Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій .
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського .
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський) .

Дослідження методів забезпечення мережної безпеки в хмарній інфраструктурі
(тема)

Виконав:
студента 2 курсу, групи АМСЗІм-22-2 .
Пономаренко В.Ю. .
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека .
(код і повна назва спеціальності)
Тип програми: освітньо-професійна .
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент .
у сфері захисту інформації .
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського .
Коваленко Т.М.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В. .
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій .
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського .
(повна назва)
Рівень вищої освіти другий (магістерський) .
Спеціальність 125 Кібербезпека .
(код і повна назва)
Тип програми освітньо-професійна
.
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації .
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Пономаренко Володимир Юрійович .
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження методів забезпечення мережної безпеки в хмарній інфраструктурі .
затверджена наказом по університету від «03» листопада 2023р. №1291Ст.

2. Термін подання студентом роботи до екзаменаційної комісії 12.01.2024 р. .

3. Вихідні дані до роботи: провайдер хмарних послуг – Amazon Web Services (AWS), хмарна інфраструктура: Virtual Private Cloud (VPC), початкова IP-адреса – 192.168.0.0, загальнодоступна та приватна підмережа – 300 і 100 вузлів відповідно, інтернет-шлюз, веб-сервер, групи безпеки, ймовірність компрометації каналів – 0,2, 0,4, 0,6, 0,8, ймовірність компрометації сервера – від 0 до 1

4. Перелік питань, що потрібно опрацювати в роботі:
1) Огляд технологій побудови хмарної інфраструктури та забезпечення мережної безпеки
2) Огляд інструментів та сервісів AWS для створення інформаційної інфраструктури
3) Аналіз та вибір засобів забезпечення мережної безпеки інфраструктури AWS
4) Дослідження мережної безпеки та ймовірності компрометації мережі у

хмарній інфраструктурі AWS .

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації ..

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Коваленко Тетяна Миколаївна		15.01.2024

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	03.11.2023	Виконано
2	Збір матеріалів для дослідження	24.11.2023	Виконано
3	Розробка 1 розділу	08.12.2023	Виконано
4	Розробка 2 розділу	18.12.2023	Виконано
5	Розробка 3 розділу	29.12.2023	Виконано
6	Розробка 4 розділу	07.01.2024	Виконано
7	Оформлення кваліфікаційної роботи	12.01.2024	Виконано

Дата видачі завдання 03 листопада 2023 року

Студент _____ Пономаренко В.Ю.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Коваленко Т.М.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 92 с., 49 рис., 10 табл., 44 джерел.

КІБЕРБЕЗПЕКА, РИЗИК, ХМАРНА ІНФРАСТРУКТУРА, AMAZON WEB SERVICES, КОМПРОМЕТАЦІЯ, СХЕМА ШАМІРА

Об’єкт дослідження – процес забезпечення інформаційної безпеки хмарної інформаційної інфраструктури.

Предмет дослідження – ризики інформаційної безпеки у хмарній інфраструктурі, метод безпечного обміну конфіденційними повідомленнями за схемою Шаміра.

Мета кваліфікаційної роботи – визначити ризики мережної безпеки у хмарній інфраструктурі AWS, розгорнути інформаційну інфраструктури та дослідити ймовірність компрометації повідомлення.

Методи дослідження – емпіричний аналіз, формалізація та порівняння, методи теорії ймовірностей.

Хмарні інфраструктури мають багато переваг, але проблеми, які пов’язані з забезпеченням інформаційної безпеки, ще потребують вирішення. В роботі проведено огляд технологій та інструментів побудови хмарної інфраструктури AWS та забезпечення мережної безпеки. Проведений в роботі аналіз хмарних технологій різних провайдерів дозволив виявити їх основні переваги та недоліки, а також переваги та недоліки хмарних інструментів AWS. В роботі проведено аналіз та вибір засобів забезпечення мережної безпеки хмарної інфраструктури AWS, наведено переваги та недоліки хмарної інфраструктури с точки зору забезпечення мережної безпеки. Також в роботі виконано розгортання хмарної інфраструктури відповідно до заданих вимог, розроблено математичну модель для розрахунку ймовірності компрометації повідомлення, яке передається за схемою Шаміра та проведено розрахунок і аналіз ймовірності компрометації повідомлення у хмарі.

ABSTRACT

Explanatory note: 92 pages, 49 figures, 10 tables, 44 sources.

CYBER SECURITY, RISK, CLOUD INFRASTRUCTURE, AMAZON WEB SERVICES, COMPROMISE, SHAMIR SCHEME.

The object of study is the process of ensuring information security of the cloud information infrastructure.

The subjects of research are information security risks in the cloud infrastructure, the method of secure exchange of confidential messages according to the Shamir scheme.

The purpose of the qualification work are identify network security risks in the AWS cloud infrastructure, deploy information infrastructure and investigate the possibility of message compromise.

Research methods are empirical analysis, formalization and comparison, methods of probability theory.

Cloud infrastructures have many advantages, but the challenges that are associated with ensuring cyber security still need to be solved. The paper provides an overview of technologies and tools for building AWS cloud infrastructure and ensuring network security. The analysis of cloud technologies of various providers conducted in the work revealed their main advantages and disadvantages, as well as the advantages and disadvantages of AWS cloud tools. The paper analyzes and selects means of ensuring network security of the AWS cloud infrastructure, gives the advantages and disadvantages of the cloud infrastructure from the point of view of ensuring network security. In the work, the deployment of the cloud infrastructure was carried out in accordance with the specified requirements, a mathematical model was developed for calculating the probability of compromising a message transmitted according to the Shamir scheme, and the calculation and analysis of the probability of compromising a message in the cloud was carried out.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

IT – інформаційні технології
AMI – Amazon Machine Images
API – Application Programming Interface
AWS – Amazon Web Services
CDN – Content Delivery Network
DDoS – Distributed Denial-of-Service Attack
DevOps – Development and Operations
DNS – Domain Name System
EC2 – Elastic Compute Cloud
ELB – Elastic Load Balancing
HTTP – HyperText Transfer Protocol
IaaS – Infrastructure as a Service
IAM – Identity and Access Management
KMS – Key Management Service
MFA – Multi-Factor Authentication
NaaS – Network as a Service
NACL – Network Access Control Lists
NAT – Network Address Translation
PaaS – Platform as a Service
RDS – Amazon Relational Database Service
S3 – Simple Storage Service
SaaS – Software as a Service
SSH – Secure Shell
VPC – Virtual Private Cloud
VPN – Virtual Private Network
VSTS – Visual Studio Team Services

WAF – Web Application Firewall

IP – Internet Protocol

ВСТУП

У хмарних технологіях зацікавлені як великі компанії, які намагаються оптимізувати свої витрати на корпоративну IT-інфраструктуру, так і малі підприємства, які не мають можливості відразу розгорнути власну інфраструктуру. Зростаючий інтерес до технологій хмарних обчислень тісно пов'язаний з економічністю їх використання. Однак, незважаючи на очевидні переваги використання хмарних обчислень, все ще є деякі проблеми, які потребують вирішення. Основними питаннями є забезпечення неспростовності та достовірності інформації на кожному етапі її існування, цілісності, конфіденційності, захисту від несанкціонованого доступу, безперебійної роботи, авторизації та збереження персональних даних користувачів, що обробляються та передаються в хмарі. Таким чином роботу, яка присвячена дослідженню мережної безпеки в хмарній інфраструктурі, можна вважати актуальною.

Метою роботи є визначення ризиків мережної безпеки у хмарній інфраструктурі AWS, розгортання інформаційної інфраструктури та дослідження ймовірності компрометації повідомлень, які передаються у хмарі за схемою Шаміра.

Текст роботи складається з чотирьох розділів.

У першому розділі здійснюється огляд технологій побудови хмарної інфраструктури та забезпечення мережної безпеки. А саме розглянути основні принципи та переваги розгортання хмарної інфраструктури. Наведено перелік основних провайдерів хмарних послуг. Здійснено огляд та аналіз основних стандартів в області хмарних обчислень. Здійснено огляд моделей побудови хмарної інфраструктури та основних сервісів які надаються у хмарах. За результатами аналізу наведені переваги та недоліки хмарних технологій. Остання частина першого розділу присвячена огляду засобів забезпечення мережної безпеки у хмарній інфраструктурі.

Другий розділ роботи присвячений огляду інструментів та сервісів AWS для створення інформаційної інфраструктури. Розглянуті у другому розділі сервіси та інструменті дозволяють створити віртуальну хмару, забезпечити віддалений доступ до інформаційних та обчислювальних ресурсів, розгорнути сервіси по обробці, зберігання та обміну інформацією та моніторингу і керуванню хмарними ресурсами. У наступній частині другого розділу описана загальна процедура

розгортання хмарної інфраструктури у AWS-хмарі. Проведений аналіз хмарних технологій різних провайдерів дозволив виявити їх основні переваги та недоліки, а також переваги та недоліки хмарних інструментів AWS.

Третій розділ присвячено аналізу та вибору засобів забезпечення мережної безпеки хмарної інфраструктури AWS. Так на початку третього розділу розглянуто концепцію інформаційної безпеки AWS, проаналізовано розподіл відповідальності в області забезпечення інформаційної безпеки за різними рівнями відповідальності. Розглянуто особливості служб безпеки AWS. Проаналізовано основні характеристики та можливості інструментів та сервісів AWS щодо забезпечення мережної безпеки у хмарній інфраструктурі. Наприкінці розділу наведено переваги та недоліки хмарної інфраструктури с точки зору забезпечення мережної безпеки.

В останньому, четвертому розділі роботи проведено дослідження рівня мережної безпеки хмарної інфраструктури AWS. Ризики мережної безпеки для хмарної інфраструктури пов’язані із захистом мережевої інфраструктури та каналів зв’язку в хмарних середовищах. Спочатку за результатами аналізу бази інцидентів у AWS хмарі ми відокремили деякі з найбільш суттєвих ризиків безпеки хмарної мережі. Подальшому у розділі наведено обґрунтування структури хмарної інфраструктуру та підмереж, наведено опис процесу розгортання хмарної інфраструктури. Далі в розділі проведено синтез математичної моделі для розрахунку ймовірності компрометації повідомлення, яке передається за схемою Шаміра. Наприкінці розділу проведено дослідження розробленої математичної моделі.

1. ОГЛЯД ТЕХНОЛОГІЙ ПОБУДОВИ ХМАРНОЇ ІНФРАСТРУКТУРИ ТА ЗАБЕЗПЕЧЕННЯ МЕРЕЖНОЇ БЕЗПЕКИ

1.1.Загальний опис хмарних сервісів

Термін «хмара» в контексті інформаційних технологій відноситься до хмарних обчислень або хмарних сервісів. Це означає використання комп'ютерних ресурсів, таких як обчислювальна потужність, зберігання даних і програмне забезпечення, доступне в Інтернеті. Аналогом хмари можна вважати великий централізований простір, де можна отримати доступ до різноманітних послуг і ресурсів через Інтернет, так само як доступ з централізованих мереж до електроенергії чи води.

У хмарних обчисленнях користувачам не потрібно безпосередньо володіти або контролювати фізичний пристрій; натомість вони можуть використовувати ресурси за потреби та платити лише за їх фактичне використання.

Хмарний сервіс (або хмарові обчислення) – це модель надання послуг інформаційної технології, яка дозволяє доступати до обчислювальних ресурсів, таких як сервери, сховище даних, бази даних, мережі, програмне забезпечення та інші, через Інтернет. Замість того, щоб управляти та підтримувати великі фізичні інфраструктури на місці, користувачі можуть користуватися послугами, які надаються в хмарі, на засадах самообслуговування.

Хмарні сервіси дозволяють організаціям ефективно використовувати технологічні ресурси, зменшуючи витрати та покращуючи гнучкість та доступність. Існує безліч провайдерів хмарних сервісів, які надають різноманітні обчислювальні, сховища, мережні та інші хмарні послуги. Кожен провайдер має свої унікальні особливості та переваги. Нижче наведені деякі з провайдерів хмарних сервісів.

Amazon Web Services (AWS) є одним з найбільш розповсюджених хмарних провайдерів. Вони пропонують широкий спектр послуг, включаючи обчислювання, сховище, бази даних, штучний інтелект, машинне навчання та інші.

Microsoft Azure є іншим великим гравцем на ринку хмарних послуг. Вони надають послуги IaaS, PaaS, SaaS та різноманітні інструменти для розробки, тестування та розгортання додатків.

Google Cloud Platform (GCP) є сервісом від Google і пропонує рішення для обчислення, сховища даних, машинного навчання, аналітики та інших сфер.

IBM Cloud включає в себе різноманітні хмарні послуги, такі як обчислювання, блокчейн, штучний інтелект та інші, призначені для підтримки корпоративних та підприємницьких вимог.

Alibaba Cloud є провайдером хмарних послуг з азійським корінням і є великим гравцем на світовому ринку. Вони надають обчислювання, сховище, бази даних та інші послуги.

Oracle Cloud пропонує хмарні послуги для обчислювання, баз даних, блокчейну та інших сфер, спрямовані на підтримку великих підприємств.

DigitalOcean спеціалізується на простих та легких у використанні хмарних послугах, таких як віртуальні сервери (Droplets), сховище та інші.

VMware Cloud надає послуги хмарного обчислення, зокрема рішення для віртуалізації та управління інфраструктурою в хмарі.

HP Helion Cloud пропонує хмарні послуги для підприємств, включаючи обчислювання, сховище та інші рішення.

Це кілька прикладів провайдерів хмарних сервісів, і ринок постійно розвивається з появою нових гравців та розширенням можливостей існуючих. Користувачі можуть вибирати провайдера відповідно до своїх унікальних потреб та вимог.

1.2.Огляд стандартів в галузі хмарних технологій

Ефективне впровадження сучасних інформаційних технологій, таких як Cloud, IoT (Internet of Things), Web та інших, неможливе без відповідних нормативних документів, що описують правові стандарти, проблеми, ризики та шляхи їх мінімізації.

Для підвищення довіри до онлайн-діяльності та мінімізації наслідків кібератак необхідно розробити та впровадити міжнародні стандарти у сфері безпеки інформаційних технологій. У сучасному інформаційному просторі, де продукти, процеси та послуги розробляються та поширюються по всьому світу, приховуючи від споживачів функціональність хмарної інфраструктури провайдера, ці стандарти стають актуальними та особливо важливими. Зараз активно розробляються стандарти та рекомендації, призначені для хмарних обчислень [1].

Значна кількість стандартів, які сьогодні використовуються для хмарних обчислень, були розроблені для «хмарних» технологій, таких як веб-сервіси та платіжні системи. Оскільки споживачі та постачальники хмарних послуг часто знаходяться в різних країнах світу, міжнародні стандарти у сфері хмарних обчислень відіграють особливу роль. Щороку у відкритому доступі з'являються нові праці, присвячені огляду та поточному стану стандартів у сфері хмарних обчислень [1-7]. Відповідно до існуючої класифікації компаній і організацій стандартизації існує наступна ієрархія рівнів:

– міжнародний (ISO/IEC [8-11], ITU [12-21]);

– федеративний (форуми та консорціуми [3, 5]);

– регіональний (CEN/CENELEC Europe [4]);

– національний (державні закони та стандарти, міністерські нормативні документи, вказівки, інструкції тощо [2, 6]).

Коли справа доходить до стандартизації хмарних технологій, національні кордони стираються, оскільки більшість постачальників послуг знаходяться в різних країнах і на різних континентах. Через відсутність міжнародних стандартів сертифікації компонентів хмарної інфраструктури та їх відповідності інформаційній безпеці, компоненти (центри обробки даних, канали та мережі зв'язку тощо) використовують сертифікати стандарту безпеки згідно з міжнародними та іноземними стандартами в суміжних галузях. Міжнародні компанії, що займаються стандартами у сфері інформаційної безпеки [2] представлені на рис. 1.1. У кожній країні також є компанії та регіональні агентства, які займаються розробкою нормативних документів у сфері інформаційної безпеки. На рис. 1.2 представлена модель взаємодії регіональних та міжнародних асоціацій у сфері хмарних технологій [22].

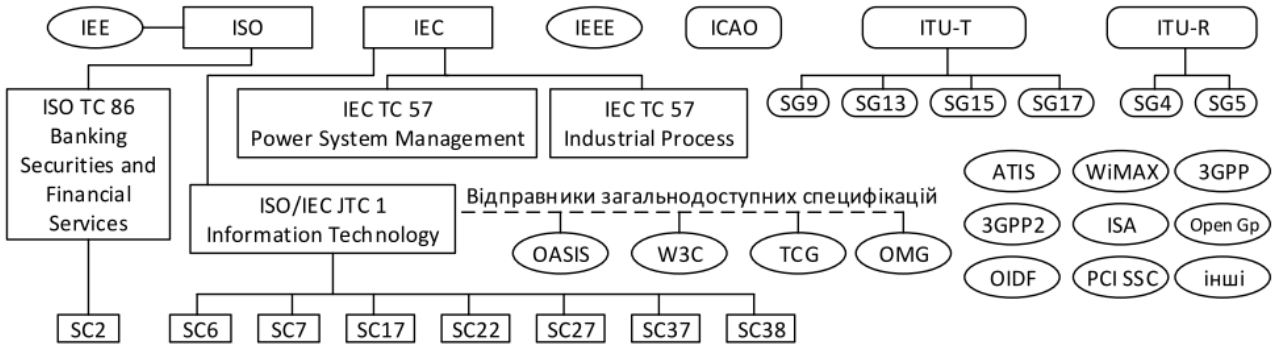


Рисунок 1.1 – Міжнародні корпорації, приймаючі участь в розробці міжнародних стандартів в галузі інформаційної безпеки хмарних технологій

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

– програмне забезпечення як послуга (Software as a Service (SaaS));

– платформа як послуга (Platform as a Service (PaaS));

– інфраструктура як послуга (Infrastructure as a Service (IaaS)).

Хмарні послуги мають позначення «X»aaS («послуга» as a service, «X» як сервіс). Спочатку хмарна парадигма включала три види послуг [23, 24]: IaaS, PaaS, SaaS.

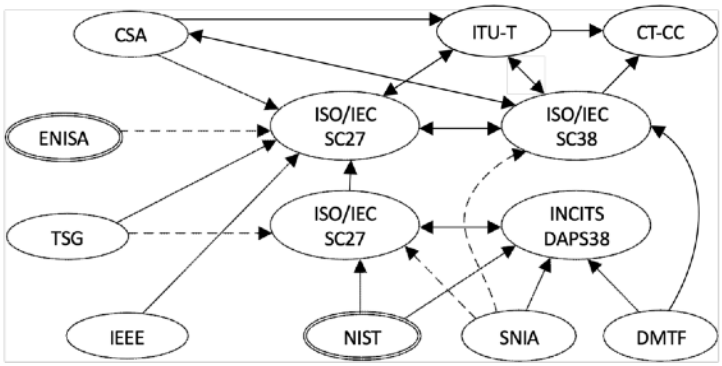


Рисунок 1.2 – Схема взаємодії між регіональними та міжнародними стандартоутворюючими корпораціями

Починаючи з 2013 року в стандартах почали вводитись назви нових видів хмарних послуг, а саме мережа як послуга (Network as a Service (NaaS)) – категорія хмарної послуги, в якій можливість, що надається споживачеві хмарної послуги, ставиться до можливостей транспортного сполучення та пов'язаним з ним мережевим можливостям [20].

З прийняттям у 2014 році міжнародного стандарту ISO17788 [8] регламентовано 7 репрезентативних категорій хмарних послуг:

– Communications as a Service (CaaS);

– Data Storage as a Service (DSaaS);

– Compute as a Service (CompaaS);

– Software as a Service (SaaS);

– Platform as a Service (PaaS);

– Infrastructure as a Service (IaaS);

– Network as a Service (NaaS).

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

– Security as a Service;

– Management as a Service;

– Identity as a Service;

– Email as a Service;

– Desktop as a Service;

– Database as a Service.

Перший нормативний документ регламентуючий поняття хмарних технологій [23] не містить інформації про надавачів послуг. Надалі фахівці NIST [25] визначили 2 типу надавачі послуг: Cloud consumer та Cloud provider.

В NIST SP 800–146 [24] – визначено Cloud consumer, Cloud provider, а також поняття Client, та акцентується увага на складність визначення ролей і відповідальності в хмарній моделі, зазначається «брокер».

Фахівці NIST в нормативних документах NIST SP 500–291[6], NIST SP 500–299 [26] визначили більш складну модель взаємодії, яка наведена на рис. 1.3, що включає:

– Cloud Consumer Person;

– Cloud Provider Person;

– Cloud Auditor;

– Cloud Broker;

– Cloud Carrier.

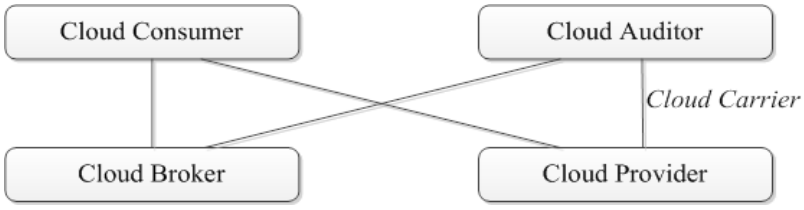


Рисунок 1.3 – Модель взаємодії учасників процесу представлення хмарних послуг згідно NIST SP 500–291:2011

Міжнародний стандарт ISO 17789 [9] вводить розширену класифікацію учасників хмарного ринку, наведена на рис. 1.4.

Рольова модель, прийнята в ISO 17788 [8] була врахована в керівництві ITU.T X1601 [15] в якому розглядаються такі визначення учасників:

– споживач хмарної послуги (cloud service customer) – це сторона (фізична особа або корпорація), яка знаходиться в ділових відносинах стосовно використання хмарних послуг;

– партнер хмарної послуги (cloud service partner) – це партнер, що бере участь в підтримці діяльності або постачальника хмарної послуги або споживача хмарної послуги або ж надає допомогу в цій діяльності;

– постачальник хмарної послуги (cloud service provider) – це сторона, яка надає хмарні послуги;

– користувач хмарної послуги (cloud service user) – це особа, пов'язана зі споживачем хмарної послуги, яке користується хмарними послугами;

– група внутрішніх користувачів (tenant) – це група користувачів хмарної послуги, спільно використовують доступ до набора фізичних і віртуальних ресурсів.

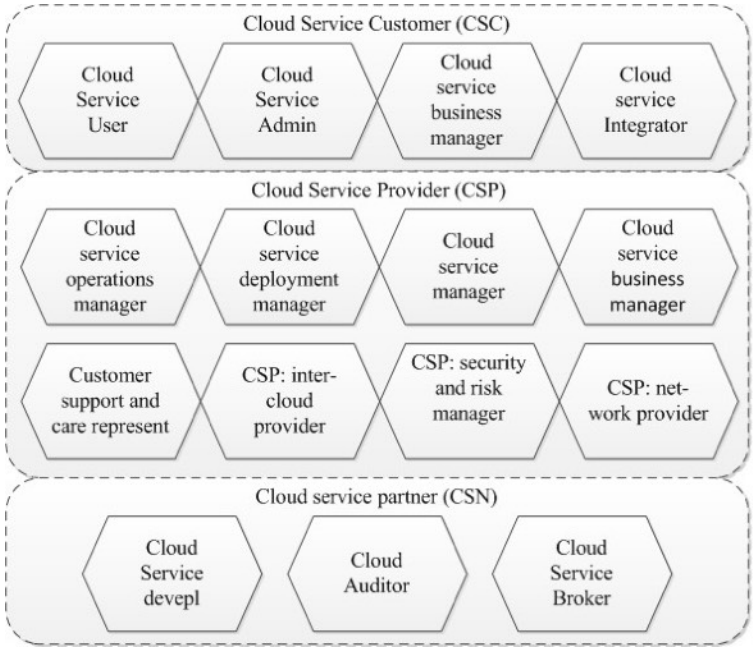


Рисунок 1.4 – Ролі учасників процесу представлення хмарних послуг згідно ISO 17789:2014

Останнім часом в стандартних визначеннях властивість «security» зазнає змін, поступово розширюється наповнення категорії «security». в останніх редакціях нормативних документів [8, 10] до трійки базових складових: конфіденційності, цілісності, доступності додають такі складові, як:

– автентичність;

– підзвітність;

– неможливість відмови від авторства;

– надійність.

Більш того, в стандарті [11] «security» визначається як стан захисту інформаційних активів, а конфіденційність, цілісність і доступність наводяться як окремий приклад цих активів.

У керівництві [21] дано визначення кібер–безпеки (cybersecurity), як набору інструментальних засобів, стратегії, принципів забезпечення безпеки, гарантій безпеки, керівних принципів, підходів до управління ризиками, дій, професійної підготовки, практичного досвіду, страхування і технологій, які можуть бути використані для захисту кібер–середовища, ресурсів корпорації і користувача.

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

1.3.Моделі розгортання хмарних технологій

Моделі розгортання хмарних технологій описують, де і як саме знаходяться обчислювальні ресурси, які використовуються у хмарі, як хмарні ресурси та послуги доступні та управляються. Ці моделі враховують рівень контролю та відповідальності за інфраструктуру та сервіси. Основні моделі розгортання хмарних технологій включають наступне:

– хмара загального користування (Public Cloud);

– хмара приватного користування (Private Cloud);

– хмара спільного користування (Community Cloud);

– гібридна хмара (Hybrid Cloud);

– мультіхмара (Multi-Cloud).

Кожна з цих моделей має свої переваги та виклики, і вибір конкретної моделі залежить від бізнес-потреб, вимог щодо безпеки, контролю, а також стратегії та інфраструктурних можливостей організації.

Приватна хмара – це модель хмарних обчислень, у якій ресурси хмарних обчислень використовуються виключно однією організацією.

У порівнянні з публічними хмарами, де ресурси доступні через Інтернет для загального користування, приватні хмари зазвичай знаходяться в середовищі, яке контролюється та керується організацією.

Важливою особливістю приватних хмар є те, що компанії самостійно налаштовують і обслуговують хмару. Створення внутрішньої хмари може бути складним і дуже дорогим, а вартість його підтримки може перевищувати вартість використання публічної хмари.

Зверніть увагу, що приватні хмари мають одну перевагу перед публічними хмарами. Це дає компаніям більше контролю над різними хмарними ресурсами, які вони пропонують, і параметрами конфігурації, доступними для них. Приватні хмари також ідеально підходять, коли вам потрібно виконати роботу, яку з міркувань безпеки не можна передати публічній хмарі.

Компанії можуть самостійно керувати приватними хмарами або делегувати це завдання зовнішньому постачальнику послуг.

Рішення приватної хмари можуть використовувати організації з високими вимогами до безпеки, які мають конфіденційні дані або відповідають суворим нормативним вимогам.

Однак створення власної інфраструктури та управління нею також може призвести до значних витрат.

Публічна хмара – це модель хмарних обчислень, у якій обчислювальні ресурси, такі як сервери, сховища даних і програмне забезпечення, надаються зовнішнім постачальником хмарних послуг і доступні для загального використання через Інтернет. Вони знаходяться поза межами корпоративної мережі. Користувачі цих хмар не мають можливості керувати цими хмарами чи підтримувати їх, усю відповідальність несе власник цієї хмари.

Публічними хмарними постачальниками є AWS, Microsoft Azure, GCP та інші. Постачальник хмарних послуг відповідає за встановлення, керування, надання та підтримку програмного забезпечення, інфраструктури додатків або фізичної інфраструктури. Клієнти платять лише за час використання ресурсу.

Абонентом послуг, що надаються, може стати будь-яка компанія та окремий користувач. Вони забезпечують простий і доступний спосіб розгортання веб-сайтів або бізнес-систем із великою масштабованістю, якої немає в інших рішеннях.

