітектур нульової довіри є розгортання брандмауерів нового покоління (NGFW). Ці вдосконалені брандмауери виходять за рамки традиційної перевірки пакетів і забезпечують детальний контроль мережевого трафіку, фільтрацію на рівні додатків і сегментацію. Сегментуючи мережу на окремі зони на основі рівнів довіри або чутливості даних, NGFW допомагають мінімізувати радіус ураження потенційних порушень і більш ефективно стримувати загрози.

Ще одним важливим аспектом побудови мережі з нульовою довірою є впровадження багатофакторної автентифікації (MFA). MFA додає додатковий рівень безпеки, вимагаючи від користувачів пройти кілька форм перевірки перед наданням доступу до ресурсів. Це може включати комбінацію того, що користувач знає (наприклад, пароль), того, що він має (наприклад, мобільний пристрій або токен), і того, ким він є (наприклад, біометричні дані). Впроваджуючи MFA, організації можуть забезпечити доступ до конфіденційних даних і ресурсів лише авторизованим користувачам з підтвердженими ідентифікаційними даними [44].

Хоча NGFW і MFA є основними компонентами багатьох архітектур нульової довіри, дуже важливо адаптувати дизайн до конкретних потреб і вимог вашої організації. Це може включати додаткові заходи, такі як сегментація мережі, управління ідентифікацією та доступом (IAM), шифрування, безперервний моніторинг та виявлення аномалій. Зрештою, метою мережі нульової довіри є створення комплексної системи безпеки, яка мінімізує ризик витоку даних і несанкціонованого доступу, незалежно від розміру і складності мережі.

Створення політики нульової довіри є вирішальним кроком у забезпеченні ефективності вашої архітектури мережевої безпеки. Метод Кіплінга, який передбачає запитання хто, що, коли, де, чому і як для кожного користувача,

пристрою і мережі, які шукають доступ, може бути корисним при розробці комплексних і детальних політик.

– Хто? – визначте користувачів та організації, які шукають доступ до ресурсів у мережі. Сюди входять працівники, підрядники, партнери та будь-які інші зацікавлені сторони.

– Що? – визначте конкретні ресурси та дані, до яких користувачі та пристрої намагаються отримати доступ. Сюди входять програми, бази даних, файли та інші ресурси.

– Коли? – визначте часові рамки, протягом яких доступ дозволений або обмежений. Це може включати обмеження доступу залежно від часу доби, дня тижня або певних подій чи обставин.

– Де? – вкажіть місця або мережі, з яких доступ дозволено або заборонено. Це можуть бути фізичні місця, IP-адреси або географічні регіони.

– Навіщо? – визначте мету або обґрунтування доступу до ресурсів. Це допомагає встановити легітимність запитів на доступ і забезпечити відповідність бізнес-вимогам і політикам безпеки.

– Як? – визначте методи або механізми, що використовуються для автентифікації та авторизації доступу. Сюди входять фактори автентифікації, такі як паролі, біометричні дані або токени безпеки, а також засоби контролю авторизації на основі ролей користувачів, привілеїв і принципу найменших привілеїв [45].

Систематично вирішуючи ці питання для кожного користувача, пристрою та мережі, які намагаються отримати доступ, організації можуть розробити комплексну політику нульової довіри, яка забезпечить дотримання принципу найменших привілеїв та мінімізує ризик несанкціонованого доступу або витоку даних. Ці політики слугують основою для впровадження ефективних засобів контролю доступу, стратегій сегментації та заходів безпеки в мережі, що в кінцевому підсумку підвищує загальний рівень безпеки та зменшує потенційні ризики.

Останнім кроком в впровадженні моделі з нульовою довірою є моніторинг мережі. Моніторинг мережі – практика для підтримки надійної безпеки та випередження потенційних загроз. Постійно спостерігаючи за мережевою активністю, ви отримуєте цінну інформацію про поведінку користувачів, взаємодію пристроїв і продуктивність додатків. Це дозволяє виявити аномалії, підозрілі дії або порушення безпеки на ранніх стадіях.

