Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Чекушкіна Нікіти Дмитровича*

академічної групи *125-20-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка моделі захисту інформації для хмарних інформаційно-комунікаційних систем на платформі AWS*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н. проф. Корченко А.О.			
розділів:				
спеціальний	ас. Олішевський І.Г.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Чекушкіну Нікіті Дмитровичу*** **академічної групи** ***125-20-3***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка моделі захисту інформації для хмарних інформаційно-комунікаційних систем на платформі AWS***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 25.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання, аналіз ситуації й проблематики, огляд хмарних рішень, характеристика AWS.	05.06.2024
Розділ 2	Обстеження ОІД підприємства, розробка моделі загроз, порушника та аналіз ризиків, розробка комплексу технічного захисту інформації для підприємства.	09.06.2024
Розділ 3	Розрахунок річних витрат на розробку комплексу технічного захисту інформації, оцінка величини збитку. Розрахунок ефективності запропонованого рішення.	17.06.2024

Завдання видано _____ Ілля ОЛІШЕВСЬКИЙ
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Нікіта ЧЕКУШКІН
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка містить 113 сторінок, 35 малюнків, 4 таблиці, 4 додатка, 11 джерел.

Об'єкт розробки: інформаційно-телекомунікаційна система товариства з обмеженою відповідальністю «ОІК» на платформі AWS.

Мета роботи: розробка моделі захисту інформації в хмарному середовищі, що забезпечує підвищення рівня безпеки інформаційних ресурсів на платформі AWS.

У першому розділі кваліфікаційної роботи проведено дослідження технічної бази системи ТОВ «ОІК», проведено аудит та аналіз загроз інформаційної безпеки в хмарі. Розроблено код для модуля автоматизованого розгортання та захисту інформації.

У спеціальній частині виконано розробку моделі захисту інформації, що включає організаційні та технічні заходи щодо захисту інформації від несанкціонованого доступу.

В економічному розділі визначено витрати на розробку та впровадження захисту інформації та проведено аналіз її економічної ефективності.

Практичне значення результатів кваліфікаційної роботи вдалося у забезпеченні захисту інформації в хмарному середовищі на платформі AWS, що підвищить рівень безпеки інформаційних ресурсів ТОВ «ОІК».

ХМАРНІ ТЕХНОЛОГІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, АНАЛІЗ РИЗИКІВ, НОРМАТИВНО ПРАВОВІ АКТИ, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЕКООМІЧНА ДОЦІЛЬНІСТЬ.

ABSTRACT

The explanatory note consists of 113 pages, 35 images, 4 tables, 4 appendices, 11 sources.

Object of development: information and telecommunication system of the limited liability company "OIK" on the AWS platform.

The purpose of the work: development of a model of information protection in the cloud environment, which ensures an increase in the level of security of information resources on the AWS platform.

In the first section of the qualification work, a study of the technical base of the OIK LLC system was conducted, an audit and analysis of threats to information security in the cloud was conducted. Developed code for automated deployment and information protection module.

In a special part, the development of the information protection model was carried out, which includes organizational and technical measures to protect information from unauthorized access.

In the economic section, the costs for the development and implementation of information protection are determined and an analysis of its economic effectiveness is carried out.

The practical significance of the results of the qualification work was achieved in ensuring the protection of information in the cloud environment on the AWS platform, which will increase the level of security of the information resources of OIK LLC.

CLOUD TECHNOLOGIES, THREAT MODEL, VIOLATOR MODEL, RISK ANALYSIS, REGULATORY LEGAL ACTS, INFORMATION SECURITY POLICY, ECONOMIC FEASIBILITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ALB – Application Load Balancer;
DDoS – Distributed Denial of Service;
IaC – Infrastructure as Code;
IaaS – Infrastructure as a Service;
IAM – Identity and Access Management;
KMS – Key Management Service;
MFA – Multifactor Authentication;
NAT – Network Address Translation;
PaaS – Platform as a Service;
RBAC – Role-Based Access Control;
SaaS – Software as a Service;
SSO – Single Sign-On;
TLS – Transport Layer Security;
VPN – Virtual Private Network;
VPC – Virtual Private Cloud;
WAF – Web Application Firewall;
АС – автоматизована система;
ІД – інформаційна діяльність;
ІТС – інформаційно-телекомунікаційна система;
НСД – несанкціонований доступ;
ОІД – об’єкт інформаційної діяльності;
ПЗ – програмне забезпечення;
СЗІ – служба захисту інформації;
ТЗІ – технічний захист інформації;
ТОВ – товариство з обмеженою відповідальністю;

ЗМІСТ

с.

ВСТУП

У сучасних умовах багато компаній з різних галузей відмовляються від використання приватних серверів на користь хмарних обчислювальних платформ. Цей перехід дозволяє значно зменшити витрати на IT-інфраструктуру та підвищити її гнучкість. Проте виникають нові виклики для керівництва підприємств та державних установ у сфері кібербезпеки. Захист систем віддаленого доступу стає критично важливим завданням, що охоплює численні аспекти та вимагає комплексного підходу.

На 2024 рік Amazon Web Services (AWS) залишається лідером на ринку хмарної інфраструктури, займаючи приблизно 31-32% світового ринку хмарних інфраструктурних послуг. AWS пропонує понад 200 послуг у 31 географічному регіоні і продовжує розширювати свою присутність. Швидке впровадження хмарних технологій, зокрема завдяки інноваціям у сфері штучного інтелекту та машинного навчання, сприяє подальшому зростанню ринку.

У сучасних умовах керування обчислювальними та мережевими ресурсами через програмний код стає все більш популярним завдяки таким інструментам, як Terraform та AWS CloudFormation. Ці технології автоматизують процес розгортання інфраструктури, підвищуючи ефективність і забезпечуючи додатковий рівень безпеки. Використання Terraform дозволяє описувати інфраструктуру як код, що спрощує її відтворення та модифікацію. AWS CloudFormation, у свою чергу, автоматизує розгортання та управління ресурсами AWS за допомогою шаблонів. Це дозволяє впроваджувати політики безпеки на рівні коду, інтегрувати перевірки безпеки в процес розгортання та забезпечувати дотримання найкращих практик кібербезпеки. Наприклад, ці інструменти можуть автоматично налаштовувати правила брандмауера, управління ідентифікацією та доступом (IAM) та інші заходи безпеки, зменшуючи вплив людського фактора і забезпечуючи високий рівень захисту інфраструктури. Крім того, можливість опису інфраструктури як коду забезпечує швидке відновлення системи в разі непередбачуваного інциденту. Завдяки автоматизованим процесам та збереженим шаблонам компанії можуть швидко розгорнути необхідні ресурси,

мінімізуючи час простою та знижуючи ризики, пов'язані з відновленням даних та працездатності систем.

Зважаючи на специфіку підприємств, де не завжди можливо забезпечити безпосередній контакт між усіма співробітниками, особлива увага має приділятися контролю доступу до системи. Необхідно налаштувати систему таким чином, щоб кожен користувач мав доступ лише до тих ресурсів, які потрібні для виконання його обов'язків, але не мав можливості втручатися у процеси, до яких йому доступ закритий.

Також важливо встановити відповідні обмеження для ускладнення зовнішніх атак. Варто налаштувати систему входу до віртуального робочого простору, використовуючи такі мережеві технології, як VPN, розмежування доступу (RBAC), єдиний вхід (SSO) та мультифакторну аутентифікацію (Multifactor Authentication). Це допоможе забезпечити надійний захист.

Враховуючи складність технічної реалізації цих заходів та їхню важливість для забезпечення надійної та безпечної системи на підприємстві, є значна потреба в залученні кваліфікованих спеціалістів не тільки у сфері кібербезпеки, але й в області конфігурації цих сервісів.

Метою цієї дипломної роботи є розробка моделі захисту інформації в інформаційно-телекомунікаційній системі товариства з обмеженою відповідальністю «ОІК» на платформі AWS. Для досягнення цієї мети були виконані наступні етапи:

– дослідження технічної бази системи ТОВ «ОІК»;

– проведення аудиту та аналізу загроз інформаційної безпеки і методів захисту інформації в хмарі;

– розробка коду для модулю автоматизованого розгортання для покращення захисту інформації від несанкціонованого доступу до хмари та тестування коду;

– розрахунок техніко-економічного обґрунтування.

Створення модуля автоматизованого розгортання завдяки описаному коду для Terraform дозволило підвищити рівень безпеки інформації за рахунок

зменшення часу розгортання хмарної мережі, що було протестовано на розробленій віртуальній мережі.

Крім того, необхідно регулярно оновлювати та патчити програмне забезпечення, навчати персонал з питань кібербезпеки та впроваджувати механізми автоматичного виявлення аномалій у поведінці користувачів. Виконання таких заходів сприятиме покращенню кібербезпеки підприємства, забезпечуючи продуктивну та безпечну роботу співробітників у віддаленому режимі.

Загалом, впровадження цих заходів допоможе підвищити рівень кібербезпеки на підприємстві. Це забезпечить стабільну та захищену роботу його інформаційної інфраструктури.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Останнім часом інформаційні технології зазнали значного розвитку, що зробило їхнє застосування ще актуальнішим. Використання цих технологій у сфері кібербезпеки є наступним еволюційним кроком, який забезпечує адаптивність, гнучкість, відкритість та мобільність захисту даних. Активно впроваджуються хмарні технології та сервіси, сприяючи створенню єдиного безпечного інформаційного простору.

Хмарні технології – це технології розподіленої обробки даних, де комп'ютерні ресурси та потужності надаються користувачам у вигляді інтернет-сервісів. Хмара – це дата-центр, окремий сервер або мережа серверів, де зберігаються програми та дані, до яких користувачі можуть підключатися через Інтернет. У контексті кібербезпеки, хмарні технології забезпечують централізоване управління захистом даних, моніторингом та реагуванням на інциденти.

Хмарний сервіс – це послуга, яка надає доступ до хмарних ресурсів за допомогою технологій «хмарних обчислень». Ці ресурси можуть легко інтегруватися в єдиний безпечний масив, що дозволяє налаштовувати і керувати ними відповідно до потреб користувачів, відкриваючи нові можливості для захисту та збереження інформації. Хмарні сервіси забезпечують надійні засоби шифрування, автентифікації та управління доступом, що значно підвищує рівень кібербезпеки в сучасному цифровому світі.

1.1.1 Аналіз проблемних питань захисту інформації в хмарних середовищах

Більшість проблем, пов'язаних із захистом користувацької інформації в хмарних сервісах, можна вирішити, застосовуючи сучасні методи криптографічного захисту, адміністративні заходи як з боку постачальників хмарних послуг, так і користувачів, а також укладенням договорів на надання послуг, які враховують індивідуальні потреби клієнтів. Додатково важливо

приймати міжнародні стандарти в цій галузі, запроваджувати державний контроль та створювати незалежних експертів для моніторингу. Наприклад, для забезпечення конфіденційності та цілісності даних, що зберігаються в хмарі, слід використовувати алгоритми цифрового підпису та шифрування відповідно до міжнародних стандартів, таких як ISO/IEC 27001 та NIST SP 800-53. ISO/IEC 27001 визначає вимоги до системи управління інформаційною безпекою (СУІБ), а NIST SP 800-53 надає рекомендації щодо заходів безпеки для інформаційних систем федерального уряду США. Для захисту від несанкціонованого доступу до користувацьких профілів доцільно застосовувати методи двофакторної автентифікації.

На сьогоднішній день багато постачальників хмарних послуг мають власні інтерфейси для програмування, що ускладнює можливість переходу користувачів від одного постачальника до іншого. Лише розробка відкритого міжнародного стандарту може вирішити цю проблему. Основні проблеми, що потребують детального аналізу та вирішення, включають:

1. Проблема привілейованих користувачів. Найбільшу загрозу для безпеки інформації в хмарі становлять користувачі з привілейованим доступом до системи або адміністратори хмарних сервісів. Для зменшення ризику деструктивних дій з їхнього боку необхідно здійснювати незалежний нагляд та контроль за їхніми діями. Статистика показує, що більшість порушень безпеки здійснюють внутрішні користувачі.

2. Невідповідність законів у сфері обробки, передачі, збереження та захисту інформації в різних країнах. Це є ключовою проблемою для можливості фізичного розміщення серверів постачальників хмарних послуг у різних країнах та регіонах, а також для користувачів з різних країн, які використовують послуги одного постачальника.

3. Довіра до постачальників послуг. Це питання може бути вирішено шляхом проведення аудиту безпеки постачальника хмарних послуг та перевірки відповідності його системи безпеки міжнародним стандартам.

4. Загальні вразливості хмарних сервісів. Вразливості в хмарних системах можуть вплинути на всіх користувачів даного постачальника, але вони також можуть бути швидко виправлені за допомогою централізованого оновлення.

5. Проблеми доступності сервісів та даних, відновлення їх роботи після збоїв або втрати даних. Це питання слід вирішувати на адміністративному та правовому рівнях. У договорах з користувачами повинні бути чітко визначені обов'язки сторін та відповідальність за обставини, що призвели до збоїв, а розслідування повинна проводити незалежна сторона.

6. Надання доступу, спільного доступу та блокування доступу до ресурсів і даних у хмарі.

7. Захист інтелектуальної власності в хмарі, включаючи програмне забезпечення та дані.

1.1.2 Моделі розгортання та надання послуг у хмарних обчисленнях

Хмарні обчислення являють собою модель, що забезпечує доступ до обчислювальних ресурсів, що налаштовуються через мережу. Ці ресурси включають комунікаційні мережі, сервери, засоби збереження даних, прикладні програми та сервіси, які можуть бути швидко надані або звільнені з мінімальними експлуатаційними витратами або втручанням з боку провайдера. Основні моделі розгортання хмарних сервісів включають приватні, громадські, публічні та гібридні хмари. Ці моделі розрізняються за категоріями користувачів, які мають доступ до ресурсів і даних хмари. Провайдери хмарних ресурсів можуть надавати такі послуги, як програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) та інфраструктура як послуга (IaaS). Хмарні обчислення забезпечують доступ до різних обчислювальних ресурсів, які можуть бути розгорнуті за допомогою кількох основних моделей. Кожна модель має свої особливості та призначення, залежно від потреб користувачів та організацій.

Приватна хмара передбачає, що обчислювальні ресурси використовуються виключно однією організацією. Вона може бути фізично розташована на території організації або керуватися третьою стороною. Приватні хмари забезпечують високий рівень контролю та безпеки, оскільки всі ресурси

знаходяться під управлінням однієї організації. Вони ідеально підходять для великих корпорацій або урядових установ, які мають строгі вимоги до конфіденційності даних і безпеки. Переваги приватних хмар: високий рівень безпеки та контролю, індивідуальна конфігурація під потреби організації, можливість інтеграції з існуючою інфраструктурою. Недоліки приватних хмар: високі витрати на створення та підтримку, обмежена масштабованість порівняно з публічними хмарами.

Громадська хмара використовується групою організацій, які мають спільні вимоги до безпеки, конфіденційності та відповідності стандартам. Вона може бути розміщена на території однієї з організацій або керуватися стороннім провайдером. Громадські хмари зазвичай створюються для специфічних галузей, таких як охорона здоров'я або фінансовий сектор, де є спільні нормативні вимоги. Переваги громадських хмар: спільне використання ресурсів і витрат, відповідність галузевим стандартам і вимогам, підвищена безпека порівняно з публічними хмарами. Недоліки громадських хмар: високі витрати порівняно з публічними хмарами, обмежена гнучкість у порівнянні з приватними хмарами.

Публічна хмара передбачає, що обчислювальні ресурси надаються стороннім провайдером і використовуються багатьма різними клієнтами. Ресурси надаються через Інтернет і можуть бути швидко масштабовані залежно від потреб користувачів. Публічні хмари є найбільш економічно вигідним варіантом, оскільки витрати на інфраструктуру розподіляються між багатьма користувачами. Переваги публічних хмар: висока масштабованість, низькі витрати на використання завдяки економії масштабу, легкий доступ до ресурсів через Інтернет. Недоліки публічних хмар: менший контроль над безпекою та конфіденційністю, можливі проблеми з продуктивністю через спільне використання ресурсів.

Гібридна хмара поєднує в собі елементи приватних і публічних хмар, дозволяючи організаціям використовувати переваги обох моделей. Наприклад, критично важливі дані можуть зберігатися в приватній хмарі, тоді як менш чутливі дані та обчислювальні ресурси можуть використовуватися в публічній

хмарі. Це забезпечує гнучкість і масштабованість, одночасно дозволяючи підтримувати високий рівень безпеки для важливих даних. Переваги гібридних хмар: гнучкість у використанні ресурсів, підвищена безпека для критичних даних, можливість економії витрат завдяки використанню публічних хмар. Недоліки гібридних хмар: складність у налаштуванні та управлінні, потреба в інтеграції різних хмарних середовищ.

Аналіз свідчить, що незалежно від моделі розгортання та обслуговування хмари, всі ключі, які використовуються у хмарному середовищі, можна розділити на дві основні категорії залежно від їх призначення та власника:

– ключі, які використовуються провайдером хмарних послуг і є його власністю;

– ключі, які використовуються клієнтами провайдера хмарних послуг і належать їм;

Наприклад, якщо хмара розгорнута як публічна та надає послуги PaaS, користувач хмари реалізує свої рішення на основі сервісу, що надається провайдером, і ці рішення використовуються клієнтами користувача. У такій ситуації користувач виступає як провайдер хмарних послуг для своїх клієнтів, і існують два класи ключів:

– ключі провайдера хмарних послуг, які включають ключі самого провайдера публічної хмари, що надає послуги PaaS, та ключі користувача хмари щодо його клієнтів;

– ключі користувача хмарних послуг, які включають ключі користувача хмари щодо провайдера хмарних послуг та ключі клієнтів користувача;

У схожий спосіб можна визначити два типи ключів для інших моделей розгортання та надання послуг у хмарі. Ця модель, де є лише дві ролі – користувач і постачальник послуг, зменшує складність аналізу безпеки управління ключами, зокрема криптографічної стійкості. Це досягається завдяки усуненню ролі аудитора хмари, який діє як пасивний елемент хмарного середовища і має доступ до нього тільки під час проведення аудиту зі строго визначеними повноваженнями.

Це також стосується посередника хмарних послуг, який для постачальника хмарних послуг виступає клієнтом, а для клієнта – як постачальник хмарних послуг. У подібний спосіб транспортувальник хмарних послуг у моделі безпеки має забезпечувати доступність сервісів, тоді як конфіденційність та цілісність даних гарантуються користувачем і постачальником хмарних послуг.

1.1.3 Характеристика AWS

AWS (Amazon Web Services) є однією з найбільш інноваційних та передових хмарних платформ у світі. Її значущість у сучасному бізнес-середовищі важко переоцінити. AWS надає широкий спектр інструментів для захисту робочих навантажень клієнтів, однак багато клієнтів не повністю усвідомлюють свою роль у забезпеченні безпеки та контролю над використанням і розгортанням ресурсів у хмарі AWS. AWS пропонує різноманітні сервіси, інструменти та технології для забезпечення безпеки хмари, включаючи контроль доступу, брандмауери, шифрування, журналювання, моніторинг та відповідність. Ці сервіси підтримують різноманітні сценарії для задоволення вимог безпеки, реєстрації користувачів, аудиту та відповідності в хмарному середовищі.

Один з головних аспектів успіху AWS полягає у її гнучкості та адаптивності. AWS пропонує безліч інструментів і сервісів, які дозволяють компаніям різного масштабу та напрямків діяльності швидко адаптуватися до змінних умов ринку. Це включає як основні інфраструктурні послуги, так і високотехнологічні рішення для обробки даних, машинного навчання, штучного інтелекту та Інтернету речей (IoT). AWS Identity and Access Management (IAM) дозволяє контролювати безпечний доступ і дії для користувачів AWS. Віртуальна приватна хмара (VPC) дозволяє вам захистити вашу хмарну інфраструктуру AWS, створивши віртуальну мережу, подібну до приватної мережі у вашому локальному центрі обробки даних. Служба керування ключами (KMS) забезпечує управління ключами шифрування для додаткового захисту ваших даних. AWS Shield і AWS Web Application Firewall (WAF) захищають ваші ресурси та додатки від загроз, таких як розподілені атаки на відмову в обслуговуванні (DDoS), налаштовуючи брандмауер на різних рівнях. AWS Config працює разом із AWS

CloudTrail і AWS CloudWatch для підтримки аудиту та керування конфігурацією всіх ресурсів AWS.

Ще однією важливою перевагою AWS є її надійність і доступність. Компанія має глобальну мережу центрів обробки даних, що забезпечує високу доступність та стійкість до відмов. Завдяки цьому клієнти можуть бути впевнені, що їхні додатки та дані завжди залишаються доступними, незалежно від обставин. AWS постійно інвестує у розвиток своєї інфраструктури, щоб забезпечити найвищий рівень продуктивності та безпеки для своїх клієнтів. AWS Artifact забезпечує доступ до документації з відповідності на вимогу аудиторів. Менеджер сертифікатів AWS дозволяє легко створювати, керувати та розгортати сертифікати SSL/TLS для використання зі службами AWS та пов'язаними внутрішніми ресурсами.

Безпека є ще одним ключовим аспектом, який робить AWS лідером на ринку хмарних рішень. AWS надає багаторівневий підхід до безпеки, що включає як фізичний захист центрів обробки даних, так і розширені механізми контролю доступу, шифрування даних та моніторинг. AWS Inspector — це автоматизована служба безпеки, яка оцінює додатки на наявність вразливостей і нормативних прогалин. AWS Macie використовує машинне навчання для автоматичного виявлення, класифікації та захисту конфіденційних даних, таких як особиста інформація. AWS GuardDuty — це служба виявлення загроз, яка постійно стежить за загрозами та небезпечними діями, такими як несанкціонований доступ або витік даних. AWS Security Hub надає глибокий огляд високопріоритетних проблем безпеки у всіх службах AWS. AWS Secrets Manager допомагає захистити доступ до програм, сервісів та IT-ресурсів без розкриття секретної інформації. AWS Detective дозволяє швидко аналізувати, досліджувати та визначати першопричину потенційних проблем безпеки або підозрілих дій.

AWS підтримує інновації та розвиток нових технологій. Компанія регулярно впроваджує нові сервіси та функції, які допомагають клієнтам залишатися на передовій лінії технологічного прогресу. Це включає рішення для аналітики, обробки великих даних, штучного інтелекту, машинного навчання та

багато іншого. Таким чином, AWS не тільки забезпечує поточні потреби своїх клієнтів, але й допомагає їм готуватися до майбутніх викликів і можливостей.