Водночас публічні хмарні сервіси пропонуються переважно в стандартних конфігураціях, тобто на основі умов найпоширеніших випадків використання. Це означає, що користувачі мають менше варіантів вибору конфігурацій порівняно з системами, де користувачі керують ресурсами. Важливо також зазначити, що споживачі мають слабкий контроль над інфраструктурою, процеси вимагають

суворих заходів безпеки, а відповідність нормативним вимогам не завжди підходить для розгортання в загальнодоступній хмарі.

Ця модель хмарних обчислень популярна серед організацій і користувачів, яким потрібна гнучкість і можливість використовувати ресурси за потреби.

Хмара спільного користування (Community Cloud) – це концепція хмарних обчислень, в якій обчислювальні ресурси використовуються спільно кількома організаціями для обміну інформацією та взаємодії між користувачами в реальному часі, незалежно від їх географічного розташування. Ця модель може бути побудована для обслуговування певної галузі або спільноти користувачів з подібними потребами та вимогами. Ця концепція підтримується різними хмарними сервісами та додатками, які полегшують комунікацію, співпрацю та обмін інформацією між користувачами та організаціями.

Хмара спільного користування спрощує комунікацію та співпрацю в сучасному бізнес-середовищі, забезпечуючи гнучкість, мобільність та ефективність у вирішенні завдань.

На відміну від загальних публічних хмарних послуг, які надаються великими хмаровими постачальниками, спільнотні хмари частіше надаються спеціалізованими компаніями або організаціями, які спеціалізуються на обслуговуванні конкретних груп або галузей.

При виборі та впровадженні хмарних рішень для спільного користування, важливо враховувати конкретні потреби та обмеження організації, а також ретельно оцінювати переваги та недоліки.

Гібридна хмара – це модель хмарного обчислення, яка поєднує в собі елементи приватної та публічної хмари. В гібридній хмарі певні обчислювальні ресурси перебувають в приватному хмарному середовищі, тоді як інші ресурси розміщені в публічному хмарному середовищі. Обидва середовища пов'язані мережею, що дозволяє передавати дані та додатки між ними. Зазвичай гібрідні хмари розгортаються організацією, і сфера відповідальності за управління хмарою розділяється між компанією та провайдером публічної хмари. Гібридні хмари надають сервіси, деякі приватні, а деякі публічні. Цей вид хмари застосовується у випадку, коли бізнес-процеси мають періоди сезонної діяльності. Таким чином, як тільки власна IT-інфраструктура не спроможна подужати з проточними задачами, частка потужності буде передана в публічну хмару, а також дозволяє користувачам отримувати доступ до ресурсів компанії (до приватної хмари) через публічну хмару. Гібридна хмара є ефективним рішенням для організацій, які мають різні

потреби щодо безпеки, ефективності та гнучкості у використанні обчислювальних ресурсів.

Мультіхмара (Multi-Cloud) – це стратегія в галузі хмарного обчислення, яка передбачає використання послуг та ресурсів більше ніж одного хмарного постачальника. У мультіхмарі організації можуть використовувати послуги різних хмарних платформ, таких як AWS, Azure, Google Cloud, або інших, для різних аспектів своєї інфраструктури та застосунків.

Для цього типу хмар властиво:

– гнучкість і неоднорідність, це можливість використовувати різні хмарні середовища для різних завдань з урахуванням їх конкретних потреб;

– зменшений ризик і надійність у разі проблем із постачальником або його недоступності інші хмарні ресурси можна використовувати для забезпечення безперервності бізнесу;

– оптимізація витрат дозволяє здійснити вибір найбільш ефективних і рентабельних хмарних ресурсів для конкретних завдань або різних частин бізнесу може допомогти оптимізувати витрати;

– співпраця та інновації – використання ресурсів від різних постачальників може стимулювати інновації та співпрацю, оскільки організація може взаємодіяти з різними службами та технологічними групами;

– відсутність прив’язки до постачальника дозволяє використовувати різних хмарних постачальників може зменшити залежність від конкретного постачальника та надати користувачам більше контролю;

– найкращий вибір для конкретних завдань: деякі хмарні постачальники можуть краще підходити для конкретних завдань, наприклад один для хостингу, інший для обчислень тощо.

Хоча багатохмарна стратегія може запропонувати такі переваги, як гнучкість і зниження ризику, вона також може вимагати більшого управління та координації для забезпечення ефективності та безпеки.

Мультіхмара є стратегією, яка дозволяє організаціям використовувати найкращі аспекти різних хмарних постачальників для оптимізації своєї інфраструктури та застосунків. Однак вона також вимагає уважного планування та управління для ефективного використання ресурсів.

1.4.Огляд основних хмарних сервісів

Хмарні сервіси охоплюють широкий спектр послуг та ресурсів, які можуть бути доступні через Інтернет та використовуватися на основі платіж за споживання. Хмарні служби класифікуються на кілька основних класів на основі наданих послуг. Нижче наведені основні категорії та приклади хмарних сервісів.

Інфраструктура як послуга (IaaS) є однією з основних моделей хмарних обчислень і представляє собою надання обчислювальних ресурсів через Інтернет. У цій моделі користувачам надається віртуальна інфраструктура, яку вони можуть використовувати для розгортання, управління та масштабування своїх додатків без необхідності інвестувати в власне обладнання та управління ним.

Однією з основних переваг IaaS є те, що вона дозволяє користувачам отримати доступ до інфраструктури без необхідності інвестувати в власне обладнання та його обслуговування. Це робить IaaS ефективним варіантом для підприємств та організацій, які шукають гнучкість та економію витрат при розгортанні та управлінні своєю інфраструктурою. Також, користувачі можуть швидко реагувати на зміни обсягів роботи та масштабувати ресурси згідно з потребами своєї організації.

Платформа як послуга (PaaS) є моделю хмарних обчислень, яка надає користувачам готове середовище для розробки, тестування та розгортання додатків без необхідності управління або конфігурацією базової інфраструктури. Користувачі можуть зосередитися на розробці програмного забезпечення, тому що багато питань щодо інфраструктури від них приховані.

Приклади PaaS-платформ включають Heroku, Google App Engine, Microsoft Azure App Service та інші. Використання PaaS може спростити розробку та управління додатками, зменшуючи завдання з інфраструктурного рівня, що дозволяє розробникам більше уваги приділяти функціональності своїх додатків.

Програмне забезпечення як послуга (SaaS) – це модель хмарних обчислень, яка надає користувачам доступ до готових до використання програм через Інтернет. У цій моделі користувачі не обов'язково управляють інфраструктурою або платформою, але можуть використовувати програмне забезпечення, доступне на хмарній платформі.

Приклади SaaS-застосунків включають Google Workspace (раніше G Suite), Microsoft 365, Salesforce, Dropbox, Slack та інші. Використання SaaS дозволяє користувачам швидко та ефективно отримувати доступ до функціональності програм без необхідності великого таємничого розгортання або управління інфраструктурою.

Хмарні системи зберігання даних є важливою частиною хмарних послуг і дозволяють користувачам зберігати, резервувати та отримувати доступ до своїх даних через Інтернет. Ці послуги надають різні можливості для сховища даних, резервного копіювання та спільного використання.

Прикладами хмарних систем зберігання є: Amazon Simple Storage Service (S3), Google Cloud Storage, Microsoft Azure Blob Storage, Dropbox, Box, Apple iCloud, pCloud. Кожен з цих сервісів має свої унікальні особливості, і користувачі можуть обирати той, який відповідає їхнім потребам та вимогам.

Хмарні служби обробки даних надають можливості для аналізу та обробки великих обсягів даних в хмарному середовищі. Ці послуги полегшують обробку та аналіз даних у хмарі, як правило, з використанням спеціалізованого програмного забезпечення та інфраструктури та дозволяють користувачам використовувати потужні обчислювальні ресурси, щоб виконати різноманітні операції обробки даних та аналізу.

Прикладами хмарних служб обробки даних є: Amazon EMR (Elastic MapReduce), Google Cloud Dataprep, Microsoft Azure Data Factory, Databricks, IBM Cloud Pak for Data, Snowflake, Apache Flink on AWS (Amazon Kinesis Data Analytics). Ці сервіси допомагають організаціям ефективно використовувати хмарні ресурси для аналізу та обробки великих обсягів даних без необхідності великих інвестицій у власну інфраструктуру.

Хмарні послуги для розробників та DevOps (Development and Operations) надають інструменти та ресурси для ефективної розробки, тестування та розгортання програмного забезпечення. Ці послуги спрощують роботу команд розробників і операторів, забезпечуючи швидку і гнучку інфраструктуру.

Прикладами хмарних послуг для розробників та DevOps є: Amazon Elastic Beanstalk, AWS CodePipeline, Google Cloud Build, Azure DevOps (раніше відомий як Visual Studio Team Services - VSTS), Travis CI, Docker Cloud, Heroku. Ці послуги допомагають розробникам та DevOps-командам автоматизувати різні етапи розробки та розгортання, що сприяє підвищенню продуктивності та ефективності розробочих процесів.

1.5. Аналіз стандартів інформаційної безпеки в хмарних мережах

Сьогодні основними організаціями, відповідальними за хмарну безпеку, є Cloud Security Alliance (CSA), до якого входять представники IT-індустрії, а також

дві державні організації в Європі та США: European Cyber and Information Security Agency (ENISA) і Національний інститут стандартів і технологій (NIST).

Кожна організація створила документ, який відповідає класифікації всіх існуючих проблем інформаційної безпеки у хмарі. Давайте розглянемо їх і порівняємо.

CSA – це некомерційна організація, заснована наприкінці 2008 року організаціями, заснованими великими IT-компаніями, зацікавленими у впровадженні хмарних технологій: Google, Microsoft, IBM, Salesforce.com, VMware та іншими організаціями.

Основним документом, який розглядає питання безпеки хмари, є «Посібник із критичних областей безпеки для хмарних обчислень». Його перша версія була опублікована в 2009 році. Ми розглянули останню і третю редакцію цього документа, яка доступна на офіційному веб-сайті організації.

Ця пропозиція, окрім питань, пов'язаних з інформаційною безпекою, розглядається хмарна архітектура та надаються рекомендації та рішення цих проблем. Загалом запитання щодо хмарної безпеки поділяються на дві великі групи: питання про керування безпекою у хмарі (питання організації) і безпека використання хмари (технічні питання). Кожна група ділиться на менші групи, які називаються доменами. Домени, пов'язані з організаційною сферою, в основному розглядаються з метою розробки рішень юридичних питань, питань політики інформаційної безпеки, управління ризиками та стандартизації. У рамках технічних питань будуть враховані питання щодо впровадження та розгортання хмарного захисту.

Європейське агентство з кібер- та інформаційної безпеки (ENISA) – це організація, яка працює над «підвищенням потенціалу Європейського Союзу, держав-членів ЄС і бізнес-спільноти для запобігання, усунення та реагування на проблеми мережевої та інформаційної безпеки» [27]

Організація ENISA підготувала та опублікувала документ «Безпека хмарних обчислень та оцінка ризиків» [28], в якому розглядаються проблеми інформаційної безпеки в хмарі, їх переваги та недоліки, існуючі ризики, аналіз та шляхи їх пом'якшення, існуючі загрози в було розглянуто середовище хмарних обчислень

Для впровадження хмарних обчислень уряд США доручив NIST розробити стандарт безпеки та конфіденційності в публічних хмарах. Тому, починаючи з 2011 року, NIST опублікував кілька документів, які визначають хмарні обчислення, розглядають проблеми хмарної інформаційної безпеки, пропонують

архітектури хмарної безпеки та надають рекомендації щодо оцінки та усунення існуючих ризиків інформаційної безпеки у хмарі.

Підхід до проблем безпеки у хмарі обговорюється в таких документах NIST: «Посібник з безпеки та конфіденційності в публічних хмарних обчисленнях» [25] і «Огляд і принципи хмарних обчислень» [24]. На відміну від розглянутих підходів від CSA та ENISA, у підході NIST проблеми безпеки чітко не розділені на такі рівні, як організаційні питання, юридичні питання та технічні питання.

Проведемо порівняння підходів та сутностей класифікацій інформаційної безпеки організацій NIST, ENISA, CSA за трьома широкими групами компонентів безпеки у хмарі: юридичні, організаційні та технічні проблеми. На основі розглянутої класифікації питання безпеки, які віднесені до кожної групи, наведені в таблиці 1.1, 1.2 та 1.3. [29] Якщо питання ІБ було розглянуто в класифікації повністю, воно відмічено як «+», якщо частково – «+/-», в разі відсутності – «-».

Таблиця 1.1 – Порівняння юридичних складових інформаційної безпеки

№	Юридичні питання	Підхід		
		CSA	ENISA	NIST
1	Відповідність міжнародним і національним стандартам, законам і нормативним актам	+	+	+
2	Угоди між постачальником і клієнтом	+	+	+
3	Право власності на електронні дані	+	+	+
4	Невідповідності в законах про електронні дані між країнами	+	+	+
5	Захист авторських прав (DRM)	+	-	-
6	Дотримання національних законів і нормативних актів щодо хмарних даних	+	+	+
7	Зміна провайдера сервісів, або його придбаний іншим провайдером, постачальником	+	+	+

Аналіз даних таблиць показує, що в основному складові інформаційної безпеки збігаються в усіх класифікаціях. Найбільш повна та структурована класифікація була надана організацією CSA, але її недоліком є об’єднання правових та організаційних проблем інформаційної безпеки. Головною перевагою

класифікації ENISA є оцінка ймовірності виникнення ризиків, пов’язаних з інформаційної безпеки, причинами їх виникнення, взаємозв’язки з іншими ризиками, та їх вплив на систему та її елементи. До недоліків класифікації NIST можна віднести відсутність поділу проблем інформаційної безпеки на три основних групи, як це було зроблено в класифікації ENISA.

Таблиця 1.2 – Порівняння організаційних мір інформаційної безпеки

№	Організаційні питання інформаційної безпеки	Підхід		
		CSA	ENISA	NIST
1	Управління ризиками (бізнес, підприємство, інформація, постачальники послуг)	+	+	+
2	Управління безпекою інформації користувачів	+	+	+
3	Довіра до постачальників послуг (аудити, перевірки, оновлення безпеки, професійна підтримка)	+	+	+
4	Захист від інсайдерів	+	+	+
5	Реагування на випадки інформаційної безпеки, моніторинг, вирішення	+	+	+
6	Захист особистих даних користувачів	-	-	+
7	Керування авторським правом	+	+	+
8	Збої хмарних служб через стихійні лиха або несправності сторонніх підтримуваних хмарних служб	+	+	+

Таблиця 1.3 – Порівняння технічних мір інформаційної безпеки

№	Технічні питання інформаційної безпеки		Підхід		
			CSA	ENISA	NIST
1	2		3	4	5
1	Доступність ресурсів та даних	Вимкнення хмарних послуг	+	+	+
		Атаки DDoS-атаки	-	+	+
		Розміщення даних	+	+	+
		Вистеження ресурсів	+	+	-
2	Переносимість забезпечення	Сполучність забезпечення	+	+	+
		Уніфікований інтерфейс	+	-	-
3	Безпеки програм та додатків	Безпечність програмного забезпечення	+	+	+
		Розмежування доступу	+	+	+
		Моніторинг активності додатків	+	+	+
		Детектування небезпечних програм	+	+	+
		Захист від модифікації образів ВМ	+	-	+
4	Захист та управління даними	Ізоляція даних	+	+	+
		Безпечне зберігання даних	+	+	+
		Шифрування даних	+	+	+
		Керування ключами	+	+	+

Продовження таблиці 1.3

1	2		3	4	5
5	Ідентифікація, автентифікація та керування доступом	Моделі ідентифікації та автентифікації	+	-	-
		Управління профілями у хмарі	+	+	+
		Сервіси автентифікації, ідентифікації, доступу до ресурсів в хмарі	+	+	+
		Реалізація ідентифікації користувачів	+	+/-	+
		Доступ до даних авторизованих користувачів	+	+	+
6	Віртуалізація	Забезпечення захисту гостьової віртуальної машини від атак	+	-	+
		Захист від неправомірних операцій адміністратора	+	+	+
		Швидкодія, збільшення числа вузлів, пікове навантаження	+	+	+
		Безпека даних рівня віртуальної машини	+	-	+

1.6.Огляд засобів забезпечення мережної безпеки у хмарній інфраструктурі

Забезпечення мережевої безпеки у хмарі вимагає комплексного підходу, оскільки дані та ресурси можуть бути розподілені у віртуальних інфраструктурах.

У хмарних мережах використовуються ті самі базові моделі та протоколи, що й у локальних мережах, тому безпека певною мірою збігається. Брандмауери відіграють важливу роль у хмарі, а також у локальних мережах. Але традиційні рішення та процеси кібербезпеки здатні захистити хмарні мережі.

Незважаючи на певну схожість між хмарою та локальними мережами, між ними є значні відмінності. Так, під час розгортання хмарних програм ми маємо справу зі складними внутрішніми мережами та додатковими компонентами керування мережею. До них можуть входити, серед іншого, сервісні мережі та контролери доступу, яких ви не знайдете в більшості локальних середовищ. У

результаті потрібні додаткові можливості, інструменти та стратегії, які можуть бути недоступні для традиційних локальних операцій робочого навантаження.

Щоб зрозуміти, що таке хмарна безпека, спочатку потрібно зрозуміти, що таке хмарна безпека взагалі. Сьогодні популярною моделлю для розуміння значення хмарної безпеки є концепція Cloud Native Application Protection Platform (CNAPP), розроблена Gartner. Платформа CNAPP розроблена для захисту хмарних програм, тобто програм, що працюють у хмарному середовищ.

Оскільки хмарні програми часто містять складну мережеву архітектуру, CNAPP має захищати багато аспектів мережевої функціональності, від брандмауерів наступного покоління та балансувальників навантаження до веб-програм та API. Крім того, вони повинні забезпечити детальну сегментацію та захист трафіку.

Оскільки кожне розгортання хмари підключається до мережі за межами хмари та використовує цю мережу для передачі даних між різними ресурсами в хмарі, безпечна мережа забезпечує основу для решти стратегії безпеки хмари. Також можна використовувати гібридне хмарне середовище, яке поєднує приватні хмари або локальні ресурси з публічними хмарними службами.

Незалежно від хмарної архітектури, усі типи хмарних середовищ (одна хмара, мультіхмарні та гібридні) залежать від мережі, яка з’єднує інфраструктуру. Тому всі вони піддаються серйозному ризику в разі порушення кібербезпеки хмари. І впровадження правильного рішення має вирішальне значення.

Також важливо зазначити, що моделі розподілу відповідальності не звільняють бізнес від необхідності забезпечувати хмарну кібербезпеку. Нагадаю, що моделі спільної відповідальності – це угоди, укладені між провайдерами хмарних обчислень та їхніми клієнтами, згідно з якими провайдер відповідає за захист певних компонентів свого хмарного середовища, а клієнти – за іншими.

З точки зору кібербезпеки моделі спільної відповідальності вимагають від хмарних провайдерів захисту фізичної мережевої інфраструктури, такої як комутатори та маршрутизатори, які забезпечують підключення до інфраструктури. Однак відповідальність за забезпечення безпеки віртуальних мереж, налаштованих клієнтом, а також трафіку, що входить і виходить із хмарного середовища через ці віртуальні мережі, лежить на клієнті.

Певним чином безпека хмарної мережі схожа на безпеку звичайної мережі. Це передбачає обмеження доступу до хмарних ресурсів за допомогою

брандмауерів, закриття вразливих портів, виявлення та блокування підозрілого мережевого трафіку тощо.

Однак в інших аспектах безпека хмарної мережі пов’язана з деякими унікальними проблемами.

Перша з них – це складність хмарних мереж. Хмарні мережі часто складніші за локальні. Вони можуть включати різноманітні підмережі, віртуальні приватні хмари (наприклад, Amazon VPC), накладені мережі та навіть з’єднуватися між кількома хмарами. Тому визначити та усунути ризики безпеці стає ще складніше.

Наступною проблемою можна вважати меншу прозорість. У хмарі підприємства не мають прямого доступу до фізичної мережевої інфраструктури, що означає меншу прозорість щодо того, що відбувається в їхній мережі.

Динамічний характер хмарних ресурсів також створює складності з точки зору інформаційної безпеки. Локальні ресурси, як правило, більш фіксовані та статичні, тоді як хмарні активи більш динамічні. Наприклад, у хмарі IP-адреси можуть швидко змінюватися, а активи можуть швидко збільшуватися або зменшуватися. Динамічний характер хмари може ускладнити запобігання ризикам безпеки.

Проблемою також є відсутність чіткого периметра мережі. Зазвичай, можна використовувати брандмауер, щоб відокремити всю локальну мережу від Інтернету, але не можливо це зробити у хмарі. Це означає, що хмарна мережа має менший периметр. Рішення постачальників можна використовувати для створення ізоляції між хмарними ресурсами та Інтернетом, але в кінцевому підсумку ці ресурси все ще можуть піддаватися загрозам на рівні мережі. З цих причин безпека хмарної мережі вимагає іншого підходу, ніж традиційний. Ви не можете перемістити інструменти та процеси з локальної мережі в хмару. Натомість вам слід розгорнути рішення безпеки, спеціально розроблені для хмарних середовищ.

Ефективний захист хмарної мережі включає три аспекти:

– комплексність – це необхідно мати можливість зупинити загрози в будь-якій публічній або приватній хмарній мережі, а також у будь-якому іншому компоненті IT-системи за допомогою єдиного рішення;

– консолідованість – це набір засобів безпеки має бути консолідованим і забезпечувати уніфіковане управління безпекою та операції;

– спільна робота – це використання аналізу загроз та інтеграція із зовнішніми інструментами дозволить спільним командам виявляти та запобігати хмарним ризикам безпеки.

Окрім впровадження правильних інструментів безпеки, дотримання найкращих практик може ще більше підвищити безпеку хмарної мережі. До них відноситься Zero Trust. Ця модель безпеки передбачає заборону взаємодії між ресурсами, підключеними до хмарної мережі, та іншими ресурсами, доки вони не пройдуть перевірку та не будуть визнані безпечними.

Обмеження хмарних об’єктів мінімально необхідними привілеями дає змогу зменшити ризик і виявлення порушень безпеки, пов’язаних із незахищеними налаштуваннями доступу. Підхід із найменшими привілеями також вносить контекст у безпеку мережі, допомагаючи адміністраторам визначити роль кожного користувача. Підсумуємо основні засоби та служби забезпечення мережевої безпеки, які можуть бути використані у хмарному середовищі у таблиці 1.4.

Таблиця 1.4 – Основні засоби та служби мережевої безпеки у хмарі

Засоби та служби	Опис	Приклади
1	2	3
1. Віртуальні приватні мережі	Віртуальні приватні мережі дозволяють створювати зашифровані тунелі між користувачами та хмарним сервісом, щоб забезпечити безпечний обмін даними через відкриті мережі.	AWS VPN, Azure VPN Gateway.
2. Брандмауери у хмарі.	Брандмауери у хмарному середовищі використовуються для фільтрації трафіку та захисту хмарних ресурсів від небезпек та атак.	AWS Network Firewall, Azure Firewall.

3. Системи виявлення та запобігання вторгнень	Системи виявлення та запобігання вторгнень аналізують мережевий трафік для виявлення та блокування потенційно шкідливих активностей.	AWS GuardDuty, Azure Security Center.
4. Антивірусні та антималваре служби	Захищають віртуальні машини та хмарні ресурси від вірусів та шкідливого програмного забезпечення.	AWS Shield, Microsoft Defender Antivirus.
5. Керування ідентифікацією та доступом (IAM)	IAM визначає та керує правами доступу користувачів та служб до хмарних ресурсів.	AWS Identity and Access Management, Azure Active Directory.

Продовження таблиці 1.4

1	2	3
6. Шифрування даних.	Забезпечує захист конфіденційності даних шляхом шифрування інформації відповідно до стандартів безпеки.	AWS Key Management Service (KMS), Azure Storage Service Encryption.
7. Системи моніторингу та аудиту.	Забезпечують моніторинг заходів безпеки та ведення аудиту подій для виявлення потенційних загроз.	AWS CloudWatch, Azure Monitor.
8. Веб-захист.	Захищає від атак на веб-додатки та забезпечує безпеку трафіку HTTP/HTTPS.	AWS WAF, Azure Application Gateway Web Application Firewall.
9. Мережева ізоляція та сегментація.	Забезпечує віртуальне розділення мережевих ресурсів для ускладнення руху в мережі.	AWS VPC, Azure Virtual Network.
10. Тестування на проникнення та аудит безпеки.	Проведення тестування на проникнення та аудит безпеки для виявлення та усунення слабких місць у конфігурації та налаштуванні.	AWS Inspector, AWS CloudTrail

Важливо вибирати та налаштовувати засоби забезпечення мережевої безпеки у хмарі відповідно до конкретних потреб та вимог організації, забезпечуючи надійний та безпечний хмарний середовища.

2. ОГЛЯД ІНСТРУМЕНТІВ ТА СЕРВІСІВ AWS ДЛЯ СТВОРЕННЯ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

2.1.Інструменти та сервіси для створення інформаційної інфраструктури

AWS надає широкий спектр інструментів та сервісів для створення інформаційної інфраструктури. В таблиці 2.1 наведено перелік ключових сервісів, які можна використовувати для різних аспектів інформаційної інфраструктури [30].

Таблиця 2.1 – Перелік ключових сервісів AWS для створення інформаційної інфраструктури

Сервіс	Опис
1	2
Amazon Virtual Private Cloud (VPC)	дозволяє вам створювати ізольовані мережі в AWS. Ви можете керувати IP-адресами, створювати підмережі та налаштовувати маршрутизацію та доступ.
Amazon Elastic Compute Cloud (EC2)	надає масштабовані віртуальні сервери в хмарному середовищі. Ви можете швидко розгортати та масштабувати віртуальні машини з різними характеристиками ресурсів.
Amazon Identity and Access Management (IAM)	ресурс керування доступом для користувачів, груп і ролей AWS, що дозволяє встановлювати рівні доступу для різних ресурсів і служб AWS, забезпечуючи при цьому обмеження безпеки та конфіденційності.
Amazon Simple Storage Service (S3)	об'єктне сховище для зберігання та отримання будь-якого об'єму даних. Використовується для зберігання файлів, даних з резервного копіювання та обробки мультимедійних контентів.
Amazon Relational Database Service (RDS)	дозволяє легко створювати, налаштовувати та масштабувати реляційні бази даних, такі як MySQL, PostgreSQL, Oracle і інші, без необхідності управління апаратним забезпеченням.
Amazon DynamoDB	повністю керований сервіс бази даних NoSQL, що забезпечує швиду, масштабовану роботу з ключами і значеннями.

AWS Lambda	сервіс для виконання коду безпосередньо відразу після події. Ви можете використовувати Lambda для автоматизації завдань, обробки подій та інтеграції з іншими сервісами.

Продовження таблиці 2.1

1	2
Amazon Elastic Block Store (EBS)	блочне сховище, яке можна прикріпити до EC2 для забезпечення тимчасового або постійного сховища.
Amazon CloudFront	служба доставки контенту (CDN), яка швидко і надійно доставляє веб-контент користувачам, використовуючи мережу кешуючих серверів для доставки контенту по всьому світу.
Amazon Route 53	масштабований сервіс DNS, який дозволяє реєструвати та управляти доменними іменами, а також керувати маршрутизацією трафіку.

AWS також надає багато послуг, таких як обчислення, зберігання, база даних, аналітика, штучний інтелект, мережеві служби, безпека та захист, такі як шифрування, засоби контролю доступу та моніторинг. AWS також пропонує багато інструментів розробки та розгортання програм. Різноманітність готових до використання інструментів, служб і шаблонів для прискорення розробки та розгортання програм. Вони дозволяють створювати та розгортати різні додатки та служби відповідно до ваших потреб, а також прискорюють весь процес розробки за допомогою готових до використання рішень та інструментів автоматизації.

2.2.Огляд основних сервісів інфраструктури AWS

2.2.1. Сервіс Amazon Elastic Compute Cloud.