Завдяки моніторингу ви можете виявляти інциденти безпеки в режимі реального часу, оперативно реагувати на загрози та зменшувати ризики до їх загострення. Крім того, мережевий моніторинг дає уявлення про продуктивність мережі, використання ресурсів і дотримання політик безпеки, що дозволяє оптимізувати інфраструктуру і підвищити загальний рівень безпеки[46].

Таким чином, після впровадження цієї моделі нешативні наслідки ризиква та загроз будуть мінімізовані та дані в хмарному середовищі будуть захищені.

Також необхідно розглянути моделі шифрування, які зможуть ефективно приховати вміст даних від зловмисників. Гібридні моделі шифрування забезпечують ефективний захист конфіденційності та цілісності даних. Вони комбінують переваги як симетричних, так і асиметричних методів шифрування, щоб забезпечити комплексний підхід до безпеки. Симетричне шифрування, завдяки своїй ефективності та швидкості, ідеально підходить для шифрування великих обсягів даних. Воно використовує один ключ для шифрування та дешифрування, що дозволяє оперативно обробляти інформацію з мінімальними затримками. Це особливо важливо для хмарних обчислень, де великі обсяги даних постійно переміщуються та обробляються.

В той самий час, асиметричне шифрування відіграє важливу роль у зберіганні та обміні ключів шифрування, забезпечуючи додатковий рівень безпеки від несанкціонованого доступу. Використовуючи пару ключів (публічний і приватний) асиметричне шифрування дозволяє безпечно передавати ключі для симетричного шифрування, знижуючи ризик їх перехоплення. Публічний ключ використовується для шифрування даних, тоді як приватний ключ, який зберігається у суворій таємниці, застосовується для

дешифрування. Це поєднання дозволяє створити більш захищену систему, де симетричне шифрування забезпечує швидкість, а асиметричне – безпеку обміну ключами.Гібридні моделі шифрування, які об'єднують ці два методи, надають комплексний підхід до захисту даних. Вони допомагають зменшити вразливості та підвищують стійкість до кіберзагроз, оскільки комбінують ефективність симетричного шифрування з безпекою асиметричного. Більше того, такий підхід сприяє оптимізації продуктивності, що особливо важливо для підприємств, що опікуються великими обсягами конфіденційної інформації [47].

Для вдосконалення методів шифрування даних в хмарному середовищі, розробимо гібридну трирівневу модель шифрування даних на основі алгоритмів RSA, BLOWFISH та DES. Теоретично ця модель шифрування може мати значний вплив на підвищення безпеки в хмарних середовищах. Дані алгоритми були вибрані з таких причин:

1. Алгоритм DES з своєю короткою генерацією ключів має дуже високу швидкість.
2. Алгоритм BLOWFISH надає підвищений рівень безпеки завдяки довгій генерації ключів.
3. RSA має високу сумісність з інтернет-обробкою та вищу безпеку в порівнянні з попередніми алгоритмами.

Для шифрування даних при їх завантаженні в хмару цей алгоритм послідовно використовує наступні ключі:

1. Дані спочатку шифруються за допомогою секретного ключа BLOWFISH.
2. Вихідні дані знову шифруються секретним ключем DES.
3. Секретний ключ BLOWFISH і секретний ключ DES шифруються за допомогою відкритого ключа RSA.

Для розшифрування алгоритм виконає такі кроки:

1. Секретний ключ BLOWFISH та секретний ключ DES розшифровуються за допомогою приватного ключа RSA клієнта.

2. Ключ DES використовується для першого розшифрування запитуваних даних.

3. Останнім кроком, щоб отримати оригінальні дані, вихідні дані розшифровуються за допомогою секретного ключа blowfish.

Розглянемо цей алгоритм на Рис.