Хмарна безпека пройшла довгий шлях від часів, коли її вважали перешкодою для переміщення даних і додатків у хмару, до сьогоднішнього дня, коли хмарна безпека є однією з основних причин, чому організації переходять до хмарних рішень. Все більше компаній визнають переваги хмарної безпеки в інноваціях, надійності та зниженні витрат. AWS є однією з найгнучкіших і безпечних хмарних платформ, яка знімає велику частину навантаження на забезпечення безпеки, традиційно пов'язаного з IT-інфраструктурою. Клієнти отримують повну конфіденційність та безпеку завдяки вбудованим функціям AWS. Вони також користуються перевагами процесів безпеки, глобальної інфраструктури та мережевої архітектури, реалізованих AWS для забезпечення відповідності суворим вимогам безпеки.

В цілому, AWS є потужним інструментом для будь-якої організації, яка прагне досягти успіху в сучасному цифровому світі. Завдяки своїй інноваційності, надійності, безпеці та широким можливостям, AWS допомагає компаніям зростати, адаптуватися до змін та залишатися конкурентоспроможними.

1.1.4 Модель спільної відповідальності

Безпека та відповідність у хмарному середовищі AWS є спільною відповідальністю між AWS і клієнтами. Ця модель спільної відповідальності знижує операційне навантаження на клієнтів, оскільки AWS займається управлінням і моніторингом компонентів від рівня віртуалізації до фізичної безпеки інфраструктури, де розгорнуті сервіси. Клієнти, зі свого боку, несуть відповідальність за керування гостьовою операційною системою, включаючи оновлення безпеки та виправлення, а також за інше прикладне програмне забезпечення, керування ним та конфігурацію брандмауерів групи безпеки.

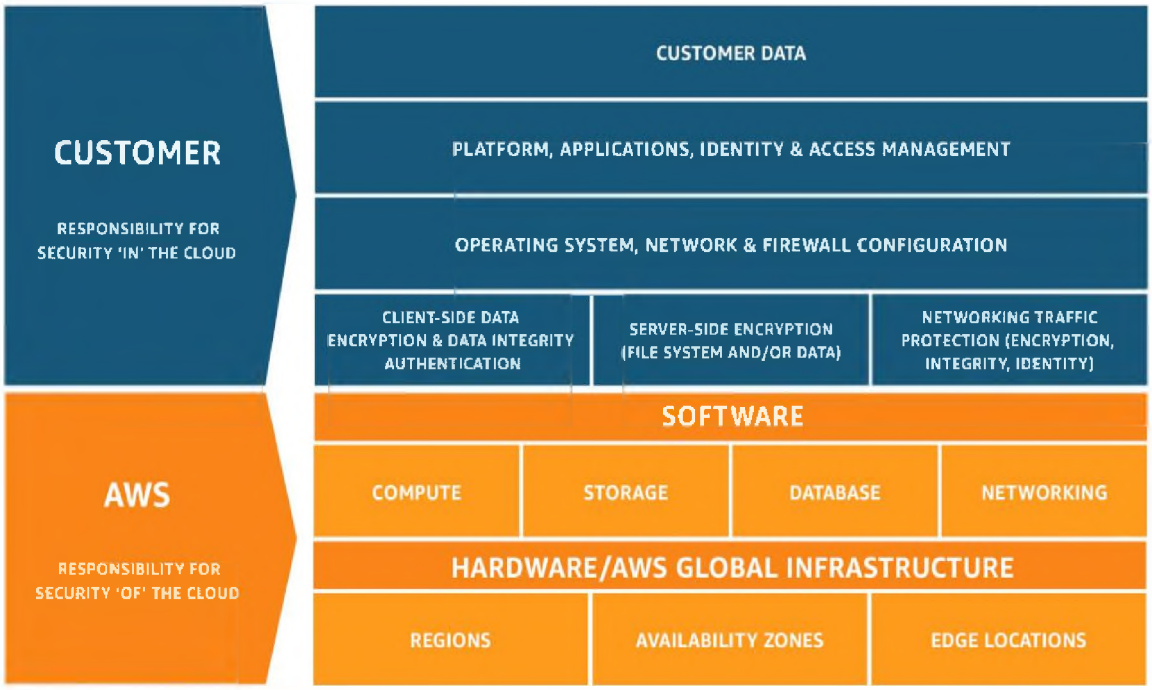

Рисунок 1.1 – Модель спільної відповідальності

Клієнти повинні уважно оцінювати сервіси, які вони використовують, оскільки їхні обов'язки залежать від обраних сервісів, інтеграції з їхнім IT-середовищем і відповідних законодавчих вимог. Такий підхід забезпечує гнучкість і контроль клієнтів над їхніми розгортаннями. AWS відповідає за безпеку інфраструктури, яка запускає всі її сервіси, включаючи апаратне забезпечення, програмне забезпечення, мережу та засоби, які підтримують хмарні сервіси AWS. Це є частиною концепції "безпека хмари". Клієнти, з іншого боку, відповідають за безпеку в хмарі, що визначається обраними хмарними сервісами AWS. Наприклад, у випадку з Amazon Elastic Compute Cloud (Amazon EC2), клієнти несуть відповідальність за управління гостьовою операційною системою, прикладним програмним забезпеченням, встановленим на екземплярах, та конфігурацією брандмауера (групами безпеки). Для сервісів, таких як Amazon S3 і Amazon DynamoDB, AWS керує інфраструктурою, операційною системою та платформою, а клієнти відповідають за управління своїми даними, включаючи налаштування шифрування та використання IAM для управління дозволами.

Модель спільної відповідальності також охоплює системи управління IT-активами. AWS забезпечує налаштування, пов'язані з фізичною інфраструктурою, тоді як клієнти керують своїми IT-ресурсами. Це дозволяє клієнтам використовувати аутсорсинг для деяких своїх IT-операцій і створювати розподілене середовище управління. Клієнти можуть використовувати документацію AWS Governance and Compliance для оцінки та перевірки налаштувань керування. AWS також надає різноманітні інструменти для спрощення керування безпекою, такі як AWS Identity and Access Management (IAM), AWS Shield, AWS Config, AWS Artifact та інші, які допомагають клієнтам забезпечити відповідність та безпеку своїх ресурсів у хмарі.

1.2 Аналіз нормативно-правової бази

Дотримання інформаційної безпеки на території України та захист її інтересів в інформаційній сфері вимагають першочергового розвитку системи правового регулювання, спрямованого на протидію загрозам цим інтересам та спрощення відповідних законодавчих процедур.

Перш за все, це пов'язано з тим, що в умовах верховенства права та існування громадянського суспільства діяльність державних органів, на які покладено першочергову відповідальність за національну безпеку, має керуватися певними правовими стандартами гарантування національної безпеки. Конституційні права і свободи громадян. Законодавчий процес у цій сфері спрямований на врегулювання мети консолідації боротьби із загрозами національній безпеці України, засобів і методів досягнення цієї мети та забезпечення схвалення політики органів державної влади.

По-друге, Україна приєдналася до міжнародного співтовариства та значно збільшила можливості забезпечення національної інформаційної безпеки, беручи участь у формуванні міжнародно-правових норм та створенні міжнародної системи забезпечення інформаційної безпеки в усьому світі та в різних країнах. в окремих штатах.

По-третє, реалізація гарантій прав і свобод громадян, захист національних інтересів України означає суттєве посилення ролі держави в регулюванні

суспільних відносин та реалізації відкритої та зрозумілої державної політики України у цій сфері.

Конституція України та Закон «Про інформацію», Закон «Про захист інформації в інформаційно-телекомунікаційних системах», Національний план інформатизації, Конституція України та закони України гарантують нормативно-правове забезпечення інформаційної безпеки у сфері прав і свобод. «Національний план планування інформатизації», «Про поштовий зв'язок», «Про хмарні послуги» та інші нормативно-правові акти регулюють такі аспекти, як забезпечення інформаційної безпеки, захист інформації, охорона державної таємниці та забезпечення захисту конфіденційної інформації. Можна відстежити кількісні пріоритети нормативно-правових дій, спрямованих на регулювання інформаційно-технологічної безпеки, як з точки зору інформаційної, так і психологічної та інформаційної безпеки у сфері прав і свобод. Це пояснюється значним розвитком інформаційних технологій і необхідністю швидко реагувати на зміни в цій сфері. Значний розрив між стандартами інформаційної безпеки та правовим контролем в Україні полягає у роздробленості нормативних актів з різною юридичною силою. Хоча в похідних законах визначено важливі аспекти, варто звернути увагу на невідповідності між різними законами та чинною конституцією. Основною особливістю національного інформаційного законодавства є наявність значного набору стандартів, але відсутність вказівок щодо їх реалізації, що призводить до низького рівня імплементації правових норм, що стосуються суспільних відносин у сфері інформаційної безпеки. Крім того, численні нормативно-правові норми, нечіткі поняття, які потребують офіційного тлумачення чи визначення, а також відсутність єдиної базової термінології (наприклад, інформаційна безпека) становлять загрозу для безпеки інформації в Україні. Аналізуючи нормативно-правові акти України у сфері інформаційної безпеки, можна зрозуміти необхідність вдосконалення законодавства у цій сфері. Добре існування компанії залежить від розвитку, якості роботи та безпеки інформаційного середовища, а також рівня нормативно-правового забезпечення цих процесів. Метою законодавства у сфері

інформаційної безпеки є закріплення національної інформаційної політики, яка базується на забезпеченні національної безпеки у сфері інформації, розвитку інформаційних технологій та засобів захисту інформації та запобігання монополізму в цій сфері. сфери, виключають розвиток деструктивних технологій, що впливають на людину, захищають авторське право та суміжні права тощо. Інформаційна безпека є невід'ємною частиною універсальної проблеми забезпечення інформацією людей, країн і суспільств. Зосередженість на захисті важливих об'єктів та законних прав та інтересів інформаційних ресурсів. Зміст поняття «інформаційна безпека» пояснюється діями відповідних відомств, науковими дослідженнями та нормативно-правовою базою. Питання відповідності національної безпеки у сфері інформаційної безпеки наразі знаходяться на стадії розробки. Забезпечення інформаційної безпеки передбачає реалізацію єдиної політики національної безпеки в інформаційній сфері через комплекс заходів в економічній, політичній та організаційній сферах, спрямованих на запобігання можливим загрозам і небезпекам для національних інтересів особи, суспільства і країни. інформаційне поле. Для встановлення та реалізації високого рівня національної безпеки в інформаційній сфері необхідно сформувати нормативно-правову систему, що регулює відносини в інформаційній сфері, уточнити основні напрями діяльності органів державного управління та створити або змінити стандарти для установ та сфери інформації. метод. Методи забезпечення інформаційної безпеки та контролю та моніторингу її діяльності. Оскільки система національної безпеки ще не створена, а національна політика, в тому числі інформаційна, є невизначеною, основні компоненти системи забезпечення інформаційної безпеки ще не завершені. Недосконаліть нормативно-правової бази негативно впливає на державне управління у цій сфері. Законодавча база України у сфері забезпечення інформаційної безпеки є незавершеною. 11 січня 2011 року Верховна Рада України прийняла поданий Кабінетом Міністрів України проект Закону про Концепцію національної інформаційної політики України (Постанова № 7251). У передмові до документу зазначено: «Ця концепція уточнює цілі, принципи,

пріоритети та основні напрямки розвитку країни в інформаційній сфері, включаючи систему виробництва, використання ресурсів і регулювання суспільних відносин, пов'язаних з інформаційною сферою». використання, поширення та зберігання інформації». Це лише окремий напрямок державної політики у сфері інформаційної безпеки, що розглядається окремо від загального забезпечення інформацією про особисту та суспільно значущу діяльність, основним аргументом національної політики є забезпечення безпеки у сфері інформаційної безпеки та інформаційних потоків, у тому числі в процесі вдосконалення співпраці між країнами. Методологія, яка включає такі основні аргументи:

1. Як об'єкт управління проаналізувати інформаційну безпеку та її складові з функціональної точки зору. Існуючі підходи до безпеки, в тому числі в області інформаційної безпеки, мають певний нормативно-правовий статус в рамках аргументу, що безпека - це захист від загроз. Ця парадигма відображена в Концепції національної безпеки України (Основи державної політики), схваленій Верховною Радою України у січні 1997 р., а також у прийнятому в Україні законі «Про основи національної безпеки України», прийнятому в липні 2003 року. Сьогодні зрозуміло, що забезпечення інформаційної безпеки є проблематичним без зміни парадигми в концепції видів безпеки та реалізації функціонального підходу. Створення моделей загроз національній безпеці та розробка захисних заходів у сфері інформаційної безпеки є компетенцією різних національних відомств. Інформаційна складова включає всі сфери, пов'язані із забезпеченням національної безпеки, тобто інформаційна безпека є спільною відповідальністю всіх міністерств, відомств та інших суб'єктів України. Лише в рамках функціонального підходу, спрямованого на забезпечення інформаційної безпеки, можливе використання наявного інтелектуального, організаційного та матеріально-технічного потенціалу для забезпечення взаємодії міністерств і відомств та координації їх діяльності. Метою є наявність функціонального підходу, здатного оцінювати та прогнозувати стан системи управління та ефективність управлінських дій для запобігання або усунення загроз

національним інтересам. Необхідність зміни концептуальної парадигми інформаційної безпеки також випливає з правових норм Основного Закону України, згідно з якими інформаційна безпека вважається однією з найважливіших функцій держави і стосується всього українського народу.

2. Захист інформаційних ресурсів в Україні, як частина процесу розширення міждержавного співробітництва, розглядається як складова частина (підсистема) загальної системи захисту інформації та важливий елемент забезпечення безпеки певної інформації. Основну сутність інформаційної безпеки можна підсумувати як низку превентивних заходів, спрямованих на забезпечення права на інформацію та свободу інформаційної діяльності, захист інформації та власності на інформацію, а також на захист інформації та інформації. Підхід до формування систем захисту інформації та практичне вирішення поставлених завдань показує, що ефективність будь-якої підсистеми напряму залежить від ефективного функціонування системи, яка цю підсистему інкапсулює. Іншими словами, вдосконалення системи інформаційної безпеки в процесі розширення міждержавного співробітництва має базуватися на ефективно функціонуючій комплексній системі забезпечення інформаційної безпеки як важливого елемента національної безпеки України.

3. Інформація та інформаційне поле розглядаються як системні складові різних сфер життя і діяльності соціальної системи. Інформаційна безпека стає все більш важливим чинником стану політики, економіки, суспільства, національної оборони, інформації та інших сфер. складова національної безпеки. Вимоги інформаційної безпеки мають бути органічно інтегровані в законодавство всіх рівнів, включаючи конституційне законодавство, основні загальні закони, організаційні закони національної системи управління, окремі закони, закони відомчі тощо. Наведемо структуру нормативно-правових актів, спрямованих на забезпечення національної інформаційної безпеки:

– конституційне законодавство. Норми, що стосуються питань інформатизації, безпеки інформації тощо, входять у нього як складові елементи;

– загальні закони, кодекси (про власність, про надра, про землю, про права громадян, про громадянство, про податки, про антимонопольну діяльність тощо), які містять норми з питань інформаційної безпеки;

– закони про організацію керування, які стосуються окремих структур господарства, економіки, системи державних органів та визначають їх статус. Вони містять окремі норми з забезпечення інформаційної безпеки. Поряд із загальними аспектами інформаційного забезпечення та інформаційної безпеки конкретного органу ці норми мають встановлювати його обов'язки з формування, актуалізації інформаційної безпеки, що представляють загальнодержавний інтерес;

– спеціальні закони, які розповсюджуються на конкретні сфери відносин, галузі господарства, процеси. До складу спеціального законодавства, яке формує правову основу інформаційної безпеки, входить Закон України «Про інформацію» та інші нормативно-правові акти. Саме цей набір законів забезпечує правову підтримку у сфері інформаційної безпеки;

– підзаконні нормативні акти, що забезпечують інформаційну безпеку;

– законодавство України, що містить норми про відповідальність за правопорушення у сфері безпеки інформації.

Правовою основою забезпечення інформаційної безпеки в Україні є Конституція України, Концепція інформаційної безпеки України, закони України, міжнародні договори, укладені Верховною Радою України, та підзаконні акти, що приймаються на їх виконання. Примітно, що цю сферу суспільних відносин регулюють понад 30 законів. Третій пункт нормативно-правових положень щодо інформаційної безпеки включає:

– загальнодержавні та міжвідомчі напрями державної політики інформаційної безпеки, що реалізуються суб'єктами у сферах їх відання;

– захист прав, свобод і законних інтересів особи, суспільства, держави;

– забезпечення інформаційного суверенітету;

– формування державної інформаційної політики та підвищення її ролі в забезпеченні інформаційної політики;

– забезпечення безпеки функціонування всіх елементів національного інформаційного простору та його інтегрування у світовий інформаційний простір;

– створення єдиної системи охорони та технічного захисту інформації обмеженого доступу, що підлягає охороні з боку держави;

– забезпечення безпеки інформаційно-телекомунікаційних систем, мереж зв'язку та використання Інтернету;

– захист національних інтересів у процесі міжнародного співробітництва;

– прогнозування ризиків державної внутрішньої і зовнішньої політики, соціально-економічного розвитку, державного будівництва;

– виявлення, попередження і нейтралізація джерел внутрішніх і зовнішніх інформаційних загроз;

– участь у двосторонніх і багатосторонніх системах забезпечення міжнародної інформаційної безпеки;

– забезпечення загальнодержавного керівництва, координації і контролю у сфері реалізації державної політики з питань інформаційної безпеки та оцінки її результативності.

Спеціальне законодавство у сфері інформаційної безпеки представлено низкою законів. Серед них «Основний закон про інформацію» займає особливе місце, оскільки встановлює правові основи всієї інформаційної діяльності. Це законодавство гарантує інформаційні права громадян України та встановлює правові основи інформаційної діяльності, включаючи спеціальні закони, такі як «Про інформацію» та «Про інформаційну безпеку», українські концепції інформаційної безпеки та закони, що регулюють інформаційну безпеку. у всіх сферах діяльності індивідів, суспільств і націй. Це охоплює політичну, економічну, оборонну, безпекову та громадський порядок, соціальну та гуманітарну, технологічну, екологічну та інформаційну сфери. Положення регулює правовідносини у сфері забезпечення інформаційної безпеки, у тому числі взаємодію органів державної влади та управління діяльністю з цих питань.

Серед важливих кроків – створення основ наукового, матеріально-технічного, фінансового та кадрового забезпечення інформаційної безпеки та здійснення контролю та моніторингу виконання чинного законодавства з питань безпеки певної інформації.

Закон України «Про основи національної безпеки України» визначає дев'ять сфер національної безпеки: зовнішньополітичну, державну безпеку, економічну, соціальну та гуманітарну, воєнну, безпеку державного кордону, внутрішньополітичну, екологічну, науково-технологічну та інформаційну. Тому інформаційна безпека є важливим елементом національної безпеки. У цьому законі системно визначено основні функції, які виконує система національної безпеки в окремих сферах. З урахуванням особливостей інформаційного поля його специфікація визначає основні функції системи захисту інформації України. Проте, незважаючи на зростання кількості законів, багато сфер соціального та цивільного життя залишаються неврегульованими на законодавчому рівні, створюючи можливості для розвитку галузевих законів. Наприклад, центральні та місцеві адміністративні органи, такі як Національний банк Китаю, Державна податкова адміністрація, Державна митна адміністрація та Національний фонд нерухомості, активно розробляють нормативно-правові документи та швидко їх переглядають і впроваджують. Недостатня правова регламентація інформаційних правовідносин надзвичайно ускладнює досягнення якісних змін у цій сфері суспільних відносин.

На сьогодні через відсутність взаємопов'язаних, чітко розроблених заходів та теоретичних напрацювань щодо забезпечення інформаційної безпеки держави існує багато перешкод на шляху до повноцінної реалізації державного обов'язку щодо забезпечення інформаційної безпеки, яка є невід'ємною частиною національної безпеки. Лише впровадження науково обґрунтованої державної інформаційної політики може створити ефективну систему протидії правопорушенням у цій сфері. Існує нагальна потреба у розробці єдиного комплексного системо утворюючого законодавчого акта, який забезпечив би:

– створення єдиної стратегії реалізації державної політики у сфері інформаційної безпеки;

– розробку організаційно-правових механізмів забезпечення інформаційної безпеки;

– визначення правового статусу суб'єктів інформаційних відносин та встановлення їх відповідальності за дотримання національного законодавства у цій сфері;

– створення системи підготовки кадрів, які працюватимуть у галузі забезпечення інформаційної безпеки.

1.3 Постановка задачі

Дана кваліфікаційна робота може послужити підґрунтям для створення системи захищеної інфраструктури на платформі AWS з використанням методології Infrastructure as a Code (IaC) з використанням Terraform. Призначенням розробки є створення та впровадження системи, яка автоматизує процес розгортання й налаштування безпеки інфраструктури AWS, забезпечуючи її відповідність сучасним стандартам кібербезпеки.

Метою розробки є автоматизація процесу побудови та управління захищеною інфраструктурою на AWS з використанням Terraform, що забезпечить високу адаптивність та безпеку системи. Для досягнення цієї мети необхідно вирішити наступні задачі:

– аналіз вимог безпеки: провести детальний аналіз вимог безпеки для хмарної інфраструктури на AWS, враховуючи міжнародні стандарти та найкращі практики;

– розробка архітектури інфраструктури: Створити архітектуру безпечної хмарної інфраструктури, яка включатиме мережеву ізоляцію, шифрування даних, автентифікацію та авторизацію користувачів;

– розробка Terraform конфігурацій: написати Terraform конфігураційні файли для автоматизованого розгортання та налаштування інфраструктури, що відповідає вимогам безпеки;

– тестування інфраструктури: провести тестування розгорнутої інфраструктури на відповідність вимогам безпеки та функціональності;

– впровадження засобів моніторингу та реагування: Інтегрувати засоби моніторингу та реагування на інциденти безпеки для оперативного виявлення та усунення загроз;

– документування процесу та результатів: Створити документацію, що детально описує процес розробки, тестування та впровадження захищеної інфраструктури на AWS.

1.4 Висновок

У даному розділі був наведений опис предметного середовища, причини, що призвели до створення даної роботи, а також можливі технічні рішення ТОВ «ОІК». Було визначене призначення розробки, а також мета. Для вирішення поставленої мети були сформовані задачі, що мають бути вирішені.

Був наведений детальний опис процесів діяльності, визначені актори, складений опис функціональної моделі, а також визначені функціональні та нефункціональні вимоги до системи, що розробляється. Було проведено огляд існуючих аналогів та визначені відмінності аналогів від розробленої системи.

Ця розробка сприятиме підвищенню рівня безпеки хмарної інфраструктури, забезпечуючи надійність та відповідність сучасним вимогам кібербезпеки за допомогою автоматизованих засобів налаштування та управління.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Відомості про підприємство ТОВ «ОІК»

Об'єктом інформаційної діяльності є інтернет-сервіс, він не має фізичного офісу, тож не є частиною інженерно-технічної споруди адреси реєстрації. Підприємство зареєстровано за адресою: м. Дніпро, вул. Січеславська, буд. 21.