Amazon Elastic Compute Cloud – це основна обчислювальна служба, що надається компанією Amazon, яка пропонує масштабовані та змінні розміри віртуальних серверів. Це дозволяє користувачам запускати програми та робочі навантаження на віртуальних машинах, відомих як екземпляри. Екземпляри EC2 призначені для задоволення різноманітних обчислювальних потреб, забезпечуючи гнучкість, контроль і можливість масштабувати ресурси на основі попиту.

EC2 пропонує широкий спектр типів екземплярів, оптимізованих для різних випадків використання, включаючи екземпляри, оптимізовані для обчислень, пам’яті, пам’яті та GPU. Приклади включають сімейства t3, c5, r5 і p3.

Образи машини Amazon (Amazon Machine Images – (AMI)) служать шаблонами для екземплярів, що містять необхідні конфігурації, програми та

навіть налаштування операційної системи. Користувачі можуть використовувати попередньо визначені AMI або створювати власні відповідно до своїх потреб.

Еластичний баланс навантаження (ELB) розподіляє вхідний трафік між кількома примірниками EC2, щоб забезпечити високу доступність і відмовостійкість. Він відіграє вирішальну роль у розподілі робочого навантаження та підвищенні стійкості програм.

Групи безпеки діють як віртуальні брандмауери для екземплярів, контролюючи трафік. Користувачі налаштовують групи безпеки, щоб визначити правила для дозволеного трафіку, підвищуючи рівень безпеки своїх екземплярів. Екземпляри запускаються з парами ключів, що забезпечує безпечний доступ. SSH використовується для екземплярів Linux, тоді як RDP використовується для екземплярів Windows. Пари ключів необхідні для безпечного підключення до екземплярів.

2.2.2. Віртуальна приватна хмара Amazon.

Віртуальна приватна хмара Amazon (VPC) – це веб-сервіс, наданий AWS, який дозволяє користувачам створювати логічно ізольований розділ хмари AWS, де вони можуть запускати та запускати ресурси AWS. VPC дозволяє користувачам контролювати свою віртуальну мережу, включаючи діапазони IP-адрес, підмережі, таблиці маршрутів і мережеві шлюзи.

По перше, VPC забезпечує логічно ізольовану частину хмари AWS, що дозволяє користувачам створювати власну приватну мережу з визначеними діапазонами IP-адрес. Користувачі можуть розділити свій VPC на підмережі, кожна з яких має власний блок CIDR (безкласова міждоменная маршрутизація). Підмережі дозволяють сегментувати ресурси та контролювати мережевий трафік. Таблиці маршрутів контролюють маршрутизацію трафіку в межах VPC. Користувачі можуть визначати власні таблиці маршрутів і пов’язувати їх із підмережами, щоб контролювати трафік.

VPC можна підключати до Інтернету через Інтернет-шлюз, що дозволяє примірникам у VPC спілкуватися з Інтернетом і навпаки. Користувачі можуть налаштовувати шлюзи трансляції мережевих адрес (NAT) або використовувати екземпляри NAT, щоб дозволити екземплярам у приватних підмережах ініціювати вихідний трафік до Інтернету, залишаючись у безпеці.

Користувачі можуть встановлювати зашифровані VPN-з'єднання між своїми локальними центрами обробки даних і своїми VPC, безпечно розширюючи свою

корпоративну мережу в хмару AWS. Direct Connect забезпечує спеціальні мережеві підключення між локальними центрами обробки даних і AWS, пропонуючи вищу пропускну здатність і меншу затримку порівняно з підключеннями VPN. Піринг VPC дозволяє користувачам підключати свої VPC і направляти трафік між ними за допомогою приватних IP-адрес. Це забезпечує зв’язок між ресурсами в різних VPC.

VPC дозволяє використовувати такі функції, як групи безпеки, NACL і приватні підмережі, які створюють безпечне середовище. Користувачі мають детальний контроль над трафіком, підвищуючи загальну безпеку.

Підсумовуючи, Amazon VPC є фундаментальним будівельним блоком AWS, який дає змогу користувачам створювати безпечне, ізольоване та настроюване мережеве середовище в хмарі. Його функції задовольняють широкий спектр випадків використання, забезпечуючи основу для розгортання масштабованих і безпечних програм на AWS.

2.2.3. Сервіс Amazon Simple Storage Service.

Amazon Simple Storage Service (Amazon S3) є облачним сервісом зберігання об'єктів, який надає масштабований та надійний доступ до даних через Інтернет. Amazon S3 часто використовується для зберігання та управління об'єктами, такими як файли, зображення, відео, бекапи, журнали, статичні веб-сайти та інші дані в хмарному середовищі. Він може бути використаний для створення резервних копій даних, забезпечення масштабованого зберігання для веб-додатків, розподілу медіа-файлів, роботи з аналітикою даних та багатьох інших варіантів.

Дані зберігаються як об'єкти у ресурсах, які називають кошиками, при цьому розмір одного об'єкта може становити до 5 ТБ. Доступ до об'єктів можна отримати за допомогою точки доступу S3 або безпосередньо за допомогою імені вузла контейнера. Amazon S3 спроектований для роботи з великими обсягами даних. Він може автоматично масштабуватися, щоб відповідати потребам ростучих обсягів інформації. Він забезпечує високий рівень доступності, який дорівнює 99,999999999 %. Дані реплікуються автоматично на різних серверах та різних центрах обробки даних.

Amazon S3 надає ряд заходів безпеки, таких як контроль доступу, шифрування, автентифікація та авторизація, щоб забезпечити конфіденційність, цілісність та доступність даних. Управління правами доступу дозволяє налаштовувати рівні доступу до ваших об'єктів, використовуючи політики

контролю доступу до об'єктів (S3 bucket policies) та управління дозволами AWS IAM. Сервіс Amazon S3 підтримує різні методи шифрування для захисту конфіденційності даних під час транзиту та зберігання. Це включає у себе шифрування в покладається (Server-Side Encryption), шифрування в злучається (Server-Side Encryption with AWS Key Management Service), та шифрування відповідно до клієнта (Client-Side Encryption).

Amazon S3 є ключовим елементом інфраструктури AWS і забезпечує надійне та високоефективне зберігання об'єктів для різних застосувань.

2.2.4. Веб-сервіс доменних імен Amazon Route 53.

Amazon Route 53 – це масштабований веб-сервіс доменних імен, який надає надійний та доступний механізм керування доменними іменами та розподілом трафіку в Інтернеті. Основними можливостями є:

– дозволяє реєструвати нові доменні імена або переносити вже існуючі;

– надає інтерфейс для ефективного управління налаштуваннями доменних імен, такими як DNS-записи, області видимості та інші параметри;

– дозволяє динамічно оновлювати DNS-записи в реальному часі, забезпечуючи миттєве реагування на зміни у вашому середовищі;

– дозволяє розподіляти трафік між різними регіонами та серверами для оптимізації продуктивності та доступності;

– моніторинг доступності ваших ресурсів та автоматичного перемикання трафіку на резервний сервер у випадку виявлення проблем;

– підтримка різних типів DNS-записів: A, AAAA, CNAME, MX, TXT та інші.

Amazon Route 53 є потужним та надійним сервісом, який допомагає забезпечити надійність та доступність ваших доменних імен та ефективно розподіляти трафік в Інтернеті.

2.2.5. Сервіс AWS Lambda.

AWS Lambda – це обчислювальний сервіс в хмарі, який дозволяє виконувати код без необхідності управління інфраструктурою. Основні можливості AWS Lambda включають:

– використовує концепцію безсерверної архітектури, де ви завантажуєте код, а сервіс автоматично масштабує його в залежності від потреб обробки;

– підтримується багато мов програмування, таких як Node.js, Python, Java, Go, Ruby та інші;

– може реагувати на події та тригери від інших сервісів, запускаючи виконання коду при настанні певних подій;

– автоматично масштабується від одного виклику до великих обсягів викликів без необхідності адміністрування серверів.

Недоліками можна вважати наведені нижче.

1) Є обмеження часу виконання для одного виклику коду (максимум 15 хвилин), що може бути недостатнім для деяких завдань.

2) При першому виклику або при тривалій перерві може бути затримка (холодний старт) перед виконанням коду.

3) Обмеженість ресурсів (CPU, пам'ять) для одного виклику, що може впливати на виконання великих завдань.

4) Для великих обсягів викликів ціна може зростати, і може стати менш вигідною порівняно з іншими моделями обчислення.

AWS Lambda є потужним інструментом для розгортання коду в хмарному середовищі, проте важливо враховувати його обмеження та вартість при виборі архітектури для проекту.

2.2.6. Сервіс баз даних Amazon Relational Database Service.

Amazon Relational Database Service (RDS) – це керований сервіс баз даних в хмарному середовищі AWS, який спрощує створення, управління та масштабування реляційних баз даних. RDS підтримує різні типи баз даних, такі як MySQL, PostgreSQL, Oracle, Microsoft SQL Server та інші. Основні можливості:

– автоматизує процеси установки, налаштування та резервного копіювання баз даних, що полегшує їх управління;

– забезпечує можливість масштабування обсягу ресурсів бази даних в залежності від потреб користувача;

– надає автоматизовані інструменти для створення резервних копій баз даних та їх відновлення у випадку втрати даних чи неполадок;

– забезпечує можливість шифрування даних під час зберігання та передачі для забезпечення безпеки;.

– автоматично надає оновлення для баз даних, забезпечуючи їх безпеку та актуальність;

– підтримує різні двигуни баз даних, такі як MySQL, PostgreSQL, Oracle, Microsoft SQL Server.

Недоліками сервісу є наступні.

1) В порівнянні з іншими альтернативами AWS RDS може обмежувати деяку гнучкість конфігурації бази даних.

2) В порівнянні з самостійно налаштованими базами даних в EC2, вартість користування RDS може бути вищою.

3) Використання RDS призводить до великої залежності від AWS, і користувачі можуть бути обмежені функціоналом, який пропонує сам сервіс.

Amazon RDS – це потужний та зручний сервіс для управління реляційними базами даних в хмарному середовищі, але важливо враховувати його обмеження та вартість при виборі для конкретного проекту.

2.2.7. Сервіс баз даних Amazon DynamoDB.

Amazon DynamoDB – це база даних NoSQL, що розроблена для швидкості та масштабованості, що робить її ідеальною для додатків з високими вимогами до продуктивності та гнучкості. Основні можливості:

– є керованою службою, що включає в себе автоматизоване масштабування та управління інфраструктурою бази даних;

– є базою даних типу NoSQL, яка дозволяє зберігати та отримувати дані в форматі ключ-значення, а також використовувати гнучкі схеми;

– здатна автоматично масштабувати потужність та обсяг зберігання для відповіді на зміни в обсягах роботи або завдань;

– дозволяє виконувати запити з низькими затримками, адже спроектована для високої продуктивності та надійності;

– відсутність строгої схеми дозволяє додавати або видаляти поля з записів без необхідності перепроектування бази даних;

– дозволяє шифрувати дані в спокої та покої під час передачі та зберігання.

Недоліками можна вважати наступні.

1) Динамічна масштабованість та великий обсяг транзакцій можуть призвести до високих витрат.

2) Не дозволяє використовувати складні SQL-подібні запити, які доступні в реляційних базах даних.

3) Обмежений в підтримці деяких типів даних порівняно з реляційними базами даних.

Amazon DynamoDB – це потужний інструмент для роботи з даними в хмарі, особливо для застосунків з вимогами до швидкості та масштабованості.

2.2.8. Служба доставки контенту Amazon CloudFront.

Amazon CloudFront – це служба CDN, яка надає розподілений спосіб доставки вмісту з використанням різноманітних серверів розміщення по всьому світу. Основною метою CloudFront є забезпечення швидкої та надійної доставки контенту користувачам шляхом розміщення копій вмісту на серверах, які знаходяться фізично ближче до кінцевих користувачів. Основні можливості:

– використовує свою глобальну мережу розподілених серверів для ефективного розподілу контенту;

– забезпечує швидку доставку вмісту завдяки використанню кешування та розташуванню серверів;

– забезпечує шифрування зв'язку між кінцевим користувачем та CloudFront за допомогою SSL/TLS;

– може розподіляти різні типи контенту, такі як статичний вміст, стріми, API запити, зображення і т. д.;

– дозволяє налаштовувати різні параметри, включаючи налаштування кешування, правила маршрутизації та інші.

До недоліків можна віднести наступні.

1) В порівнянні з іншими CDN-послугами, вартість CloudFront може бути вищою для певних обсягів трафіку.

2) CloudFront спрямований на розподілення контенту, і він може бути менш ефективним для інших завдань, таких як обчислення або обробка даних.

3) Перші запити на новий контент можуть мати затримку через необхідність кешування на різних серверах.

4) Деякі параметри кешування можуть бути обмежені в порівнянні з більш гнучкими CDN.

Amazon CloudFront є потужним інструментом для забезпечення швидкої та надійної доставки контенту для кінцевих користувачів по всьому світу.

2.2.9. Служба управління доступом Amazon Identity and Access Management.

Amazon Identity and Access Management (IAM) – це служба управління доступом, яка дозволяє керувати правами доступу користувачів та інших сутностей в середовищі AWS. IAM надає інструменти для налаштування та

управління аутентифікацією та авторизацією для ресурсів AWS. Основні можливості:

– дозволяє контролювати, як користувачі та інші сутності (ролі, групи) отримують доступ до ресурсів AWS;

– забезпечує можливість аутентифікації користувачів і авторизації їхнього доступу до конкретних AWS-ресурсів;

– дозволяє створювати ролі з конкретними правами та надавати їх іншим сутностям, таким як EC2 і Lambda;

– дозволяє групам користувачів об'єднуватися, щоб легше керувати правами доступу;

– підтримка многофакторної аутентифікації для підвищення рівня безпеки облікових записів.

Як недоліки можна вважати такі.

1) Налаштування IAM може бути складним завданням, особливо для користувачів без великого досвіду в AWS.

2) Недостаток деяких розширених аудитованих подій, які б дозволили більшу прозорість та слідкування за діями користувачів.

3) Велика можливість помилкової конфігурації, яка може призвести до надання невірних прав доступу.

4) Деякі служби можуть не підтримувати всі можливості IAM на повну міру.

5) Відсутність універсальних шаблонів доступу для різних сценаріїв.

Хоча Amazon IAM надає потужні інструменти для управління доступом до ресурсів AWS, важливо бути уважним при його конфігурації та забезпечити належний рівень безпеки для облікових записів і ресурсів.

2.3.Підсумковий порівняльний аналіз інструментів розгортання інформаційної інфраструктури AWS

Порівняння інструментів інформаційної інфраструктури AWS з іншими провайдерами зазвичай залежить від конкретних вимог, потреб бізнесу та специфіки проектів. Важливо враховувати, що кожен провайдер хмарних послуг має свої особливості та переваги. В табл. 2.2 наведено загальні порівняльні характеристики між AWS і двома іншими провайдерами хмарних послуг – Microsoft Azure та Google Cloud Platform.

Таблиця 2.2 – Порівняння інструментів хмарних провайдерів

Провайдер	Переваги	Недоліки
Amazon Web Services	Найбільший ринок та широкий спектр послуг. Глибоке портфоліо сервісів для різних потреб (обчислення, зберігання, бази даних, машинне навчання, IoT, безпека і т. д.). Глобальна мережа дата-центрів (регіони та доступні зони). Сильна екосистема і підтримка спільноти.	Може бути вищою вартість для деяких послуг порівняно з іншими провайдерами.
Microsoft Azure	Інтеграція зі стеком Microsoft та широкий функціонал для підтримки корпоративних рішень. Зручний інтерфейс та інструменти для розробників. Глибока інтеграція зі службами Windows та підтримка іншими мовами програмування.	Менший ринок порівняно з AWS. Деякі служби можуть бути менш розвиненими або менше популярними.
Google Cloud Platform	Спеціалізовані сервіси для машинного навчання та обробки даних. Інноваційні рішення та підходи, зокрема Kubernetes. Гнучка система ціноутворення.	Менший ринок та менший вибір регіонів порівняно з AWS та Azure. Може виникнути менше сторонніх інтеграцій порівняно з AWS та Azure.

Аналіз переваг та недоліків інструментів інформаційної інфраструктури AWS допомагає зрозуміти, наскільки ефективно можна використовувати ці сервіси для досягнення бізнес-цілей (табл. 2.3).

Індивідуальний аналіз потреб, бюджету та конкретних вимог може допомогти визначити, наскільки AWS підходить для конкретного бізнесу. Важливо ураховувати обставини та контекст використання при оцінці переваг та недоліків.

Таблиця 2.3 – Аналіз інструментів розгортання інформаційної інфраструктури AWS

Переваги	Недоліки
Гнучкість та масштабованість: AWS надає гнучкість вибору ресурсів та послуг, які можна масштабувати в залежності від потреб бізнесу.	Вартість: Витрати на використання AWS можуть бути високими, особливо для невеликих підприємств чи стартапів.
Велика кількість сервісів, що охоплюють обчислення, сховище, бази даних, мережі, штучний інтелект, аналітику та інше.	Складність: У великого спектру послуг може виникати складність у виборі та конфігурації необхідних рішень.
Глобальна присутність та висока доступність: AWS має дата-центри в численних регіонах світу, що забезпечує високу доступність та надійність послуг.	Залежність від Інтернету: безперервний доступ до інтернету необхідний для використання більшості AWS-послуг.
Безпека та захист даних: AWS надає широкий спектр інструментів для забезпечення безпеки, включаючи управління ключами, брандмауери, сервіси ідентифікації та контролю доступу.	Періодичні збої та відмови. Хоча AWS розробляється для високої доступності, періодично можливі збої або відмови в роботі, що може впливати на бізнес-процеси.
Інтеграція та екосистема: AWS інтегрується з багатьма іншими сервісами та рішеннями, утворюючи широку екосистему для розробників та підприємств.	Підтримка та обслуговування. В деяких випадках може виникати складність у підтримці та отриманні необхідної допомоги, особливо для користувачів із меншого досвіду.
Послуги штучного інтелекту та машинного навчання: AWS пропонує послуги штучного інтелекту та машинного навчання, такі як Amazon SageMaker, що полегшують впровадження та розвиток інтелектуальних рішень.	Сфокусованість на хмарових рішеннях. Для підприємств, які мають обладнання або інфраструктуру на місці, перехід до хмарових рішень може виявитися витратним та складним.

3. АНАЛІЗ ТА ВИБІР ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ МЕРЕЖНОЇ БЕЗПЕКИ ІНФРАСТРУКТУРИ AWS

3.1.Концепції інформаційної безпеки AWS

AWS є провідним постачальником хмарних послуг, і безпека його хмарної платформи є спільною відповідальністю між AWS та його клієнтами. AWS забезпечує безпечну інфраструктуру, а клієнти відповідають за безпеку своїх даних, програм і конфігурацій у середовищі AWS. Згідно цієї модель спільної відповідальності на AWS накладається відповідає за роботу, контроль і управління компонентами від рівня віртуалізації до рівня фізичної безпеки об'єктів, де надаються послуги, що дозволяє зменшити операційне навантаження на клієнтів. Клієнти несуть відповідальність за підтримку програмного забезпечення, яке використовує клієнт (включаючи оновлення та виправлення безпеки), і налаштування груп безпеки, які надаються платформою AWS. Клієнти повинні уважно поставитися до вибору послуги, оскільки обов'язки, пов'язані з нею, відрізняються залежно від послуги, яка застосовується, інтеграції в їх IT-систему та чинних нормативних актів та законів. Ця система спільної відповідальності також сприяє гнучкості та дозволяє клієнтам брати участь у розгортанні та виконанні систем. Наведений поділ відповідальності формулюють як «безпеку хмари» та «безпеку у хмарі». Це продемонстровано на схемі нижче (рис. 3.1) [31].

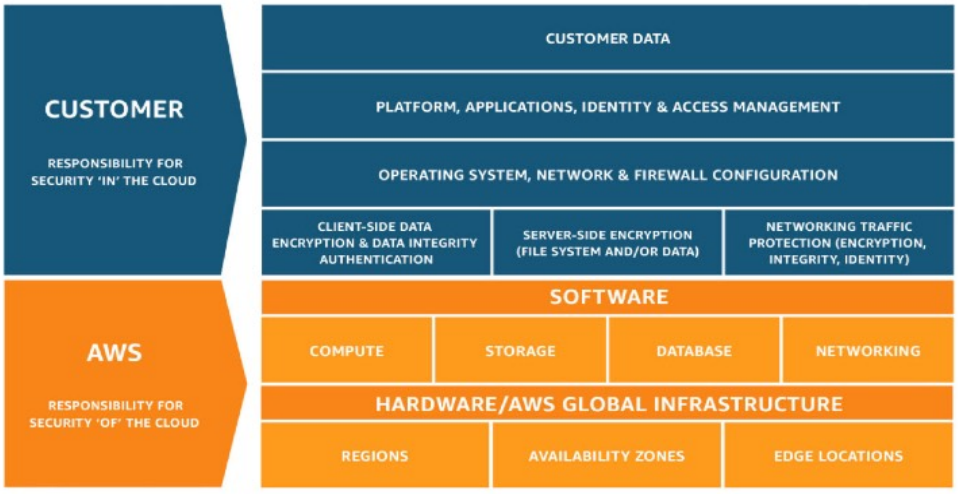


Рисунок 3.1 – Модель спільної відповідальності AWS

Відповідальність AWS за «безпеку хмари». AWS відповідає за безпеку хмарної інфраструктури AWS, на якій працюють усі запропоновані послуги. Ця інфраструктура включає апаратне та програмне забезпечення, мережі та об'єкти, на яких працюють хмарні сервіси AWS.

Обов'язки клієнта – це «безпека в хмарі». Відповідальність клієнта визначатиметься хмарними службами AWS, вибраними для використання. Вибір послуги визначає обсяг конфігураційної роботи, яку клієнт повинен виконати в рамках своїх обов'язків щодо безпеки. Наприклад, така служба, як Amazon EC2, належить до сервісів «інфраструктура як послуга» (IaaS), тому покладає на клієнта обов'язок реалізації необхідних налаштувань безпеки та усіх адміністративних завдань.

Під час розгортання екземплярів Amazon EC2 клієнти несуть відповідальність за керування сервісними компонентами, встановленими на екземплярі, будь-яким прикладним програмним забезпеченням або гостьовою операційною системою (включно з виправленнями та оновленнями безпеки), а також їх конфігурацію, конфігурацію брандмауера, надану AWS (командою безпеки) для кожного екземпляра.

Для таких абстрактних сервісів, як Amazon DynamoDB та Amazon S3, на AWS покладається керування рівнями платформи, операційної системи та інфраструктури, в той час як клієнти здобувають доступ до кінцевих точок для отримання та зберігання даних.

Клієнти несуть відповідальність за використання інструментів IAM для забезпечення відповідних дозволів, класифікацію ресурсів і керування власними даними (залучачи параметри шифрування).

Ця модель спільної відповідальності між клієнтами та AWS [29-33] також поширюється на системи управління IT-активами. Відповідальність за управління IT-середовищем розподіляється між AWS і клієнтом, як і завдання використання, тестування та управління системами контролю IT-ресурсів. AWS звільняє Клієнтів від тягаря керування налаштуваннями безпеки, підтримуючи налаштування, пов'язані з фізичною інфраструктурою, у середовищі AWS і звільняючи Клієнтів від їхнього керування. Клієнти можуть використовувати доступну документацію щодо управління та відповідності AWS для проведення необхідних оцінок і перевірки налаштувань керування. В таблиці 3.1 зведено розподіл відповідальності між клієнтами та AWS.

Таблиця 3.1 – Аналіз розподілу відповідальності між клієнтами та AWS

Рівні відповідальності	Заходи AWS	Обов'язки клієнта
1	2	3
Фізична безпека	Центри обробки даних AWS фізично захищені засобами контролю доступу, спостереження та моніторингу. Географічно розподілені центри обробки даних пропонують резервування та доступність.	Клієнти покладаються на заходи фізичної безпеки AWS і не повинні намагатися отримати доступ або відвідати центри обробки даних AWS.
Безпека мережі	Virtual Private Cloud дозволяє клієнтам створювати ізольовані мережі з контролем над діапазонами IP-адрес, підмережами та таблицями маршрутів. Групи безпеки та списки контролю доступу до мережі (NACL) контролюють трафік.	Клієнти налаштовують VPC, групи безпеки та NACL відповідно до своїх вимог безпеки.
Керування ідентифікацією та доступом	IAM дозволяє клієнтам керувати користувачами, ролями та дозволами. Багатофакторна автентифікація (MFA) підвищує безпеку облікового запису.	Клієнти визначають користувачів і дозволи IAM і керують ними, дотримуючись принципу найменших привілеїв.
Шифрування даних	AWS забезпечує шифрування в стані спокою та під час передачі. Служба керування ключами AWS (KMS) дозволяє клієнтам керувати ключами шифрування.	Клієнти налаштовують шифрування своїх даних, керують ключами та впроваджують безпечні протоколи передачі.

Логування та моніторинг	AWS CloudTrail забезпечує журналювання викликів AWS API та дозволяє контролювати ресурси та програми.	Клієнти використовують CloudTrail і CloudWatch для моніторингу та аналізу журналів подій безпеки.

Продовження таблиці 3.1

1	2	3
Захист від DDoS	AWS Shield забезпечує захист від DDoS, включаючи стандартний для всіх клієнтів і розширений для додаткових функцій. AWS Web Application Firewall допомагає захистити від веб-експлойтів.	Клієнти налаштовують параметри AWS Shield і керують ними відповідно до своїх конкретних потреб безпеки.
Відповідність і сертифікати	AWS проходить регулярні перевірки безпеки та сертифікації, включаючи ISO, SOC і PCI DSS.	Клієнти використовують інформацію про відповідність і сертифікацію, надану AWS, щоб переконатися, що їхні програми відповідають певним вимогам.
Реагування на інцидент	AWS має групу реагування на інциденти для управління та реагування на інциденти безпеки.	Клієнти несуть відповідальність за реагування на інциденти, включаючи виявлення, звітування та вирішення інцидентів безпеки в своєму середовищі AWS.
Модель спільної відповідальності	AWS дотримується моделі спільної відповідальності, вказуючи обов’язки щодо безпеки як AWS, так і її клієнтів.	Клієнти розуміють і виконують свої обов'язки в рамках моделі спільної відповідальності.
Найкращі методи безпеки	AWS надає розширену документацію, офіційні документи та найкращі практики безпеки.	Клієнти дотримуються найкращих практик безпеки AWS, щоб підвищити безпеку своїх програм і даних.

3.2.Аналіз служб мережної безпеки AWS

Розглянемо служби, що можуть бути використані для забезпечення мережної безпеки AWS. За результатами аналізу наявного набору служб безпеки AWS, ми відокремили наступні [34]:

– Identity and Access Management дозволяє керувати доступом до ресурсів AWS шляхом надання та управління ідентифікаторами та повноваженнями, використання Multi-Factor Authentication (MFA);

– Amazon Virtual Private Cloud дозволяє створювати ізольовані мережі в AWS та керувати мережевим трафіком, може бути використаний для створення приватних мереж, визначення мережевих політик;

– AWS WAF служить для захисту веб-додатків від різних атак, таких як SQL-ін'єкції та кросс-сайтові атаки, може бути використаний для налаштування правил для фільтрації HTTP-трафіку, виявлення та блокування потенційно шкідливих запитів;

– Amazon Inspector дозволяє автоматизувати оцінку безпеки інфраструктури, виявлення вразливостей та рекомендацій щодо поліпшення безпеки;

– AWS CloudTrail веде журнал подій, що дозволяє аудитувати дії користувачів та системних подій в AWS;

– Amazon GuardDuty – це система виявлення загроз для автоматичного виявлення підозрілих активностей та вразливостей в облікових записах та ресурсах;

– AWS Key Management Service дозволяє керувати ключами шифрування для захисту конфіденційної інформації;

– AWS Shield – це служба захисту від DDoS-атак для захисту від розподілених атак на відмову в обслуговуванні.

Це лише невелика частина інструментів та служб, які AWS надає для забезпечення мережної безпеки. Важливо ретельно налаштовувати та комбінувати ці інструменти для максимальної ефективності та захисту вашої інфраструктури.