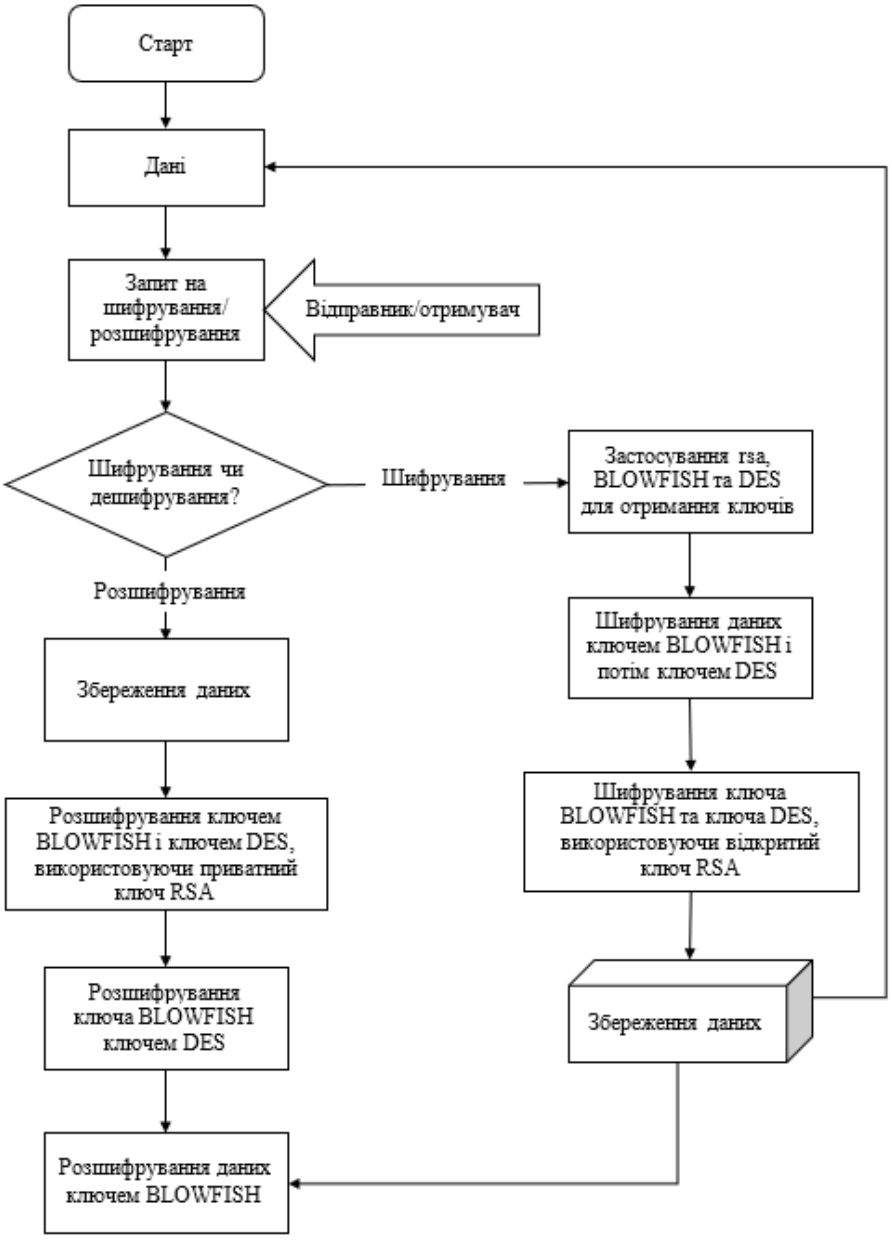

Рис. 3.2. Повний алгоритм трирівневої моделі шифрування даних

На останок, розглянемо ще деякі тенденції розвитку шифрування, які різні організації впроваджують в свої хмарні середовища для подальшого вдосконалення наявних методів шифрування.

Кордонні обчислення – це парадигма розподілених обчислень, яка переносить обчислення і носії даних ближче до джерела даних. Поява кордонних обчислень породило потребу в спеціалізованих рішеннях для шифрування, розроблених спеціально для кордонних середовищ. З огляду на те, що обробка даних відбувається все частіше на місці їх створення, забезпечення безпеки даних під час їх передачі та в процесі спокою стає невід'ємною частиною процесу. Технології шифрування, адаптовані для кордонних обчислювальних середовищ, відіграють ключову роль у захисті даних від перехоплення або несанкціонованого доступу, особливо тоді, коли обробка виходить за межі звичайних центрів обробки даних або хмарних середовищ.