ТОВ «ОІК» надає широкий асортимент послуг з економії коштів при використанні хмарних провайдерів й їх послуг. На ОІД виконується підключення облікових записів користувачів після чого надаються рекомендації щодо шляхів економії коштів на наявній інфраструктурі клієнта. Підприємство працює з понеділка по п'ятницю. Графік роботи з 9:00 до 18:00. Перерва з 13:00 до 14:00. Робочих годин на місяць: 172.

Організаційна структура ТОВ «ОІК»:

1 Директор – 1чол.;

2 Розробники – 4 чол.;

3 Системний адміністратор – 1 чол.;

4 Інженери контролю якості – 2 чол.;

5 Бухгалтер – 1 чол.;

На підприємстві функціонує АС «Excel» (рис. 2.1.). ПЗ використовується для контролю усіх фінансових операцій, а також контролю матеріально-технічного забезпечення, активів підприємства, персоналу і розрахунку заробітної плати. Доступ до робочого простору кожен з працівників отримує через VPN "Pritunl", технічний сервіс забезпечує цілодобовий доступ до інформаційно-комунікаційних мереж виробництва співробітникам, надає можливість централізовано віднестись до забезпечення технічної захищеності, та відповідності вимогам держави відносно захисту інформації.

2.1.1 Обстеження інформаційної діяльності підприємства

Метою обстеження є підготовка вихідних даних для визначення актуальних технологій та політик, що використовуються підприємством та

вивчення можливості їх модифікації для впровадження моделі захисту інформації.

Щоб провести обстеження інформаційної діяльності підприємства необхідно:

– провести загальний аналіз підприємства, в результаті чого написати загальну характеристику організації (пункт 2.1);

– дослідити логічне та технічне середовище ТОВ «ОІК»;

– визначити актуальні політики та технології захисту інформації, що використовуються виробництвом;

– визначити типи користувачів, рівні їх доступів;

– визначити технології, які будуть використані для вдосконалення моделі захисту інформації.

2.1.2 Обстеження ІТС

Хмарна архітектура передбачає собою відсутність необхідності утримання технічної бази виробництва, але для розуміння механізму роботи політик та нижче наведено топологію підприємства (рис. 2.1).

Основні компоненти ІТС:

1. Amazon Virtual Private Cloud (VPC): Публічні підмережі: Розташовані в різних зонах доступності для забезпечення високої доступності. Використовуються для розміщення загальнодоступних ресурсів. Приватні підмережі: Використовуються для розміщення приватних ресурсів, таких як бази даних і обчислювальні ресурси.

2. CloudFront: Використовується для доставки контенту з низькою затримкою до клієнтів.

3. VPN: Забезпечує захищений доступ до ресурсів в VPC для працівників через VPN ALB (Application Load Balancer).

4. ALB (Application Load Balancer): VPN ALB: Забезпечує балансування навантаження для VPN з'єднань. Публічний ALB: Забезпечує балансування навантаження для загальнодоступних вебзастосунків.

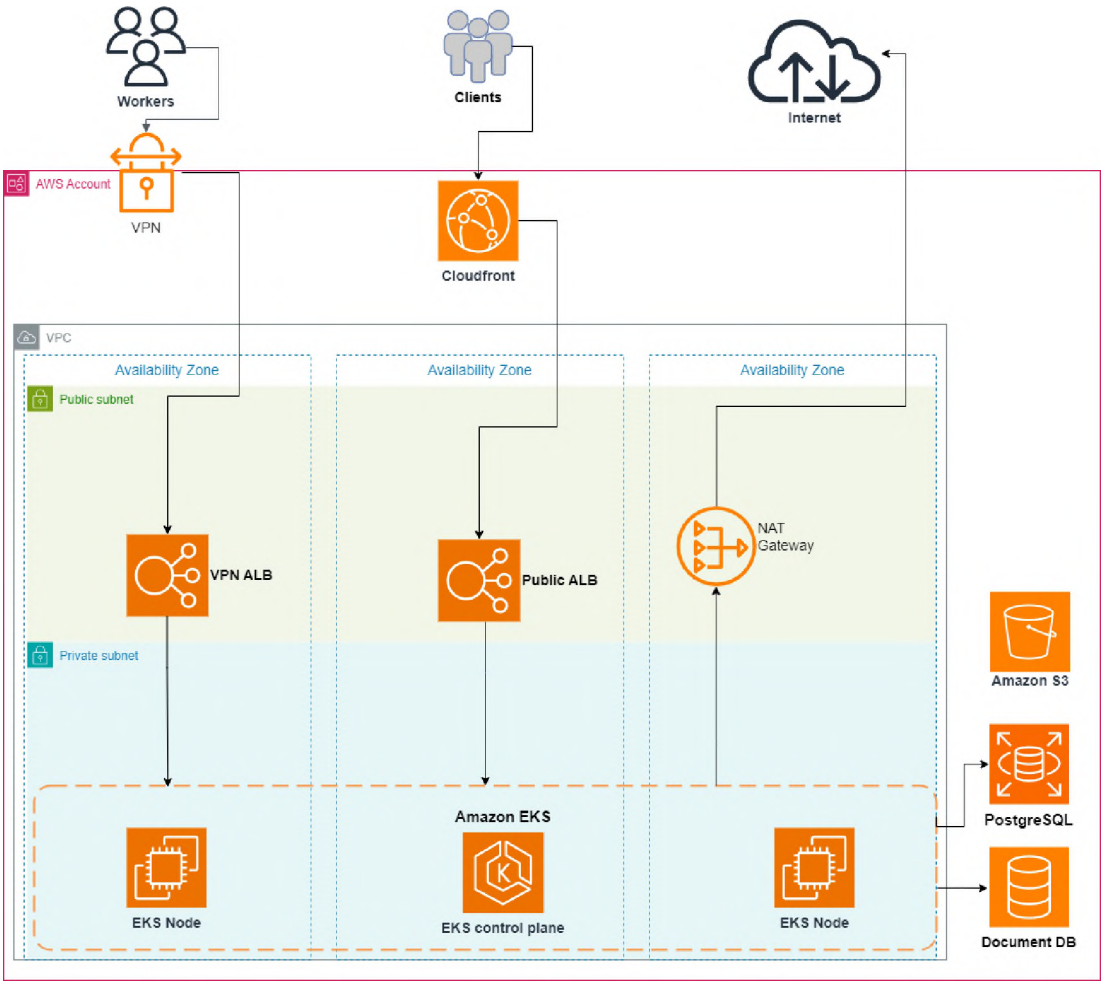

Рисунок 2.1 – Схематичне зображення топології виробництва

5. NAT Gateway: Дозволяє ресурсам в приватних підмережах доступ до Інтернету для завантаження оновлень і програмного забезпечення.

6. Amazon EKS (Elastic Kubernetes Service): EKS контрольний вузол: Керує кластером Kubernetes. EKS вузли: Запускають контейнери, що обробляють запити користувачів і співробітників.

7. Сервіси зберігання і бази даних: Amazon S3: Використовується для зберігання всіх необхідних даних, включаючи логи та технічну інформацію. PostgreSQL: Використовується як реляційна база даних для зберігання

інформації про товари та інші супутні дані. Document DB: Використовується для зберігання документів і структурованих даних.

Ноутбуки для працівників:

Використовуються для виконання робочих обов'язків. Всі працівники забезпечені однаковими ноутбуками HP Pavilion 15-eh1070wm за рахунок компанії з наступними характеристиками:

Характеристика комп'ютерів (9 шт.):

- процесор – AMD Ryzen 5 5500U;
- ОЗУ – 16 ГБ DDR4;
- вінчестер – 1 ТБ SSD;
- відеокарта – Radeon RX Vega 7;
- тип системи – 64-разрядная ОС;
- операційна система – Windows 10;
- монітор: 15.6" IPS (1920x1080) Full HD;
- додатково: сканер відбитків пальців.

Програмне забезпечення:

АС «Excel» – використовується для контролю фінансових операцій та матеріально-технічного забезпечення.

Microsoft Office 2023, Google Chrome, Skype, Excel, Pritunl Client, Slack, Visual Studio Code, Terrafrom, LENS, Kubectl, AWS CLI – основні програмні засоби для роботи працівників.

Таким чином, архітектура ІТС ТОВ «ОІК» забезпечує високу надійність та безпеку інформаційних ресурсів, а також гнучкість у масштабуванні ресурсів відповідно до потреб підприємства.

2.2 Аналіз загроз інформації, що циркулює в ОІД

У товаристві з обмеженою відповідальністю «ОІК» обробляється та зберігається значна кількість конфіденційної інформації, включаючи персональні

дані клієнтів, контракти, дані облікових записів, фінансові операції та інша інформація. Втрата або незаконний доступ до цих даних може мати серйозні наслідки, такі як фінансові збитки, втрата клієнтів і погіршення репутації компанії. Отже, необхідно забезпечити надійний захист інформаційних ресурсів від несанкціонованого доступу.

Оцінка рівня конфіденційності:

К0: Розголошення призведе до серйозних матеріальних втрат або повного збою системи.

К1: Розголошення може спричинити значні матеріальні втрати, якщо не будуть вжиті відповідні заходи захисту.

К2: Розголошення може призвести до певних матеріальних втрат.

К3: Розголошення може викликати матеріальні збитки в окремих випадках.

К4: Розголошення може призвести до незначних збитків лише в рідкісних випадках.

Оцінка рівня цілісності:

Ц0: Незаконні зміни спричинять неправильну роботу системи в цілому або значної її частини, наслідки будуть незворотними.

Ц1: Незаконні зміни можуть викликати неправильну роботу системи з часом, якщо не буде вжито заходів захисту, наслідки будуть незворотніми.

Ц2: Незаконні зміни можуть призвести до неправильної роботи системи з часом, але наслідки будуть оборотними.

Ц3: Незаконні зміни не викликатимуть збою в роботі системи, наслідки будуть оборотними.

Ц4: Незаконні зміни не впливатимуть на роботу системи.

Оцінка рівня доступності:

Д0: Порушення доступності не призведе до матеріальних збитків або збою в роботі системи.

Д1: Порушення доступності призведе до мінімальних збитків матеріального прибутку, але робота системи не порушується, загальний дохід залишається незмінним або незначно зменшується.

Д2: Порушення доступності призведе до середніх збитків матеріального прибутку протягом поточного кварталу, робота системи не порушується, можливі відставання від конкурентів.

Д3: Порушення доступності призведе до збитків матеріального прибутку, робота системи ускладняється, загальний дохід може знизитися до половини поточного рівня.

Д4: Порушення доступності призведе до найвищих збитків матеріального прибутку протягом декількох кварталів, необхідні радикальні рішення щодо доступності інформації на підприємстві.

Захист інформації є критично важливим, оскільки навіть незначні деталі можуть бути використані зловмисниками або конкурентами для компрометації чи завдання економічної шкоди. Таким чином, ретельний захист інформаційних ресурсів є пріоритетним завданням для ТОВ «ОІК». Нижче у таблиці 2.1 наведено перелік інформації, що обробляється на підприємстві.

Таблиця 2.1 – Перелік інформації яка циркулює в ОІД

№	Інформація	Вид зберігання	Оцінка рівнів	Правовий режим
1	Перелік послуг	Електронний	К4 Ц3 Д1	Відкрита
2	Інформація про працівників і займані ними посади	Електронний	К2 Ц2 Д4	Конфіденційна
3	Інформація щодо організації	Електронний	К2 Ц2 Д4	Конфіденційна
4	База даних клієнтів	Електронний	К1 Ц2 Д3	Комерційна таємниця
5	Програмний код сервісів	Електронний	К1 Ц2 Д3	Комерційна таємниця
6	Інформація про фінансову діяльність організації	Електронний	К1 Ц1 Д3	Конфіденційна

Продовження таблиці 2.1

7	Бухгалтерський облік	Електронний	К1 Ц2 Д3	Комерційна таємниця
8	Договори про співпрацю з хмарними провайдерами	Електронний	К4 Ц3 Д1	Конфіденційна

2.2.1 Обстеження середовища користувачів ІТС

Директор – 1 особа. Координує діяльність всього персоналу, проводить зустрічі з постачальниками хмарних послуг, рекламними агентствами та VIP-клієнтами.

Бухгалтер – 1 особа. Веде бухгалтерський і фінансовий облік, а також здійснює інші економічні розрахунки.

Розробник – 4 особи. Займаються розробкою, вдосконаленням та виправленням програмного коду інтернет-сервісу.

Інженер з контролю якості – 2 особи. Забезпечують тестування та перевірку працездатності програмного коду, відповідають за технічну підтримку клієнтів, відповідають на їхні запити та питання, надають асистентську допомогу у використанні сервісів або послуг компанії.

Системний адміністратор – 1 особа. Відповідає за підтримку та налаштування внутрішніх комп'ютерів та інфраструктури, включаючи мережі, сервери та внутрішні ПК. Займається налаштуванням та установкою програмного забезпечення, стежить за роботою сайту та оновлює його інформаційне наповнення. Також надає допомогу в роботі з базами даних та здійснює дистанційну підтримку та налаштування систем. Виконує обов'язки клауд-інженера, що включає управління хмарною інфраструктурою, моніторинг і підтримку хмарних сервісів та вирішення технічних проблем, пов'язаних з хмарними рішеннями.

Матриця доступу до інформації наведена в таблиці 2.3 у котрій R – перегляд інформації, W – модифікація інформації, D – видалення інформації.

Таблиця 2.2 – Матриця доступу до інформації

Інформація	Директор	Бухгалтер	Розробники	Інженер з контролю якості	Системний адміністратор
1	R	R	R,W,D	R	R,W,D
2	R,W,D	R,W	R	R	R
3	R,W,D	R	R	R	R
4	R	R	R,W	R	R,W,D
5	R	-	R,W,D	-	R,W,D
6	R,W,D	R,W,D	-	-	-
7	R	R,W,D	-	-	-
8	R,W,D	R	-	-	-

2.2.2 Модель порушника

При побудові моделі порушника для хмарної інформаційно-телекомунікаційної системи виникають складнощі пов'язані з потребою врахування моделі розгортання хмари, рівень контролю провайдера й користувачів над інфраструктурою хмари й моделі надання послуг. Побудова моделі порушника та моделі загроз дозволяє сформувати вимоги до систем захисту інформації у хмарних ІТС. Модель порушника передбачає абстрактний опис його поведінки, який може бути формальним або неформальним. Ця модель відображає практичні та теоретичні можливості правопорушника, його попередні знання, обізнаність, час та місце дій тощо.

Категорії осіб, з числа яких може бути порушник:

Внутрішні порушники (працівники провайдера хмарних послуг, працівники користувача, сторонні особи з доступом до ресурсів ІТС хмари);

Пв1 – директор, системний адміністратор;

Пв2 – Розробники;

Пв3 – Інженери контролю якості;

Пв4 – Бухгалтер;

Пв5 – Оператори технічної підтримки;

Зовнішні порушники (особи, що не мають безпосереднього доступу до ресурсів ІТС хмари).

Пз1 – конкуренти;

Пз2 – кримінальні структури;

Пз3 – випадкові особи.

Рівень можливостей порушника:

РМ1: Запуск фіксованого набору завдань (програм) з передбаченими функціями обробки інформації;

РМ2: Створення та запуск власних програм з новими функціями обробки інформації;

РМ3: Управління функціонуванням ІТС хмари (вплив на базове ПЗ, склад і конфігурацію устаткування);

РМ4: Проектування, реалізація та ремонт апаратних компонентів ІТС хмари з можливістю включення нових засобів з новими функціями обробки інформації.

Рівень ознайомлення з системою:

РО1: Користувачі без спеціальних знань з обчислювальної техніки та програмування;

РО2: Особи з базовим або високим рівнем знань у галузі обчислювальної техніки та програмування;

РО3: Особи, що володіють інформацією про функціональні особливості визначеної ІТС хмари;

РО4: Особи з високим рівнем знань та досвідом роботи з технічними засобами системи хмари;

РО5: Особи з інформацією про функції та механізм дії засобів захисту в визначеній ІТС хмари.

Характер дій порушника:

ХД1: Випадковий порушник (користувачі, обслуговуючий персонал, що ненавмисно порушили політику безпеки);

ХД2: Пасивний порушник (авторизований користувач, що навмисно порушив політику безпеки, але не вживає рішучих дій);

ХД3: Активний порушник (порушник, який не приховує своїх дій та використовує всі доступні методи та засоби для порушення безпеки);

ХД4: Віддалений порушник (порушник, що використовує засоби віддаленого доступу до інформаційних об'єктів).

Методи та засоби, що використовує порушник:

МЗ1: Агентурні методи одержання відомостей;

МЗ2: Пасивні технічні засоби перехоплення інформаційних сигналів;

МЗ3: Штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;

МЗ4: Активний вплив на АС, що змінює конфігурацію системи.

Мета, яку переслідує порушник:

МТ1: Авторизація та отримання атрибутів доступу з найбільшими правами до ресурсів ІТС для ознайомлення з конфіденційною інформацією, її модифікації чи знищення;

МТ2: Пошук та/або здобуття атрибутів доступу осіб з найбільшими правами;

МТ3: Проникнення на місця розміщення компонентів, елементів чи ресурсів АС та нанесення збитків;

МТ4: Установка фізичних або програмних засобів для знімання або модифікації інформації;

МТ5: Здійснення спроб несанкціонованого доступу до обчислювальних ресурсів, інформаційних ресурсів, базового та прикладного ПЗ, а також до телекомунікаційної підсистеми.

Способи реалізації загроз:

СР1: Технічні канали (побічні електромагнітні випромінювання, акустичні, віброакустичні, оптичні, радіо та радіотехнічні, хімічні та інші канали);

СР2: Спеціальний вплив (формування полів і сигналів для руйнування системи захисту або порушення цілісності інформації);

СР3: Несанкціонований доступ (підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів).

Мотиви порушника:

М1: Безвідповідальність;

М2: Самоствердження;

М3: Вилучення матеріальної вигоди;

М4: Помста.

Рівень загрози, яку несе порушник, наведено з розподілом від 1 до 5. Мінімальне значення - 1, максимальне – 5.

У таблиці 2.3 наведена модель порушника для ОІД ТОВ «ОІК».

Таблиця 2.3 – Модель порушника

Категорія осіб	Рівень можливостей	Рівень ознайомлення з системою	Характер дій	Методи та засоби	Мета порушника	Способи реалізації загроз	Мотиви порушника	Рівень загрози
Пв1	РМ4	РО4	ХД3	М33, М34	МТ1, МТ4	СР3	М3, М4	5
Пв2	РМ3	РО3	ХД2	М32, М33	МТ1, МТ2	СР3	М1, М2	4
Пв3	РМ3	РО3	ХД2	М32, М33	МТ1, МТ2	СР3	М1, М2	4
Пв4	РМ2	РО2	ХД1	М31, М32	МТ1, МТ3	СР2	М1	3

Продовження таблиці 2.3

Пв5	РМ1	РО1	ХД1	МЗ1	МТ1, МТ3	СР1	М1	2
Пз1	РМ2	РО3	ХД3	МЗ3, МЗ4	МТ2, МТ5	СР3	М3	4
Пз2	РМ3	РО4	ХД4	МЗ4	МТ1, МТ3, МТ5	СР1, СР3	М3	5

Отже, найбільшу загрозу для ОІД становлять порушники з групи Пз2 (кримінальні структури), оскільки ці особи мають мотив і достатній рівень кваліфікації. Значну загрозу можуть також представляти порушники з групи Пв1 (директор, системний адміністратор), оскільки вони мають доступ до всіх інформаційних ресурсів підприємства. Проте, враховуючи, що ці особи мають безпосередню зацікавленість у роботі підприємства, їх можна не вважати потенційною загрозою.

2.2.3 Модель загроз

Наведені в пункті 2.2.2 потенційні можливості порушника дозволили розробити модель загроз для хмарних сервісів (обчислень). Детальний опис цієї моделі загроз наведено в таблиці 2.3, де зазначено об'єкт загрози, мету порушника, ймовірність реалізації загрози та мету захисних заходів.

Оцінювання рівнів загроз для інформації на об'єкті здійснюється за двома критеріями: рівень збитків та ймовірність реалізації загрози. Рівень небезпеки конкретної загрози визначається як добуток цих показників.

Рівень збитків визначається показниками, що відображають втрати компанії у випадку реалізації загрози. У даному контексті збитками вважаються витрати часу на відновлення втрачених властивостей інформації.

Рівні збитків класифікуються наступним чином:

– значний (від 12 до 24 годин);
– помірний (від 2 до 12 годин);

– незначний (до 2 годин).

Ймовірність реалізації загрози оцінюється числовим значенням від 0 до 1:

– 0 - відсутність загрози;

– 0.1 - мінімальна ймовірність реалізації загрози;

– 1 - найвища ймовірність реалізації загрози.

У таблиці 2.4 показані рівні загроз для інформації.

Таблиця 2.4 – Модель загроз інформації

№	Об'єкт загрози	Мета	Методи захисту	Ймовірність реалізації	Рівень збитків при ...	Рівень загрози
1	Управління та моніторинг безпеки хмарних сервісів	Отримання несанкціонованого доступу до хмарної інфраструктури	Застосування систем контролю доступу, політик безпеки, атестація персоналу	0.25	3	0.75
2	Обладнання для контролю доступу	Отримання несанкціонованого доступу до хмарних ресурсів або управління хмарною інфраструктурою	Використання захищених ключових носіїв для автентифікації	0.75	3	2.25
3	Хмарні ресурси	Отримання несанкціонованого доступу до файлів, баз даних або використання обчислювальних ресурсів	Впровадження механізмів обмеження доступу, шифрування даних, моніторинг роботи	0.25	3	0.75

Продовження таблиці 2.4

4	Хмарне середовище: сервіси, додатки та інфраструктура	Порушення прав доступу до сервісів, додатків та об'єктів інфраструктури. Несанкціонований доступ до функцій управління інфраструктурою, даних сервісів та користувачів хмари. Зараження шпигунським ПЗ та вірусами	Використання технологій розмежування та обмеження доступу, контроль цілісності об'єктів та їх моніторинг	0.75	3	2.25
5	Віртуальні мережі в межах хмарної інфраструктури	Прослуховування трафіку, порушення цілісності та доступності, організація атак DoS, несанкціоноване підключення до мережі	Використання засобів захисту даних у мережі, систем виявлення та протидії мережевим атакам, моніторинг роботи	0.1	3	0.3
6	Гіпервізор	Повний контроль над розгорнутими віртуальними середовищами	Захист гіпервізора та контроль його налаштувань	0.1	3	0.3
7	Фізичне обладнання	Встановлення засобів несанкціонованого доступу, модифікація або знищення обладнання	Використання систем контролю доступу, політик безпеки, атестація персоналу. Створення контрольованої зони	0.1	3	0.3

Продовження таблиці 2.4

8	Допоміжні системи (живлення, охорона, безпека, охолодження)	Порушення доступності центрів обробки даних (ЦОД)	Використання систем контролю доступу, політик безпеки, атестація персоналу	0.25	3	0.75
9	Управління та моніторинг роботи хмарної інфраструктури	Отримання несанкціонованого доступу до налаштувань хмарної інфраструктури	Використання технологій розмежування та обмеження доступу, моніторинг дій адміністраторів	0.25	3	0.75
10	Зв'язки між хмарними центрами обробки даних (ЦОД)	Порушення доступності ЦОД, отримання несанкціонованого доступу до інформації, що передається між ЦОД	Використання надійних протоколів з міцними криптографічними алгоритмами	0.1	3	0.3

2.2.4 Методи захисту

На основі аналізу поточного стану стандартизації та використання хмарних сервісів була розроблена модель хмарних обчислень, порушень та загроз хмарних сервісів, яка може виявляти найбільш критичні питання та першочергові завдання для вирішення у хмарних сервісах. Завданнями захисту критичних ключів та інформації є забезпечення конфіденційності, цілісності, автентичності та доступності. Аналіз ситуації показав, що загрози, пов’язані з критично важливими даними в хмарному середовищі, включають витоки, несанкціоноване знищення, перехоплення та атаки. Це стосується, зокрема, пам'яті, ослаблення та несанкціонованого використання ключів.