3.2.1. Аналіз сервісу управління ідентифікацією та доступом AWS.

Identity and Access Management (IAM) призначена для керування ідентичністю та доступом користувачів до ресурсів AWS і які дії вони можуть виконувати. До основних можливостей IAM можна віднести:

– можливість створювати користувачів та групи, для яких визначаються права доступу, а також забезпечувати підтвердження ідентичності через MFA;

– дозволяє визначити права доступу за допомогою політик, які визначають, які ресурси можуть бути доступні та які операції можна виконувати, а також реалізує принцип найменшого привілею (максимального обмеження прав доступу для забезпечення безпеки);

–забезпечує надання тимчасового доступу користувачам, сервісам або ресурсам за допомогою встановлених ролей та визначення ролей, які можуть передавати свої права доступу іншим ролям.

IAM дозволяє створювати гнучкі та безпечні сценарії управління доступом, що важливо для забезпечення конфіденційності та цілісності даних в хмарному середовищі AWS. Правильна конфігурація та ефективне використання IAM стає ключовою складовою стратегії безпеки (зокрема, мережної безпеки) в AWS.

3.2.2. Аналіз сервісу віртуальної приватної хмари AWS.

Amazon Virtual Private Cloud – це сервіс, який дозволяє вам створювати власні ізольовані віртуальні мережі в обласному середовищі AWS. Amazon VPC надає контроль над віртуальною мережею, включаючи вибір вашого IP-адресного простору, налаштування таблиць маршрутизації та конфігурацію сегментів підмереж. Основними можливостями є:

– сегменти підмереж (Subnets) дозволяють розділити IP-адресний простір на сегменти підмереж для створення логічно ізольованих частин мережі;

– можливість вибрати власний IP-адресний простір для віртуальної мережі;

– використання інтернет-шлюзу для з'єднання VPC з Інтернетом;

– VPC Peering забезпечує пряме з'єднання між різними VPC без використання інтернету.

– AWS VPN використовується для побудови захищених з'єднань між корпоративною інфраструктурою та VPC;

– Security Groups (аналог файерволу на рівні екземплярів) та NACLs (списки керування доступом на рівні підмереж) забезпечують керування доступом до екземплярів та ресурсів.

Security Groups (SG) та Network Access Control Lists (NACLs) є двома основними засобами контролю доступу в мережах Amazon VPC на AWS. Обидва ці засоби дозволяють визначати правила безпеки для контролю трафіку в вашій віртуальній приватній хмарі. Однак вони використовуються на різних рівнях мережі та мають свої особливості. Порівняння цих сервісів наведено у табл. 3.2.

Обидва ці інструменти можна комбінувати для створення високої безпеки в мережах Amazon VPC. У багатьох сценаріях застосування обох засобів дозволяє забезпечити гнучкі та деталізовані правила безпеки для вашого інфраструктурного середовища.

Таблиця 3.2 – Порівняння інструментів SG та NACLs

	Security Groups	Network Access Control Lists
Рівень	Що контролює: Робота на рівні інстанцій (екземплярів). Керування доступом: Специфікується для кожного екземпляру. Дозволяє визначити, який трафік допускається чи забороняється в конкретний екземпляр.	Що контролює: Робота на рівні підмереж (subnets). Керування доступом: Задає правила для контролю трафіку, який входить та виходить з підмережі.
Природа правил	Стан: Stateful (запам'ятовує стан з'єднань). Правила: Специфікується правила для дозволу чи блокування трафіку. Якщо ви вказуєте правило для дозволу вхідного трафіку, то вихідний трафік, пов'язаний з цим з'єднанням, автоматично дозволяється.	Стан: Stateless (не запам'ятовує стан з'єднань). Правила: Визначається як окремі правила для вхідного та вихідного трафіку. Якщо ви вказуєте правило для вхідного трафіку, це не автоматично дозволяє вихідний трафік пов'язаний із з'єднанням.
Особливості	Автоматичне оновлення: Автоматично оновлюється для дозволу вихідного та вхідного трафіку для нових інстанцій. Використання в групах: Інстанція може належати багатьом групам. Використовується для створення "білих списків" правил доступу.	Автоматичне Оновлення: Потрібно оновлювати вручну, воно не автоматично додається для нових підмереж або інстанцій. Використання в підмережах: Одна NACL використовується для кожної підмережі. Використовується для створення "чорних списків" правил доступу.

3.2.3. Аналіз сервісу AWS Key Management System.

AWS KMS – це повністю управляючий сервіс, призначений для створення, керування та використання криптографічних ключів в середовищі AWS, надає інструменти для захисту конфіденційності та цілісності даних, забезпечуючи безпеку при їхньому зберіганні, передачі або обробці в хмарному середовищі. Ця служба відіграє важливу роль у захисті даних, що зберігаються у вашій програмі.

Основними можливостями AWS KMS є:

– сервіс дозволяє створювати Customer Master Keys (CMKs), які служать основними криптографічними ключами для шифрування та розшифрування даних;

– підтримка як симетричних, так і асиметричних ключів (симетричні ключі використовуються для шифрування/розшифрування, тоді як асиметричні ключі використовуються для створення цифрового підпису та перевірки підпису);

–дозволяє визначати політики доступу для керування правами користувачів та ролей на використання ключів, що використовується разом з AWS IAM;

– ключі можна реплікувати в різні регіони для забезпечення відновлення в разі відмови; є можливість зонної ізоляції для забезпечення безпеки ключів в межах зони доступності;

– автоматично оновлює та зберігає ключі в безпечному середовищі, що включає автоматичну зміну симетричних ключів для зберігання даних;

–можливість інтеграції з AWS CloudHSM для використання апаратних засобів для створення та управління ключами.

AWS KMS дозволяє забезпечити потрібний рівень безпеки для обробки конфіденційної інформації в AWS, забезпечуючи високий рівень управління ключами та інтеграції з іншими сервісами для безпечної роботи з даними.

3.2.4. Аналіз сервісу AWS Shield.

AWS Shield – це послуга AWS, яка надає захист від DDoS-атак (атак з великою кількістю запитів для завдання перевантаження мережі чи сервісів). AWS Shield спеціалізується на захисті інфраструктури та додатків в хмарному середовищі від різних видів атак, зокрема DDoS. Це послуга, що доступна в двох варіантах: стандартному та розширеному. AWS Shield Standard є безкоштовним для всіх клієнтів і забезпечує захист від найпоширеніших атак, спрямованих на вашу програму або веб-сайт AWS. AWS Advanced Protection забезпечує вищий

рівень захисту та інтеграцію з іншими службами, такими як брандмауери веб-додатків і доступ до AWS DDoS Response Team.

Основні характеристики та можливості AWS Shield:

– захист від різних видів DDoS-атак, таких як атаки на рівні мережі (наприклад, SYN/ACK flood) та атаки на рівні застосунків (наприклад, HTTP GET/ POST flood);

– система реагує на атаки в реальному часі, намагаючись заблокувати шкідливий трафік та захистити ресурси від перевантаження;

– використовує алгоритми машинного навчання для визначення шаблонів та аномального трафіку;

– захист на рівні краю (Edge Protection), який означає, що атаки блокуються ще до того, як вони дістаються до ресурсів в середині AWS;

– захист на рівні протоколів (TCP, UDP, DNS) дозволяє розпізнавати та фільтрувати шкідливий трафік, спрямований на різні ресурси;

– надає інструменти для моніторингу та звітності щодо атак, дозволяючи організаціям аналізувати та вдосконалювати свою стратегію захисту;

– інтеграція з Amazon WAF дозволяє поєднати захист від DDoS з захистом на рівні додатків, що дозволяє виявляти та блокувати не лише надмірний трафік, але і спроби вразити додаток;

– інтегрується з AWS Global Accelerator для маршрутизації та збереження найкращого доступного шляху для трафіку, що дозволяє мінімізувати вплив атаки на доступність.

Використання AWS Shield є ключовим компонентом стратегії безпеки в хмарному середовищі, забезпечуючи захист від DDoS-атак та збереження доступності ресурсів. Це особливо важливо для бізнес-застосунків та сервісів, де відмова в обслуговуванні може призвести до серйозних наслідків.

3.2.5. Аналіз сервісу AWS Web Application Firewall.

AWS WAF – це служба для захисту веб-додатків від різних видів веб-атак, яка дозволяє налаштовувати правила безпеки для фільтрації HTTP- та HTTPS-трафіку, що проходить через різні AWS-ресурси, такі як Amazon CloudFront, Amazon API Gateway та Application Load Balancer. Основні можливості AWS WAF включають:

– сервіс постачається зі стандартними правилами, які дозволяють виявляти і блокувати загрози, такі як атаки SQL-впровадження та XSS, до яких можна створювати власні правила, які відповідають конкретним потребам застосунку;

– дозволяє створювати білі та чорні списки IP-адрес для фільтрації трафіку, що дозволяє обмежити доступ до вашого застосунку лише з конкретних географічних областей;

– використовує машинне навчання для навчання на основі шаблонів та виявлення нових атак та інтегроване з AWS Managed Rules для автоматичного оновлення захисту від нових загроз;

– метрики та події AWS WAF можна переглядати у консолі CloudWatch а також AWS WAF WebACL Logs може бути налаштований для зберігання в Amazon S3 для подальшого аналізу та аудиту.

AWS WAF допомагає захистити ваші веб-додатки від різноманітних загроз, забезпечуючи гнучкість та налаштування правил безпеки відповідно до ваших потреб. Використання AWS WAF є важливою складовою стратегії безпеки для захисту від атак на рівні додатків.

3.2.6. Аналіз сервісу Amazon GuardDuty.

Amazon GuardDuty – це моніторинговий сервіс від AWS, який надає виявлення загроз для безпеки вашого хмарного середовища, використовує аналіз логів, мережевого трафіку та викликів API для виявлення ненормальної або підозрілої активності, що може вказувати на потенційні загрози безпеки. Основні можливості:

– аналізує логи, виклики API та мережевий трафік для виявлення аномальної або підозрілої активності в хмарному середовищі;

– спрямований на виявлення як зовнішніх, так і внутрішніх атак, включаючи спроби несанкціонованого доступу, вторгнення та виведення даних;

– аналізує виклики API та виявляє підозрілу активність, яка може свідчити про атаки або неправомірне використання ресурсів;

– виявлення дій, що можуть свідчити про зловживання привілеями або неправомірний доступ до ресурсів;

– вивчає мережевий трафік для виявлення підозрілої активності, пов'язаної з ботнетами чи іншими загрозами;

– надає деталізовані логи та можливості автоматизації відповідей на виявлені загрози;

– забезпечує масштабованість для ефективного виявлення загроз в навантажених хмарних середовищах.

Аналіз використання Amazon GuardDuty для мережної безпеки полягає в його інтеграції в стратегію оборони в глибину та моніторингу заходів безпеки. GuardDuty може ефективно виявляти велику кількість загроз та допомагати організаціям оперативно реагувати на потенційні вторгнення та інші атаки в хмарному середовищі AWS.

3.3.Переваги та недоліки хмарної інфраструктури с точки зору забезпечення мережної безпеки

Для забезпечення інформаційної та мережної безпеки хмарна інфраструктура має наступні переваги:

– надійність платформи: програмні та апаратні складники платформи розгортаються в хмарі більш рівномірно, ніж у більшості звичних центрів обробки даних, що позволяє краще автоматизувати операції безпеки, виправлення збоїв у компонентах платформи та тестування;

– доступність ресурсів: динамічне масштабування системних ресурсів, а також аварійне відновлення та резервування можна застосовувати для підняття сталості системи до атак шляхом відмови в обслуговуванні, а також для жвавого відновлювання після критичних випадків;

– наявність спеціалізованого персоналу: хмарний провайдер бере експертів у галузі інформаційної безпеки для забезпечення хмарної безпеки, дозволяючи їм повністю сконцентруватися на питанні безпеки;

– централізація даних: застосовування хмари, як єдиного місця для обробки та зберігання даних, що позволяє в деяких випадках збільшити безпеку відносно з розпорошеним зберіганням даних на портативних комп’ютерах, вбудованих або збережених на мобільних стойках;

– централізоване керування, тестування системи безпеки та її налаштування;

– резервне копіювання та відновлення: постачальники хмарних послуг можуть забезпечити вищий рівень резервного копіювання та відновлення на географічній основі, ніж традиційні центри обробки даних;

– мобільність кінцевого клієнта: завдяки хмарній архітектурі клієнти можуть застосовувати різні мобільні прилади з доступом до Інтернету, невисокою

обчислювальною потужністю, браузером та/або декількома встановленими програмами для доступу до ключових IT-ресурсів.

Особливості побудови, організації та використання хмарних обчислень призводять до специфічних з точки зору інформаційної безпеки недоліків.

1) Основним недоліком загальнодоступних хмар є те, що користувачі відповідають за обмін ресурсами та компонентами з іншими користувачами, про які вони не знають на логічному рівні, це дозволяє зловмиснику використовувати вразливі місця в хмарі для отримання несанкціонованого доступу до ресурсів.

2) При використанні хмарних сервісів користувач делегує відповідальність за інформацію хмарному провайдеру, що підвищує ризик інформаційної безпеки. Користувач стає залежним від хмарного провайдера і може втратити не тільки логічний контроль над інформацією, але й фізичний контроль над нею.

3) Публічна хмара значно складніша за традиційний центр обробки даних. Велика кількість компонентів, які складають хмару, дозволяє проводити атаки на різних рівнях абстракції. Поряд з компонентами, які обслуговують обчислення загального призначення, такими як розповсюдження додатків, монітори віртуальних машин, гостьові віртуальні машини, зберігання даних, існують також компоненти, які мають компонент керування, включаючи самообслуговування, облік ресурсів, керування квотами, реплікацію та відновлення даних, моніторинг рівня обслуговування та навантаження на управління.

4) Уніфікованість програмного та апаратного забезпечення платформи призводить до умов коли єдиний недолік впливатиме на усіх користувачів та всю хмару.

5) Для адміністрування хмар та керування Інтернет-сервісами та програмами використовується незахищена мережа. Коли організація переходить на хмарні обчислення, виникають нові небезпеки для захищених внутрішніх мереж і ресурсів. Також необхідне віддалене адміністрування за допомогою ненадійного способу передачі інформації.

4. ДОСЛІДЖЕННЯ РІВНЯ МЕРЕЖНОЇ БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ AWS

4.1. Аналіз ризиків мережної безпеки для хмарної інфраструктури AWS

Ризики мережної безпеки для хмарної інфраструктури пов’язані із захистом мережевої інфраструктури та каналів зв’язку в хмарних середовищах. За результатами аналізу бази інцидентів у AWS хмарі відокремлені деякі з найбільш суттєвих ризиків безпеки хмарної мережі. Результати наведено у таблиці 4.1.

Таблиця 4.1 – Ризики мережної безпеки для хмарної інфраструктури AWS

Параметр	Опис
1	2
1. Несанкціонований доступ	
Ризик	Неавторизовані користувачі, які отримують доступ до хмарної мережі, можуть призвести до витоку даних, збоїв у роботі служби та можливого зловживання ресурсами.
Приклад атаки	У 2019 році неправильно налаштований сегмент AWS S3 відкрив конфіденційні дані мексиканського банку Bancomext. Неправильна конфігурація дозволила несанкціонований доступ, що призвело до значного порушення даних.
Шляхи пом’якшення	Впровадження надійних механізмів автентифікації, дотримання принципу найменших привілеїв і регулярна перевірка доступу користувачів.
2. Незахищені інтерфейси та API	
Ризик	Зловмисники можуть використати недоліки хмарних інтерфейсів і API, щоб отримати неавторизований доступ або порушити роботу служб.
Приклад атаки	У 2018 році вразливість безпеки на сервері Kubernetes API дозволила зловмисникам виконувати неавторизовані дії, потенційно впливаючи на безпеку контейнерних програм і служб.

Шляхи пом’якшення	Регулярно оновлюйте та захищайте API, використовуйте безпечні протоколи зв’язку та встановлюйте належні механізми автентифікації та авторизації.

Продовження таблиці 4.1

1	2
3. Перехоплення даних	
Ризик	Якщо дані, що передаються, не зашифровані належним чином, вони можуть бути перехоплені зловмисниками, що призведе до компрометації даних.
Приклад атаки	У 2014 році вразливість «Heartbleed» у OpenSSL виявила конфіденційні дані, зокрема імена користувачів і паролі, під час проходження мережею. Постраждали багато хмарних сервісів, що підкреслює ризик перехоплення даних.
Шляхи пом’якшення	Застосовуйте надійні протоколи шифрування для даних, що передаються, і використовуйте безпечні канали зв’язку.
4. Неадекватний моніторинг мережі	
Ризик	Відсутність видимості мережевої діяльності ускладнює виявлення інцидентів безпеки та швидке реагування на них.
Приклад атаки	Порушення даних Equifax у 2017 році сталося через те, що компанія не змогла швидко виявити підозрілу активність у мережі та відреагувати на неї. Хакери скористалися вразливістю, що призвело до несанкціонованого доступу та викрадання даних.
Шляхи пом’якшення	Запроваджуйте безперервний моніторинг, використовуйте системи виявлення та запобігання вторгненням і аналізуйте мережеві журнали на наявність підозрілих дій.
5. DDoS-атаки	
Ризик	Розподілені атаки типу «відмова в обслуговуванні» можуть перевантажувати ресурси хмарної мережі, спричиняючи збої в роботі служби.

Приклад атаки	У 2020 році Amazon Web Services (AWS) зазнали серії DDoS-атак, які тимчасово порушили роботу кількох відомих веб-сайтів і служб, розміщених на платформі, вплинувши на доступ користувачів.
Ш л я х и пом’якшення	Реалізуйте стратегії пом'якшення DDoS, використовуйте мережі доставки контенту (CDN) і співпрацюйте з постачальником хмарних послуг, щоб підвищити стійкість мережі.

Продовження таблиці 4.1

1	2
6. Недостатня сегментація	
Ризик	Неадекватна сегментація мережі може призвести до бічного переміщення зловмисників, дозволяючи їм вільно пересуватися в мережі.
Приклад атаки	У 2013 році сталося порушення безпеки даних Target через недостатню сегментацію мережі. Зловмисники переміщувалися всередині мережі, скомпрометувавши системи торгових точок і викравши інформацію про кредитні картки.
Шляхи пом’якшення	Запровадьте належну сегментацію мережі, щоб ізолювати критичні активи та обмежити вплив потенційного порушення.
7. Уразливості у віртуалізації	
Ризик	Використання вразливостей у платформах віртуалізації може призвести до неавторизованого доступу або зламу віртуальних машин.
Приклад атаки	Уразливість «Venom» у 2015 році вплинула на контролер віртуальних гнучких дисків віртуальних машин, потенційно дозволяючи зловмисникам виходити з віртуальних машин і отримувати доступ до конфіденційних даних у хост-системі.
Шляхи пом’якшення	Регулярно оновлюйте та виправляйте платформи віртуалізації, запроваджуйте належну ізоляцію між віртуальними машинами та дотримуйтесь найкращих практик щодо безпеки гіпервізора.
8. Неправильно налаштовані брандмауери та групи безпеки	
Ризик	Неправильні конфігурації в правилах брандмауера та групах безпеки можуть призвести до несанкціонованого доступу до служб і даних.
Приклад атаки	У 2018 році неправильна конфігурація брандмауера AWS розкрила конфіденційні фінансові дані клієнтів GoDaddy. Неправильно налаштований брандмауер дозволив неавторизований доступ до сегмента S3.
Шляхи пом’якшення	Регулярно перевіряйте та переглядайте конфігурації брандмауера, дотримуйтеся принципу найменших привілеїв і ефективно використовуйте групи безпеки.

Продовження таблиці 4.1

1	2
9. Зловмисні внутрішні загрози	
Ризик	Інсайдери зі зловмисними намірами можуть використати свій доступ для порушення безпеки мережі.
Приклад атаки	У 2021 році колишнього співробітника Tesla звинуватили в зловмисному зміненні коду в системах компанії. Інсайдерська загроза підкреслила ризик неправомірного використання авторизованими особами своїх привілеїв доступу.
Шляхи пом’якшення	Впроваджуйте моніторинг активності користувачів та регулярні тренінги з безпеки та встановлюйте суворий контроль доступу.
10. Залежність від сторонніх постачальників	
Ризик	Покладаючись на сторонніх постачальників мережевих послуг, це створює залежності та потенційні ризики, пов’язані з їхніми заходами безпеки.
Приклад атаки	Атака програми-вимагача NotPetya 2017 року використовувала вразливість стороннього програмного забезпечення (MeDoc), яке широко використовується в Україні. Атака порушила роботу різних організацій, продемонструвавши ризики, пов’язані із залежністю від сторонніх постачальників.
Шляхи пом’якшення	Перевіряйте та вибирайте авторитетних постачальників, проводите регулярні оцінки безпеки та створюйте плани на випадок збоїв у наданні послуг.
11. Безпека постачальника хмарних послуг	
Ризик	Методи безпеки постачальника хмарних послуг, зокрема безпека центру обробки даних, можуть вплинути на загальну безпеку хмарної мережі.
Приклад атаки	У 2020 році неправильна конфігурація в службі зберігання BLOB-об’єктів Microsoft Azure розкрила особисті дані мільйонів клієнтів служби підтримки Microsoft. Неправильна конфігурація дозволила отримати неавторизований доступ до даних.
Шляхи пом’якшення	Виберіть надійного та сумісного постачальника хмарних послуг, ознайомтеся з його заходами безпеки та співпрацюйте, щоб забезпечити безпечне середовище.

Усунення цих ризиків безпеки хмарної мережі вимагає поєднання надійних технічних заходів, постійного моніторингу та дотримання найкращих практик безпеки. Організаціям необхідно прийняти проактивний підхід до безпеки, включаючи регулярні аудити, моніторинг і співпрацю з постачальниками хмарних послуг для забезпечення безпечного мережевого середовища. Регулярні оцінки безпеки та отримання інформації про нові загрози є важливими для підтримки безпечного середовища хмарної мережі.

4.2.Розгортання хмарної інфраструктури AWS

Згідно завданню нам необхідно створити хмарну інфраструктуру, яка відповідає наступним вимогам:

– IP-адреса віртуальної приватної хмари (Virtual Private Cloud - VPC) - 192.168.0.0/16;

– VPC повинна містити загальнодоступну та приватну підмережу;

– кількість вузлів у загальнодоступній підмережі – 300;

– кількість вузлів у приватній підмережі – 100;

– для забезпечення зв’язку з мережею Інтернет необхідно встановити інтернет-шлюз;

– в хмарній інфраструктурі необхідно розгорнути веб-сервер;

– для забезпечення мережної безпеки необхідно створити групи безпеки.

За результатами проведеного аналізу завдання зроблено висновок, що, для реалізації цих вимог, достатньо в хмарній інфраструктурі, що розгортається, використовувати один регіон.

Інформаційна інфраструктура містить такі елементи як вебсервер та база даних. Ці елементи виконують різні функції та мають різни вимоги з точки зору мережних технологій та кібербезпеки.

Вебсервер є інтерфейсом для доступу та обробки даних. Для нього є характерним доступ від великої кількості користувачів та великої кількості IP-адрес. Таким чином, його рекомендується встановлювати територіально ближче до місця концентрації трафіку (розміщення користувачів). Це дозволяє зменшити навантаження на мережні ресурси та покращити параметри якості обслуговування.

Сервер баз даних відповідає за зберігання даних, доступ до нього здійснюється в основному з вузла вебсервера, що значно зменшує як кількість IP-адрес з якими здійснюється обмін, так і навантаження на мережу. З точки зору

кібербезпеки сервер баз даних є критичним елементом цієї інформаційної системи, оскільки пошкодження або компрометація цього елементу може призвести до повної втрати даних. Тому його слід розміщувати в більш захищеному середовищі (з більш обмеженим доступом та в місці подалі від природних катаклізмів, військових конфліктів, нестабільних регіонів, тощо).

Спираючись на вище зазначене, в роботі запропоновано розмістити вебсервер та сервер баз даних в різних зонах доступності (Availability Zone - AZ): вебсервер в AZ, яка територіально наближена до місця концентрації користувачів, а сервер баз даних – у максимально захищеній.

У кожній з цих зон доступності необхідно створити підмережі та відповідні групи безпеки. Так, для вебсервера необхідно дозволити доступ від користувачів за протоколами HTTP та HTTPS, а також за протоколом SSH – для здійснення керування та налаштування віртуальної машини, на якій встановлено вебсервер лише з окремої IP-адреси. Для серверу баз даних необхідно встановити обмеження, щоб доступ був можливий тільки від вебсервера.

Для забезпечення зв’язку з зовнішньою мережею Інтернет створюємо інтернет шлюз (Internet Gateway – IGW). Для веб-сервера створюємо екземпляр віртуальної машини (Elastic Compute Cloud – EC2) на якому необхідно встановити відповідне програмне забезпечення.

Наступною задачею є розрахунок та вибір діапазонів IP-адрес для кожної з підмереж таким чином, щоб виконувалися вимоги щодо їх ємності.

Приватна мережа має містити 100 вузлів (IP-адрес). Для цього достатньо використовувати для частини адреси хоста 7 бітів, що забезпечує 128 комбінацій адрес. В Amazon Web Services деякі IP-адреси в кожній підмережі резервуються для службових потреб (внутрішній маршрутизатор VPC, служба DNS та додаткові адреси, які зарезервовані на майбутнє). Зазвичай резервуються перші чотири та останні дві адреси в кожній підмережі. Тобто із 128 можливих комбінацій можна використовувати для власних цілей лише 122, що більше 100, які необхідно було створити за завданням. Серед зарезервованих комбінацій дві комбінації використовуються як адреси мережі та адреси широкосмугової розсилки, це 192.168.0.128 та 192.168.0.255 (перший містить всі біти – нульові; останній –всі одиниці). Таким чином, IP-адреси: 192.168.0.128, 192.168.0.129, 192.168.0.130, 192.168.0.131, 192.168.0.254 та 192.168.0.255 зарезервовані для службових потреб AWS і не повинні використовуватися для призначення хостам. Інші IP-адреси в діапазоні від 192.168.0.132 до 192.168.0.253 вільні для використання. Тобто

запропоновано використовувати мережу 192.168.0.128/25 та розмістити адреси у вільному діапазоні: 192.168.0.141 – 192.168.0.240.

Відповідно публічна мережа має містити 300 вузлів (IP-адрес). Таким чином, достатньо використовувати для частини адреси хоста 9 бітів, що забезпечує 512 комбінацій адрес. Аналогічно вище розглянутому випадку з цих 512 можливих комбінацій 6 є зарезервованими, і для власних цілей вільними є 506 (що більше 300 необхідних за завданням). Тобто запропоновано використовувати мережу 192.168.2.0/23, де IP-адреси в діапазоні від 192.168.2.3 до 192.168.3.253 є вільні для використання. Для мережі, що розгортається адреси вузлів в діапазоні 192.168.2.10 – 192.168.3.53.

З метою забезпечення доступу зсередини приватної мережі до мережі Інтернет запропоновано встановити шлюз NAT (NAT Gateway). Використання цього елементу забезпечує доступ вузлів з приватної мережі до мережі Інтернет залишаючи ці вузли недоступними з зовнішньої мережі.