Ця тенденція має велике значення для різноманітних сфер застосування, особливо в галузі пристроїв Інтернету речей (IoT) та інших кордонних систем, де забезпечення конфіденційності та безпеки даних є основним завданням. З огляду на поширення кордонних обчислень у різних галузях, росте потреба у надійних механізмах шифрування для захисту конфіденційної інформації, що циркулює через ці децентралізовані мережі. Впровадження рішень шифрування для кордонних обчислень дозволить організаціям знизити ризики та посилити систему безпеки своїх кордонних розгортань, що збільшить рівень довіри та впевненості в цілісності їхніх методів обробки даних.

Автоматизація спричинює значні трансформації в технології шифрування, особливо в контексті управління ключами. Автоматизовані системи управління ключами (KMS) перевертають звичайні підходи до розгортання та контролю над ключами шифрування. Шляхом автоматизації процесів генерації, розподілу та керування життєвим циклом ключів, ці системи мінімізують людський вплив і значно підвищують ефективність шифрування. Цей тренд не лише зміцнює заходи безпеки, але й зменшує адміністративне навантаження на IT-відділи. Віддаючи відповідальність за ключі автоматизованим системам, це відкриває IT-

командам можливість зосередитися на інших важливих аспектах інформаційної безпеки. Це, в свою чергу, сприяє створенню більш надійних та стійких заходів захисту від нових загроз.

Квантова криптографія – це новітній напрям у захисті даних, що використовує принципи квантової механіки для захисту інформації від потенційних квантових атак. В основі квантової криптографії лежить квантовий розподіл ключів (QKD) – технологія, яка дозволяє генерувати ключі шифрування за допомогою квантових процесів, роблячи їх невразливими для розшифрування звичайними засобами. Хоча квантова криптографія все ще перебуває на початковій стадії розвитку, вона потенційно може докорінно змінити хмарне шифрування, пропонуючи безпрецедентний рівень безпеки [48].

Висновки до розділу 3

У цьому розділі ми розглянули перспективи вдосконалення методів шифрування даних у сфері хмарних обчислень. Аналіз тенденцій розвитку шифрування надало нам розуміння їх важливості для розробки та впровадження ефективних стратегій захисту даних. Постійної уваги потребують такі ключові питання, як мультихмарні сервіси та моделі з нульовою довірою.

Рекомендації, запропоновані для подальшого вдосконалення, показують, що існують величезні можливості для посилення заходів безпеки, які застосовуються при зберіганні та передачі даних у хмарних середовищах. Контроль над мережевим трафіком, гібридні моделі шифрування, кордонні обчислення, автоматизація та квантова криптографія допомагають організаціям зосередити увагу на оптимізації алгоритмів шифрування для кращої обробки великих обсягів даних, характерних для хмарних обчислень. Це включає вдосконалення ключових процесів управління для забезпечення безперебійної та безпечної роботи.

Оскільки технології захисту даних в хмарному середовищі продовжують розвиватися, постійна адаптація та вдосконалення методів шифрування буде

мати важливе значення для захисту конфіденційної інформації в хмарі. Це дозволить організаціям залишатися на передовій захисту даних, забезпечуючи безпеку і надійність своїх інформаційних систем.

Висновки

Хмарні обчислення стали невід'ємною частиною сучасної IT-інфраструктури, надаючи значні переваги у зручності, масштабованості та ефективності обробки даних. Однак із зростанням їхнього використання також збільшується ризик витоків та несанкціонованого доступу до даних.

Симетричне шифрування, як відомо, дозволяє проводити оперативне та ефективне шифрування, але його успішність значною мірою залежить від безпеки зберігання ключів. У той час як асиметричне шифрування робить можливим безпечний обмін ключами та забезпечує високий стандарт безпеки, особливо в контексті передачі даних через непротеїновані мережі, воно вимагає значних ресурсів для своєї реалізації.

В хмарних обчисленнях існують різноманітні загрози та вразливості, серед яких можна виокремити несанкціонований доступ, витоки даних, проблеми віртуалізації та недостатню надійність зберігання ключів.

Для забезпечення ефективного захисту даних у хмарних середовищах наразі важливо активно працювати над постійним вдосконаленням методів шифрування. Це включає в себе впровадження новітніх алгоритмів та технологій, а також постійне удосконалення управління ключами. Рекомендується використовувати сучасні криптографічні методи, які відповідають найсвіжішим стандартам безпеки. Крім того, важливо впроваджувати системи управління ключами, що дозволяють знижувати ризики, пов'язані зі зберіганням та розповсюдженням ключів. Доцільно також застосовувати методи багатофакторної аутентифікації для підвищення рівня захисту даних.