Безперечно, найбільша загроза для критичних даних користувачів у середовищі хмарних обчислень походить від адміністратора хмарної служби, який має доступ до середовища, де розгортаються хмарні програми користувача. Також було детально проаналізовано стан безпеки та вимоги до управління інформаційною безпекою з точки зору нормативних документів і стандартів. Використання комплексу організаційно-технічних заходів і технічних засобів забезпечує високий рівень безпеки в хмарному обчислювальному середовищі. Зокрема, на рівні користувача власники ключів захищені з необхідним рівнем безпеки; на каналі зв'язку між користувачем і хмарою забезпечується захищений канал зв'язку, де обидві сторони аутентифікують одна одну, і стабільність вище, ніж стабільність ключа передачі. Для послуг ідентифікації, автентифікації, авторизації та управління правами доступу використовуються надійні протоколи автентифікації та стабільні алгоритми шифрування. Для послуг ідентифікації, автентифікації, авторизації та управління правами доступу використовуються надійні протоколи автентифікації та стабільні алгоритми шифрування. Нижче розглянуто деякі з найпоширеніших і найнадійніших протоколів, які використовуються для забезпечення безпеки в хмарних обчислювальних середовищах:

Протоколи автентифікації:

OAuth 2.0: OAuth 2.0 є протоколом відкритої авторизації, який дозволяє додаткам отримати обмежений доступ до ресурсів користувача без необхідності передавати облікові дані користувача. Широко використовується для автентифікації та авторизації в вебдодатках, мобільних додатках і сервісах API. Підтримує сценарії автентифікації з декількома факторами.

OpenID Connect: OpenID Connect є рівнем ідентифікації, побудованим поверх OAuth 2.0. Він дозволяє клієнтам перевіряти ідентичність користувачів на основі автентифікації, виконаної постачальником OpenID, а також отримувати основну інформацію про профіль користувача. Використовується для єдиної автентифікації (SSO) та управління доступом до вебдодатків та мобільних додатків.

SAML (Security Assertion Markup Language): SAML є XML-базованим стандартом для обміну аутентифікаційними та авторизаційними даними між різними сторонами, зокрема, між постачальником ідентифікаційних даних та постачальником послуг. Використовується для корпоративних вебдодатків, що підтримують єдину автентифікацію, зокрема у великих організаціях і підприємствах.

Алгоритми шифрування:

AES (Advanced Encryption Standard): AES є симетричним блоковим шифром, який був прийнятий як стандарт шифрування урядом США. Він підтримує ключі розміром 128, 192 і 256 біт. Застосування: Використовується для захисту даних на рівні транспортного протоколу, зберігання даних та у багатьох інших додатках, де потрібне високоефективне шифрування.

RSA (Rivest–Shamir–Adleman): RSA є асиметричним криптографічним алгоритмом, який використовує пару ключів (відкритий і закритий ключ) для шифрування та підпису даних. Застосування: Використовується для захисту даних при передачі, цифрових підписів, а також для обміну ключами.

SHA (Secure Hash Algorithm): SHA є сімейством криптографічних хеш-функцій, розроблених Агентством національної безпеки США (NSA). Вони генерують унікальний хеш-код фіксованої довжини для будь-якого вхідного повідомлення. Використовується для забезпечення цілісності даних, перевірки цифрових підписів та автентифікації повідомлень.

Протоколи захисту передачі даних:

TLS (Transport Layer Security): TLS є криптографічним протоколом, що забезпечує безпеку зв'язку через комп'ютерні мережі. Він забезпечує конфіденційність, цілісність даних та автентифікацію серверів і клієнтів. Використовується для захисту HTTP (HTTPS), електронної пошти (SMTP, IMAP/POP3), VoIP та інших протоколів передачі даних.

IPsec (Internet Protocol Security): IPsec є набором протоколів для забезпечення безпечного обміну IP-пакетами через IP-мережу. Він забезпечує автентифікацію, шифрування та цілісність даних. Використовується для

створення віртуальних приватних мереж (VPN) та забезпечення захисту між мережевих з'єднань.

Застосування цих протоколів та алгоритмів шифрування забезпечує високий рівень захисту даних у хмарних обчислювальних середовищах, мінімізуючи ризики витоку, перехоплення та несанкціонованого доступу до критично важливої інформації.

Одним з важливих аспектів захисту є навчання персоналу. Проведення регулярних тренінгів та семінарів дозволяє співробітникам краще розуміти актуальні загрози та методи їх запобігання. Це включає розпізнавання фішингових атак, безпечне використання програмного забезпечення, а також правильне поводження з конфіденційною інформацією.

Фільтри електронної пошти є ще одним важливим методом захисту. Вони допомагають виявляти та блокувати фішингові листи, спам та інші шкідливі повідомлення, які можуть становити загрозу для інформаційної безпеки організації.

Застосування AWS WAF (Web Application Firewall) також є ефективним методом захисту. AWS WAF дозволяє захищати вебдодатки від поширених вебзагроз, таких як атаки типу DDoS, бот-атаки та інші типи шкідливого трафіку. WAF забезпечує контроль доступу до вебдодатків, що допомагає зменшити ризики несанкціонованого доступу та зловживання.

На основі вищезазначеного було визначено, що найкращим варіантом є використання інструменту IaC (Infrastructure as Code). Ці інструменти застосовують ключі шифрування та дозволяють контролювати хмарну інфраструктуру за допомогою коду. Цей підхід мінімізує кількість осіб, які мають доступ до хмарного керування, і час, необхідний для створення та модифікації інфраструктури. Зменшення часу розгортання інфраструктури знижує ймовірність перехоплення даних порівняно з розгортанням стандартних ресурсів через вебінтерфейс AWS.

Хмарні технології, окрім забезпечення гнучкості та масштабованості, також є методом захисту завдяки передачі частини відповідальності за безпеку

вендору. Використання хмарних рішень дозволяє організаціям зосередитися на своїй основній діяльності, залишаючи питання фізичної безпеки, оновлення програмного забезпечення та інші технічні аспекти спеціалізованим хмарним провайдерам. Це забезпечує високий рівень надійності та безпеки, оскільки великі хмарні провайдери мають більше ресурсів для забезпечення захисту даних та виконання вимог нормативних актів.

2.3 Розробка й вдосконалення інфраструктури

В цьому розділі ми розглянемо процес розробки та вдосконалення інфраструктури, використовуючи AWS сервіси для забезпечення безпеки, надійності та ефективності роботи хмарних інформаційно-комунікаційних систем ТОВ «ОІК». Діаграма, наведена нижче, допоможе зрозуміти структуру інфраструктури та її ключові компоненти.

Опис інфраструктури:

В цьому розділі ми розглянемо процес розробки та вдосконалення інфраструктури, використовуючи AWS сервіси для забезпечення безпеки, надійності та ефективності роботи хмарних інформаційно-комунікаційних систем ТОВ «ОІК». Діаграма, наведена нижче, допоможе зрозуміти структуру інфраструктури та її ключові компоненти. Основні компоненти нашої інфраструктури включають:

AWS Account з підтримкою єдиної системи аутентифікації (SSO) та мультифакторної автентифікації (MFA): забезпечує додатковий рівень безпеки шляхом вимоги додаткового способу підтвердження (наприклад, код з мобільного додатку) під час входу в обліковий запис, а також спрощує управління доступом до ресурсів за допомогою єдиної системи аутентифікації (SSO), що дозволяє централізовано керувати доступом до всіх AWS сервісів та інтегрується з зовнішніми постачальниками ідентифікацій, такими як Azure AD.

CloudFront – це мережа доставки контенту (CDN), яка покращує продуктивність вебдодатків, доставляючи контент з найближчих до користувача серверів.

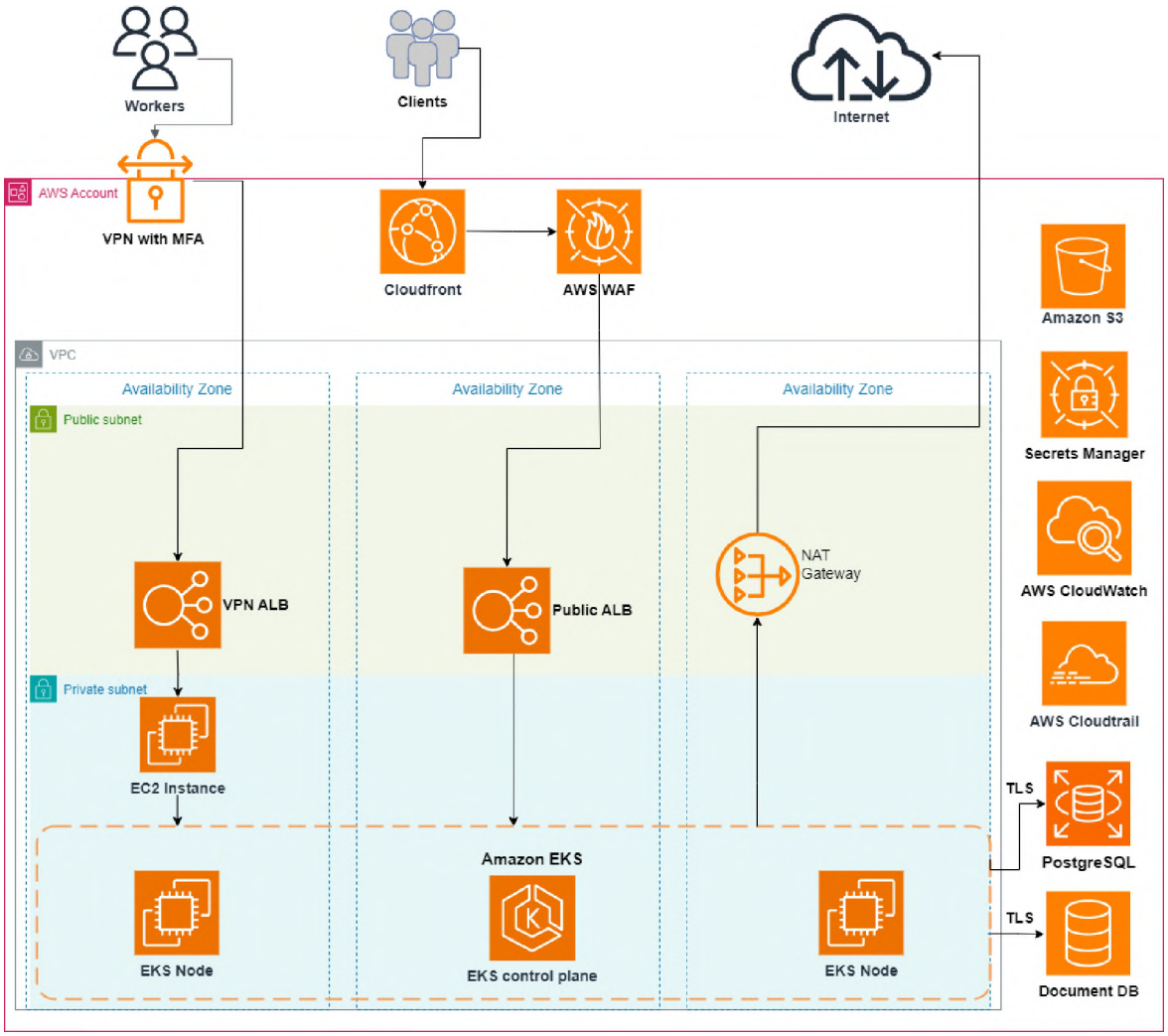

Рисунок 2.2 - Вдосконалена топологія виробництва

VPN сервер для безпечного доступу до внутрішніх ресурсів з підтримкою мультифакторної автентифікації (MFA): забезпечує захищений доступ до внутрішніх ресурсів через Інтернет, шифруючи трафік між користувачем і сервером. Додатковий рівень безпеки досягається завдяки використанню мультифакторної автентифікації (MFA), яка вимагає додаткового способу підтвердження (наприклад, через мобільний додаток) під час підключення до VPN.

AWS WAF – це вебаплікаційний файрвол, що захищає вебдодатки від поширених вебатак, таких як SQL-ін'єкції та Cross-Site Scripting (XSS).

Virtual Private Cloud (VPC) – це логічно ізольована секція AWS Cloud, де можна запускати ресурси AWS в визначеній віртуальній мережі.

Публічні підмережі (public subnets) містять ресурси, які повинні бути доступними з Інтернету.

Приватні підмережі (private subnets) містять ресурси, які не повинні бути доступними напряму з Інтернету.

Application Load Balancers (ALB) автоматично розподіляє вхідний трафік вебзастосунків між кількома цільовими серверами, підвищуючи доступність і відмовостійкість додатків.

Amazon Elastic Kubernetes Service (EKS) – це керований сервіс Kubernetes, що полегшує запуск, управління та масштабування контейнеризованих додатків за допомогою Kubernetes.

NAT Gateway для безпечного виходу в Інтернет з приватних підмереж, NAT Gateway дозволяє інстанціям у приватних підмережах підключатися до Інтернету або інших AWS сервісів, але блокує вхідний трафік з Інтернету.

Amazon S3 (Simple Storage Service) – це об'єктне сховище, що забезпечує масштабоване, високо доступне та безпечне зберігання даних.

Amazon RDS (Relational Database Service) – це керований сервіс для реляційних баз даних, що спрощує налаштування, експлуатацію та масштабування баз даних.

Amazon Document DB – це керована база даних, сумісна з MongoDB, яка призначена для масштабування та продуктивності.

AWS Secrets Manager допомагає захищати доступ до секретів, таких як паролі, ключі API та конфіденційні дані, шляхом їх централізованого зберігання та контролю доступу.

Amazon CloudWatch – це сервіс моніторингу та управління, який забезпечує дані та аналізи для ресурсів AWS, додатків та служб, що виконуються на AWS.

AWS CloudTrail – це сервіс, який надає можливість аудиту, відстеження та логування активності користувачів, API дзвінків та інших дій, виконаних у вашій AWS інфраструктурі.

Мультифакторна автентифікація (MFA) – це метод захисту доступу до системи, який вимагає два або більше способів підтвердження особи користувача. Це значно підвищує рівень безпеки, оскільки навіть якщо один із факторів буде скомпрометовано, інші залишаться захищеними. Основні фактори автентифікації включають:

– Щось, що ви знаєте: пароль або PIN-код.

– Щось, що у вас є: мобільний телефон або апаратний токен.

– Щось, що ви є: біометричні дані, такі як відбитки пальців або розпізнавання обличчя.

Єдина система аутентифікації (SSO) – це технологія, яка дозволяє користувачам здійснювати доступ до декількох додатків або сервісів, використовуючи одні і ті ж облікові дані для входу. SSO спрощує управління доступом та підвищує зручність користування, знижуючи кількість паролів, які користувачі повинні запам'ятовувати.

Terraform – це інструмент для управління інфраструктурою як кодом (IaC), що дозволяє створювати, змінювати та версіонувати інфраструктуру безпечно та ефективно. За допомогою Terraform можна описати всю хмарну інфраструктуру у вигляді конфігураційних файлів, що забезпечує можливість автоматизації та повторного використання коду.

Terraform дозволяє користувачам описувати інфраструктуру за допомогою конфігураційних файлів на основі мови HashiCorp Configuration Language (HCL) або JSON. Ці файли містять опис ресурсів, їхніх властивостей та залежностей, що робить можливим автоматичне створення, зміни та перестворення інфраструктури.

Основні Можливості Terraform:

– інфраструктура як код (IaC): Terraform дозволяє описати інфраструктуру у вигляді коду, що забезпечує повторне використання конфігурацій та їх автоматизацію. Це також сприяє стандартизації інфраструктури та полегшує її управління;

– контроль версій: конфігураційні файли Terraform можуть зберігатися в системах контролю версій, таких як Git. Це дозволяє відстежувати зміни, повертатися до попередніх версій конфігурацій та забезпечує прозорість у процесах управління інфраструктурою;

– планування змін: Terraform надає можливість попереднього перегляду змін, які будуть внесені до інфраструктури, за допомогою команди Terraform plan. Це дозволяє уникнути небажаних змін та покращує контроль над процесами;

– модульність та повторне використання: конфігурації Terraform можуть бути організовані у модулі, які можуть бути повторно використані в різних проектах. Це сприяє стандартизації та економії часу на розробку;

– підтримка багатохмарності: Terraform підтримує широкий спектр постачальників хмарних послуг, що дозволяє створювати та управляти ресурсами в різних хмарах з одного інструменту. Це також полегшує міграцію між хмарними платформами.

Репліки (Replicas) – це копії баз даних, що забезпечують високу доступність та відмовостійкість. Наприклад, у RDS можна налаштувати репліки для читання, щоб розподілити навантаження читання з основної бази даних.

Снапшоти (Snapshots) – це знімки стану бази даних або сховища в певний момент часу, що дозволяють відновити дані у випадку втрати або пошкодження. Вони можуть використовуватися для резервного копіювання та відновлення даних.

Lens – це потужний інструмент для управління кластерами Kubernetes. Lens надає інтуїтивно зрозумілий інтерфейс для моніторингу, управління та налагодження Kubernetes кластерів, що значно спрощує роботу з ними.

CI/CD (Continuous Integration and Continuous Deployment) – це набір методик та практик в розробці програмного забезпечення, які автоматизують процеси інтеграції коду, тестування та розгортання. Мета CI/CD – забезпечити безперервну доставку якісного програмного забезпечення з мінімальними затримками та людськими помилками.

Безперервна інтеграція (Continuous Integration) – це практика, при якій розробники регулярно об'єднують зміни коду в основний репозиторій кілька разів на день. Кожне об'єднання автоматично перевіряється за допомогою тестувань, що дозволяє виявити та виправити помилки на ранніх етапах розробки. Основні переваги CI включають:

– рання виявленість помилок: автоматизоване тестування допомагає швидко виявити дефекти в коді;

– зменшення ризику інтеграції: часті, маленькі інтеграції знижують ризики великих конфліктів при об'єднанні коду;

– покращення якості коду: постійне тестування допомагає підтримувати високий рівень якості коду;

– прискорення розробки: швидка ідентифікація проблем дозволяє розробникам оперативно їх виправляти.

Безперервне розгортання (Continuous Deployment) – це практика, яка автоматизує процеси розгортання коду на продуктивне середовище після успішного проходження всіх тестувань. CD забезпечує швидке і часте розгортання нових версій програмного забезпечення, мінімізуючи затримки між розробкою та випуском нових функцій або виправлень. Основні переваги CD включають:

– швидке розгортання: автоматизація розгортання дозволяє швидко впроваджувати нові функції та виправлення.

– зменшення часу до ринку: швидке випускання нових версій зменшує час виходу продукту на ринок.

– підвищення надійності: автоматизовані процеси розгортання зменшують кількість людських помилок.

– постійне вдосконалення: часті релізи дозволяють отримувати швидкий зворотний зв'язок від користувачів і оперативно вдосконалювати продукт.

– контроль якості: під час розгортання є можливість впровадження додаткових перевірок задля мінімізації людського фактору.

Поліпшення інфраструктури:

1. Перевірка VPC конфігурації: всі ноди EKS та VPN сервер для доступу до EKS і додатків, що працюють в ньому, розташовані в приватних підмережах. Це підвищує безпеку, запобігаючи прямому доступу до них з Інтернету.

2. Додавання MFA до процесу автентифікації VPN серверу: для забезпечення додаткового рівня безпеки, до процесу автентифікації VPN серверу буде додано мультифакторну автентифікацію (MFA). Це забезпечить додатковий захист від несанкціонованого доступу.

3. Переведення IAM користувачів у SSO IAM Identity Center на основі Azure AD: для спрощення управління доступом та покращення безпеки, всі IAM користувачі будуть переведені у SSO IAM Identity Center, використовуючи Azure AD як джерело ідентичностей. Це дозволить централізовано управляти доступом до ресурсів AWS.

4. Використання Secrets Manager для зберігання секретних значень: всі секретні значення для додатків, що працюють в EKS, будуть зберігатися в AWS Secrets Manager. Це забезпечить безпечне управління секретами, такими як паролі, ключі API та інші конфіденційні дані.

5. Шифрування трафіку між EKS та Document DB і RDS (TLS): для забезпечення безпеки даних, трафік між Amazon EKS та базами даних (Document DB та RDS) буде шифруватися за допомогою TLS. Це запобігає можливості перехоплення даних під час передачі.

6. Реплікація снапшотів БД в інший регіон для відмовостійкості: для забезпечення відмовостійкості інфраструктури, будуть налаштовані реплікації снапшотів баз даних в інший регіон. Це дозволить швидко відновити роботу у разі виникнення катастрофи в основному регіоні.

7. Створення WAF правил та підключення його до CloudFront: для захисту вебдодатків від загроз, таких як DDoS атаки та SQL ін'єкції, будуть створені правила AWS WAF. WAF буде підключений до CloudFront для забезпечення захисту на рівні контент-мережі.

8. Створення CloudTrail для збору подій: забезпечення детального аудиту подій, буде налаштований AWS CloudTrail для збору всіх дій в обліковому записі AWS. Це дозволить відстежувати всі виклики API та зміни конфігурацій.

9. Налаштування SNS та EventBridge для оповіщення про певні дії: оперативного інформування про важливі події, будуть створені правила для Amazon EventBridge (раніше Amazon CloudWatch Events) та налаштований Amazon SNS для відправки оповіщень. Це дозволить отримувати повідомлення про певні дії, такі як зміни конфігурацій або виявлення підозрілих дій.

Головні нововведення:

1. Впровадження масштабованої архітектури: Створено гнучку та масштабовану архітектуру, яка дозволяє легко розширювати інфраструктуру в міру зростання потреб бізнесу.

2. Інтеграція з CI/CD пайплайнами: Інтеграція з системами безперервної інтеграції та безперервного розгортання (CI/CD) для автоматизації процесів розробки та деплойменту. Це дозволяє швидко та ефективно вносити зміни в додатки та інфраструктуру.