Діаграма хмарної інфраструктури AWS представлена на рис. 4.1

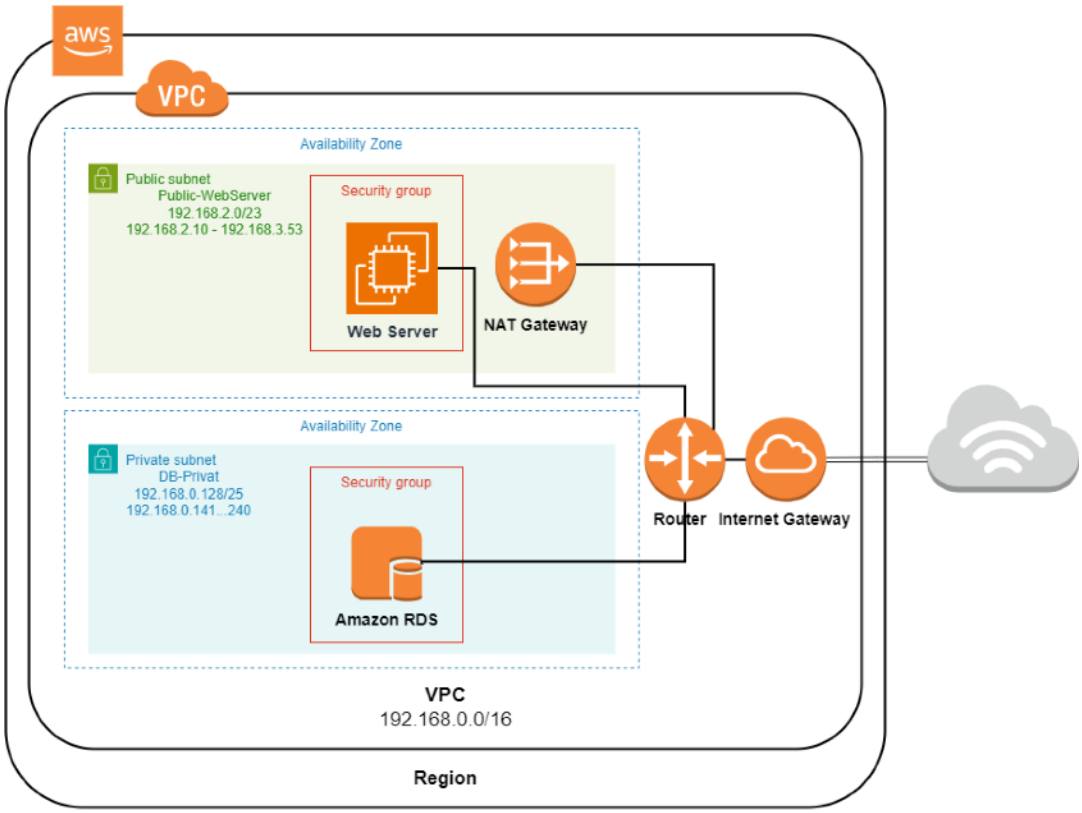


Рисунок 4.1 – Структура хмарної інфраструктури, що розгортається

Для розгортання описаної інфраструктури необхідно зробити наступне:

– створити віртуальну приватну хмару;

– створити публічну та приватну підмережу;

– створити інтернет шлюз та приєднати його до віртуальної приватної хмари;

– створити та налаштувати шлюз NAT;

– створити та налаштувати таблиці маршрутизації, приєднати їх до підмереж;

– створити та налаштувати групи безпеки;

– створити, налаштувати за запустити віртуальну машину EC2 для вебсерверу у публічній мережі;

– створити, налаштувати за запустити екземпляр серверу баз даних (Amazon RDS).

Для створення віртуальної приватної хмари необхідно відкрити консоль «Amazon VPC», встановити необхідний регіон (US East (N.Virginia)) та тиснути «Create VPC». У панель, яка з'явиться на екрані (рис. 4.2) ввести:

– ім'я віртуальної приватної хмари – WebServer-RDS;

– налаштування діапазону IP-адрес.

Інші параметри залишити за умовчанням.

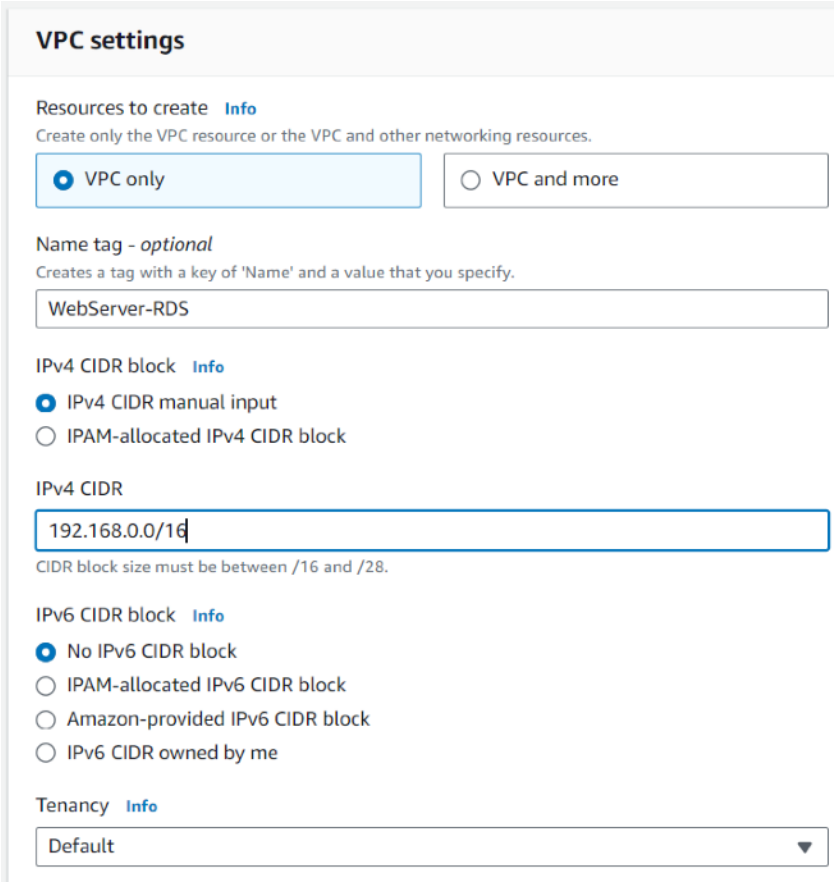


Рисунок 4.2 – Панель створення віртуальної приватної мережі

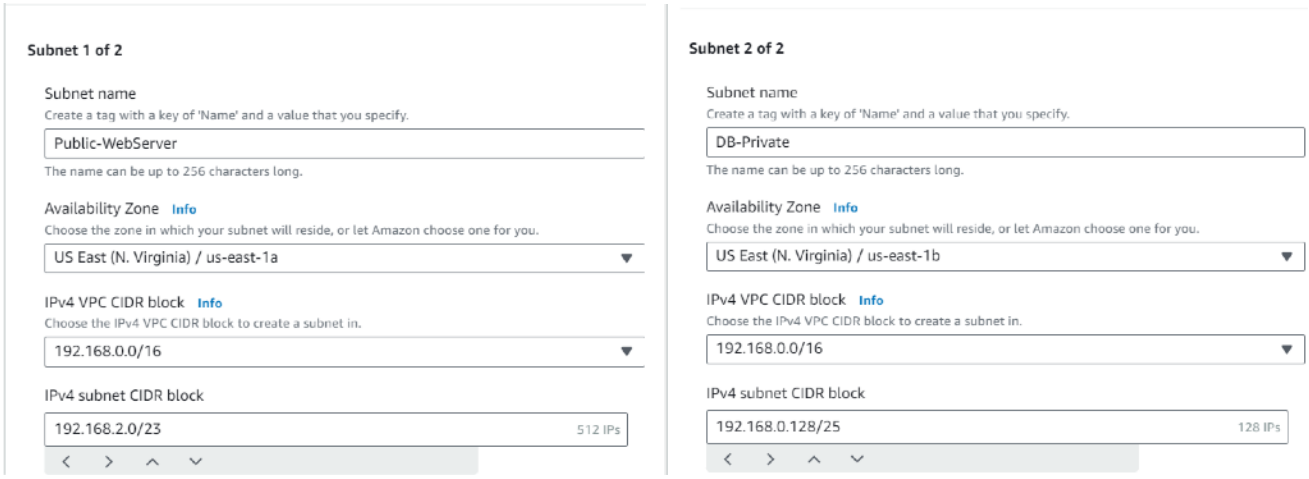
Для створення публічної та приватної підмережи необхідно відкрити консоль «Subnets» та натиснути «Create subnet». У панелі, яка з’явиться на екрані необхідно зробити:

– в полі «VPC ID» (рис. 4.3) вибрати ім’я віртуальної приватної хмари – WebServer-RDS;

– в панелі налаштування параметрів підмережі (рис. 4.4,а) необхідно: вказати ім’я підмережі – «Public-WebServer»; обрати зону доступності – «US East (N.Virginia) / us-east-1a» та налаштування діапазону IP-адрес – 192.168.2.0/23;

– натиснути «Add new subnet» та у панелі, що з’явиться (рис. 4.4,б) вказати аналогічні параметри для приватної мережі: ім’я підмережі – «DB-Private»; зону доступності – «US East (N.Virginia) / us-east-1b» та налаштування діапазону IP-адрес – 192.168.0.128/25.

Рисунок 4.3 – Поле вибору VPC ID



а) б)

Рисунок 4.4 – Панель налаштування підмереж

Як результат у віртуальній приватні хмарі буде створено публічна та приватна підмережа у різних зонах доступності (рис. 4.5).

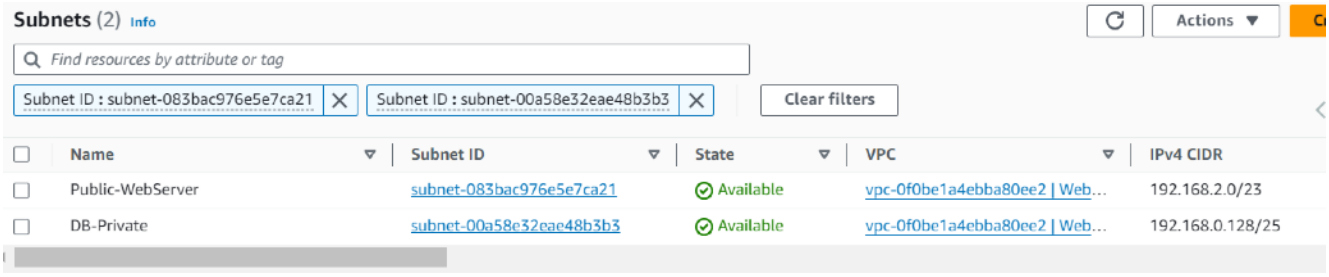
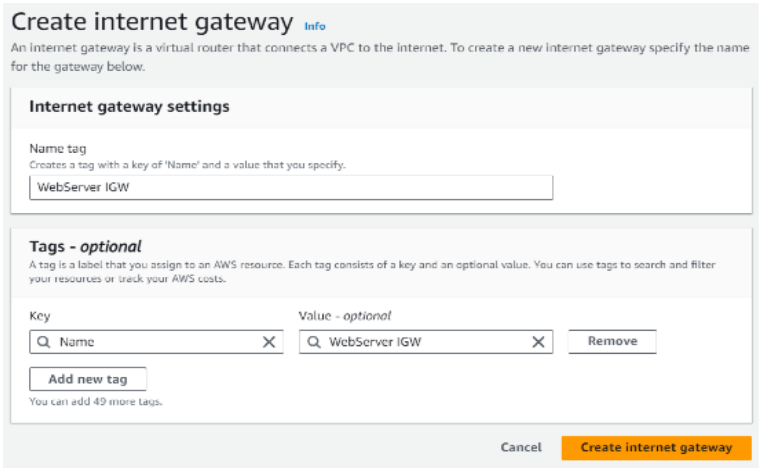


Рисунок 4.5 – Підмережі, що були створені

Для створення інтернет шлюзу необхідно відкрити консоль «Internet gateways» та натиснути «Create internet gateway». У панелі, яка з'явиться на екрані (рис. 4.6,а) необхідно вказати ім'я інтернет шлюзу – «WebServer IGW» та натиснути «Create internet gateway». Наступним кроком необхідно приєднати інтернет шлюз до віртуальної приватної хмари. Для цього необхідно натиснути «Actions» та в меню обрати пункт «Attach to VPC». В панелі на екрані (рис. 4.6,б) для параметру «Available VPC» вибрати ім'я віртуальної приватної хмари – WebServer-RDS.



а)

б)

Рисунок 4.6 – Створення та приєднання інтернет шлюзу

Для створення шлюзу NAT необхідно відкрити консоль «NAT gateways» та натиснути «Create NAT gateway». У панелі, яка з'явиться на екрані (рис. 4.7) необхідно:

– вказати ім'я шлюзу NAT – Public-NAT_GW;

– обрати підмережу в якої буде встановлено шлюз – Public-WebServer;

– вказати тип з'єднання – Public;

– натиснути кнопку «Allocate Elastic IP» щоб створити новий екземпляр виділеної публічної IP-адреси;

– натиснути кнопку «Create NAT gateway».

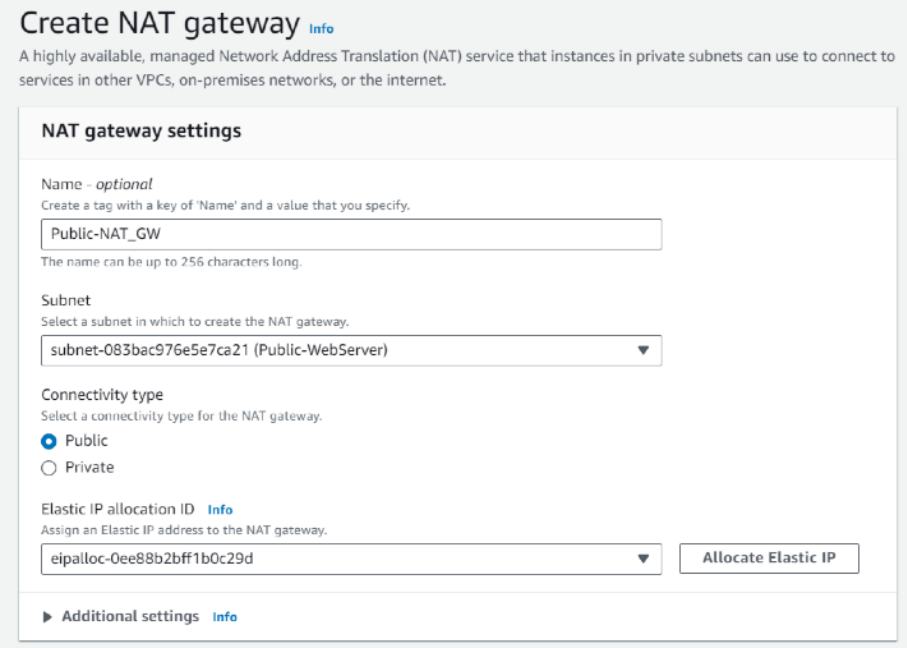
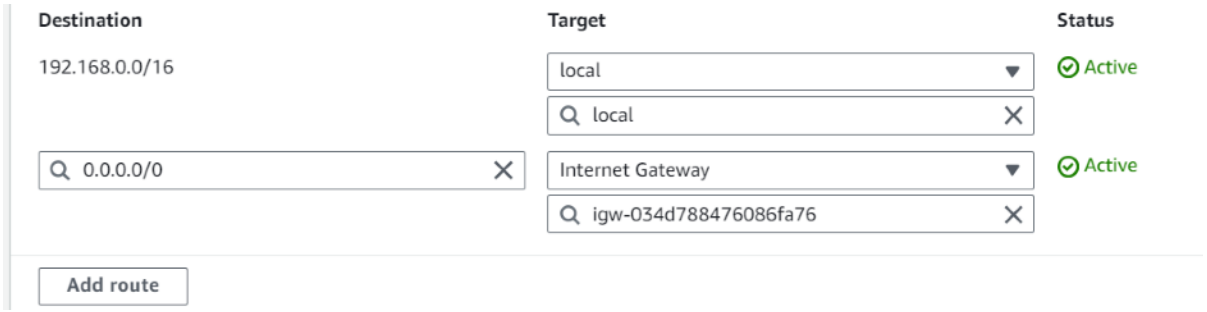


Рисунок 4.7 – Панель створення та налаштування шлюзу NAT

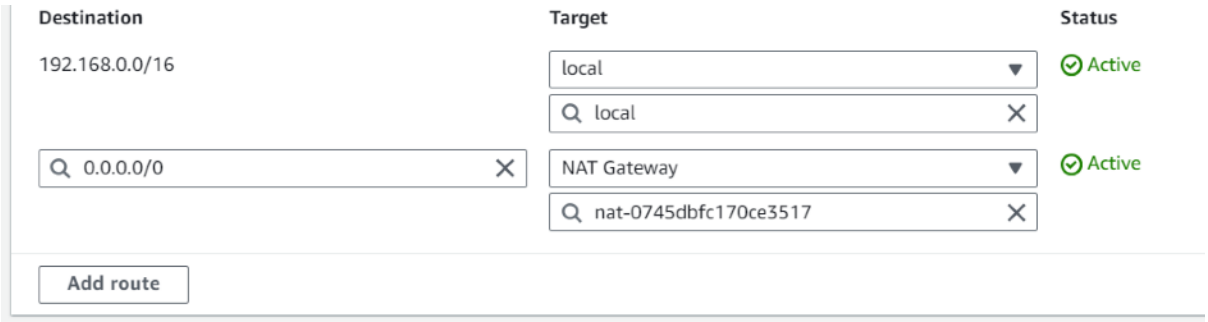
Наступним кроком створено таблиці маршрутизації для публічної та приватної мережі. Для цього в консолі «Route tables» необхідно створити таблиці маршрутизації натиснувши кнопку «Create route table». Для кожної таблиці маршрутизації необхідно вказати ім'я: «Public-Subnet» та «Privat-Subnet» відповідно.

Налаштування таблиць маршрутизації здійснюється як наведено на рис. 4.8.

Для таблиці маршрутизації публічної мережі необхідно додати шлях до інтернет шлюзу для всіх IP-адрес за межами віртуальної приватної хмари (рис. 4.8,а), а для таблиці маршрутизації приватної мережі необхідно додати шлях до шлюзу NAT (рис. 4.8,б).



а)



б)

Рисунок 4.8 – Панелі налаштування таблиць маршрутизації

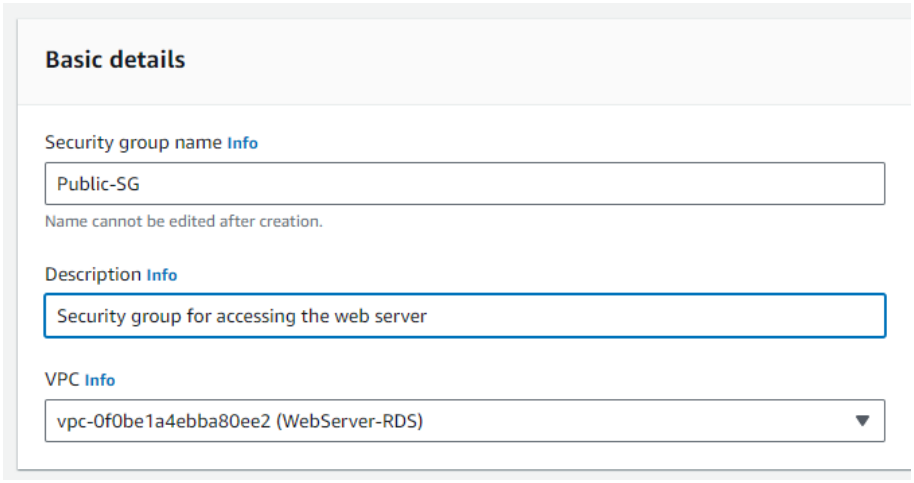
Далі створено групи безпеки для вебсерверу та серверу баз даних. Для цього необхідно відкрити консоль «Security groups» та натиснути «Create security group». У панелі, яка з’явиться на екрані (рис. 4.9) необхідно:

– вказати ім’я групи безпеки – Public-SG;

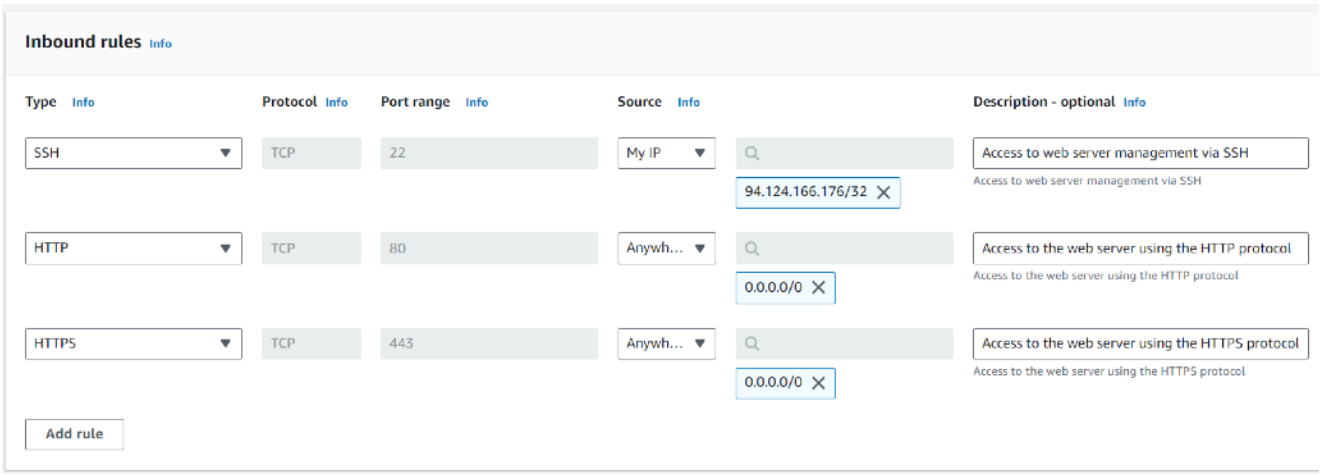
– задати опис для групи безпеки в полі «Description»;

– в полі «VPC» (рис. 4.9,а) вибрати ім’я віртуальної приватної хмари – WebServer-RDS.

За допомогою кнопки «Add rule» необхідно додати правила (рис. 4.9,б) доступу від користувачів за протоколами HTTP та HTTPS, вказавши в якості IP-адреси джерела – 0.0.0.0/0, що відповідає будь-якому адресу. Далі необхідно додати правило, яке дозволяє доступ за протоколом SSH для здійснення керування та налаштування віртуальної машини, на якій встановлено вебсервер. Цей доступ необхідно налаштувати таким чином, щоб обмежити можливість керування лише з окремої IP-адреси (94.124.166.176/32). Правило для вихідного трафіку залишити без змін.



а)



б)

Рисунок 4.9 – Панель налаштування групи безпеки для вебсерверу

Під час створення групи безпеки для серверу баз даних (рис. 4.10) необхідно:

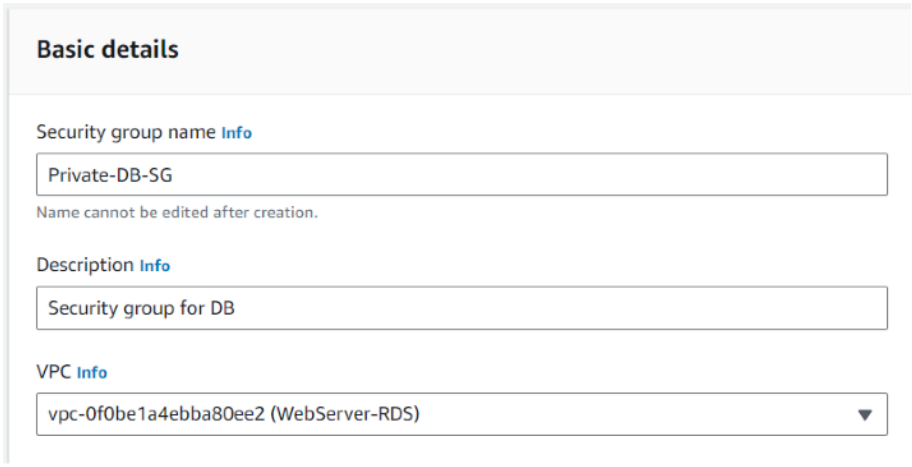
– вказати ім’я групи безпеки – Private-DB-SG;

– задати опис для групи безпеки в полі «Description»;

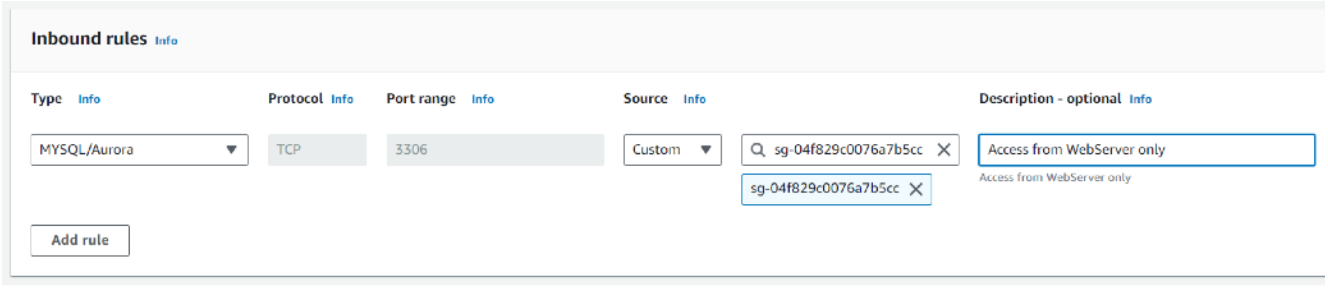
– в полі «VPC» (рис. 4.10,а) вибрати ім’я віртуальної приватної хмари – WebServer-RDS.

За допомогою кнопки «Add rule» необхідно додати правило для вхідного трафіку (рис. 4.10,б) щоб доступ був можливий тільки від вебсерверу. Для цього необхідно в полі «Type» вибрати протокол – MySQL/Aurora, а в якості джерела вказати групу безпеки – Public-SG (яка відповідає вебсерверу).

Правило для вихідного трафіку залишити без змін.



а)



б)

Рисунок 4.10 – Панель налаштування групи безпеки для сервера баз даних

На останньому етапі створено екземпляри віртуальної машини для вебсерверу та екземпляр серверу бази даних.

Створення екземпляру віртуальної машини EC2 здійснено наступним чином.

В консолі «Amazon EC2» необхідно натиснути «Launch instance». В панелі, що з’явиться необхідно вказати ім’я екземпляру – WebServer (рис. 4.11).

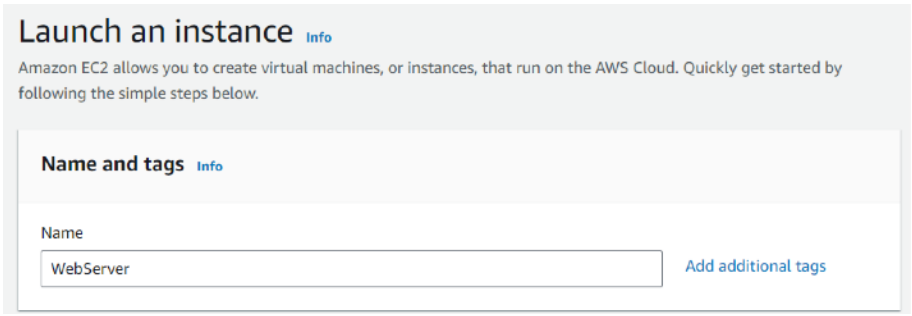


Рисунок 4.11 – Налаштування імені екземпляру EC2

В панелі «Under Application and OS Images (Amazon Machine Image)» (рис. 4.12), необхідно вибрати – Amazon Linux, а потім обрати – Amazon Linux 2023 AMI. Інші параметри в цій панелі залишити без змін.