Загальні рекомендації з вдосконалення методів шифрування включають інтеграцію новітніх технологій, таких як квантова криптографія, та використання машинного навчання для виявлення аномалій та попередження атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alam T. Cloud Computing and its role in the Information Technology. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*. 2020. Vol. 1, no. 2. P. 108–115. URL: https://doi.org/10.34306/itsdi.v1i2.103

2. DRAFT – Evaluation of Cloud Computing Services Based on NIST 800-145. *National Institute of Standards and Technology (NIST)*. URL: https://www.nist.gov/system/files/documents/2017/05/31/evaluation_of_cloud_computing_services_based_on_nist_800-145_20170427clean.pdf#:~:text=NIST%20SP%20800-145%20provides,provisioned%20and%20released%20with%20minimal

3. What is Cloud Computing? *IBM* : веб-сайт. URL: https://developer.ibm.com/caas-storage/skillscollection/dna/live/explorer-cloud/en/_attachments/What-is-Cloud-Computing-1-.pdf

4. The NIST Definition of Cloud Computing. Special Publication 800-145. Recommendations of the National Institute of Standards and Technology. 2011. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

5. Four types of cloud computing service models you must know about. *LinkedIn*. URL: https://www.linkedin.com/pulse/four-types-cloud-computing-service-models-you-must-know-vaghela

6. The Basics of Cloud Computing. *CISA*. URL: https://www.cisa.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf

7. Okhyoa B., Uzoma B. A research on cloud computing. *Researchgate*. 2022. URL: http://dx.doi.org/10.13140/RG.2.2.22087.57762

8. B. Patel P. H., Kansara P. N. Cloud Computing Deployment Models: A Comparative Study. *International Journal of Innovative Research in Computer Science & Technology*. 2021. Vol. 9, no. 2. P. 45–50. URL: https://doi.org/10.21276/ijircst.2021.9.2.8

9. Cloud Computing: The Concept, Impacts and the Role of Government Policy. *OECD Digital Economy Papers*. 2014. no. 240. URL: https://www.oecd-

ilibrary.org/science-and-technology/cloud-computing-the-concept-impacts-and-the-role-of-government-policy_5jxzf4lcc7f5-en

10. The Role of Cloud Computing in the Development of Information Systems for SMEs / R. C. Carlos et al. *Journal of Cloud Computing*. 2017. P. 1–7. URL: https://doi.org/10.5171/2017.736545

11. Suryateja P. S. Threats and Vulnerabilities of Cloud Computing A Review. *International Journal of Computer Sciences and Engineering*. 2018. Vol. 6, no. 3. P. 297–302. URL: https://doi.org/10.26438/ijcse/v6i3.297302

12. Chou T.-S. Security Threats on Cloud Computing Vulnerabilities. *International Journal of Computer Science and Information Technology*. 2013. Vol. 5, no. 3. P. 79–88. URL: https://doi.org/10.5121/ijcsit.2013.5306

13. Bamiah M., Brohi S. Seven Deadly Threats and Vulnerabilities in Cloud Computing. *International journal of advanced engineering sciences and technologies*. Vol No. 9, Issue No. 1, P. 87-90. URL: https://expert.taylors.edu.my/file/rems/publication/107903_643_1.pdf

14. Son K. Cyber Security Threats & Vulnerabilities in Cloud Computing and Security Measurements. *Global Scientific Journals*. 2020, Vol. 8, Issue 9, P. 927-968. URL: https://www.globalscientificjournal.com/researchpaper/Cyber_security_threats_and_vulnerabilities_in_cloud_computing_and_security_measurements.pdf

15. Jang-Jaccard J., Nepal S., Guo Y. Cybersecurity threats in cloud computing. *Australian Journal of Telecommunications and the Digital Economy*. 2013, Vol. 1, No. 1. P. 4.1-4.17. URL: https://telsoc.org/sites/default/files/tja/pdf/ajtde_2013_1_1_04-jangjacquard_nepal_guo_0.pdf