3. Покращена система моніторингу та логування: Впровадження додаткових інструментів моніторингу та логування, таких як Amazon CloudWatch та AWS CloudTrail, для підвищення прозорості та контрольованості інфраструктури.

4. Розширена мережа безпеки: Використання AWS WAF, VPN Server та мультифакторної автентифікації (MFA) для забезпечення високого рівня безпеки і захисту від потенційних загроз.

5. Автоматизація управління секретами: Впровадження AWS Secrets Manager для централізованого та безпечного управління секретами та конфіденційною інформацією.

6. Покращене резервне копіювання та відновлення: Налаштування реплікації снапшотів баз даних в інші регіони та використання снапшотів для резервного копіювання та відновлення даних у випадку втрати або пошкодження.

7. Підвищена відмовостійкість: Впровадження механізмів для забезпечення відмовостійкості, таких як репліки баз даних та автоматичний балансувальник навантаження (ALB), що забезпечують безперебійну роботу сервісів.

8. Оптимізація мережевих ресурсів: Використання NAT Gateway для безпечного виходу в Інтернет з приватних підмереж та CloudFront для доставки контенту з низькою затримкою.

9. Удосконалена система управління доступом: Переведення IAM користувачів у SSO IAM Identity Center на основі Azure AD для спрощення управління доступом та покращення безпеки.

Ці покращення спрямовані на підвищення рівня безпеки, надійності та ефективності роботи хмарної інфраструктури. Кожне з них сприяє захисту даних, оптимізації управління доступом та забезпеченню безперебійної роботи сервісів у різних умовах.

2.3.1 Перевірка й автоматизація VPC

Віртуальна мережа розташована в регіоні Europe (Ireland) eu-west-1. Такий вибір обумовлений двома факторами: віддаленість обчислювального центру від України, що забезпечує прийнятну затримку між запитом до сервера й поверненням даних, та найнижчою ціною на використовувані обчислювальні ресурси в регіоні. У VPC наявні три зони доступності, що підвищує відмово стійкість і безперервність роботи у разі виходу з ладу компонента чи цілої зони доступності AWS.

За замовчуванням, підмережі не мають доступу до Інтернету. Для надання доступу необхідно створити Інтернет-шлюз (IGW). Додатково, ми створимо три публічні підмережі в кожній зоні доступності для підвищення надійності та високої доступності. Маршрутизація до Інтернет-шлюзу (IGW) для публічних підмереж створюється автоматично за допомогою Terraform модуля VPC, що дозволяє всім пакетам з серверів у підмережах направлятися до шлюзу. Така архітектура забезпечить доступ до ресурсів у цих підмережах з будь-якого місця у світі.

```
locals {
  cidr_preset1 = ["10.0.0.0/19", "10.0.32.0/19", "10.0.64.0/19"]
  cidr_preset2 = ["10.0.96.0/19", "10.0.128.0/19", "10.0.160.0/19"]
}

module "vpc" {
  source  = "terraform-aws-modules/vpc/aws"
  version = "5.1.0"
  name            = var.name
  cidr            = "10.0.0.0/16"
  azs             = ["eu-west-1a", "eu-west-1b", "eu-west-1c"]
  public_subnets  = local.cidr_preset1
  private_subnets = local.cidr_preset2

  map_public_ip_on_launch = true
  enable_dns_hostnames    = true
  enable_nat_gateway      = true
  single_nat_gateway      = var.single_nat_gateway

  default_network_acl_ingress = [{
    protocol   = -1
    rule_no    = 100
    action     = "allow"
    cidr_block = "0.0.0.0/0"
    from_port  = 0
    to_port    = 0
  },{
    protocol   = "tcp"
    rule_no    = 10
    action     = "allow"
    cidr_block = "10.0.0.0/16"
    from_port  = 22
    to_port    = 22
  },{
    protocol   = "tcp"
    rule_no    = 20
    action     = "deny"
    cidr_block = "0.0.0.0/0"
    from_port  = 22
    to_port    = 22
  },{
    protocol   = "tcp"
    rule_no    = 30
    action     = "deny"
    cidr_block = "0.0.0.0/0"
    from_port  = 3389
    to_port    = 3389
  }]
}
```

Рисунок 2.3 – Код Terraform конфігурації VPC

Також буде створено приватні підмережі в кожній зоні доступності. Приватні підмережі не мають маршрутизації до IGW і, отже, недоступні ззовні. Але вони будуть маршрутизовані на NAT шлюз для доступу ресурсів до мережі Інтернет. Конфігурація Terraform автоматично визначає маршрутизацію для приватних підмереж через NAT шлюз. Додатково у Terraform модулі VPC прописані списки керування доступом до мережі (ACL), які дозволяють або

забороняють певний вхідний або вихідний трафік на рівні підмережі, вони приміняються в порядку з їх номером від меншого до більшого. Наприклад:

– правило з номером 100 дозволяє весь вхідний трафік з будь-якої IP-адреси;

– правило з номером 10 дозволяє вхідний трафік по TCP порту 22 (SSH) для внутрішньої мережі;

– правило з номером 20 забороняє вхідний трафік по TCP порту 22 з будь-якої IP-адреси;

– правило з номером 30 забороняє вхідний трафік по TCP порту 3389 (RDP) з будь-якої IP-адреси.

2.3.2 Додавання MFA до процесу автентифікації VPN серверу

Для забезпечення додаткового рівня безпеки, до процесу автентифікації VPN серверу буде додано мультифакторну автентифікацію (MFA). Це забезпечить додатковий захист від несанкціонованого доступу.

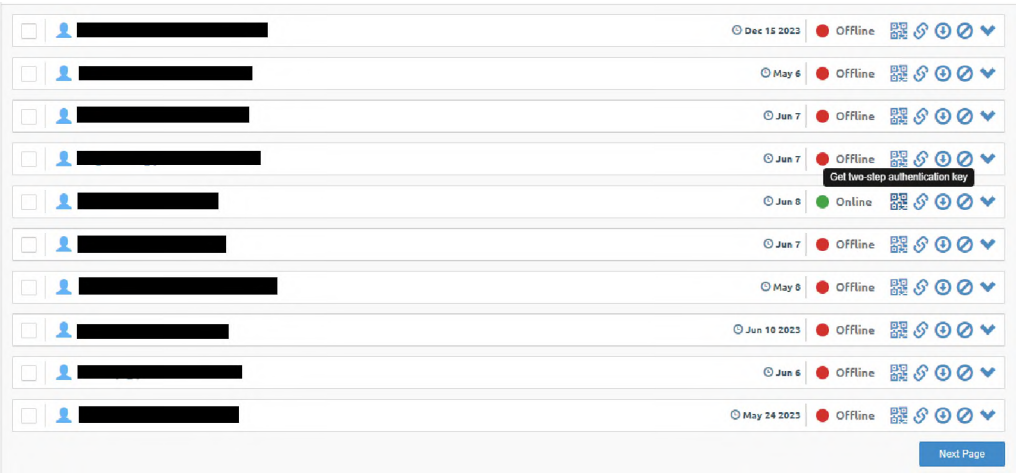

Рисунок 2.4 – Сторінка конфігурації користувачів VPN Pritunl

MFA передбачає використання кількох методів перевірки, що включають щонайменше два з наступних факторів автентифікації:

1. Щось, що ви знаєте – наприклад, пароль або PIN-код.

2. Щось, що ви маєте – наприклад, апаратний токен або мобільний пристрій, який генерує одноразові паролі (OTP).

3. Щось, що ви є – наприклад, біометричні дані (відбиток пальця, розпізнавання обличчя).

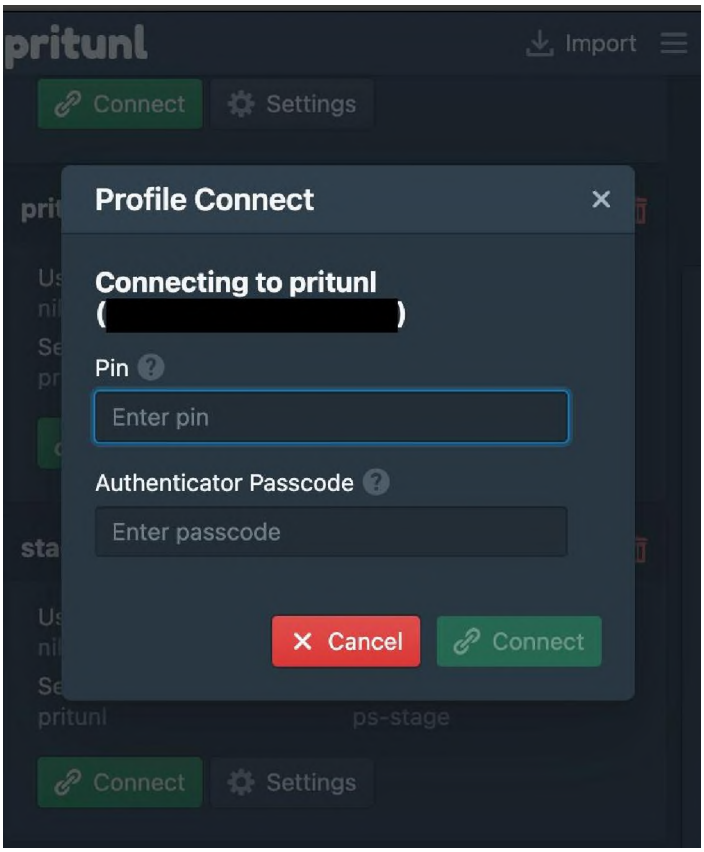

Рисунок 2.5 – Вікно автентифікації користувача VPN Pritunl

Для реалізації MFA на VPN сервері буде використано комбінацію пароля та одноразового пароля (OTP), який генерується мобільним додатком аутентифікації (наприклад, Google Authenticator або Authy). Процес автентифікації користувача на VPN сервері виглядатиме наступним чином:

1. Користувач вводить свій основний пароль.

2. Після успішної перевірки пароля, сервер запитує одноразовий пароль (OTP).

3. Користувач відкриває додаток аутентифікації на своєму мобільному пристрої та вводить згенерований OTP.

4. Сервер перевіряє валідність OTP. У разі успіху, користувач отримує доступ до VPN.

Впровадження MFA значно підвищить безпеку VPN серверу, оскільки навіть у випадку компрометації основного пароля зловмиснику знадобиться додатковий фактор автентифікації для доступу до системи. Це забезпечує більш надійний захист від потенційних атак і несанкціонованого доступу.

2.3.3 Впровадження політики SSO з IAM Identity Center

AWS пропонує кілька способів налаштувати єдиний вхід для своїх послуг. Один із них — використання служби AWS Identity and Access Management (IAM) для створення ролей та прив'язок ролей, які надають користувачам доступ до певних ресурсів AWS. Основний спосіб — використання постачальника ідентифікаційної інформації (IdP), такого як Azure AD або Okta, для аутентифікації користувачів та надання їм доступу до ресурсів AWS. Для налаштування нашого способу під'єднання знадобиться root акаунт організації, оскільки саме через нього буде здійснюватися налаштування Single Sign-On на стороні AWS і регулювання рівня доступу до інших облікових записів організації.

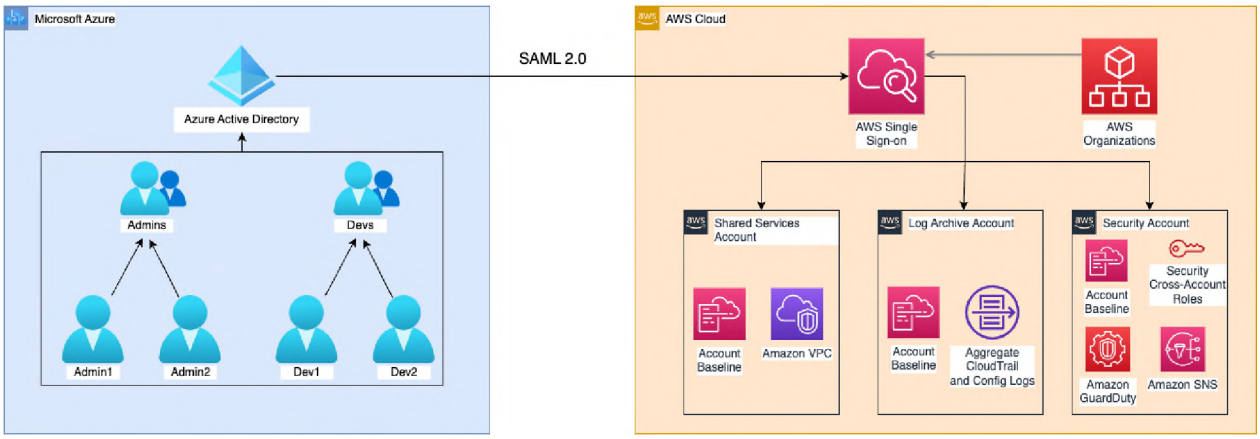

Рисунок 2.6 – Схема підключення Azure AD до AWS

Перш за все необхідно в Microsoft Azure зайти в Azure AD й створити Enterprice application й додати в нього групи з користувачами.

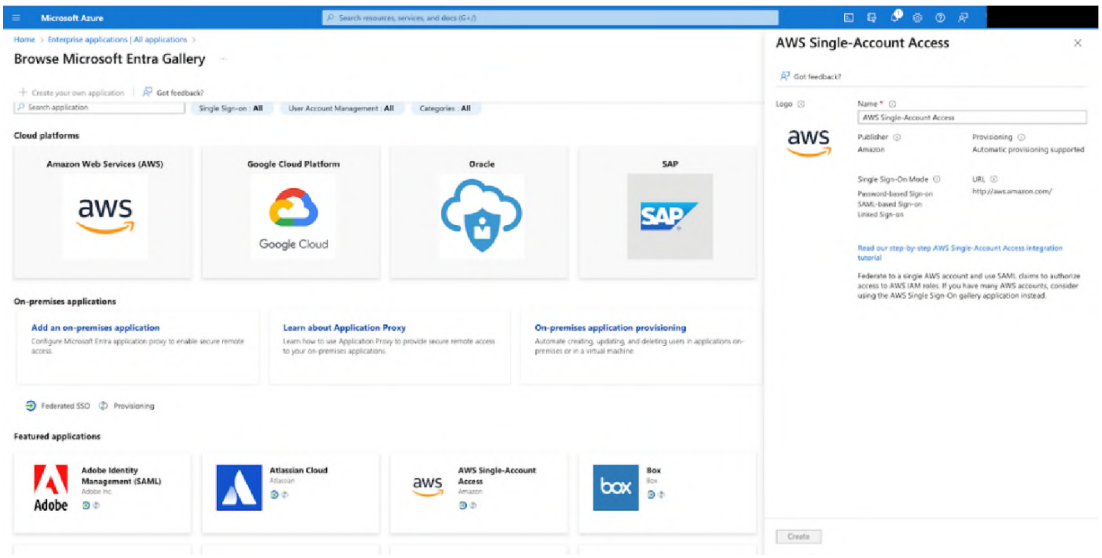

Рисунок 2.7 – Сторінка Azure AD

Створивши додаток для AWS у вкладці Single Sign-on треба скачати «Federation Metadata XML», він нам знадобиться для IAM Identity Center. У головному акаунті організації, переходимо до IAM Identity Center й вмикаємо його натискаючи на відповідну кнопу.

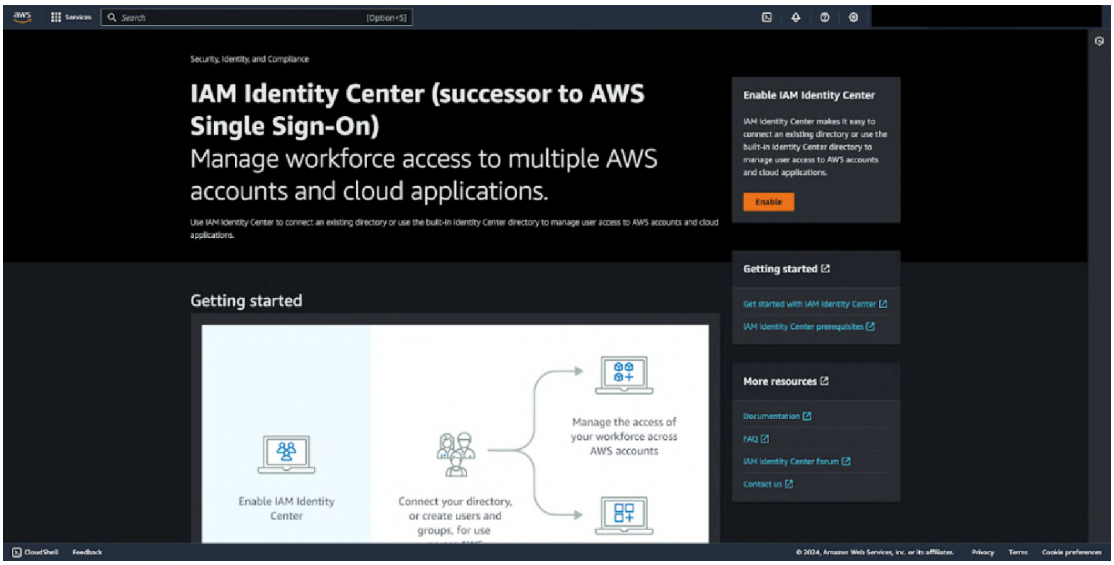

Рисунок 2.8 – Сторінка AWS IAM Identity Center

Увімкнувши IAM Identity Center в головному аккаунті організації, наступним кроком необхідно перейти в налаштування й у вкладці «Choose identity source» обрати пункт «External identity provider».

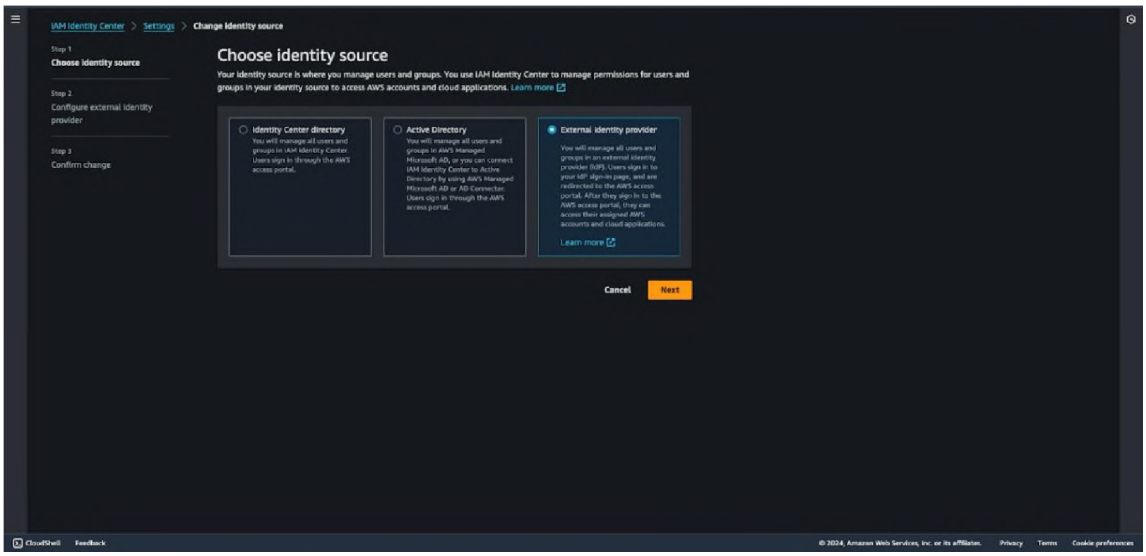

Рисунок 2.9 – Сторінка вибору постачальника ідентичностей

Далі необхідно обмінятись «SAML metadata» між AWS & Azure AD, для цього додаємо «Federation Metadata XML» у консолі AWS й зберігаєте собі файл «Service provider metadata», щоб потім додати його у додаток створенний в Azure AD.

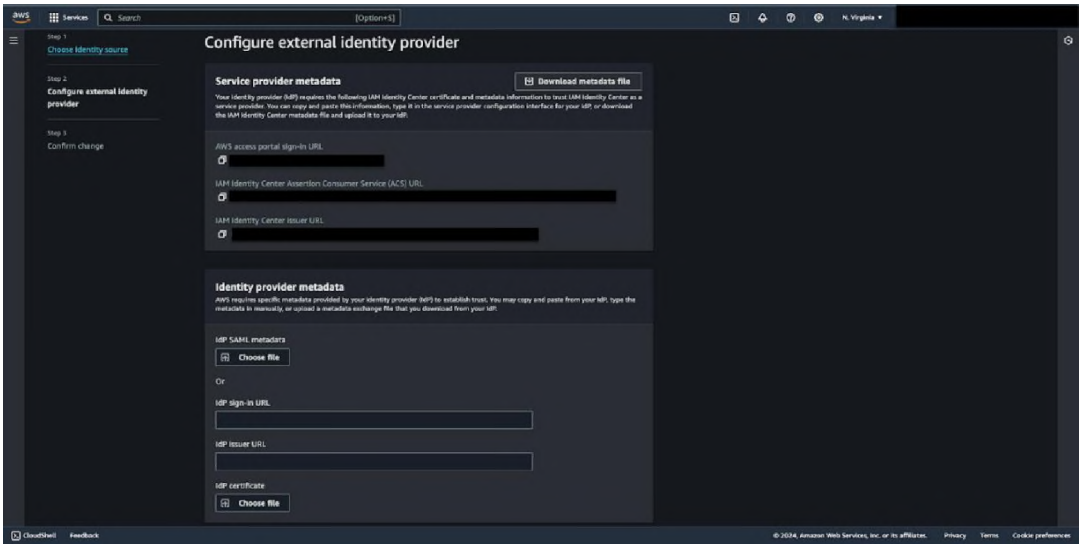

Рисунок 2.10 – Конфігурація зовнішнього постачальника сутностей

Також для автоматизованої синхронізації юзерів між Azure AD & AWS треба у налаштуваннях IAM Identity Center у пункті «Provisioning» вмикаємо

автоматичну синхронізацію й копіюємо SCIM endpoint й Access token, щоб у подальшому додати його до аплікації в Microsoft Azure. Перейшовши до Microsoft Azure в аплікації котра створена для AWS у влкадці «Single Sign-on» треба загрузити раніше встановлений «Service provider metadata», й щоб увімкнути автоматичну синхронізацію - перемикаємо режим на автоматичний, вставляємо раніше скопійовані значення SCIM endpoint й Access token й натискаємо кнопку «Test connection», якщо на рівні з полями значень ви бачите відповідні галочки - значить з'єднання встановлене.