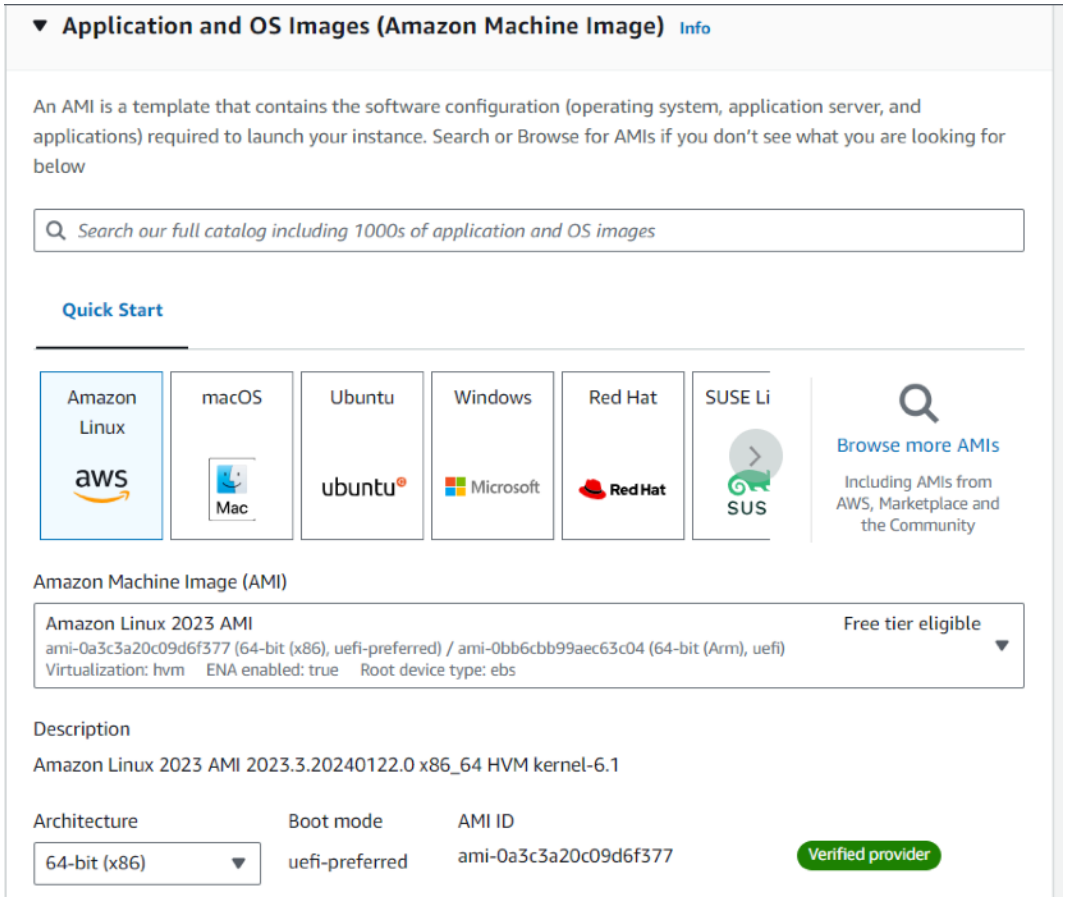


Рисунок 4.12 – Налаштування операційної системи віртуальної машини

На панелі «Under Instance type» (рис. 4.13) необхідно обрати – t2.micro, а в панелі «Key pair (login)» обрати – Diplom-Keys, який був створений раніше.

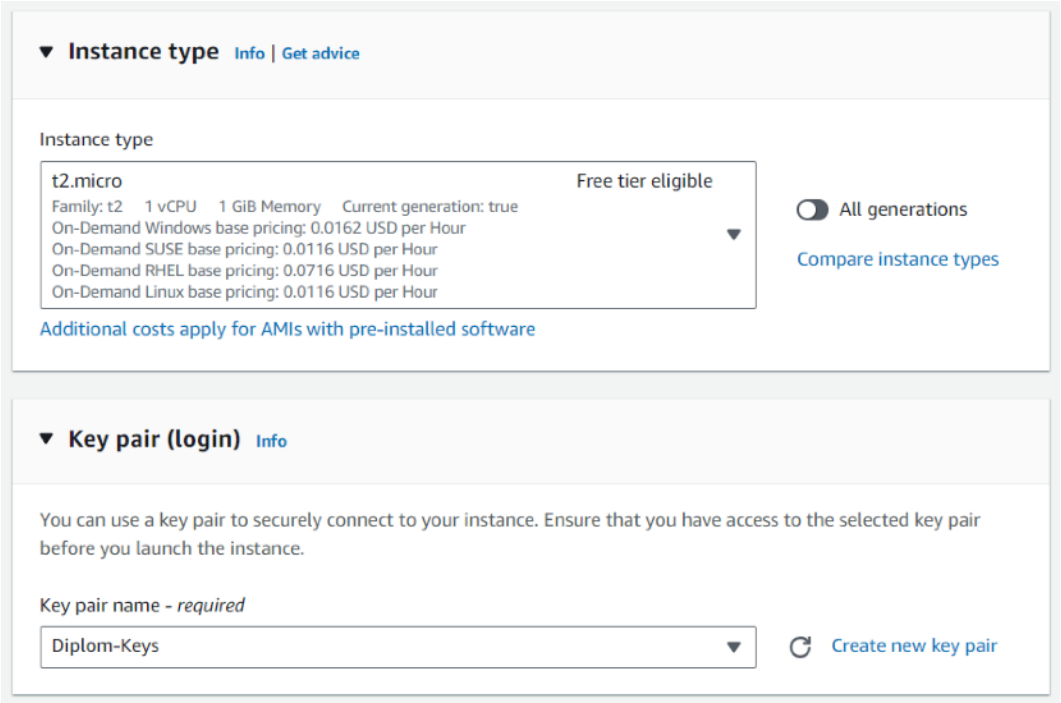


Рисунок 4.13 – Налаштування типу екземпляру та секретного ключа безпеки

На панелі «Network settings» (рис. 4.14), необхідно зробити наступні налаштування:

– в полі «VPC» обрати ім’я віртуальної приватної хмари – WebServer-RDS;

– вказати підмережу в якій буде створений екземпляр EC2, для цього в полі «Subnet» необхідно вказати ім’я публічної мережі – Public-WebServer;

– дозволити автоматичне призначення публічної IP-адреси, обравши «Enable» у полі «Auto-assign public IP»;

– обрати пункт «Select exesting security group», щоб можна було призначити екземпляру, який створюється існуючу групу безпеки для вебсерверу – Public-SG.

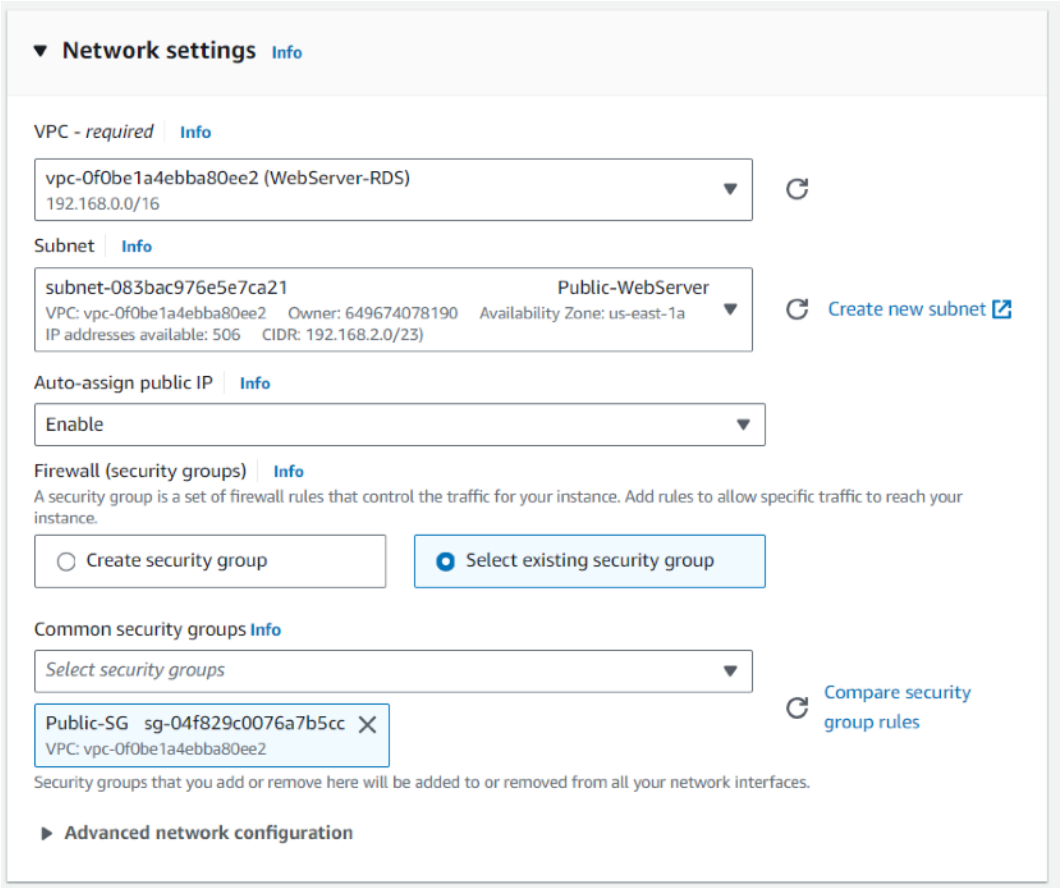


Рисунок 4.14 – Мережні налаштування екземпляру EC2

Створення екземпляру серверу баз даних здійснено наступним чином.

В консолі «Databases» натиснути «Create database» та в панелі, що з’явиться необхідно обрати – Standard create (рис. 4.15) та обрати тип бази даних – MySQL.

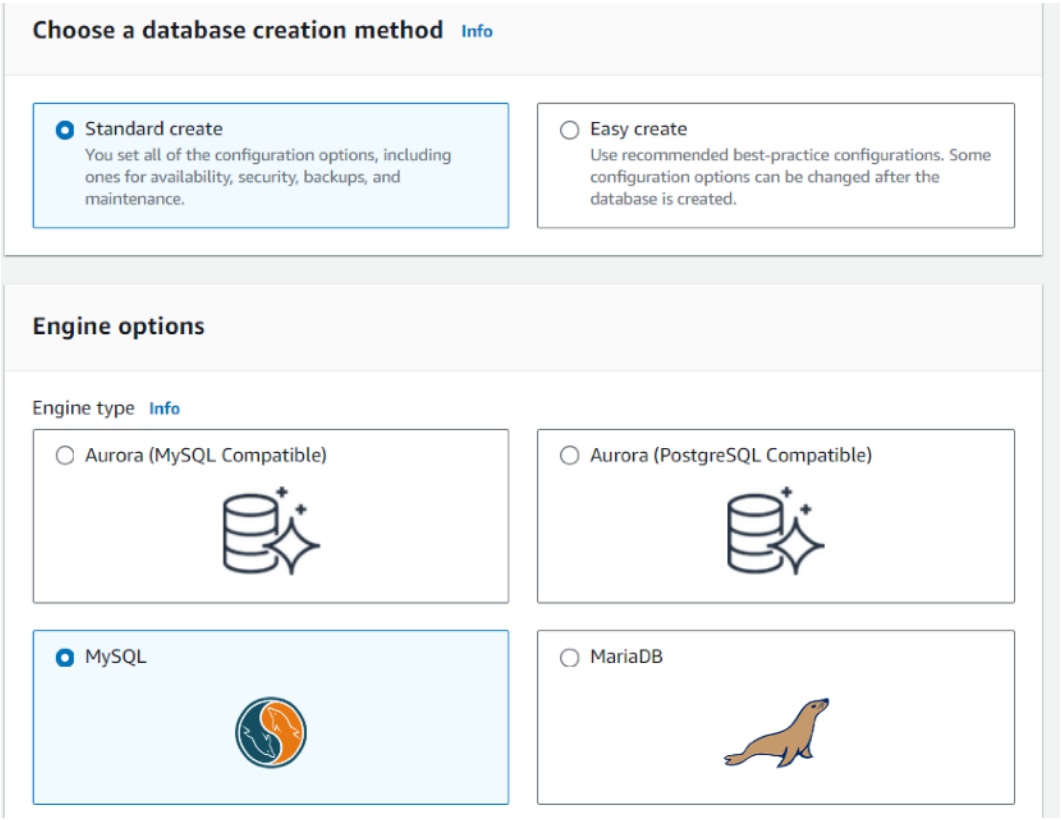


Рисунок 4.15 – Початкова панель створення серверу баз даних

В якості шаблону бази даних обирати – Free tier (рис. 4.16)

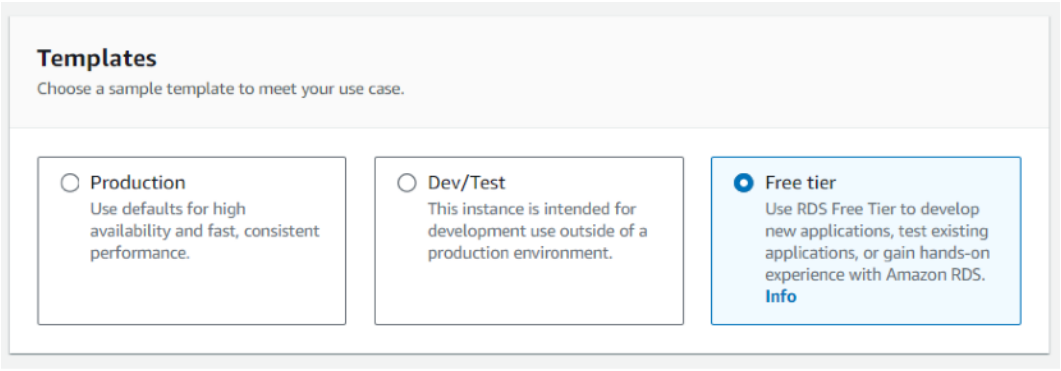


Рисунок 4.16 – Панель шаблону бази даних

В секції «Settings» (рис. 4.17) необхідно встановити:

– ідентифікатор бази даних вказавши в полі «DB instance identifier» – WebServer-DB;

– в полі «Master username» вказати ідентифікатор користувача – admin;

– поле «Auto generate a password» залишити не відміченим;

– в полях «Master password» та «Confirm password» – ввести та підтвердити пароль доступу.

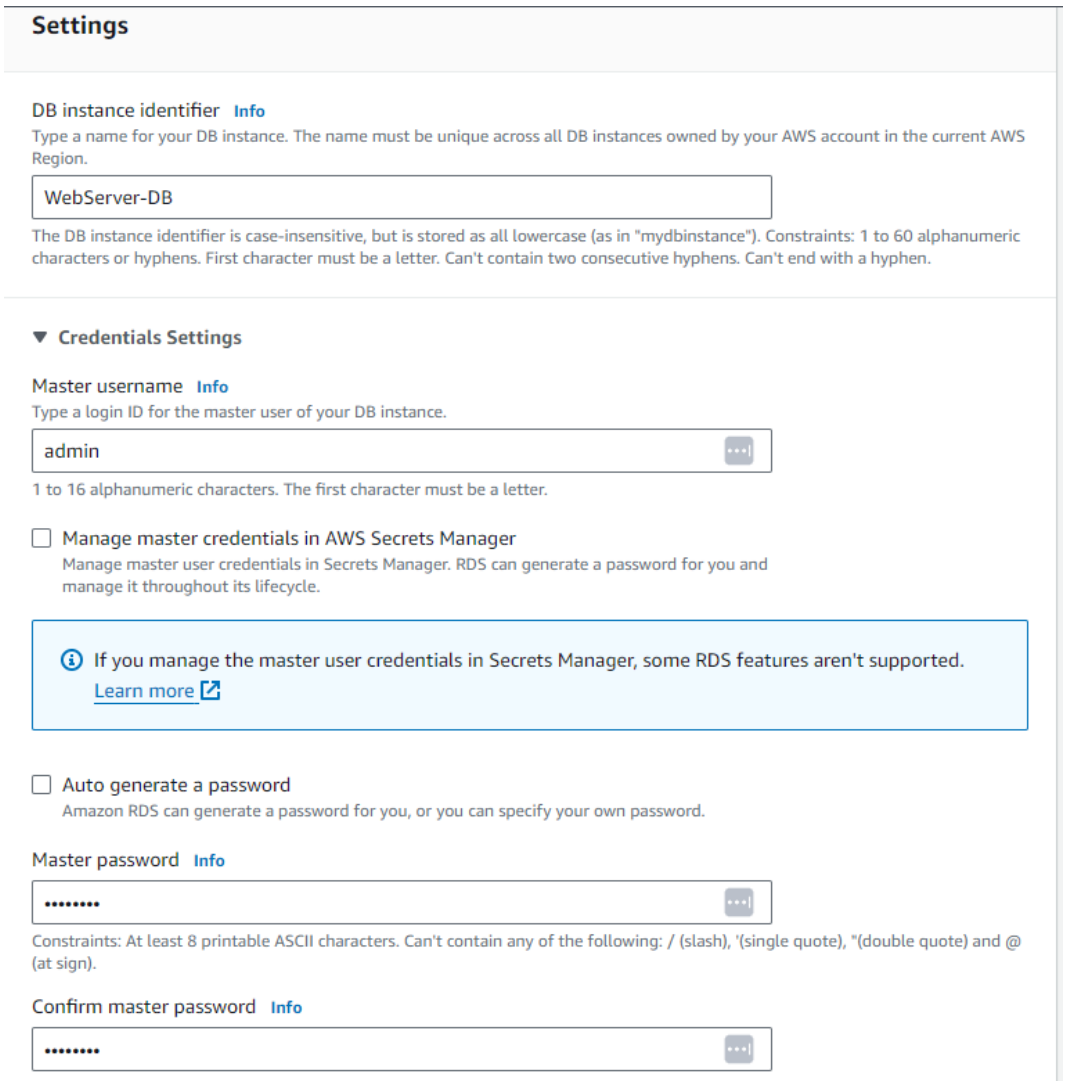


Рисунок 4.17 – Секція налаштувань серверу баз даних

В секції конфігурації екземпляру бази даних (рис. 4.18) необхідно в полі «Burstable classes (includes t classes)» встановити значення – db.t3.micro.

В секції «Connectivity» (рис. 4.19) обрати опцію «Don`t connect to an EC2 compute resource», що дозволяє здійснити ці налаштування вручну та зробити наступні налаштування:

– в полі «Virtual private cloud (VPC)» вказати віртуальну приватну хмару – WebServer-RDS;

– в полі «DB Subnet Group» дозволити автоматичне створення групи підмереж, обравши опцію – Create new DB Subnet Group;

– заборонити публічний доступ до бази даних обравши в полі «Public access» опцію – No.

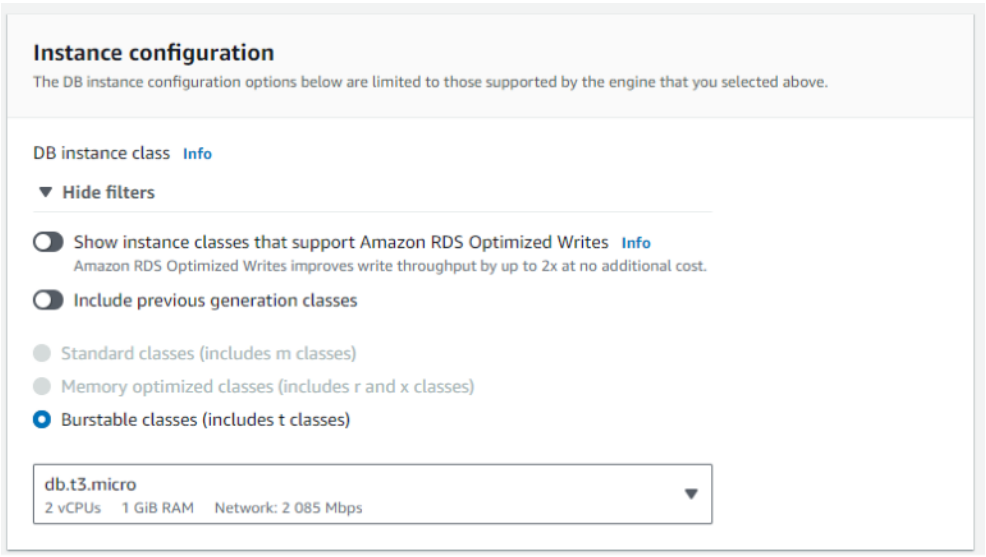


Рисунок 4.18 – Секція конфігурації екземпляру бази даних

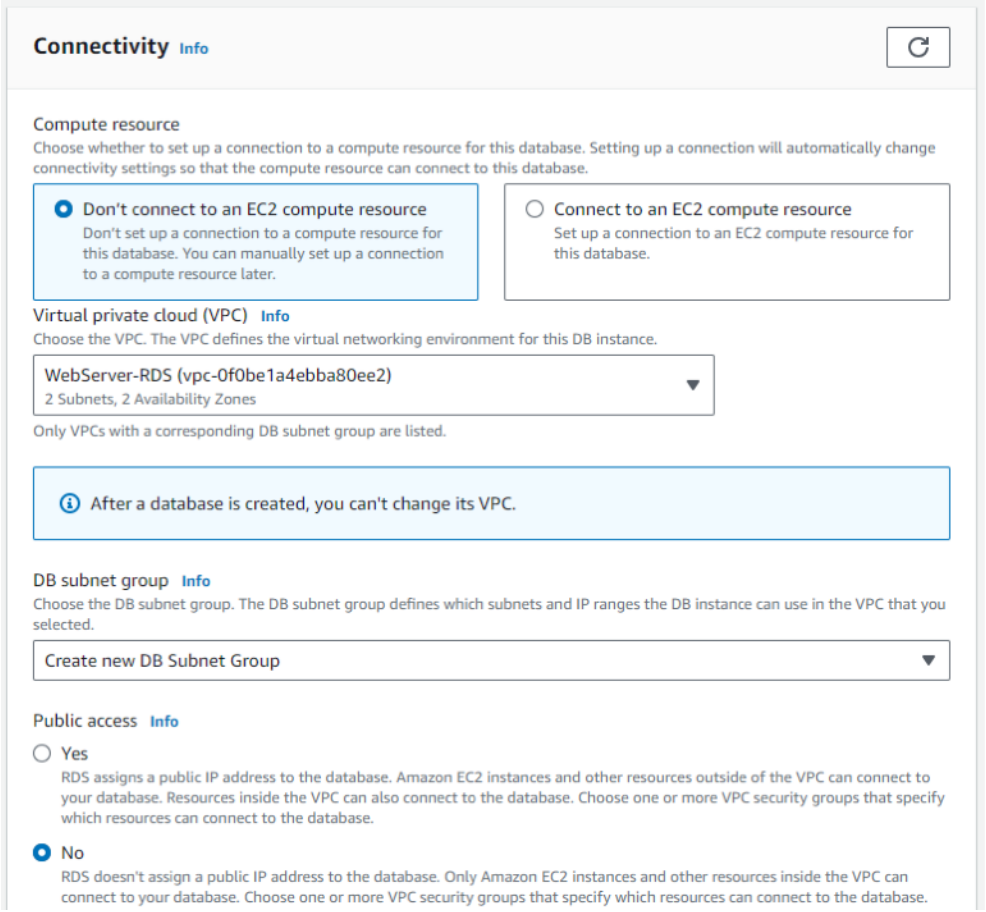


Рисунок 4.19 – Секція конфігурування з’єднання

Далі необхідно приєднати до екземпляру бази даних існуючу групу безпеки – Private-DB-SG та вказати зону доступності – us-east-1b (рис. 4.20). Інші параметри у секції залишити без змін.

В секції «Database authentication» обрати опцію – Password authentication (рис. 4.21).

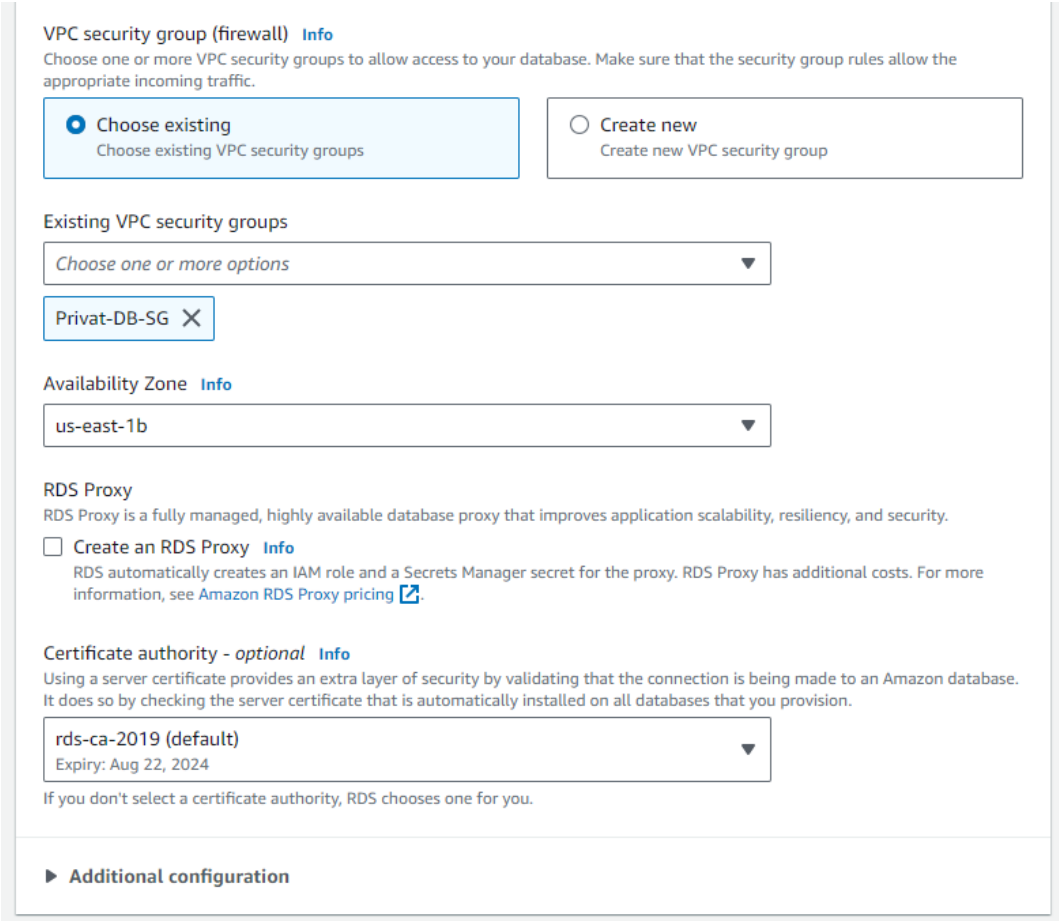


Рисунок 4.20 – Налаштування безпеки у секції конфігурування з’єднання

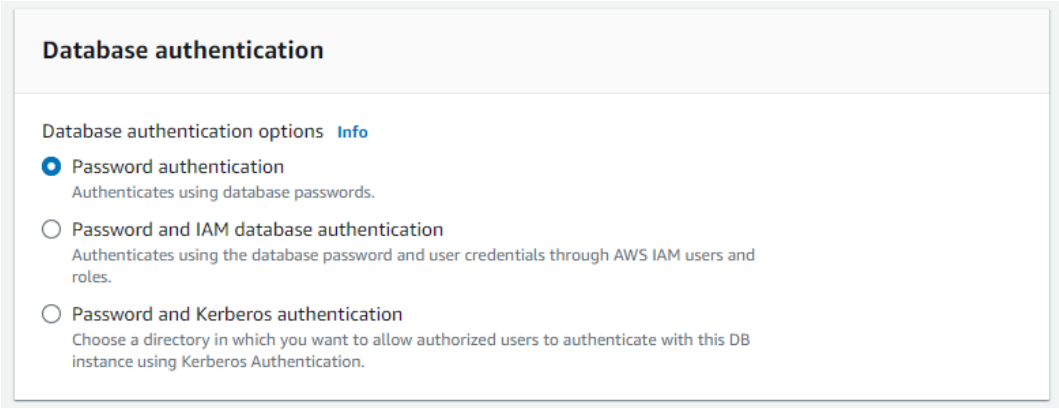


Рисунок 4.21 – Секція конфігурування аутентифікації бази даних

В секції додаткових конфігурацій (рис. 4.22) вказати початкове ім’я бази даних – WebServer. Інші параметри залишити без змін та натиснути кнопку «Create database» щоб створити та запустити екземпляр серверу баз даних.