16. Pericherla S. Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art. *The ISC Int'l Journal of Information Security*. 2023, Vol. 15, No. 1, P. 1–58. URL: https://www.isecure-journal.com/article_154670_e5e692199d1faab97eac08d75daae657.pdf

17. What is cloud encryption? *CrowdStrike* : веб-сайт. URL: https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-encryption/

18. Posey B. What are 3 encryption for cloud storage best practices? *TechTarget* : веб-сайт. URL: https://www.techtarget.com/searchstorage/answer/What-are-3-encryption-for-cloud-storage-best-practices

19. Naveed R., Abbas H. Security Requirements Specification Framework for Cloud Users. *Future Information Technology*. 2014, P. 297-305. URL: https://www.researchgate.net/publication/259221222_Security_Requirements_Specification_Framework_for_Cloud_Users

20. Geethu T., Prem J., Afsar P. Cloud computing security using encryption technique. URL: https://www.researchgate.net/profile/Prem-Vazhacharickal/publication/258201428_Cloud_computing_security_using_encryption_technique/links/5774de2808aead7ba06f8a84/Cloud-computing-security-using-encryption-technique.pdf

21. Shinde M., Taur R. Encryption Algorithm for Data Security and Privacy in Cloud Storage. *American Journal of Computer Science and Engineering Survey*. 2015, Vol. 3, No. 1, P. 34-39 URL: https://dl.icdst.org/pdfs/files2/5f863290ce0f6692e2620e8917c9eadf.pdf

22. Moore T., Conlon S., Hewarathna A., Dissanayaka T. Encryption Methods and Key Management Services for Secure Cloud Computing: A Review. *Midwest Instruction and Computing Symposium* : матеріали конференції. University of Northern Iowa, 2023. URL: https://www.researchgate.net/publication/369777264_Encryption_Methods_and_Key_Management_Services_for_Secure_Cloud_Computing_A_Review

23. Nandgaonkar A., Kulkarni P. Encryption Algorithm for Cloud Computing. *International Journal of Computer Science and Information Technologies*. Vol. 7(2), 2016, P. 983-989. URL: https://ijcsit.com/docs/Volume%207/vol7issue2/ijcsit20160702124.pdf

24. Alenezi M., Alabdulrazzaq H. Symmetric Encryption Algorithms: Review and Evaluation study. *International Journal of Communication Networks and Information Security*. 2020, Vol. 12(2). URL: https://www.researchgate.net/publication/349324592_Symmetric_Encryption_Algorithms_Review_and_Evaluation_study

25. Suo1 S., Xi1 W., Cai1 T., Jian G., Yao1 H., Li J.. Encryption Technology in Information System Security. *Advances in Computer Science Research*. 2019, Vol. 87. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiz_q_3_5iFAxX3X_EDHYKQCyI4ChAWegQIERAB&url=https%3A%2F%2Fwww.atlantis-press.com%2Farticle%2F55917219.pdf&usg=AOvVaw1ObiYIfcpm7CYDySi2TwAz&opi=89978449

26. Sadeeq J., Charu G., Tariq S. Data Encryption Standard. A Symmetric Cryptographic Algorithm. *Stockholms universitet*. 2006. URL: https://people.dsv.su.se/~tasa9018/data/DES.pdf

27. Symmetric key distribution using symmetric encryption *Prasad V. Potluri Siddhartha Institute of Technology*. URL: http://pvpsit.ac.in/dep_it/lecture%20notes/CNS/UNIT%203_CNS.pdf

28. Ayushi A. A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications*. Vol. 1, No. 15. URL: https://ijcaonline.org/volume1/number15/pxc387502.pdf

29. Pandey S., Farik M. Best Symmetric Key Encryption - A Review. *International journal of scientific & technology research*. 2017, Vol. 6, Is. 06. URL: https://www.academia.edu/33665649/Best_Symmetric_Key_Encryption_A_Review

30. Performance Evaluation of Symmetric Data Encryption Algorithms: AES and Blowfish / B. A. Buhari et al. *Saudi Journal of Engineering and Technology*. 2019. Vol. 04, no. 10. P. 407–414. URL: https://doi.org/10.36348/sjeat.2019.v04i10.002