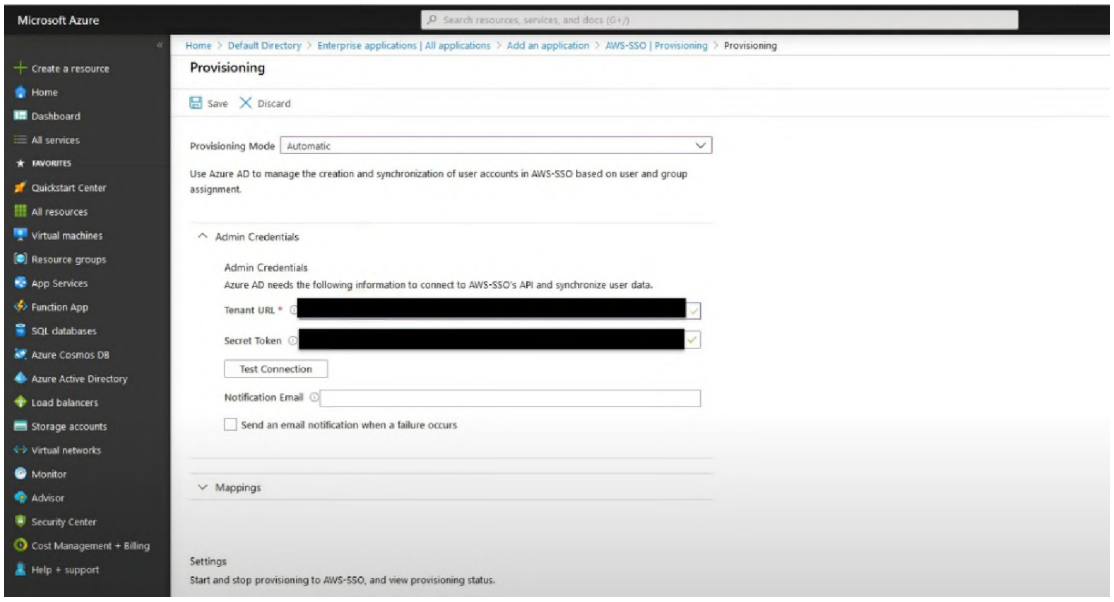

Рисунок 2.11 –Під'єднання Azure AD до AWS IAM Identity Center

Отже, після налаштування SSO, при додаванні груп та користувачів до цієї аплікації, вони автоматично переносяться до AWS IAM Identity Center. Аналогічно працює і видалення: якщо користувача видалити в Azure AD, то при наступній синхронізації він також видалиться в AWS. Автоматична синхронізація відбувається з певною періодичністю, тому для внесення змін може знадобитися деякий час або можна синхронізувати вручну, якщо це терміново.

Після появи груп та користувачів в консолі можна переходити до налаштування доступу. Важливо дотримуватись принципу найменших привілеїв

при розподілі ролей і доступів до облікових записів. Також рекомендується зменшувати час дії токену, який надається користувачу при аутентифікації.

Після перевірки ролей та інших конфігурацій можна відмовитись від використання IAM користувачів в облікових записах вашої організації. Це значно підвищить рівень безпеки інфраструктури, централізує керування обліковими записами і полегшить комунікацію в команді, замінивши десятки паролів і відповідних MFA на один логін і пароль від пошти з відповідним двофакторним аутентифікатором.

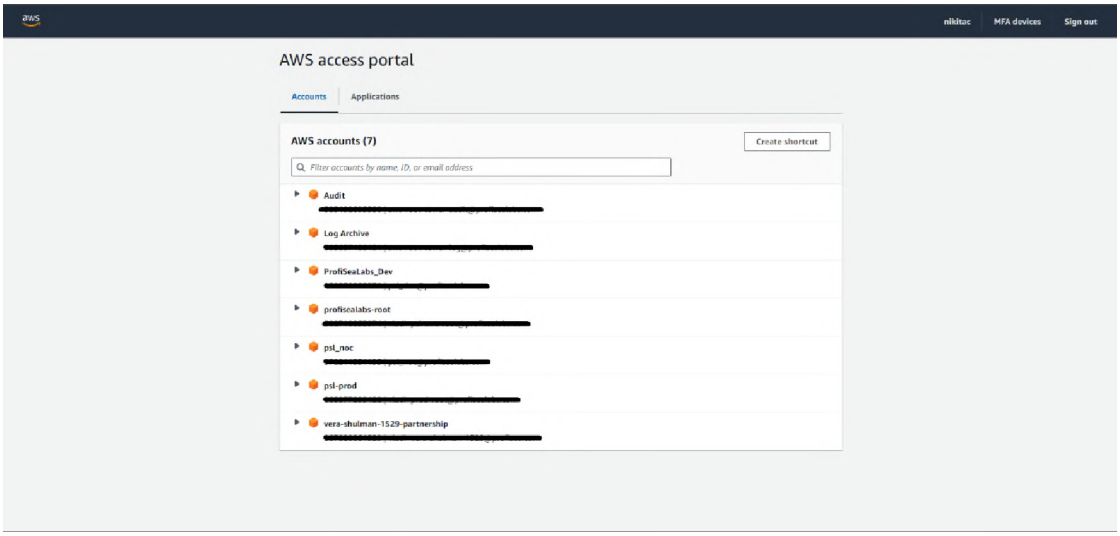

Рисунок 2.12 – Сторінка входу в облікові записи SSO

Цей підхід значно підвищує ефективність управління доступами і спрощує процеси аутентифікації та авторизації, забезпечуючи більш надійний захист від несанкціонованого доступу.

2.3.4 Впровадження Secrets Manager

Для забезпечення безпечного управління секретами, такими як паролі, ключі API та інші конфіденційні дані, всі секретні значення для додатків, що працюють в Amazon Elastic Kubernetes Service (EKS), будуть зберігатися в AWS Secrets Manager. AWS Secrets Manager забезпечує централізоване зберігання та керування секретами, що дозволяє знижувати ризики, пов'язані з витоком даних та несанкціонованим доступом.

Основні переваги використання AWS Secrets Manager включають:

1. Автоматичне ротація секретів: AWS Secrets Manager дозволяє автоматично змінювати секрети через задані інтервали часу або за вимогою, що підвищує безпеку додатків.

2. Контроль доступу: Доступ до секретів контролюється за допомогою політик AWS Identity and Access Management (IAM), що дозволяє чітко визначати, які користувачі та сервіси можуть отримати доступ до секретних даних.

3. Безпечне шифрування: Всі секрети зберігаються в зашифрованому вигляді, використовуючи ключі шифрування AWS Key Management Service (KMS), що забезпечує додатковий рівень захисту.

4. Інтеграція з іншими сервісами AWS: AWS Secrets Manager легко інтегрується з іншими сервісами AWS, такими як Amazon EKS, AWS Lambda, Amazon RDS та інші, що дозволяє спрощувати управління секретами в різних середовищах.

5. Аудит та моніторинг: AWS Secrets Manager забезпечує можливість ведення аудиту та моніторингу доступу до секретів за допомогою AWS CloudTrail, що дозволяє відстежувати всі операції з секретами та виявляти підозрілі активності.

```
resource "helm_release" "external_secrets" {
  name             = "external-secrets"
  repository       = "https://charts.external-secrets.io"
  chart            = "external-secrets"
  namespace        = "external-secrets"
  create_namespace = true
  reset_values     = true
  values = [file("values/external-secrets.yaml")]
}
```

Рисунок 2.13 – Створення Helm-чарту для External Secrets

Для використання секретів у додатках, що працюють в EKS, можна налаштувати інтеграцію з AWS Secrets Manager за допомогою Kubernetes Secrets. Це дозволяє автоматично завантажувати секрети з AWS Secrets Manager та

використовувати їх у контейнерах додатків. Ось приклад коду для налаштування цієї інтеграції:

Цей ресурс відповідає за розгортання Helm-чарту для External Secrets. External Secrets дозволяє інтегрувати секрети з AWS Secrets Manager в Kubernetes. Helm-чарт – це набір файлів, який описує ресурси Kubernetes, необхідні для розгортання додатку або сервісу в кластері Kubernetes. Helm-чарти спрощують управління складними додатками шляхом їх пакування, конфігурації та версіонування. Вони дозволяють розгортати та оновлювати додатки в Kubernetes за допомогою однієї команди, значно спрощуючи процеси розгортання та управління.

```
resource "kubectl_manifest" "secret_store" {
  yaml_body = templatefile(
    "manifests/secret_store.yaml", {
      region              = var.aws_region,
      aws-service-account = "aws-service-account",
      namespace-name      = "devops",
      secret-store-name   = "aws-secrets-store"
    }
  )

  depends_on = [
    resource.helm_release.external_secrets,
    resource.kubectl_manifest.secrets_manager[0]
  ]
}
```

Рисунок 2.14 – Terrafrom ресурс Secret Store

Цей ресурс створює Kubernetes маніфест для налаштування Secret Store в Kubernetes. Використовує шаблон «manifests/secret_store.yaml» з передачею параметрів, таких як регіон AWS, ім'я облікового запису сервісу, простір імен та назва секретного магазину. Залежить від успішного створення ресурсу «helm_release.external_secrets» та «kubectl_manifest.secrets_manager».

Цей ресурс створює маніфест для облікового запису сервісу (Service Account) в Kubernetes, який матиме доступ до секретів з AWS Secrets Manager.

```
resource "kubectl_manifest" "secrets_manager" {
  yaml_body = templatefile(
    "manifests/secrets_manager_sa.yaml", {
      service-account-name      = "aws-service-account",
      namespace-name            = "devops",
      aws-service-account-role = "arn:aws:iam::${data.aws_caller_identity.current.account_id}:role/${aws_iam_role.secrets_manager[0].name}"
    }
  )

  depends_on = [
    resource.helm_release.argocd,
    resource.helm_release.external_secrets
  ]
}
```

Рисунок 2.15 – Terrafrom ресурс Secrets Manager

```
data "aws_iam_policy_document" "secrets_manager" {
  statement {
    effect = "Allow"

    actions = [
      "secretsmanager:GetResourcePolicy",
      "secretsmanager:GetSecretValue",
      "secretsmanager:DescribeSecret",
      "secretsmanager:ListSecretVersionIds",
      "secretsmanager:ListSecrets",
    ]

    resources = [
      "*"
    ]
  }
}
```

Рисунок 2.16 – Terrafrom ресурс Secrets Manager

Використовує шаблон «manifests/secrets_manager_sa.yaml» з передачею параметрів, таких як ім'я облікового запису сервісу, простір імен та роль облікового запису AWS. Залежить від ресурсів «helm_release.argocd» та «helm_release.external_secrets».

Створює IAM політику, яка дозволяє доступ до секретів у AWS Secrets Manager.

Ресурс «aws_iam_policy» створює IAM політику з ім'ям, яке включає префікс і політику, визначену у попередньому ресурсі. «aws_iam_policy_document» створює IAM політику, яка дозволяє асоціювати

роль з вебідентифікацією (Web Identity) для облікового запису сервісу в Kubernetes.

```
resource "aws_iam_policy" "secrets_manager" {
  name_prefix = "${var.cluster_name}-secrets_manager"
  policy      = data.aws_iam_policy_document.secrets_manager[0].json
}

data "aws_iam_policy_document" "secrets_manager_webidentity" {
  statement {
    effect = "Allow"
    actions = [
      "sts:AssumeRoleWithWebIdentity"
    ]
    condition {
      test     = "StringEquals"
      variable = "${replace(var.cluster_oidc_issuer_url, "https://", "")}:sub"

      values = [
        "system:serviceaccount:devops:aws-service-account"
      ]
    }
    condition {
      test     = "StringEquals"
      variable = "${replace(var.cluster_oidc_issuer_url, "https://", "")}:aud"
      values = [
        "sts.amazonaws.com"
      ]
    }
    principals {
      type = "Federated"

      identifiers = [
        var.oidc_provider_arn
      ]
    }
  }
}
```

Рисунок 2.17 – Terrafrom ресурс Secrets Manager

Ресурс «aws_iam_role» створює IAM роль з політикою асоціації вебідентифікації. Ресурс «aws_iam_policy_attachment» прикріплює створену IAM політику до ролі.

Після створення та розгортання цих ресурсів, можемо створити секрет в AWS Secrets Manager під назвою «sentry_dsn_backend» ключ-значення.

```
resource "aws_iam_role" "secrets_manager" {
  assume_role_policy = data.aws_iam_policy_document.secrets_manager_webidentity[0].json
  name_prefix        = "${var.cluster_name}-secrets_manager"
}

resource "aws_iam_policy_attachment" "secrets_manager" {
  name       = aws_iam_policy.secrets_manager[0].name
  policy_arn = aws_iam_policy.secrets_manager[0].arn

  roles = [
    aws_iam_role.secrets_manager[0].name
  ]
}
```

Рисунок 2.18 – Terrafrom ресурс Secrets Manager

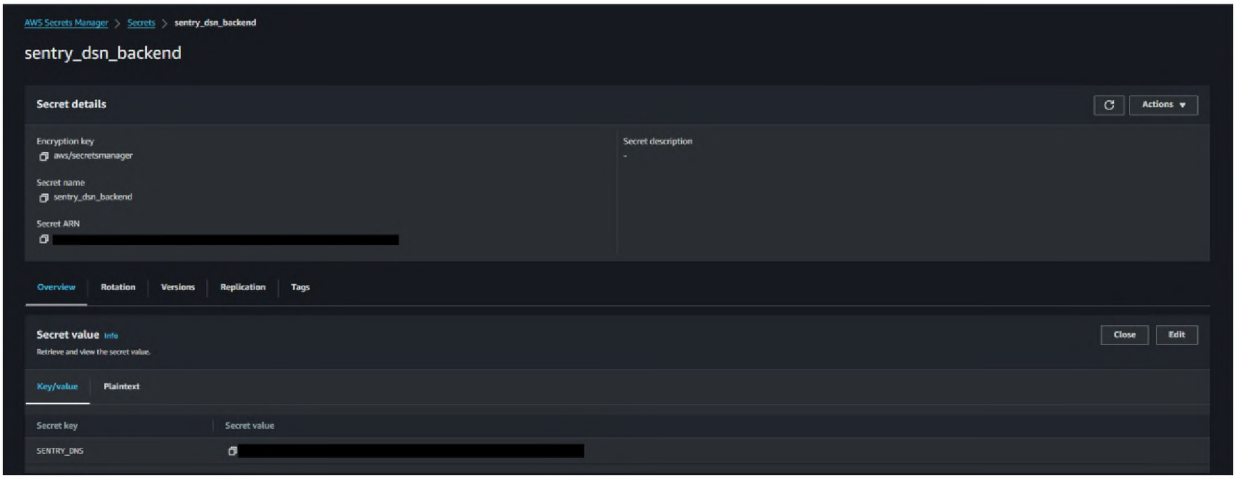

Рисунок 2.19 – Демонстрація секрету в AWS Secret Manager

Після створення серекрету в консолі AWS щоб синхронізувати його в наш EKS кластер в пространство імен «pslabs» ми створюємо наступни Kubernetes маніфест.

```
apiVersion: kubernetes-client.io/v1
kind: ExternalSecret
metadata:
  name: sentry_dsn_backend
  namespace: pslabs
spec:
  backendType: secretsManager
  roleArn: arn:aws:iam::[redacted]:policy/stage-secrets_manager20230525181243556300000008
  region: eu-west-1
  data:
    - key: sentry_dsn_backend
      name: psentry_dsn_backend
      property: SENTRY_DNS
```

Рисунок 2.20 – Створення External Secret Kubernetes маніфесту

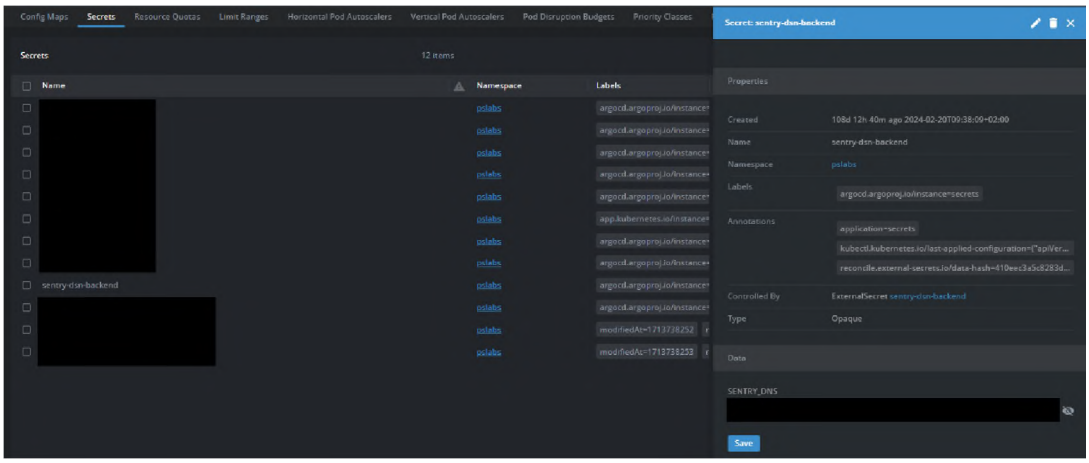

Рисунок 2.21 – Демонстрація синхронізованого секрету в EKS кластері

Таким чином, використання AWS Secrets Manager для зберігання секретних значень забезпечує високий рівень безпеки та зручність управління конфіденційними даними в додатках, що працюють в Amazon EKS.

2.3.5 Шифрування трафіку між EKS та БД

Для забезпечення безпеки даних, трафік між Amazon Elastic Kubernetes Service (EKS) та базами даних, такими як Amazon DocumentDB та Amazon Relational Database Service (RDS), буде шифруватися за допомогою Transport Layer Security (TLS). Використання TLS забезпечує захист даних від можливих перехоплень під час передачі між компонентами системи. Amazon EKS підтримує інтеграцію з Amazon DocumentDB і RDS, що дозволяє налаштовувати шифрування трафіку між контейнерами в кластері та базами даних. Для цього потрібно впевнитися, що всі підключення до баз даних використовують TLS.

TLS – це криптографічний протокол, призначений для забезпечення безпечної передачі даних у мережі Інтернет. Метод шифрування TLS використовується для захисту конфіденційності та цілісності переданих даних, а також для автентифікації комунікаційних сторін.

Основні етапи роботи TLS:

1. Рукостискання (Handshake):

– встановлення з'єднання: клієнт надсилає серверу запит на встановлення з'єднання.

– вибір параметрів шифрування: клієнт і сервер обмінюються інформацією для вибору параметрів шифрування, включаючи версію протоколу TLS, алгоритми шифрування та хешування.

– сертифікати та автентифікація: сервер надсилає клієнту свій цифровий сертифікат, який підтверджує його справжність. Клієнт перевіряє сертифікат за допомогою довіреного сертифікаційного центру. Опціонально клієнт може також надіслати серверу свій сертифікат для двосторонньої автентифікації.

– генерація сесійного ключа: клієнт і сервер спільно генерують сесійний ключ, який буде використовуватися для симетричного шифрування подальших даних.

2. Передача зашифрованих даних:

– шифрування: усі передані дані шифруються з використанням сесійного ключа. Це забезпечує конфіденційність даних, оскільки їх можуть прочитати лише клієнт і сервер;

– цілісність: для забезпечення цілісності даних використовується MAC (Message Authentication Code), який дозволяє виявити будь-які зміни в переданих даних.

3. Завершення з'єднання:

Закриття сесії: Після завершення передачі даних клієнт і сервер закривають TLS-сесію. Це включає обмін спеціальними повідомленнями про закриття з'єднання, що забезпечує належне завершення сесії.

Переваги TLS:

– конфіденційність: шифрування даних забезпечує їх захист від перехоплення сторонніми особами;

– цілісність: механізми контролю цілісності гарантують, що дані не були змінені під час передачі;

– автентифікація: використання цифрових сертифікатів дозволяє автентифікувати комунікаційні сторони, забезпечуючи їх справжність.

TLS широко використовується в Інтернеті для захисту вебсайтів (HTTPS), електронної пошти (SMTP, IMAP, POP3), VPN та інших мережевих протоколів.

Для налаштування TLS для Amazon DocumentDB в рамках інфраструктури, описаної за допомогою Terraform, необхідно додати відповідний код конфігурації. Ось приклад конфігурації Terraform для створення кластеру Amazon DocumentDB з увімкненим шифруванням та захистом за допомогою KMS (Key Management Service).

```
resource "random_password" "warehouse" {
  length = 24
}
```

Рисунок 2.22 – Ресурс для генерації випадкового паролю

Цей ресурс генерує випадковий пароль довжиною 24 символи для використання як пароль адміністратора DocumentDB. Це забезпечує високий рівень безпеки, оскільки пароль є складним та випадковим.

```
resource "aws_kms_key" "docdb_warehouse" {
  multi_region            = true
  description             = "DocumentDB warehouse cluster KMS key"
  deletion_window_in_days = 10
}
```

Рисунок 2.23 – Ресурс для генерації KMS ключу

Цей ресурс створює ключ KMS (Key Management Service) для шифрування даних в DocumentDB. Ключ є мульти-регіональним, що дозволяє

використовувати його в різних регіонах, і має вікно видалення в 10 днів, що забезпечує захист від випадкового видалення.

```
resource "aws_docdb_cluster" "warehouse" {
  cluster_identifier           = "${var.environment}-warehouse"
  backup_retention_period      = 14
  db_subnet_group_name         = var.subnet_group_name
  deletion_protection          = true
  engine                       = "docdb"
  engine_version               = "4.0.0"
  master_username              = "root"
  master_password              = random_password.warehouse.result
  preferred_maintenance_window = "mon:02:00-mon:02:30"
  apply_immediately            = true
  final_snapshot_identifier    = "final-snapshot-${var.environment}-warehouse"
  storage_encrypted            = true
  kms_key_id                   = aws_kms_key.docdb_warehouse.arn
  vpc_security_group_ids = [
    var.infra_security_group
  ]
}
```

Рисунок 2.24 – Ресурс створення Document DB кластеру

Цей ресурс створює кластер DocumentDB з ідентифікатором, який визначається змінною середовища «cluster_identifier». Період збереження бекапів встановлено на 14 днів, що забезпечує надійне резервне копіювання даних. Ім'я підмережевої групи задається змінною «var.subnet_group_name», яка визначає мережеве середовище для кластера. Захист від видалення кластера увімкнений за допомогою налаштування «deletion_protection», що запобігає випадковому видаленню ресурсу. Кластер використовує DocumentDB як двигун бази даних з версією 4.0.0, що забезпечує сучасні функції та високу продуктивність. Ім'я адміністратора бази даних встановлено як «master_username», а для підвищення безпеки використовується випадковий пароль, згенерований раніше. Вікно для технічного обслуговування визначено з понеділка 02:00 до понеділка 02:30, що дозволяє проводити планові роботи без значного впливу на роботу системи. Зміни до конфігурації застосовуються негайно завдяки налаштуванню «apply_immediately». Перед видаленням кластера створюється остаточний знімок з ідентифікатором «final_snapshot_identifier», що дозволяє зберегти

важливі дані. Дані в кластері зберігаються в зашифрованому вигляді завдяки налаштуванню «storage_encrypted», а для шифрування використовується ключ KMS, ідентифікатор якого задається змінною «kms_key_id», «vpc_security_group_ids»: Ідентифікатори VPC Security Group для забезпечення безпеки мережі.

```
resource "aws_docdb_cluster_instance" "warehouse" {
  count = var.docdb_warehouse_instance_count

  identifier                 = "${var.environment}-warehouse-${count.index}"
  cluster_identifier         = aws_docdb_cluster.warehouse.id
  instance_class             = var.docdb_warehouse_instance_type
  preferred_maintenance_window = "mon:02:00-mon:02:30"
  apply_immediately          = true
  auto_minor_version_upgrade = true
}
```

Рисунок 2.25 – Ресурс створення Document DB серверу

Цей ресурс створює сервери DocumentDB для кластера, де кількість серверів визначається змінною «var.docdb_warehouse_instance_count». Ідентифікатори серверів мають формат «${var.environment}-warehouse-${count.index}», що дозволяє легко ідентифікувати кожен сервер. Сервери прив'язані до кластера за допомогою ідентифікатора кластера «cluster_identifier», який визначається через ресурс «aws_docdb_cluster.warehouse.id». Клас серверів встановлюється за допомогою змінної «var.docdb_warehouse_instance_type», яка визначає конфігурацію обладнання. Вікно для технічного обслуговування визначено з понеділка 02:00 до понеділка 02:30, що дозволяє проводити планове обслуговування без суттєвого впливу на роботу системи. Зміни до конфігурації застосовуються негайно завдяки налаштуванню «apply_immediately», а автоматичне оновлення до незначних версій забезпечується параметром «auto_minor_version_upgrade».