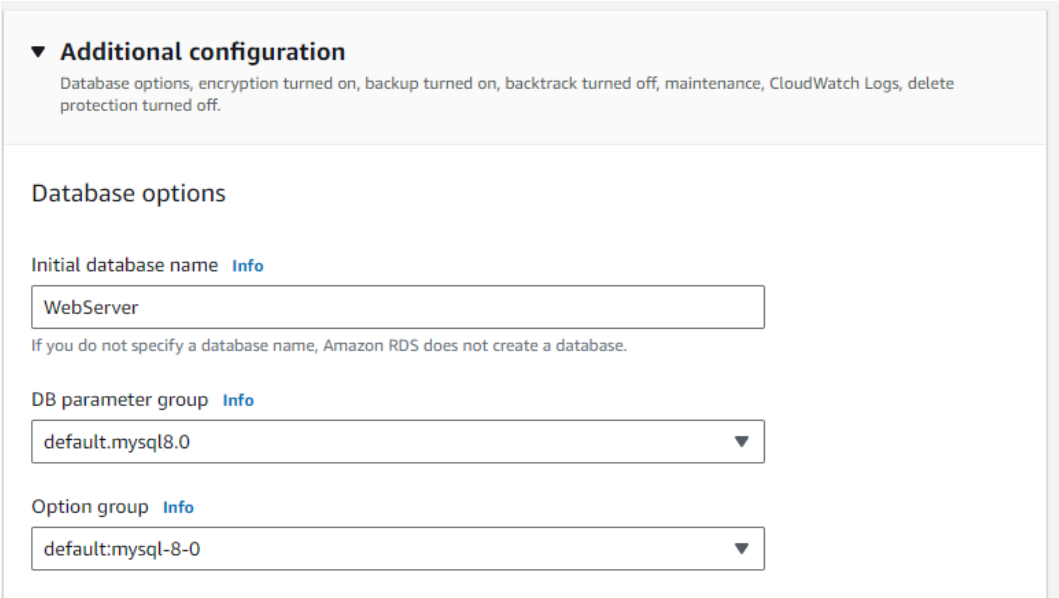


Рисунок 4.22 – Секція додаткових конфігурацій

Наведений вище опис дозволяє створити необхідну інформаційну інфраструктуру у хмарі AWS, яка відповідає вимогам вказаних у завданні.

Після створення інфраструктури необхідно здійснити перевірку налаштувань та зв'язності. Спочатку необхідно з'ясувати публічну IP-адресу вебсерверу, яку можна знайти в консолі «Amazon EC2» (рис. 4.23) у полу «Public IPv4 address» - це 23.20.9.134.

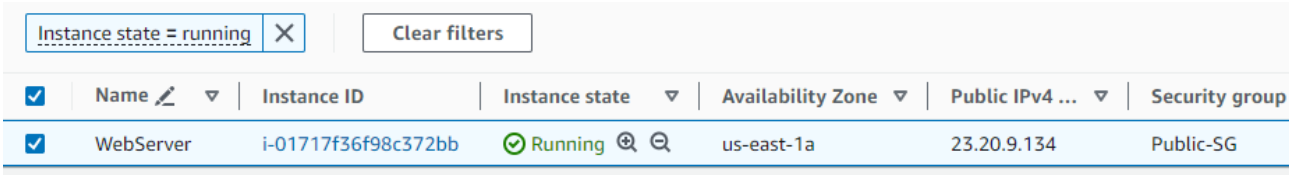


Рисунок 4.23 – Інформація з параметрами екземпляру вебсерверу

Наступним кроком необхідно перевірити власну IP-адресу скориставшись ресурсом – https://myip.ms/ (рис. 4.24). Визначена ресурсом IP-адреса співпадає з IP-адресою вказаною в налаштуваннях групи безпеки вебсерверу.

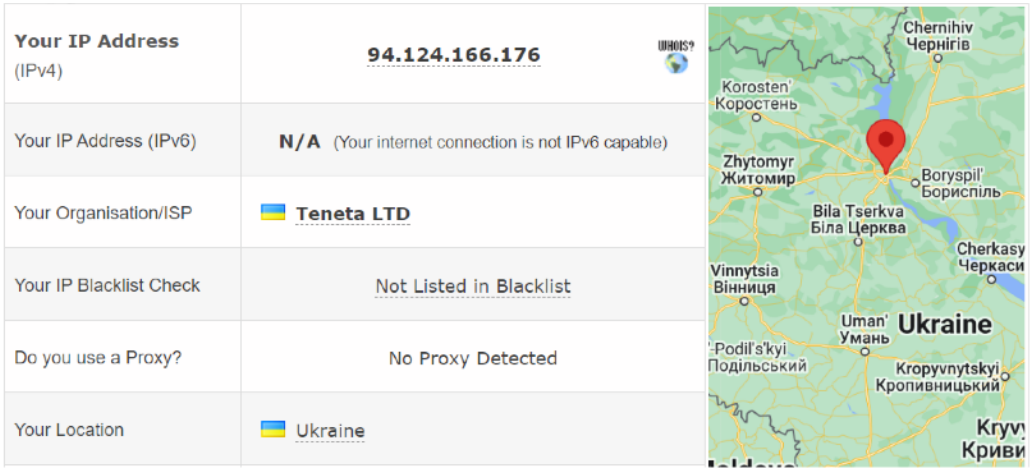
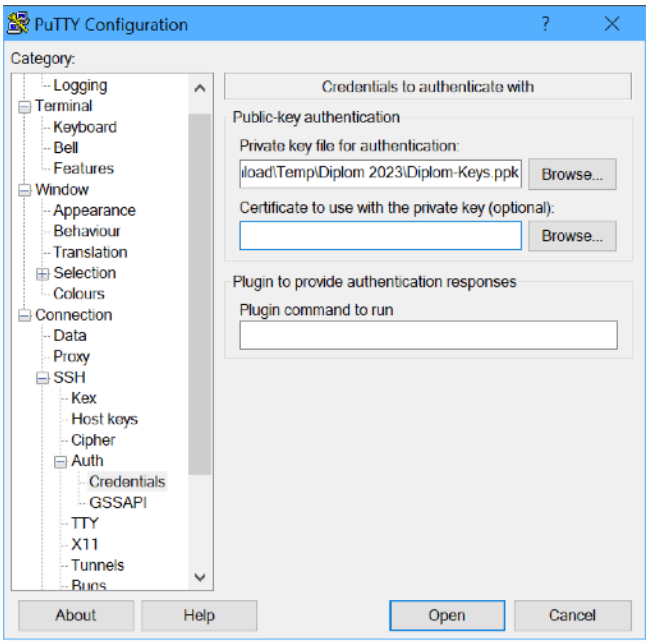


Рисунок 4.24 – Визначення власної IP-адреси

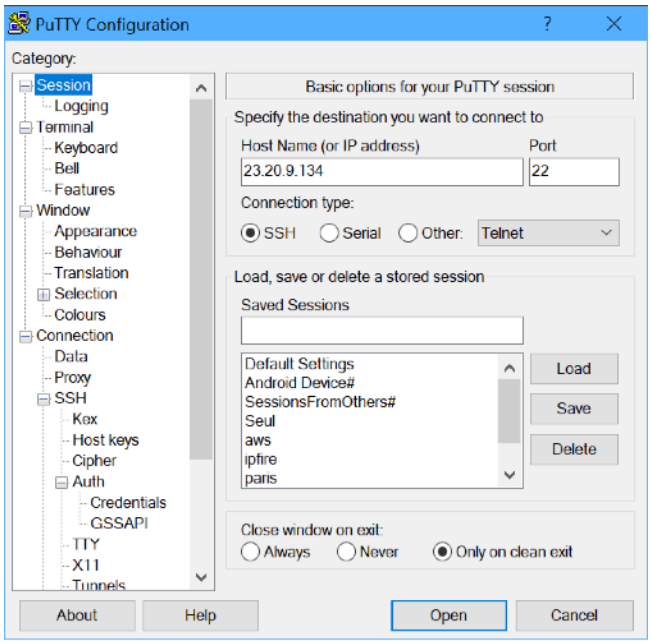
Для приєднання до вебсерверу за протоколом SSH необхідно запустити термінал PuTTY (або інший SSH-клієнт), відкрити панель автентифікації (рис. 4.25,а) та вказати файл з ключем – Diplom-Keys.ppk. На панелі з параметрами з'єднання (рис. 4.25,б) вказати публічну адресу вебсерверу – 23.20.9.134 та натиснути кнопку «Open».

Повинно здійснитися з'єднання з вебсервером (рис. 4.26) за протоколом SSH та запитати логін користувача. Необхідно ввести – ec2-user.

Успішність цих операцій вказує на доступність вебсерверу для керування за протоколом SSH. Необхідно завершити з'єднання ввівши в термінал команду – exit.



а)



б)

Рисунок 4.25 – Налаштування терміналу PuTTY

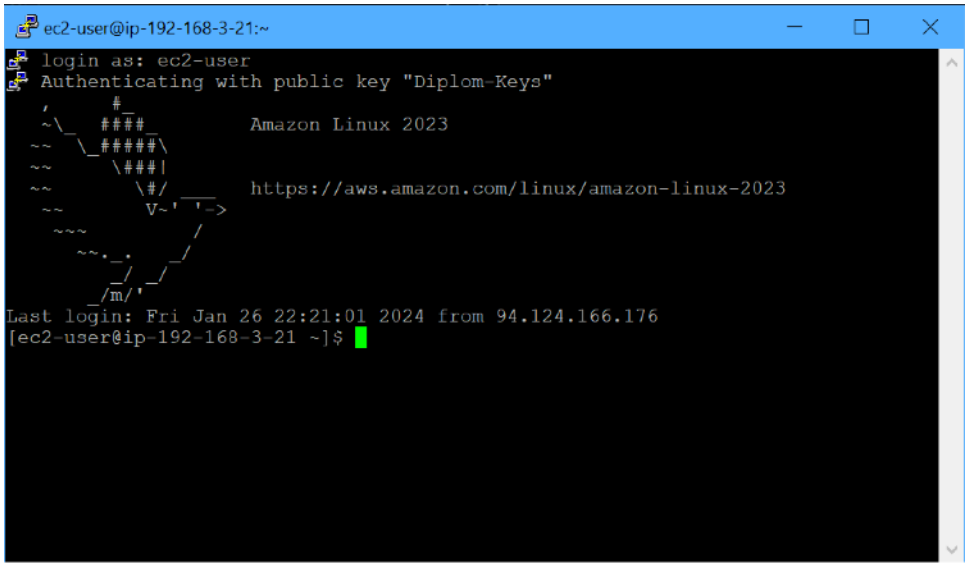


Рисунок 4.26 – Вікно терміналу PuTTY після вдалого з’єднання

Далі необхідно перевірити доступність вебсерверу з іншої IP-адреси. Для того щоб змінити власну IP-адресу з якої здійснюється з’єднання можна скористуватися VPN-сервісом. Необхідно встановити VPN-з’єднання та знову перевірити власну IP-адресу за допомогою ресурсу https://myip.ms/ (рис. 4.27).

З рисунку 4.27 можна визначити, що після встановлення VPN-з’єднання IP-адреса з якої здійснюється з’єднання змінилася та не співпадає з IP-адресою вказаною в налаштуваннях групи безпеки вебсерверу.

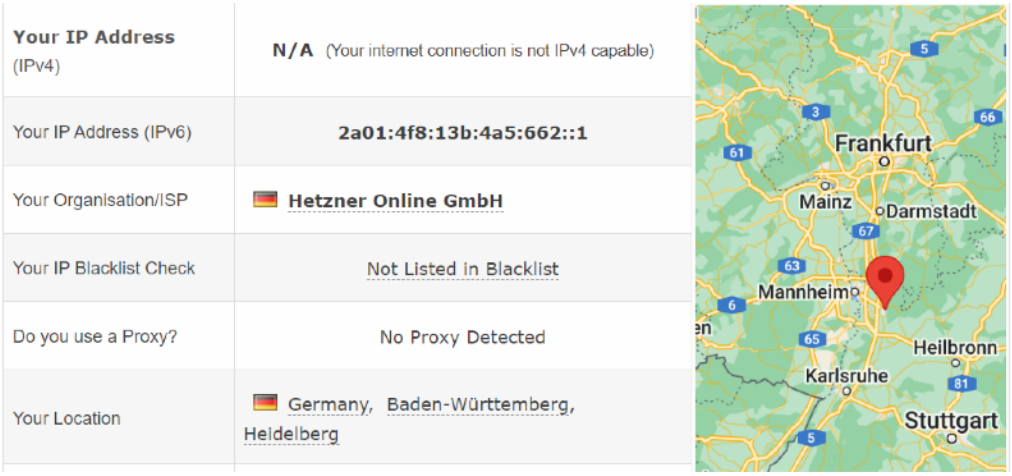


Рисунок 4.27 – Визначення власної IP-адреси після встановлення VPN-з’єднання

Необхідно знову спробувати встановити з’єднання з вебсервером за протоколом SSH за допомогою терміналу PuTTY (або іншого). Після зміни IP-

адреси (встановлення VPN-з’єднання) з’єднання з вебсервером повинно бути невдалим (рис. 4.28). Необхідно вимкнути VPN-з’єднання.

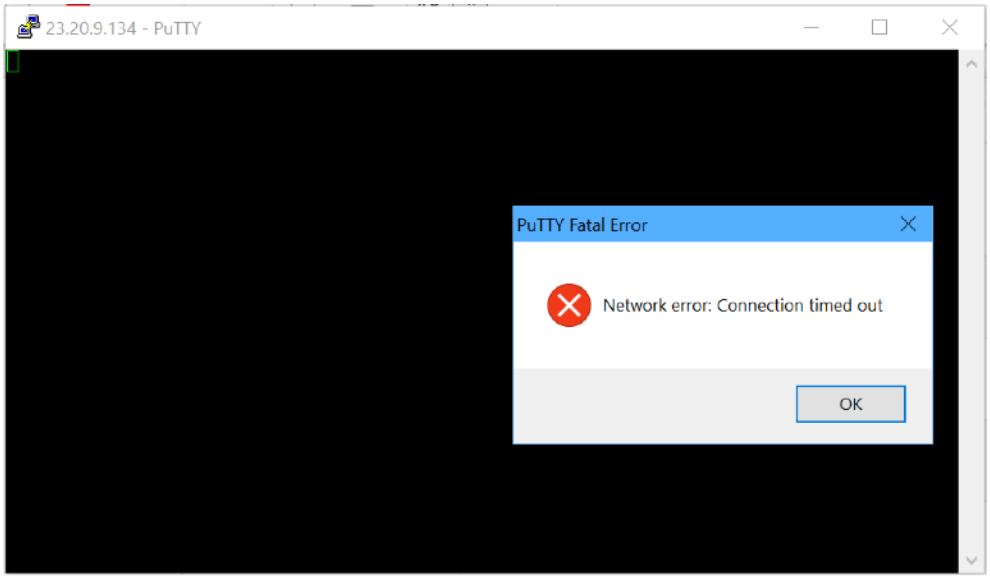


Рисунок 4.28 - Вікно терміналу PuTTY після невдалого з’єднання

Якщо з’єднання без використання VPN є вдалим, а з використанням VPN – невдалим, то це свідчить про коректність налаштувань групи безпеки вебсерверу, яке дозволяє з’єднання за протоколом SSH.

Далі необхідно перевірити можливість доступу вебсерверу до зовнішньої мережі. Для цього необхідно знов з’єднатися з вебсервером за допомогою терміналу PuTTY при вимкненому VPN-з’єднанню. Після входу, необхідно протестувати за допомогою ping доступність будь-якою зовнішньої IP-адреси, наприклад – 8.8.8.8. Для цього до терміналу необхідно ввести команду – ping 8.8.8.8 (рис. 4.29)

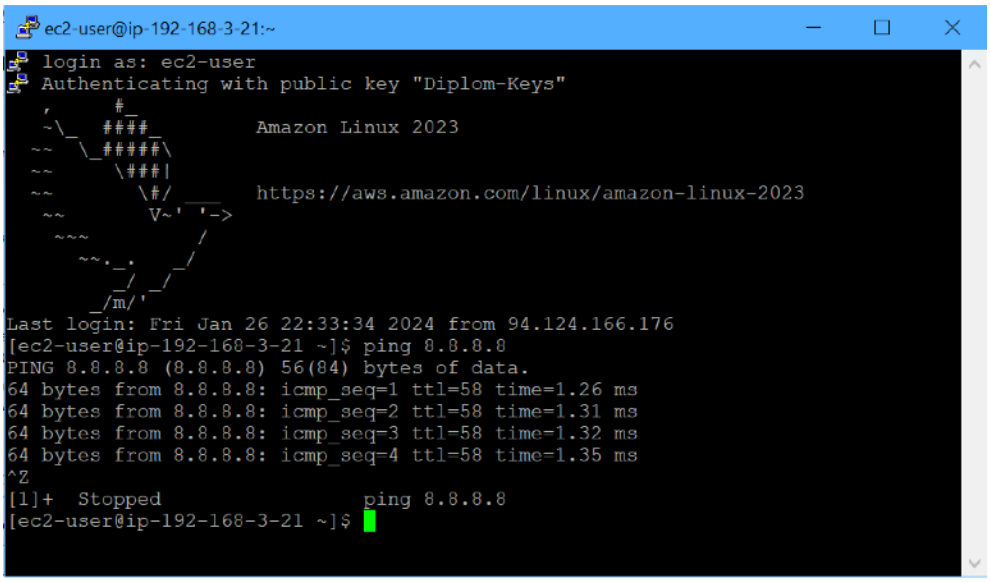


Рисунок 4.29 – Тестування доступу до зовнішньої мережі

Наявність відповідей вказує на наявність доступу до зовнішньої мережі для вебсервера.

Далі необхідно перевірити можливість доступу до вебсерверу зі зовнішньої мережі та коректність його налаштувань. Для цього необхідно відкрити веббраузер та в поле адреси ввести адресу – http://23.20.9.134/ (рис. 4.30).

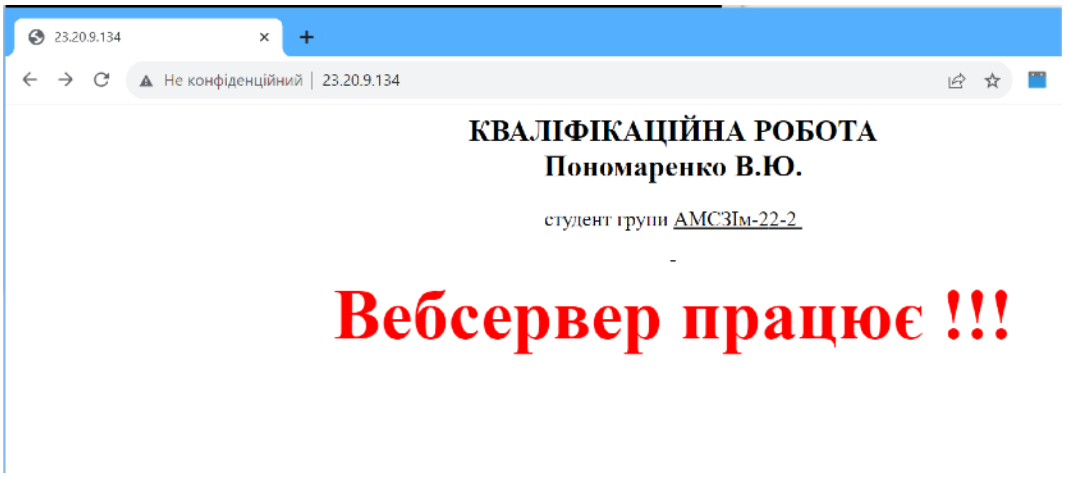


Рисунок 4.30 – Тестова сторінка вебсерверу

Повинно з’явитися тестова сторінка, що вказує на доступність вебсерверу та коректне його налаштування.

Наступним необхідно протестувати наявність доступу від вебсервера до серверу баз даних Amazon RDS. Для цього в поле адреси ввести адресу – http://23.20.9.134/SamplePage.php (рис. 4.31). В вікні веббраузера повинно з’явитися сторінка з інформацією з серверу баз даних. Необхідно спробувати додати до бази даних додатковий запис, який після заповнення полів та натискання кнопки «Add Data» відобразитися на сторінці у таблиці. Якщо ця операція буде вдалою, то це свідчить про доступність серверу баз даних та його коректне налаштування.

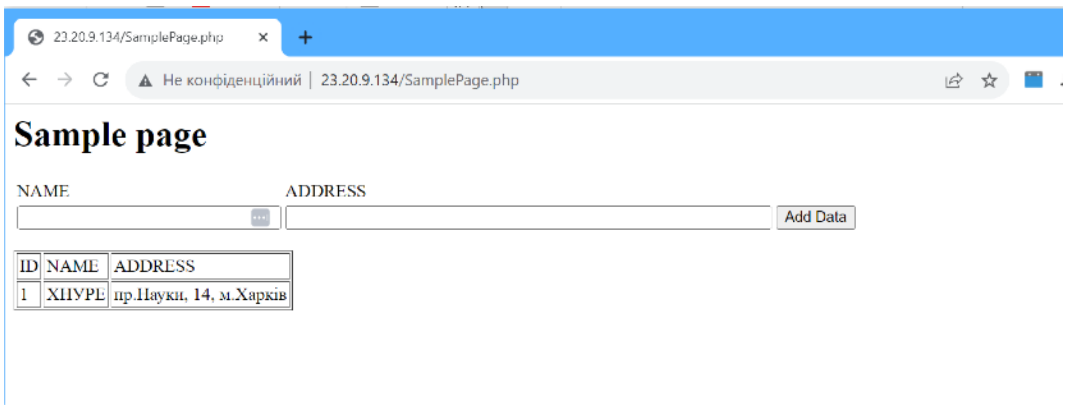


Рисунок 4.31 – Сторінка з’єднання з сервером баз даних

Якщо всі описані тести будуть вдалими, то це свідчить про коректне налаштування груп безпеки, таблиць маршрутизації та інших налаштувань хмарної інфраструктури.

4.3.Дослідження ймовірності компрометації повідомлення у хмарній інфраструктурі AWS

4.3.1. Використання багатошляхової маршрутизації для підвищення конфіденційності передачі повідомлень у хмарній інфраструктурі.

Створена інформаційна інфраструктура містить віртуальні елементи які забезпечують обмін повідомленнями між іншими компонентами хмарної інфраструктури. Ці зв’язки є логічними та спираються на фізичну мережну інфраструктуру, яка передає ці повідомлення між територіально розподіленими компонентами фізичної інфраструктури провайдера хмарних послуг. Загрози інформаційній безпеці можуть виникати як на логічному (програмному) рівні так і на фізичному (зокрема мережному) рівні. Критичними з точки зору кібербезпеки є обмін повідомленнями між різними зонами доступності хмарної інфраструктури, що на пряму впливають на безпеку обміну повідомленнями між вебсервером та сервером баз даних.

Для підвищення рівня інформаційної безпеки у мережі можна використовувати обмін повідомленнями з використанням багатошляхової маршрутизації та попередньо розділення повідомлення на частини за схемою Шаміра [35, 36]. Завдяки використанню такої схеми ймовірність компрометації повідомлення може бути зменшена, оскільки для цього зловмисник повинен скомпрометувати всі шляхи, по яких розділяються частини повідомлення.

Розглянутий та вдосконалений в роботах інших авторів [36, 37] механізм безпечної маршрутизації SPREAD передбачає:

– знаходження множини маршрутів між джерелом та отримувачем, які не перетинаються;

– фрагментація повідомлення, яке передається, на декілька частин за схемою Шаміра;

– поділ частин повідомлення за маршрутами.

Використання такого механізму призводить до ситуації, коли за відомою зловмиснику схемою поділу повідомлення, компрометація повідомлення в цілому буде лише у випадку компрометації всіх маршрутів, що використовувалися. Множина шляхів у мережі можна розділити на два типи: шляхи, що не перетинаються, і шляхи, що перетинаються, тобто мають спільні вузли або канали [35, 38]. Для шляхів, які не перетинаються спільними є лише джерело та отримувач повідомлення. Якщо шляхи мають хоча б один спільний канал або вузол, то такі шляхи є шляхами, що перетинаються. Від типу шляхів, залежить складність розрахунку ймовірності компрометації повідомлення. Крім того при розрахунку ймовірності компрометації повідомлення вважається, що якщо шлях містить хоча б один канал, який скомпрометований, то всі фрагменти повідомлення які передавалися цим шляхом вважаються скомпрометованими.

Для забезпечення безпеки під час обміну повідомленнями між вебсервером та сервером баз даних Amazon RDS в роботі пропонується використовувати у фізичній мережній інфраструктурі, яка з’єднує зони доступності хмарної інфраструктури, фрагментацію за схемою Шаміра та багатошляхову маршрутизацію.

4.3.2. Розрахунок ймовірності компрометації повідомлень.

Розробку математичної моделі необхідно почати з аналізу структури та місць можливої компрометації під час обміну повідомленнями між вебсервером та сервером баз даних. Передача повідомлення здійснюється наступним шляхом: повідомлення передаються з вебсервера до маршрутизатора зони доступності в якій він знаходиться; далі повідомлення передаються по фізичний мережі через різні маршрутизатори з використанням багатошляховой маршрутизації; потім ці повідомлення надходять до маршрутизатора іншої зони доступності, де знаходиться сервер баз даних Amazon RDS.

Таким чином описану вище структуру мережі можна представити у вигляді наступного графу, як наведено на рис. 4.32.

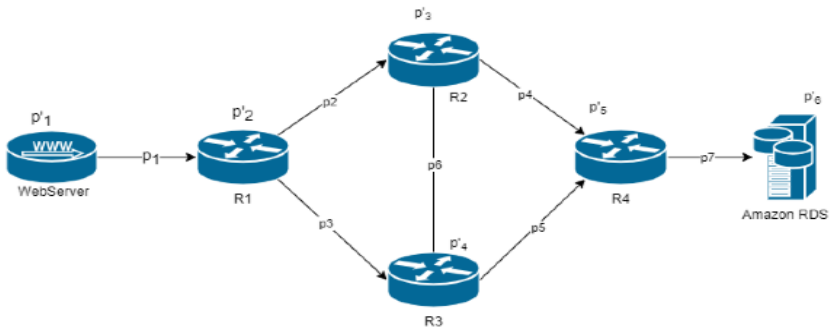


Рисунок 4.32 – Спрощена структура мережі хмарної інфраструктури

Введені наступні позначення, щодо структури мережі:

– p_i, i = 1…7 – ймовірність компрометації віртуального або фізичного каналу;

– p'_j, j = 1…6 – ймовірність компрометації маршрутизатору або віртуального сервера (вузла).

Розглянемо математичну модель схеми Шаміра наведену у роботі [39]. Введені при створенні моделі позначення зведені у таблиці 4.2.