31. AES Decrypt function. *IBM*. URL: https://www.ibm.com/docs/en/app-connect-pro/7.5.5?topic=reference-aes-decrypt-function

32. Shallal Q. Bokhari M. A Review on Symmetric Key Encryption Techniques in Cryptography. *International Journal of Computer Applications*, 2019. URL: https://www.researchgate.net/publication/333118027_A_Review_on_Symmetric_Key_Encryption_Techniques_in_Cryptography

33. Thorsteinson P. .Net Security and Cryptography. 2003. URL: https://ptgmedia.pearsoncmg.com/images/013100851X/samplechapter/013100851X_ch04.pdf

34. Diffie-Hellman key agreement. *IBM*. URL: https://www.ibm.com/docs/en/zos/2.4.0?topic=ssl-diffie-hellman-key-agreement

35. Kumar Y., Munjal R., Sharma H. Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures. *International Journal of Computer Science and Management Studies*. 2011, Vol. 11, Issue 03, P. 60-63. URL: https://www.researchgate.net/publication/267411519_Comparison_of_Symmetric_and_Asymmetric_Cryptography_with_Existing_Vulnerabilities_and_Countermeasures

36. Tripathi R., Agrawal S. Comparative Study of Symmetric and Asymmetric Cryptography Techniques. *International Journal of Advance Foundation and Research in Computer*. 2014, Volume 1, Issue 6, P. 68-76. URL: https://ijafrc.org/Volumn1/Vol_issue6/9.pdf

37. Uma K., Karthik G., Vishnu Prasath R. A comparative analysis of Symmetric and Asymmetric key cryptography. *Journal of Chemical and Pharmaceutical Sciences*. 2017. Volume 10 Issue 1, P. 324-326. URL: https://jchps.com/issues/Volume%2010_Issue%201/66-0701016.pdf

38. A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms. *International Journal of Innovative Research in Science, Engineering and Technology*. 2015, Vol. 4, Issue 3. P. 1028-1031. URL: https://www.ijirset.com/upload/2015/march/43_A_COMPARATIVE.pdf

39. Cyberattacks and Security of Cloud Computing: A Complete Guideline / M. Dawood et al. *Symmetry*. 2023. Vol. 15, no. 11. P. 1981. URL: https://doi.org/10.3390/sym15111981

40. NIST Special Publication 800-207. Zero Trust Architecture. *National Institute of Standards and Technology*. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

41. Understanding GDPR, HIPAA, PCI DSS, and CCPA: A Guide to Data Protection Laws. *TeckPath*. URL: https://teckpath.com/understanding-gdpr-hipaa-pci-dss-and-ccpa-a-guide-to-data-protection-laws/

42. Malhotra S., Singh W. An efficacy analysis of data encryption architecture for cloud platform. *Procedia Computer Science*. 2023. Vol. 218. P. 989–1002. URL: https://doi.org/10.1016/j.procs.2023.01.079

43. Asset Discovery: The First Step in Attack Surface Management. *LinkedIn*. URL: https://www.linkedin.com/pulse/asset-discovery-first-step-attack-surface-management-m9eec

44. Williamson J., Curran K. Best Practice in Multi-factor Authentication. *Semiconductor Science and Information Devices*. 2021. Vol. 3, no. 1. URL: https://doi.org/10.30564/ssid.v3i1.3152

45. An authentic Zero Trust guide. *ON2IT*. URL: https://isaca.nl/wp-content/uploads/Downloads/Square%20Tables/2021/2021%2010%2013%202021%20An%20Authentic%20Zero%20Trust%20Guide.pdf

46. Kebande V. R., Karie N. M., Ikuesan R. A. Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information Technology*. 2020. URL: https://doi.org/10.1007/s41870-020-00585-8

47. Timothy D., Santra A. A hybrid cryptography algorithm. *2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS).* URL: https://www.researchgate.net/publication/321894570_A_hybrid_cryptography_algorithm_for_cloud_computing_security

48. Stebila D., Mosca M., Lütkenhaus N. The Case for Quantum Key Distribution. *International Conference on Quantum Comunication and Quantum Networking*. URL: https://www.researchgate.net/publication/24013176_The_Case_for_Quantum_Key_Distribution