Для забезпечення реплікації снапшотів DocumentDB між різними регіонами застосовується комбінація KMS ключа та лямбда-функції. Ресурс «docdb_warehouse_replication_kms» створює KMS ключ для шифрування даних

реплікованого снапшоту DocumentDB кластера з використанням провайдера «aws.replication». Цей ключ має вікно видалення в 10 днів, що забезпечує захист від випадкового видалення.

```
resource "aws_kms_key" "docdb_warehouse_replication_kms" {
  provider                = aws.replication
  description             = "DocumentDB warehouse replication cluster KMS key"
  deletion_window_in_days = 10
}
```

Рисунок 2.26 – KMS ключ для шифрування реплікованого снапшоту

Lambda-функція «snapshot_replication_lambda» відповідає за процес реплікації. Вона виконується на основі коду, збереженого в архіві «snapshot_replication_lambda.zip», і працює під роллю «aws_iam_role.snapshot_replication_lambda_role». Функція написана на Python 3.10 з максимальним часом виконання 300 секунд. Середовище виконання лямбда-функції включає змінні, що визначають регіони джерела та призначення, ідентифікатор кластера та ARN KMS ключа для шифрування.

```
resource "aws_lambda_function" "snapshot_replication_lambda" {
  filename         = "${path.module}/lambda_code/snapshot_replication_lambda.zip"
  function_name    = "snapshot_replication_lambda"
  role             = aws_iam_role.snapshot_replication_lambda_role.arn
  handler          = "snapshot_replication_lambda.lambda_handler"
  source_code_hash = filebase64sha256("${path.module}/lambda_code/snapshot_replication_lambda.zip")
  runtime          = "python3.10"
  timeout          = 300

  environment {
    variables = {
      SOURCE_REGION      = var.aws_region
      DESTINATION_REGION = var.aws_replication_region
      CLUSTER_IDENTIFIER = aws_docdb_cluster.warehouse.id
      KMS_KEY            = aws_kms_key.docdb_warehouse_replication_kms.arn
    }
  }
}
```

Рисунок 2.27 – Створення Lambda

Для взаємодії з AWS SDK Lambda використовує бібліотеки boto3 та botocore. Спочатку визначається останній знімок кластера DocumentDB в регіоні

джерела за допомогою функції «get_latest_documentdb_snapshot», яка використовує метод «describe_db_cluster_snapshots» клієнта DocumentDB для отримання списку доступних знімків і сортує їх за часом створення, щоб визначити останній знімок. Після цього Lambda створює клієнтів DocumentDB для обох регіонів і описує знімок у регіоні джерела для отримання його ARN.

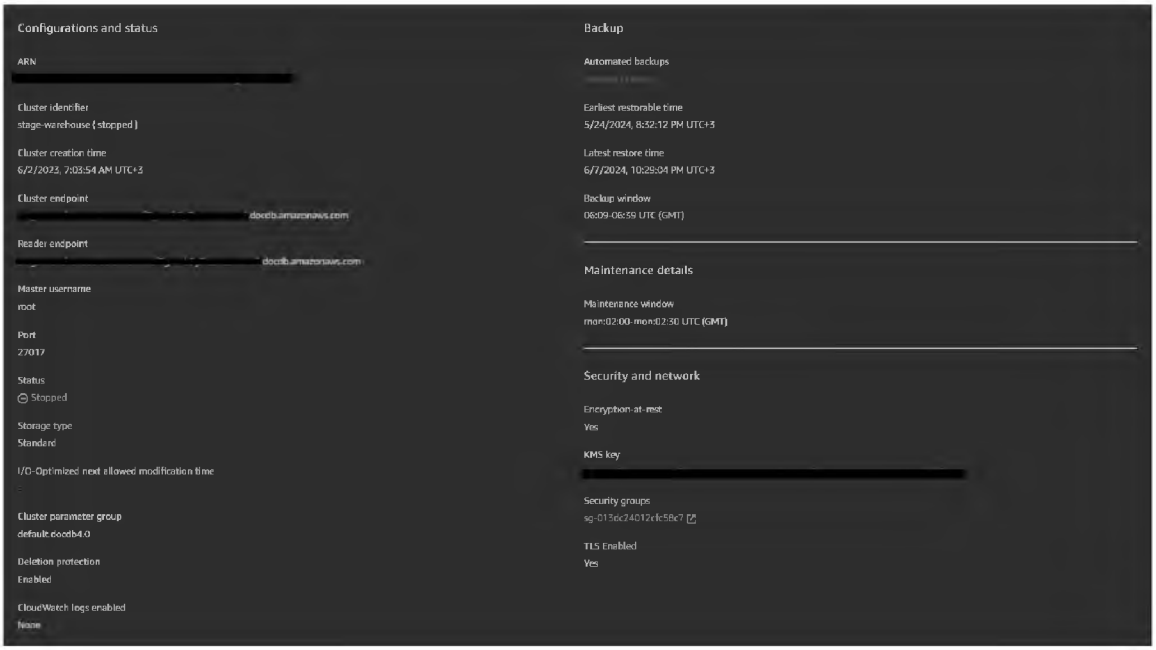

Рисунок 2.28 – Сторінка конфігурації Document DB в консолі AWS

Потім функція намагається скопіювати знімок до регіону призначення за допомогою методу «copy_db_cluster_snapshot», вказуючи ідентифікатор ключа KMS для шифрування. Якщо копіювання проходить успішно, функція повертає код статусу 200 з повідомленням про успішну операцію. У разі помилки функція повертає код статусу 400 з описом помилки.

```
import boto3
import os
import json
from botocore.exceptions import ClientError
def get_latest_documentdb_snapshot(source_region):
    client = boto3.client('docdb', region_name=source_region)
    response = client.describe_db_cluster_snapshots(
```

```
            DBClusterIdentifier= os.getenv('CLUSTER_IDENTIFIER'),
            SnapshotType='automated',
            MaxRecords=100
        )
        if 'DBClusterSnapshots' not in response:
            return response
        sorted_snapshots = sorted(response['DBClusterSnapshots'], key=lambda x:
x['SnapshotCreateTime'], reverse=True)
        if sorted_snapshots:
            latest_snapshot_id = sorted_snapshots[0]['DBClusterSnapshotIdentifier']
            return latest_snapshot_id
        else:
            return None
    def lambda_handler(event, context):
        source_region = os.getenv('SOURCE_REGION')
        destination_region = os.getenv('DESTINATION_REGION')
        cluster_identifier = os.getenv('CLUSTER_IDENTIFIER')
        source_snapshot_identifier = get_latest_documentdb_snapshot(source_region)
        destination_snapshot_identifier = source_snapshot_identifier.replace(":","-") + '-copy'
        source_client = boto3.client('docdb', region_name=source_region)
        destination_client = boto3.client('docdb', region_name=destination_region)
        response = source_client.describe_db_cluster_snapshots(
            DBClusterSnapshotIdentifier=source_snapshot_identifier
        )
        source_snapshot_arn = response['DBClusterSnapshots'][0]['DBClusterSnapshotArn']
        try:
            response = destination_client.copy_db_cluster_snapshot(
                SourceDBClusterSnapshotIdentifier=source_snapshot_arn,
                TargetDBClusterSnapshotIdentifier=destination_snapshot_identifier,
                KmsKeyId = os.getenv('KMS_KEY'),
                CopyTags=True
        )
        except Exception as e:
            return {
                'statusCode': 400,
                'body': f"{e}"
                }
        return {
            'statusCode': 200,
            'body': f"Snapshot '{source_snapshot_identifier}' copied to
'{destination_snapshot_identifier}' in {destination_region} region."
        }
```

Цей підхід забезпечує автоматизовану реплікацію знімків DocumentDB між регіонами, використовуючи можливості AWS Lambda та KMS для забезпечення безпеки і надійності даних.

Налаштування TLS для Amazon RDS

Amazon RDS також підтримує підключення з використанням TLS для підвищення безпеки. Налаштування підключення з використанням TLS для Amazon RDS включає наступні кроки:

```
resource "aws_db_subnet_group" "db" {
  name       = var.environment
  subnet_ids = [var.vpc_private_subnet_ids[0], var.vpc_private_subnet_ids[2]]
}
```

Рисунок 2.29 – Створення підмережевих груп для бази даних

Цей ресурс створює підмережеву групу для бази даних, використовуючи підмережі з приватних підмереж VPC. Підмережева група дозволяє RDS серверам взаємодіяти в межах визначених підмереж. Далі необхідно створити випадковий пароль як в Document DB.

```
resource "aws_db_instance" "rds" {
  allocated_storage                   = 5
  max_allocated_storage               = 100
  auto_minor_version_upgrade          = false
  db_subnet_group_name                = aws_db_subnet_group.db.name
  backup_retention_period             = 14
  deletion_protection                 = true
  delete_automated_backups            = false
  enabled_cloudwatch_logs_exports     = ["postgresql"]
  engine                              = "postgres"
  engine_version                      = local.postgres_version
  instance_class                      = var.rds_instance_type
  db_name                             = "pslabs"
  identifier                          = var.environment
  maintenance_window                  = "Mon:02:00-Mon:02:30"
  multi_az                            = var.rds_multi_az
  username                            = "root"
  password                            = random_password.rds.result
  publicly_accessible                 = false
  storage_type                        = "gp3"
  storage_encrypted                   = true
  kms_key_id                          = aws_kms_key.rds_psl.arn
  final_snapshot_identifier = "final-snapshot-${var.environment}-main"
  apply_immediately         = true

  vpc_security_group_ids = [
    var.infra_security_group
  ]
}
```

Рисунок 2.30 – Створення серверу бази даних Amazon RDS

Ресурс «aws_db_instance» відповідає за створення серверу бази даних Amazon RDS з використанням PostgreSQL. Цей сервер має початковий об'єм зберігання 5 ГБ, з можливістю автоматичного збільшення до 100 ГБ. Автоматичні оновлення до незначних версій вимкнені для забезпечення стабільності роботи. Сервер використовує підмережеву групу, створену раніше, та зберігає резервні копії протягом 14 днів, з увімкненим захистом від видалення. Автоматичне видалення резервних копій вимкнене, а логи бази даних експортуються до CloudWatch для моніторингу.

База даних працює на PostgreSQL з версією, визначеною локальною змінною, і розгорнута на сервері класу, вказаного у змінній «var.rds_instance_type». Ім'я бази даних встановлено як «pslabs», а ідентифікатор серверу визначається змінною середовища «var.environment». Вікно для технічного обслуговування встановлено з понеділка 02:00 до понеділка 02:30, з підтримкою режиму Multi-AZ для забезпечення високої доступності. Адміністратором бази даних є користувач «root» з випадковим паролем, згенерованим раніше. Сервер не має публічного доступу, використовує сховище типу gp3, яке шифрується за допомогою ключа KMS, вказаного у змінній «aws_kms_key.rds_psl.arn».

Перед видаленням серверу створюється остаточний знімок з ідентифікатором «final-snapshot-${var.environment}-main», а зміни до конфігурації застосовуються негайно. Сервер працює в межах визначених VPC Security Group для забезпечення безпеки мережі.

Ресурс «aws_db_instance_automated_backups_replication» налаштовує автоматичне резервне копіювання сервер бази даних RDS в іншому регіоні. Кількість резервних копій визначається змінною «var.aws_replication_region», і якщо ця змінна не порожня, створюється один ресурс. Сервер, з якого буде здійснюватися резервне копіювання, визначається через його ARN, що отримується з ресурсу «aws_db_instance.rds». Період зберігання резервних копій встановлений на 14 днів. Шифрування резервних копій здійснюється за допомогою ключа KMS, ідентифікатор якого знаходиться у змінній

«aws_kms_key.rds_psl_replication[0].arn». Для виконання резервного копіювання в іншому регіоні використовується провайдер «aws.replication».

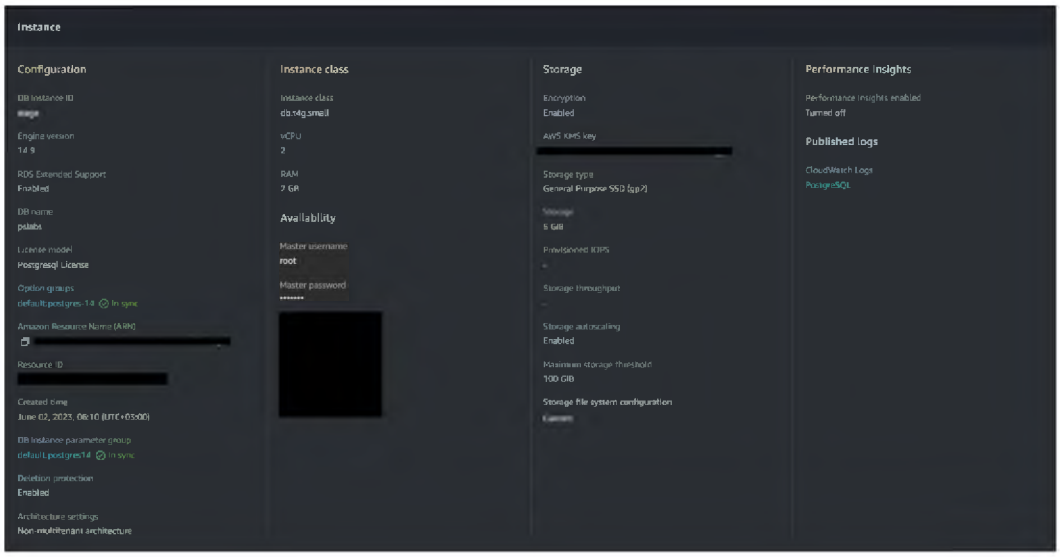

Рисунок 2.31 – Сторінка конфігурації RDS в консолі AWS

Шифрування трафіку за допомогою TLS забезпечує:

– конфіденційність даних: захист даних від перехоплення під час передачі між компонентами;

– цілісність даних: забезпечення цілісності даних, переданих між EKS та базами даних, шляхом запобігання модифікації даних під час передачі;

– аутентифікація серверів: перевірка автентичності серверів баз даних, з якими здійснюється підключення.

```
resource "aws_db_instance_automated_backups_replication" "rds_replication" {
  count                  = var.aws_replication_region != "" ? 1 : 0
  source_db_instance_arn = aws_db_instance.rds.arn
  retention_period       = 14
  kms_key_id             = aws_kms_key.rds_psl_replication[0].arn

  provider = aws.replication
}
```

Рисунок 2.32 – Автоматичне резервне копіювання Amazon RDS

Використання TLS для шифрування трафіку між Amazon EKS та Amazon DocumentDB і RDS є критично важливим елементом забезпечення безпеки даних в хмарних середовищах. Навіть зважаючи на той факт, що точки доступу між Amazon EKS й базами даних не виходять з приватної мережі, навіть в ній у ротенційного порушника не вийде перехопити ІОД. Це дозволяє знизити ризик перехоплення та несанкціонованого доступу до даних, що передаються, і підтримувати високий рівень захисту інформаційних систем.

2.3.6 Налаштування AWS WAF

У цьому розділі розглядається створення правил AWS WAF (Web Application Firewall) та їх підключення до CloudFront для захисту вебдодатків від загроз, таких як DDoS атаки та SQL ін'єкції. Використовуючи Terraform, ми створюємо ресурс WAF ACL, який визначає набір правил для фільтрації HTTP/HTTPS запитів. Цей WAF ACL має глобальний охоплення (scope = "CLOUDFRONT") і забезпечує захист на рівні контент-мережі.

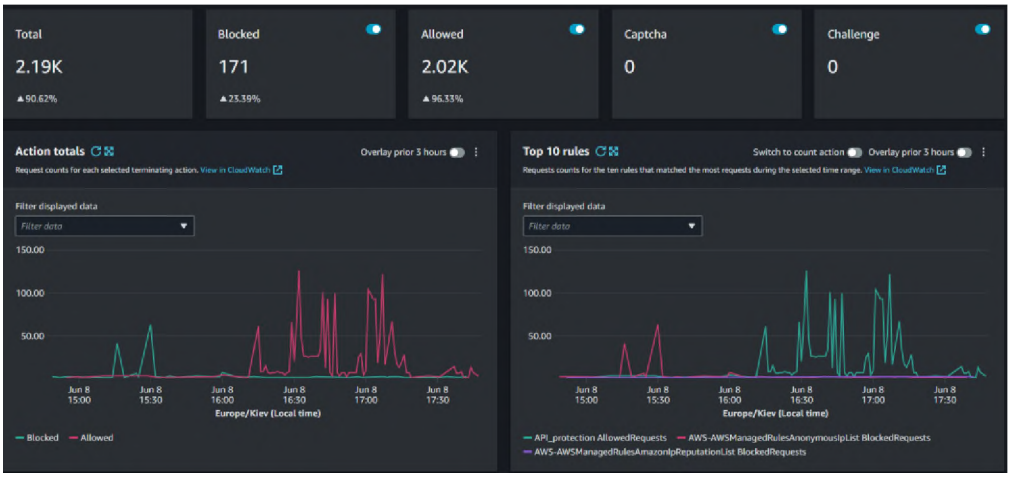

Рисунок 2.33 – Метрики створенного WAF ACL

Першим кроком є створення ACL з назвою, що визначається змінною середовища «var.environment», з дозволеним доступом за замовчуванням:

```
resource "aws_wafv2_web_acl" "waf" {
  name  = var.environment
```

```
scope = "CLOUDFRONT"
default_action {
  allow {}
}
```

Правила додаються до ACL для блокування доступу до певних сторінок. Наприклад, правило "cms-admin-pages" блокує доступ до URI, що починаються з "/cms-admin", якщо IP-адреса не належить до дозволеного набору IP-адрес VPN. Подібні правила створюються для блокування доступу до сторінок, що починаються з "/_util" та "/django-admin":

```
rule {
  name = "cms-admin-pages"
  priority = 0
  action {
    block {}
  }
  statement {
    and_statement {
      statement {
        byte_match_statement {
          positional_constraint = "STARTS_WITH"
          search_string = "/cms-admin"

          field_to_match {
            uri_path {}
          }
          text_transformation {
            type = "NONE"
            priority = 0
          }
        }
      }
      statement {
        not_statement {
          statement {
            ip_set_reference_statement {
              arn = aws_wafv2_ip_set.vpn.arn
            }
          }
```

```
      }
     }
    }
   }
   visibility_config {
    cloudwatch_metrics_enabled = false
    metric_name = "admin-pages"
    sampled_requests_enabled   = false
   }
  }
  rule {
   name = "cms-util-pages"
   priority = 1
   action {
    block {}
   }
   statement {
    and_statement {
     statement {
      byte_match_statement {
       positional_constraint = "STARTS_WITH"
       search_string = "/_util"
       field_to_match {
        uri_path {}
       }
       text_transformation {
        type = "NONE"
        priority = 0
       }
      }
     }
     statement {
      not_statement {
       statement {
        ip_set_reference_statement {
         arn = aws_wafv2_ip_set.vpn.arn
        }
       }
      }
     }
    }
   }
```

```
    visibility_config {
      cloudwatch_metrics_enabled = false
      metric_name  = "cms-util-pages"
      sampled_requests_enabled   = false
    }
  }
  rule {
    name = "django-admin-pages"
    priority = 2
    action {
      block {}
    }
    statement {
      byte_match_statement {
        positional_constraint = "STARTS_WITH"
        search_string = "/django-admin"
        field_to_match {
          uri_path {}
        }
        text_transformation {
          type = "NONE"
          priority = 0
        }
      }
    }
    visibility_config {
      cloudwatch_metrics_enabled = false
      metric_name = "django-admin-pages"
      sampled_requests_enabled   = false
    }
  }
  visibility_config {
    cloudwatch_metrics_enabled = false
    metric_name = "All"
    sampled_requests_enabled   = false
  }
  provider = aws.global
}
```

Крім того, створюється набір IP-адрес VPN, який містить IP-адресу, визначену змінною (var.vpn_elastic_ip), для забезпечення доступу тільки з дозволених IP-адрес:

```
resource "aws_wafv2_ip_set" "vpn" {
  name = "vpn"
  description = "VPN IP set"
  scope = "CLOUDFRONT"
  ip_address_version = "IPV4"
  addresses = ["${var.vpn_elastic_ip}/32"]
  provider = aws.global
}
```

Для логування створюється група журналів AWS CloudWatch з відповідною конфігурацією логування для WAF. Це дозволяє зберігати журнали збереження даних WAF на CloudWatch, забезпечуючи видимість та моніторинг запитів, що проходять через WAF:

```
resource "aws_cloudwatch_log_group" "waf_cloudwatch_log_group" {
  name = "aws-waf-logs-API_protection"
  retention_in_days = 30
}
resource "aws_wafv2_web_acl_logging_configuration" "api_protection_logging" {
  log_destination_configs = [aws_cloudwatch_log_group.waf_cloudwatch_log_group.arn]
  resource_arn = "${aws_wafv2_web_acl.api_protection.arn}"
}
resource "aws_cloudwatch_log_resource_policy" "waf_cloudwatch_log_policy" {
  policy_document =
data.aws_iam_policy_document.waf_cloudwatch_log_policy_document.json
  policy_name = "api-protection-cloudwatch-log"
}
```

Додатково створюється ACL для захисту API з регіональним охопленням (scope = "REGIONAL"). У цьому ACL визначено кілька правил, зокрема для дозволу доступу з сервісів моніторингу, таких як Pingdom, а також для блокування IP-адрес з низькою репутацією та анонімних IP-адрес за допомогою