Таблиця 4.2 – Позначення, які використовуються в математичній моделі

Позначення	Пояснення
N	– загальна кількість фрагментів, на які розбивається повідомлення за схемою Шаміра;
T	– мінімальна кількість фрагментів, необхідних для відновлення надісланого повідомлення ($T \le N$);
n_k	– цілочисельна змінна, що характеризує кількість фрагментів повідомлення, переданих k-м шляхом;
M	– кількість шляхів, що не перетинаються;
M_k	– кількість елементів у k-го шляху;
p_k	– ймовірність компрометації k-го шляху;
p_k^j	– ймовірність компрометації j-го каналу у k-му шляху;
p_{msg}	– ймовірність компрометації повідомлення

M'_k	– кількість вузлів у k-му шляху;
p'^{j}_{k}	– ймовірність компрометації j-го вузла у k-му шляху

У разі використання схеми Шаміра при T < N повинні виконуватись умова:

$$N - T + 1 \le n_k \le T - 1, i = 1 \ldots M .$$

При використанні схеми без надмірності, тобто коли T = N ця умова має вигляд:

$$1 \le n_i \le T - 1, i = 1 \ldots M .$$

Для розрахунку ймовірності p_k компрометації k-го шляху, що складається з M_k елементів, використовується формула:

$$p_k = 1 - \left(1 - p_k^1\right)\left(1 - p_k^2\right)\cdots\left(1 - p_k^{M_k}\right) = 1 - \prod_{j=1}^{M_k}\left(1 - p_k^j\right).$$

При цьому змінні n_k (k = 1…M) мають відповідати такій умові:

$$\sum_{k=1}^{M} n_k = N .$$

У випадку використання передачі N фрагментів повідомлення M шляхами, що не перетинаються, з фрагментацією повідомлення за схемою Шаміра, ймовірність компрометації повідомлення можна визначити за формулою:

$$p_{msg} = \prod_{k=1}^{M} p_k . \qquad (4.1)$$

На відміну від попередньо розглянутої математичної моделі, в цьому випадку додатково враховується ймовірність компрометації віртуальних серверів

та віртуальних машин (вузлів), які можна розглядати як додаткові послідовні елементи у шляху. Застосовуючи цей підхід до хмарної інфраструктури ймовірність p_k компрометації k-го шляху між вебсервером та сервером баз даних можна відповідно знайти як:

$$p_k = 1 - (1 - p_k^1)(1 - p_k^2)\cdots\left(1 - p_k^{M_k}\right)\left(1 - p'^1_k\right)\left(1 - p'^2_k\right)\cdots\left(1 - p'^{M`_k}_k\right) = = 1 - \prod_{j=1}^{M_k}\left(1 - p_k^j\right)\prod_{j=1}^{M`_k}\left(1 - p'^j_k\right).$$

Однак, у разі безпечної маршрутизації шляхами, що перетинаються, події, пов'язані з компрометацією шляхів та вузлів, стають сумісними, тобто формула (4.1) для розрахунку ймовірності компрометації повідомлення використовуватись не може.

Для того щоб здійснити розрахунок ймовірності компрометації повідомлення виділено декілька частин у структурі мережі. До першої частині віднесено частину мережі, яка містить вебсервер, канал зв’язку до маршрутизатора R1 зони доступності. До другої частині – сукупність підмереж та маршрутизаторів фізичної мережі між зонами доступності, які забезпечує доставку повідомлень між маршрутизаторами зон доступності R1 та R4. До третій – відповідно частину мережі, яка забезпечує доставку повідомлень між маршрутизатором R4 та Amazon RDS. Схему поділу мережі представлено на рис.4.33.

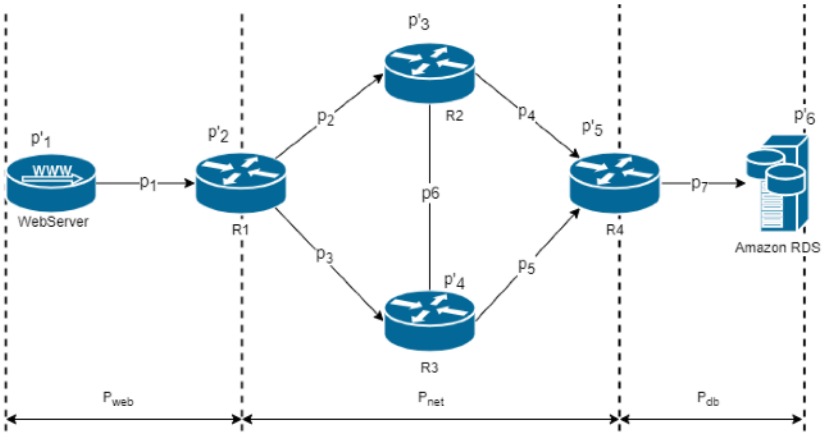


Рисунок 4.33 – Перетворення структури мережі у хмарі

Таким чином можна визначити ймовірності компрометації для цих частин. Так, для першої частини p_{web} враховує ймовірність компрометації вебсервера,

віртуального каналу (шляху) між вебсервером та R1 та ймовірність компрометації віртуального маршрутизатора R1.

Для другої частині ймовірність компрометації p_{net} враховує ймовірності компрометації каналів між маршрутизаторами R1, R2, R3 та R4, а також ймовірності компрометації маршрутизаторів R2 та R3.

Для третьої частини ймовірність компрометації p_{db} враховує ймовірності компрометації віртуального маршрутизатора R4 та сервера баз даних Amazon RDS, а також віртуального каналу (шляху) між ними.

В результаті такого спрощення, структуру мережі можна привести до зображеної на рис. 4.34.

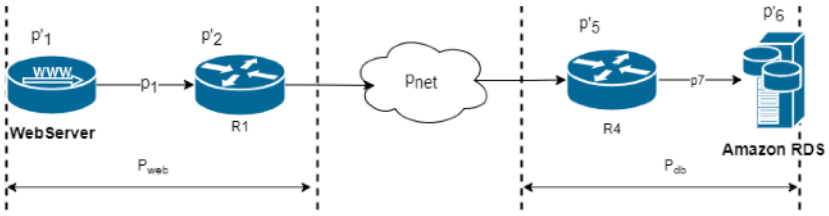


Рисунок 4.34 – Спрощена структура мережі у хмарі

В цьому випадку структура мережі містить послідовне з’єднання трьох частин та відповідно повідомлення можна вважати скомпрометованим, якщо воно було скомпрометовано хоча б в одному з цих частин. Тобто

$$p_{msg} = 1 - \left(1 - p_{web}\right)\left(1 - p_{net}\right)\left(1 - p_{db}\right). \quad (4.2)$$

Перша та третя частина також містить послідовне з’єднання елементів та відповідно ймовірності компрометації для них можна визначити як

$$p_{web} = 1 - \left(1 - p'_1\right)\left(1 - p_1\right)\left(1 - p'_2\right); \quad (4.3)$$

$$p_{db} = 1 - \left(1 - p'_5\right)\left(1 - p_7\right)\left(1 - p'_6\right). \quad (4.4)$$

Визначення ймовірності p_{net} ускладнено, оскільки містить шляхи, що перетинаються, та події, пов'язані з компрометацією шляхів та вузлів, стають сумісними.

Але якщо проаналізувати причини, які можуть призвести до компрометації віртуальних та фізичних маршрутизаторів (як це зроблено в попередніх розділах

роботи), то можна прийти до висновку, що віртуальні маршрутизатори мають більшість вразливостей, характерних для елементів фізичної інфраструктури. Крім того, додатково ним властиві вразливості та ризики, характерні для елементів хмарної інфраструктури. Це, призводить до того, що віртуальні маршрутизатори є більш вразливими, та мають більшу ймовірності компрометації. Зогляду на це, в математичній моделі маршрутизатори R2 та R3 можна вважати відносно надійними, і вважати їх ймовірністі компрометації $p'_3 = 0$ та $p'_4 = 0$. Враховуючі це, можна використати формулу запропоновану у роботі [39], яка враховує лише ймовірності компрометації каналів зв'язку та виведена для аналогічної топології. Таким чином ймовірність компрометації для другої частині можна визначити, як

$$p_{net} = q_6\left(1 - \left(1 - p_2p_3\right)\left(1 - p_4p_5\right)\right) + p_6\left(1 - q_2q_4\right)\left(1 - q_3q_5\right), \quad (4.5)$$

де $q_j = \left(1 - p_j\right)$ – ймовірність події, що j-й канал не буде скомпрометовано.

Проведено дослідження впливу ймовірності компрометації віртуальних каналів та вузлів на результуючу ймовірність компрометації повідомлення у хмарній інфраструктурі.

Спочатку проведено дослідження цієї залежності в умовах коли або вузли є надійними та скомпрометованими можуть бути лише канали ($p`_j = 0,\ p_i \neq 0$) або навпаки – компрометація можлива лише для вузлів, а канали є надійними ($p`_j \neq 0,\ p_i = 0$). Для цього ймовірність компрометації прирівняна вузлів до нуля, а ймовірність компрометації каналів змінено від 0 до 1. Аналогічно зроблено для каналів: ймовірність компрометації каналів прирівняна до нуля, а ймовірність компрометації вузлів змінено від 0 до 1. Результати розрахунку ймовірності компрометації повідомлення за математичною моделлю (4.2-4.5) для обох випадків (надійних вузлів та надійних каналів) зведені на рис. 4.26.

За результатами порівняння графічних залежностей ймовірності компрометації повідомлення для випадку надійних вузлів та випадку надійних віртуальних каналів можна зробити висновок, що вплив ймовірності компрометації вузлів більший. Так у випадку надійних віртуальних каналах при зростанні ймовірності компрометації вузлів результуюча ймовірність

компрометації повідомлення збільшується швидше чим при аналогічному зростанні ймовірності компрометації віртуальних каналів.

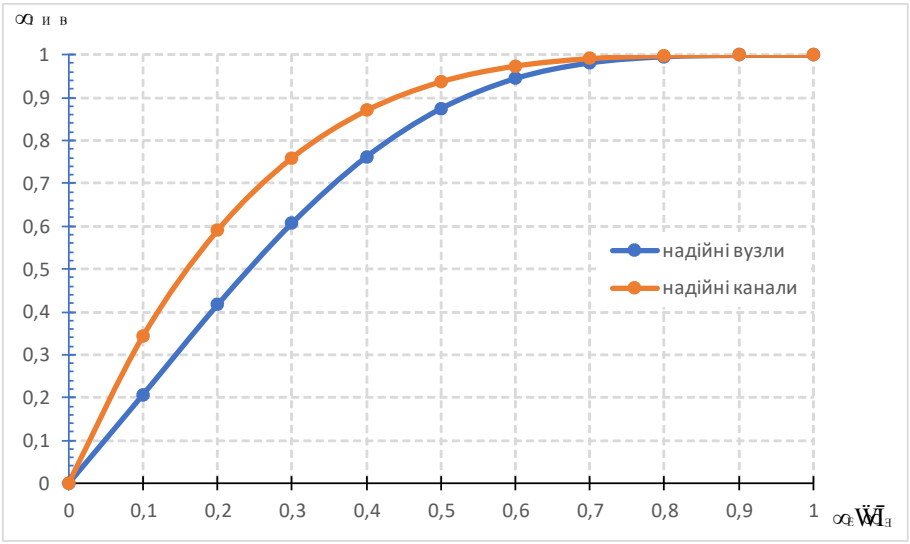


Рисунок 4.35 – Графік залежності ймовірності компрометації повідомлення від ймовірності компрометації вузлів та каналів хмарної інфраструктури

Такий ефект можна пояснити тим, що через вузли, які в дослідженні можуть бути скомпрометовані, трафік проходить нефрагментованим за схемою Шаміра, таким чином при компрометації вузла одразу компрометується повідомлення. У випадку ж компрометації каналу, в більшості випадків для топології, скомпрометованими стають лише частина повідомлення.

На наступному етапі дослідження встановлено однакову ймовірність компрометації каналів, а ймовірність компрометації вузлів змінено від 0 до 1 кроком 0,1 ($p_i = const,\ p_i \neq 0;\ p`_j \in \{0;0,1;0,2;0,3;0,4;0,5;0,6;0,7;0,8;0,9;1\}$) . Такий експеримент повторено для різних значень ймовірності компрометації каналів ($p_i \in \{0,2;0,4;0,6;0,8\}$). Результати розрахунку ймовірності компрометації повідомлення за математичною моделлю (4.2-4.5) зведені на рис. 4.27.

За результатами порівняння графічних залежностей ймовірності компрометації повідомлення від ймовірності компрометації вузлів при фіксованих значеннях ймовірності компрометації каналів можна зробити висновок, що при збільшенні ймовірності компрометації вузлів результуюча ймовірність компрометації повідомлення швидко зростає. Крім того можна помітити, що при

ймовірності компрометації каналів більше ніж 0,6 ймовірність компрометації повідомлення наближається до 1 (тобто майже кожне повідомлення є скомпрометованим) та змінюється слабо при зміні ймовірності компрометації вузлів.

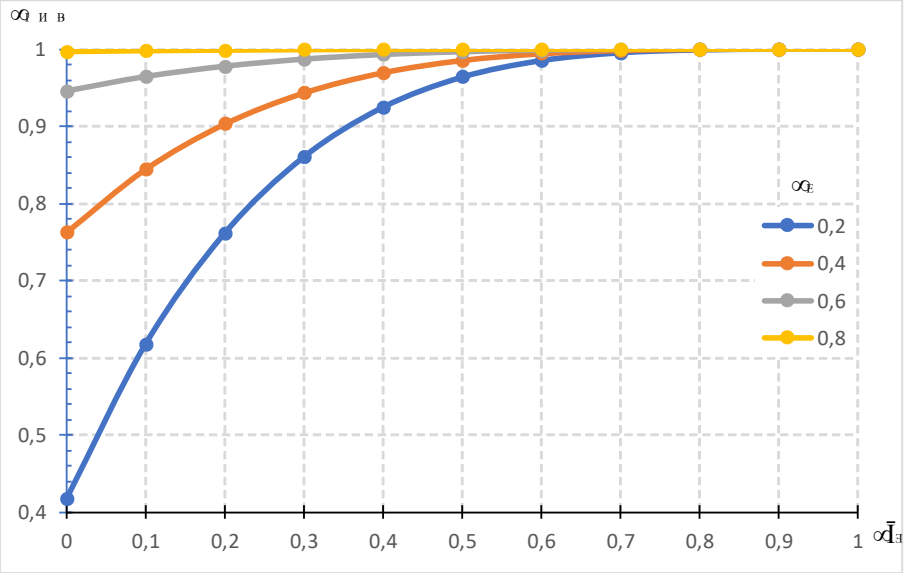


Рисунок 4.36 – Графік залежності ймовірності компрометації повідомлення від ймовірності компрометації вузлів при фіксованих значеннях ймовірності компрометації каналів

Останнім дослідженням є розрахунок ймовірності компрометації повідомлення при однаковій ймовірність компрометації вузлів, а ймовірність компрометації віртуальних каналів змінено від 0 до 1 кроком 0,1 ($p'_j = \text{const},\ p'_j \neq 0;\ p_i \in \{0;0{,}1;0{,}2;0{,}3;0{,}4;0{,}5;0{,}6;0{,}7;0{,}8;0{,}9;1\}$) . Такий експеримент повторено для різних значень ймовірності компрометації віртуальних каналів ($p'_j \in \{0{,}2;0{,}4;0{,}6;0{,}8\}$). Результати розрахунку ймовірності компрометації повідомлення за математичною моделлю (4.2-4.5) зведені на рис. 4.28.

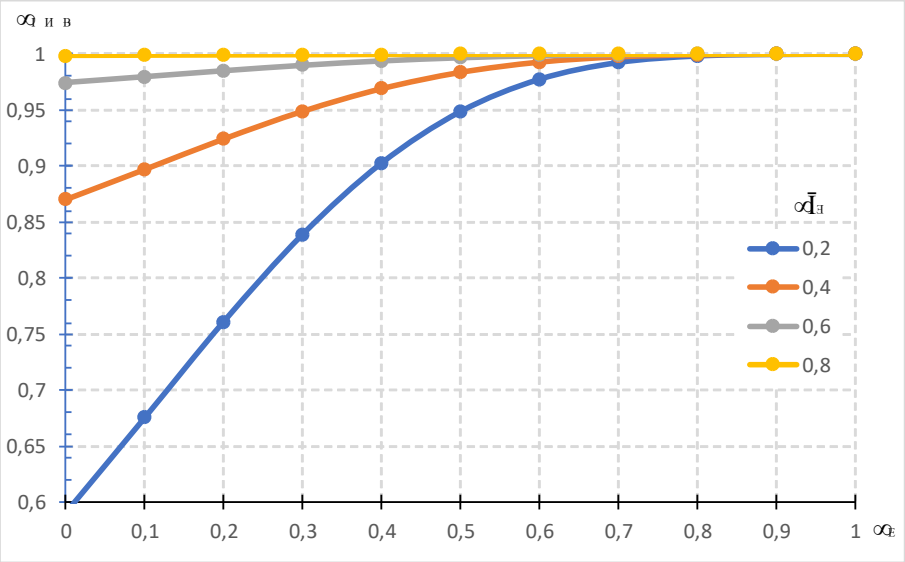


Рисунок 4.37 – Графік залежності ймовірності компрометації повідомлення від ймовірності компрометації каналів при фіксованих значеннях ймовірності компрометації вузлів

Аналогічно попередньому, можна зробити висновок з аналізу залежностей (рис. 4.37). Так само, при збільшенні ймовірності компрометації каналів, результуюча ймовірність компрометації повідомлення швидко зростає, ймовірність компрометації повідомлення стрімко наближається до 1 при ймовірності компрометації каналів більших ніж 0,5.

Додатково за аналізом графіків (рис. 4.35 – 4.37) можна зробити висновок, що при ймовірності компрометації каналів більше ніж 0,2 та/або при ймовірності компрометації віртуальних вузлів більших ніж 0,1 – ймовірність компрометації повідомлення дуже висока – більше 50 %. Такі значення ймовірності компрометації вузла недопустимі та означають, що більше половини повідомлень буде скомпрометовано.

ВИСНОВКИ

Хмарні обчислення це комбінація кількох ключових технологій і багато дослідників вважають їх наступним поколінням IT-архітектури. Незважаючи на переваги хмарних обчислень, багато питань безпеки ще не повністю проаналізовані.

В роботі проведено огляд інструментів хмарної інфраструктури AWS та забезпечення мережної безпеки. Проведений в роботі аналіз хмарних технологій різних провайдерів дозволив виявити їх основні переваги та недоліки. Проведено аналіз засобів забезпечення мережної безпеки хмарної інфраструктури AWS, наведено переваги та недоліки с точки зору забезпечення мережної безпеки.

Основними перевагами слід вважати: наявність у хмарних провайдерів спеціалізованого персоналу для централізованого керування, тестування системи безпеки та її налаштування; надійність платформи; доступність ресурсів; мобільність кінцевого клієнту; централізацію даних.

До основних недоліків с точки зору мережної безпеки є: складність системи, загальне багато користувальницьке середовище; однорідність програмного та апаратного складу платформи; використання Інтернету для доступу зі застосуванням незахищеного каналу; втрата користувачем повного контролю над ресурсами.

Також обґрунтовано структуру хмарної інфраструктури, описано процес її розгортання, проведено синтез математичної моделі розрахунку ймовірності компрометації повідомлення, що передається за схемою Шаміра та проведено її дослідження. Дослідження моделі показало, що вплив ймовірності компрометації вузлів більший. Так у випадку надійних каналах при зростанні ймовірності компрометації вузлів результуюча ймовірність компрометації повідомлення збільшується швидше чим при аналогічному зростанні ймовірності компрометації каналів.

Крім того виявлено, що при ймовірності компрометації каналів більше ніж 0,6 та/або при ймовірності компрометації вузлів більших ніж 0,5 ймовірність компрометації повідомлення наближається до 1.

При ймовірності компрометації каналів більше ніж 0,2 та/або при ймовірності компрометації вузлів більших ніж 0,1 – ймовірність компрометації повідомлення дуже висока – більше 50 %. Такі значення ймовірності

компрометації вузла недопустимі та означають, що більше половини повідомлень буде скомпрометовано.

Окремі результати роботи доповідались на XVI міжнародній науково-практичній конференції «Інформаційні технології і автоматизація – 2023» [40 - 42].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Храмцовська Н. Стандарти та посібники з використання хмарних обчислень. *Information Management*. 2013. № 3. С. 12–21.

2. NIST IR 8074 Vol. 2. Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity. URL: https://nvlpubs.nist.gov/nistpubs/ir/2015/ NIST.IR.8074v2.pdf (дата звернення: 15.12.2023).

3. D:A-5.1 Report on A4Cloud contribution to standards. URL: https://www.cloudaccountability.eu/sites/default/files/D15.1%20Report%20on%20A4Cloud%20contribution%20to%20standards_0.pdf (дата звернення: 15.12.2023).

4. Hibbard E.A. Latest in Cloud Computing Standards. URL: http://www.slideshare.net/rnewton/summary-cloudstandardseahv2130225 (дата звернення: 15.12.2023).

5. Cisco Global Cloud Index: Forecast and Methodology, 2014-2019. URL: https://www.cisco.com/c/dam/m/en_us/service-provider/ciscoknowledgenetwork/files/547_11_10-15-DocumentsCisco_GCI_Deck_2014-2019_for_CKN__10NOV2015_.pdf (дата звернення: 15.12.2023).

6. NIST SP 500-291 version 2. NIST Cloud Computing Standards Roadmap. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf (дата звернення: 15.12.2023).

7. ITU-T. FG Cloud TR. Version 1.0. (02/2012). Part 6: Overview of SDOs involved in cloud computing. URL: http://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P6-PDF-E.pdf (дата звернення: 15.12.2023).

8. ISO/IEC 22123-1:2023. Information technology – Cloud computing. Part 1: Vocabulary. Brussels: European Committee for Electrotechnical Standardization, 2023. 18 p.

9. ISO/IEC 22123-3:2023. Information technology – Cloud computing. Part 3: Reference architecture. Brussels: European Committee for Electrotechnical Standardization, 2023. 59 p.

10. ISO/IEC 27000:2018. Information technology – Security techniques. Information security management systems. Geneva: International Organization for Standardization, 2018. 27 p.

11. ISO/IEC 15408-1:2022. Information security, cybersecurity and privacy protection – Evaluation criteria for IT security. Part 1: Introduction and general model. Brussels: European Committee for Electrotechnical Standardization, 2022.

12. Recommendation ITU-T Y.3500. Information technology – Cloud computing – Overview and vocabulary. Geneva: International Telecommunication Union, 2014. 18 p.

13. Recommendation ITU-T Y.3501. Cloud computing framework and high-level requirements. Geneva: International Telecommunication Union, 2013. 26 p.

14. Recommendation ITU-T Y.3502. Information technology – Cloud computing – Reference architecture. Geneva: International Telecommunication Union, 2014. 62 p.

15. Recommendation ITU-T Y.3503. Requirements for desktop as a service. Geneva: International Telecommunication Union, 2014. 34 p.

16. Recommendation ITU-T Y.3510. Cloud computing infrastructure requirements. Geneva: International Telecommunication Union, 2013. 28 p.

17. Recommendation ITU-T Y.3511. Framework of inter-cloud computing. Geneva: International Telecommunication Union, 2014. 46 p.

18. Recommendation ITU-T Y.3512. Cloud computing – Functional requirements of Network as a Service. Geneva: International Telecommunication Union, 2014. 36 p.

19. Recommendation ITU-T Y.3513. Cloud computing – Functional requirements of Infrastructure as a Service. Geneva: International Telecommunication Union, 2014. 26 p.

20. Recommendation ITU-T X.1601. Fundamentals of cloud computing security. Geneva: International Telecommunication Union, 2014. 32 p.

21. ITU-T Recommendation X.1205. Cyber Security Review. Geneva: International Telecommunication Union, 2008. 64 p.

22. Полякова Т.А., Хімченко О.І. Правові проблеми забезпечення інформаційної безпеки під час використання хмарних технологій. *Правова інформатика.* 2013. № 2. С. 12–16.

23. NIST SP 800-145. The NIST Definition of Cloud Computing. Gaithersburg: National Institute of Standards and Technology, 2011. 7 p. URL: https://doi.org/10.6028/NIST.SP.800-145 (дата звернення: 15.12.2023).

24. NIST SP 800-146. Cloud Computing Synopsis and Recommendations. Gaithersburg: National Institute of Standards and Technology, 2012. 81 p. URL: https://doi.org/10.6028/NIST.SP.800-146 (дата звернення: 15.12.2023).

25. NIST SP 800-144. Guidelines on Security and Privacy in Public Cloud Computing. Gaithersburg: National Institute of Standards and Technology, 2011. 80 p. URL: https://doi.org/10.6028/NIST.SP.800-144 (дата звернення: 15.12.2023).

26. NIST SP 500-299. Cloud Computing Security Reference Architecture. National Institute of Standards and Technology. URL: https://csrc.nist.gov/pubs/sp/500/299/ipd (дата звернення: 14.12.2023).

27. Catteddu D., Hogben G. Cloud Computing Information Assurance Framework. Technical report. European Network and Information Security Agency, 2009. URL: https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework/@@download/fullReport (дата звернення: 14.12.2023).

28. Catteddu D., Hogben G. Cloud Computing Security Risk Assessment. Technical report. European Network and Information Security Agency, 2009. URL: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/@@download/fullReport (дата звернення: 14.12.2023).

29. Ковальчук Я.В. Удосконалення модуля автоматизованого розгортки хмарного постачальника AWS : магістерська атестаційна робота випускника освітнього ступення «магістр». М-во освіти та науки України, нац. авіаційний ун-т. Київ, 2020. 84 с. URL: https://er.nau.edu.ua/bitstream/NAU/45802/1/%D0%A4%D0%9A%D0%9A%D0%9F%D0%86_2020_125_%D0%9A%D0%BE%D0%B2%D0%B0%D0%BB%D1%8C%D1%87%D1%83%D0%BA%D0%AF%D0%92.pdf (дата звернення: 25.12.2023)

30. What Is AWS. URL: https://aws.amazon.com/what-is-aws/?nc1=f_cc (дата звернення: 25.12.2023)

31. Shared Responsibility Model. URL: https://aws.amazon.com/compliance/shared-responsibility-model/?nc1=h_ls (дата звернення: 25.12.2023).

32. Amazon EC2 FAQs – AWS. URL: https://aws.amazon.com/ec2/faqs/ ?nc1=h_ls (дата звернення: 25.12.2023).

33. Лисаков В. І. Використання клаудпровайдера AWS для забезпечення безпеки вебзастосувань : пояснювальна записка до атестаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 125 – Кібербезпека. М-во освіти та науки України, Харків. нац. ун-т радіоелектроніки. Харків, 2021. 71 с. URL: https://openarchive.nure.ua/handle/document/19465 (дата звернення: 23.11.2023)

34. Joe Baron, Hisham Baz, Tim Bixler, Biff Gaut. AWS Certified Solutions Architect Official Study Guide. Sybex: Study Guide edition, 2009. 504 p.

35. Лемешко О.В., Єременко О.С., Невзорова О.С. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість. Харків: ХНУРЕ, 2020. 308 с.

36. Lou W., Liu W., Zhang Y., Fang Y. SPREAD: improving network security by multipath routing in mobile ad hoc networks. *Wirel. Netw.* 2009. № 15(3). P. 279–294.

37. Alouneh S., Agarwal A., En-Nouaary A. A novel path protection scheme for MPLS networks using multi-path routing. *Comput. Netw.* 2009. № 53(9). P. 1530–1545.

38. Yeremenko O. Enhanced flow-based model of multipath routing with overlapping by nodes paths, *Proceedings of the 2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, 2015. P. 42-45.

39. Лемешко О.В., Єременко О.С., Євдокименко М.О., Коваленко Т.М. Методика розрахунку ймовірності компрометації конфіденційних повідомлень при безпечній маршрутизації в інфокомунікаційних мережах з використанням шляхів, які перетинаються. *Проблеми телекомунікацій.* 2021. № 2(29). С. 15–27. URL: https://doi.org/10.30837/pt.2021.2.02 (дата звернення: 15.12.2023).

40. Пономаренко В. Ю. Проблемні аспекти інформаційної безпеки сервісу SaaS. *Інформаційні технології і автоматизація – 2023*: матеріали XVI міжнар. наук.-практ. конф., м. Одеса, 19-20 жовт. 2023 р. Одеса, 2023. С. 96–98 с.

41. Пономаренко В. Ю. Рекомендації щодо безпеки хмарних програм за допомогою технології DevSecOps. *Інформаційні технології і автоматизація – 2023*: матеріали XVI міжнар. наук.-практ. конф., м. Одеса, 19-20 жовт. 2023 р. Одеса, 2023. С. 98–100.

42. Пономаренко В. Ю. Аналіз атак програм-шантажистів у Microsoft Azure. *Інформаційні технології і автоматизація – 2023*: матеріали XVI міжнар. наук.-практ. конф., м. Одеса, 19-20 жовт. 2023 р. Одеса, 2023. С. 100–102.