керованих правил AWS. Для захисту від ботів додається правило «AWS-AWSManagedRulesBotControlRuleSet», яке використовує керовані правила для визначення категорій ботів, таких як моніторинг, пошукові системи та SEO, і підраховує їх запити:

```
resource "aws_wafv2_web_acl" "api_protection" {
 name  = "API_protection"
 scope = "REGIONAL"
 default_action {
  allow {}
 }
 rule {
  name     = "pingdom"
  priority = 0
  statement {
   or_statement {
    statement {
     label_match_statement {
      scope = "LABEL"
      key   = "awswaf:managed:aws:bot-control:bot:name:pingdom"
     }
    }
    statement {
     label_match_statement {
      scope = "LABEL"
      key   = "awswaf:managed:aws:bot-control:bot:category:monitoring"
     }
    }
   }
  }
  action {
   allow {}
  }
  visibility_config {
   cloudwatch_metrics_enabled = true
   metric_name = "pingdom"
   sampled_requests_enabled   = true
  }
 }
 rule {
```

```
  name  = "AWS-AWSManagedRulesAmazonIpReputationList"
  priority = 1
  statement {
   managed_rule_group_statement {
    name = "AWSManagedRulesAmazonIpReputationList"
    vendor_name = "AWS"
   }
  }
  override_action {
   none {}
  }
  visibility_config {
   cloudwatch_metrics_enabled = true
   metric_name = "AWS-AWSManagedRulesAmazonIpReputationList"
   sampled_requests_enabled   = true
  }
 }
 rule {
  name = "AWS-AWSManagedRulesAnonymousIpList"
  priority = 2
  statement {
   managed_rule_group_statement {
    name = "AWSManagedRulesAnonymousIpList"
    vendor_name = "AWS"
   }
  }
  override_action {
   none {}
  }
  visibility_config {
   cloudwatch_metrics_enabled = true
   metric_name = "AWS-AWSManagedRulesAnonymousIpList"
   sampled_requests_enabled   = true
  }
 }
 rule {
  name = "AWS-AWSManagedRulesBotControlRuleSet"
  priority = 3
  statement {
   managed_rule_group_statement {
    name = "AWSManagedRulesBotControlRuleSet"
    vendor_name = "AWS"
```

```
      rule_action_override {
        name = "CategoryMonitoring"
        action_to_use {
          count {}
        }
      }
      rule_action_override {
        name = "CategorySearchEngine"
        action_to_use {
          count {}
        }
      }
      rule_action_override {
        name = "CategorySeo"
        action_to_use {
          count {}
        }
      }
      scope_down_statement {
        label_match_statement {
          scope = "LABEL"
          key   = "awswaf:managed:aws:bot-control:bot:category:monitoring"
        }
      }
    }
  }
  override_action {
    count {}
  }
  visibility_config {
    cloudwatch_metrics_enabled = true
    metric_name = "AWS-AWSManagedRulesBotControlRuleSet"
    sampled_requests_enabled   = true
  }
}
```

Також додаються два правила обмеження швидкості (rate limit) на основі IP-адреси джерела та переадресованої IP-адреси, які блокують запити, що перевищують встановлений ліміт. Це забезпечує додатковий захист від надмірного навантаження на сервер:

```
rule {
  name  = "SourceIPRateLimit"
  priority = 4
  action {
    block {}
  }
  statement {
    rate_based_statement {
      limit  = local.rate_based_limit
      aggregate_key_type = "IP"
    }
  }
  visibility_config {
    cloudwatch_metrics_enabled = true
    metric_name = "SourceIPRateLimit"
    sampled_requests_enabled   = true
  }
}
rule {
  name = "ForwardedIPRateLimit"
  priority = 5
  action {
    block {}
  }
  statement {
    rate_based_statement {
      limit = local.rate_based_limit
      aggregate_key_type = "FORWARDED_IP"
      forwarded_ip_config {
        fallback_behavior = "MATCH"
        header_name = "X-Forwarded-For"
      }
    }
  }
  visibility_config {
    cloudwatch_metrics_enabled = true
    metric_name = "ForwardedIPRateLimit"
    sampled_requests_enabled   = true
  }
}
```

```
  visibility_config {
    cloudwatch_metrics_enabled = true
    metric_name = "API_protection"
    sampled_requests_enabled   = true
  }
}
```

Завершальним етапом є конфігурація видимості для всіх правил та ACL загалом, з метриками та збереженням запитів у журналах CloudWatch для подальшого аналізу.

2.3.7 Вдосконалення аудиту з використанням Cloudtrail

У цьому розділі розглядається створення CloudTrail для збору подій та налаштування SNS і EventBridge для оповіщення про певні дії. Для забезпечення детального аудиту подій буде налаштований AWS CloudTrail для збору всіх дій в обліковому записі AWS. Це дозволить відстежувати всі виклики API та зміни конфігурацій. Першим кроком є створення політики для CloudTrail за допомогою Terraform, що дозволяє збирати дані про події в обліковому записі. Далі налаштовується Amazon SNS та Amazon EventBridge для оповіщення про певні дії. Правила для EventBridge створюються для надсилання сповіщень про зміни конфігурацій або виявлення підозрілих дій:

```
resource "aws_cloudwatch_event_bus_policy" "default_event_bus" {
  policy = data.aws_iam_policy_document.default_event_bus_policy.json
  event_bus_name = "default"
}
```

У цьому розділі розглядається створення CloudTrail для збору подій та налаштування SNS і EventBridge для оповіщення про певні дії. Для забезпечення детального аудиту подій буде налаштований AWS CloudTrail для збору всіх дій в обліковому записі AWS. Це дозволить відстежувати всі виклики API та зміни конфігурацій. Першим кроком є створення політики для CloudTrail за допомогою Terraform, що дозволяє збирати дані про події в обліковому записі. Далі налаштовується Amazon SNS та Amazon EventBridge для оповіщення про певні

дії. Правила для EventBridge створюються для надсилання сповіщень про зміни конфігурацій або виявлення підозрілих дій.

Для забезпечення відправки повідомлень в Slack канал створюється правило EventBridge, яке реагує на події, зібрані CloudTrail, та спрямовує їх до Lambda-функції:

```
resource "aws_cloudwatch_event_rule" "slack_rule" {
  name = var.rule_name
  description = "Send Notification to slack #cloudtrail channel"
  event_pattern = file("./rule_policy.json")
}
resource "aws_cloudwatch_event_target" "slack_target" {
  rule = aws_cloudwatch_event_rule.slack_rule.name
  arn  = aws_lambda_function.cloudtrail_alert_lambda.arn
}
resource "aws_lambda_permission" "event_bridge_to_lambda" {
  statement_id  = "AllowExecutionFromCloudWatch"
  action = "lambda:InvokeFunction"
  function_name = var.lambda_name
  principal = "events.amazonaws.com"
  source_arn = aws_cloudwatch_event_rule.slack_rule.arn
}
```

Ці ресурси дозволяють налаштувати правила для EventBridge та зв'язати їх з Lambda-функцією, яка обробляє сповіщення та надсилає їх до Slack. Lambda-функція зчитує події, витягує відповідну інформацію, форматує повідомлення та надсилає його у вказаний Slack канал.

```
import urllib3
import json
import os
http = urllib3.PoolManager()
def get_account_name(account_id):
    account_names = {
        "111111111111": "Worksapce",
    }
    return account_names.get(account_id, "Unknown")
def lambda_handler(event, context):
```

```
    url = os.environ['SLACK']
    try:
      request_params = event["detail"]["requestParameters"]
      changes = json.dumps(remove_empty_dicts(request_params), indent=4) if
isinstance(request_params, dict) \
        else json.dumps(request_params, indent=4)
      account_name = get_account_name(event["detail"]["recipientAccountId"])
      text = "\n".join(['<!channel>',
        f'*Service*: *CloudTrail*',
        f'*EventTime*: {event["detail"]["eventTime"]}',
        f'*EventName*: {event["detail"]["eventName"]}',
        f'*AwsRegion*: {event["detail"]["awsRegion"]}',
        f'*AccountId*: {event["detail"]["recipientAccountId"]}',
        f'*AccountName*: {account_name}',
        f'*UserIdentity*: {event["detail"]["userIdentity"]["arn"]}',
        f'*UserAgent*: {event["detail"]["userAgent"]}',
        f'*Changes*: \n{changes}'])
    except:
      text = "Parsing Error"
      print({"message": event["detail"]})
    msg = {
      "channel": os.environ['CHANNEL'],
      "username": "CloudTrail_Alert",
      "text": text,
      "icon_emoji": ""
    }
    encoded_msg = json.dumps(msg).encode("utf-8")
    resp = http.request("POST", url, body=encoded_msg)
    print(
      {
        "message": event["detail"],
        "status_code": resp.status,
        "response": resp.data
      }
    )
  def remove_empty_dicts(d):
    for k, v in list(d.items()):
      if isinstance(v, dict):
        remove_empty_dicts(v)
        if not v:
          del d[k]
      elif isinstance(v, list):
```

```
            for item in v:
                if isinstance(item, dict):
                    remove_empty_dicts(item)
                    if not item:
                        v.remove(item)
    return d
```

Для забезпечення належної видимості та управління логами створюється група журналів CloudWatch:

```
resource "aws_cloudwatch_log_group" "cloudtrail_slack_notification" {
 name = "/aws/lambda/cloudtrail_slack_notification"
 retention_in_days = 14
}
```

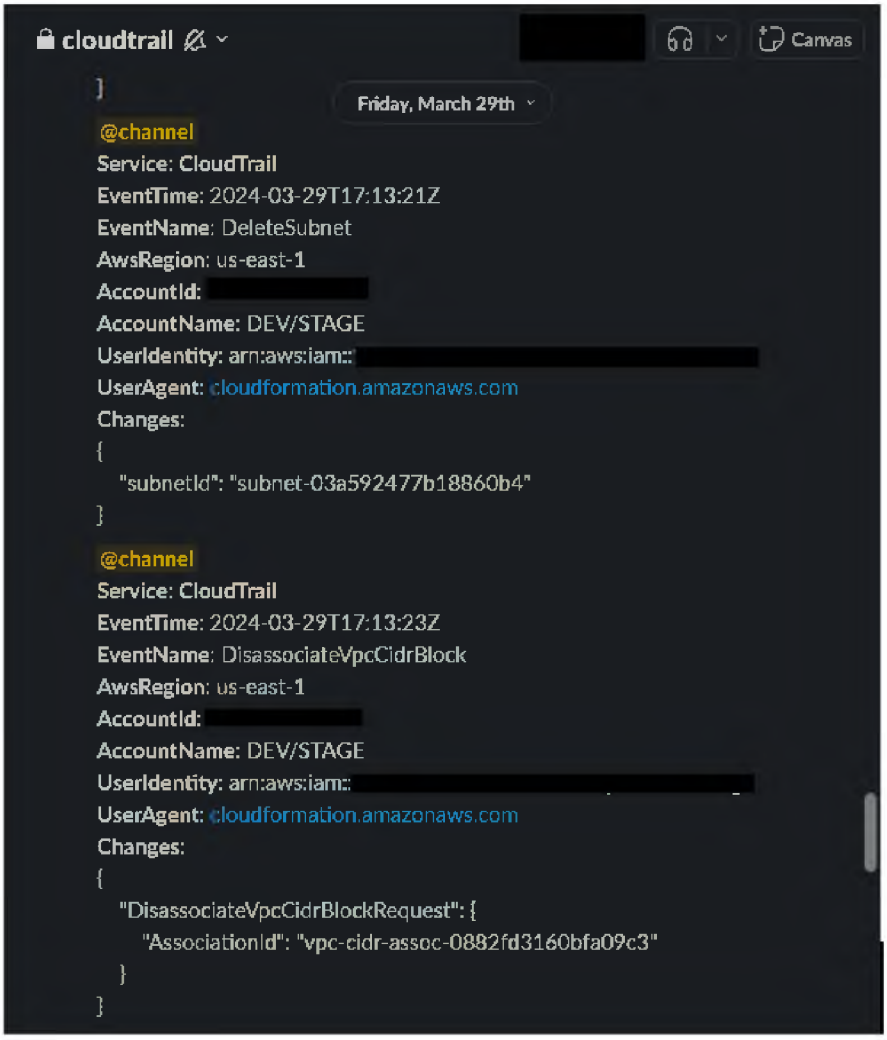

Рисунок 2.34 – Демонтсрація нотифікацій в Slack

Таким чином, налаштування AWS CloudTrail для збору подій у поєднанні з SNS та EventBridge для оперативного оповіщення забезпечує детальний аудит та можливість швидкого реагування на важливі події в обліковому записі AWS.

2.4 Висновок

На основі проведеного аналізу інформаційної діяльності ТОВ «ОІК» можна зробити наступні висновки:

1. Організаційна структура та технічне середовище: ТОВ «ОІК» є підприємством, що не має фізичного офісу, проте забезпечує високий рівень технічної підтримки та безпеки своїх інформаційних ресурсів через хмарні технології та послуги. Всі працівники мають доступ до робочого простору через VPN, що забезпечує централізоване управління та захист інформації.

2. Загрози інформаційної безпеки: Виявлено значні загрози, пов'язані з обробкою та зберіганням конфіденційної інформації, таких як персональні дані клієнтів, фінансові дані та програмний код сервісів. Важливим аспектом є забезпечення конфіденційності, цілісності та доступності інформації, що циркулює в організації.

3. Модель порушника: Розроблено модель порушника, яка враховує внутрішні та зовнішні загрози, рівень можливостей порушника, його обізнаність з системою, характер дій та методи реалізації загроз. Це дозволяє детально зрозуміти потенційні ризики та розробити відповідні заходи захисту.

4. Захист інформаційних ресурсів: Важливим елементом забезпечення інформаційної безпеки є впровадження надійних засобів захисту, таких як шифрування даних, мультифакторна автентифікація, контроль доступу та моніторинг системи. Використання хмарної інфраструктури AWS дозволяє автоматизувати ці процеси та зменшити вплив людського фактора.

Таким чином, комплексний підхід до захисту інформації в ТОВ «ОІК» забезпечує надійну роботу інформаційної системи, зменшує ризики втрати даних та підвищує рівень довіри клієнтів до компанії. Впровадження розробленої моделі захисту інформації дозволяє підприємству ефективно реагувати на

сучасні виклики у сфері кібербезпеки та забезпечувати відповідність найкращим практикам та стандартам.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Обґрунтування витрат на розробку моделі захисту інформації

Метою даного розділу є визначення витрат на розробку комплексу технічного захисту інформації ТОВ «ОІК». У цьому розділі в грошовому вираженні обґрунтовується необхідність створення моделі захисту інформації на платформі AWS, як критичного заходу для забезпечення безпеки даних у хмарному середовищі.

Для визначення витрат на розробку інфраструктури та оцінки економічної доцільності даної інфраструктури потрібно виконати наступні розрахунки:

1. Розрахунок капітальних витрат на проектування та впровадження моделі захисту інформації для хмарних інформаційно-комунікаційних систем на платформі AWS;

2. Розрахунок річних експлуатаційних витрат на функціонування моделі захисту інформації для хмарних інформаційно-комунікаційних систем на платформі AWS;

3. Розрахунок капітальних витрат при втраті інформації, за відсутності даної моделі захисту (розрахунок збитків).

3.1.1 Розрахунок витрат на розробку моделі захисту інформації

Витрати на розробку та впровадження моделі захисту інформації на ТОВ «ОІК» складаються з одноразових капітальних витрат та щорічних витрат на підтримку дієздатності та технічного забезпечення нововведень.

3.2 Розрахунок капітальних фіксованих витрат

Капітальні витрати - це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Щоб розрахувати вартість створення моделі захисту інформації необхідно розрахувати вартість машинного часу ($С_{мч}$) і помножити на кількість витрачених годин для створення моделі захисту, а програмне забезпечення для віддаленого доступу до Amazon постачається компанією безкоштовно.

P = 41 Вт*год = 0,041 кВт*год (номінальна потужність ноутбуку, на якому виконувались роботи по оновленню політики автентифікації)

C_e = 4,32 грн/кВт (вартість електроенергії)

Первісна вартість ($П_в$) ноутбука становить 30 849 грн, і він знаходиться в експлуатації вже 2 роки. Цей пристрій амортизується за прямолінійним методом, а термін його корисного використання ($Т_{кв}$) становить 7 років, Ліквідаційна вартість ($Л_в$) пристрою становить 4407 грн, тому щорічна сума амортизаційних відрахувань ($А_в$) буде розрахована за формулою:

$$А_в = \frac{П_в - Л_в}{Т_{кв}} \quad (3.1)$$

Щорічна сума амортизаційних відрахувань дорівнює 3777,43 грн, а норма амортизації (На) розраховується за формулою:

$$Н_а = \frac{1}{Т_{кв}} * 100\% \quad (3.2)$$

Норма амортизації становить 14,29%. На початок цього року залишкова вартість склала:

$$С_{мч} = P * C_e + \frac{Ф_{зал} * Н_а}{F_р} + \frac{К_{лпз}}{F_р} \quad (3.3)$$

де P – встановлена потужність ПК, кВт;

C_e – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

$$Ф_{зал} = 30849 - 3777,43 = 27071,57 \text{ грн}$$

$$К_{ппз} = 2\ 841,16 \text{ грн на один комп'ютер /рік}$$

$$С_{мч} = 0,041 * 4,32 + \frac{27071,57 * 0,1429}{1920} + \frac{2\ 841,16}{1920} = 3,67 \text{ грн/год}$$

Також розрахунку підлягає розробка моделі захисту інформації, але враховуючи що все необхідне ПЗ й його аткуалізація, що використовує підприємство лягає на системного адміністратора бо це його прямі зобов'язання їх оплата іде за рахунок заробітної плати співробітнику.

$$З_{мч} = t + С_{мч} \quad (3.4)$$

$$З_{мч} = 20 * 3,67 = 73,4 \text{ грн}$$

Вартість машинного часу для розробки політики безпеки інформації на ПК (Змч). Де (t) – трудомісткість розробки політики безпеки інформації на ПК, годин. (Смч) – вартість 1 години машинного часу ПК грн/година.

$$З_{зп} = t + З_{іб} \quad (3.5)$$

$$З_{зп} = 20 * 227,27 = 4545,4 \text{ грн}$$

Заробітна плата виконавця для розробки політики безпеки інформації (Ззп). Де (t) – тривалість розробки політики безпеки, годин. (Зіб) – середньогодинна заробітна плата спеціаліста грн/година.

$$К_{рп} = З_{зп} + З_{мч} \quad (3.6)$$

$$К_{рп} = 4545{,}4 + 73{,}4 = 4618{,}8 \text{ грн}$$

Витрати на розробку політики безпеки інформації (Крп) складаються з витрат на заробітну плату спеціаліста (Ззп) і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації (Змч).

$$К = К_{рп} \quad (3.7)$$

$$К = 4618{,}8 \text{ грн}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають: 4 тисячі 618 грн 8 коп.

3.3 Розрахунок річних поточних експлуатаційних витрат

Поточні витрати включають в себе:

– AWS CloudFront – 91,34 грн/міс (тобто 1096,08 грн/рік);

– AWS WAF – 405,94 грн/міс (тобто 4871,28 грн/рік);

– AWS KMS – 40,59 грн/міс за 1 шт. (тобто за використання 5 екземплярів 2435,4 грн/рік);

– AWS Lambda 8,12 за 1 млн запитів (оскільки сумарне використання цього сервісу не перевищило даного показника – 97,44 грн/рік);

– AWS Secret Manager – 16,24 грн/шт (використання 5 об'єктів – 947,4 грн/рік);

– AWS CloudTrail – 0 грн/міс (Amazon виставив ціну за збільшення терміну зберігання або збільшення цінності, використання зі стандартними налаштуваннями входить у безкоштовний рівень тому 0 грн/рік);

– Знімки – 0,81 грн/ГБ (загальна постійна кількість ГБ для зберігання резервних копій дорівнює 14, тоді 136 грн/рік);

– AWS SNS – 0,081 грн/шт (у середньому маємо 155 повідомлень у місяць тож 150,66 грн/рік);

– Amazon EventBridge – 15,59 грн/міс за 1 млн (тобто 187,08 грн/рік).

Річні експлуатаційні витрати на функціонування вдосконаленої інфраструктури (С) складуть 9 тисяч 921 грн 34 коп. на рік.

$$\text{С} = 9921{,}34 \text{ грн}$$

3.4 Оцінка величини можливого збитку від атаки

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки ($П_п$).

Місячний фонд робочого ($F_р$) часу складає 176 годин. Річний – 1920 годин. Час простою внаслідок атаки ($t_п$) = 3 год.

$$П_п = \frac{З_с}{F_р} * t_п \qquad (3.8)$$

$$П_п = \frac{270000}{176} * 3 = 4602{,}27 \text{ грн}$$

де ($З_с$) – сумарна заробітна плата персоналу, 270000 грн.

Витрати на відновлення працездатності системи включають кілька складових:

де $П_{пві}$ – витрати на повторне введення інформації, грн.;

$П_{пв}$– витрати на відновлення системи, грн.;

$П_{зч}$– вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи ($З_с$), які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу ($t_{ві}$) = 3 год.:

$$П_{ві} = \frac{З_с}{F_р} * t_{ві} \quad (3.9)$$

$$П_{ві} = \frac{90000}{176} * 3 = 1534{,}09 \text{ грн}$$

Витрати на відновлення системи визначаються часом відновлення після атаки ($t_в$)= 3 год. і розміром середньої заробітної плати за годину системного адміністратора:

$$П_{пв} = 227{,}27 * 3 = 681{,}81 \text{ грн.}$$

Витрати на відновлення працездатності системи:

$$П_в = П_{ві} + П_{пв} + П_{зч} \quad (3.10)$$

$$П_в = 1534{,}09 + 681{,}81 + 0 = 2215{,}9 \text{ грн}$$

де ($П_{зч}$) = 0 грн. - вартість для витрат на заміну частин.

$О_{чп}$= 4500000 грн. - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = \frac{О_{чп}}{F_р} * (Ч_п + Ч_в + Ч_{ві}) \quad (3.11)$$

$$V = \frac{4500000}{1920} * (3 + 3 + 3) = 21093{,}75 \text{ грн}$$

Де $F_р$– річний фонд робочого часу, 1920 годин;

$t_п$ – 3 годин простою після атаки;

$t_в$ – 3 годин відновлення після атаки;

$t_{ві}$ – 3 годин повторного введення втраченої інформації під час атаки;

Таким чином, загальний збиток від атаки на інформаційну систему при реалізації загрози складе:

$$U = П_п + П_в + V \quad (3.12)$$

$$U = 4602{,}27 + 2215{,}9 + 21093{,}75 = 27911{,}92 \text{ грн}$$

Таким чином, загальний збиток від атак на вузол або сегмент корпоративної мережі підприємства складе:

$$B = \sum_i * \sum_n * U \quad (3.13)$$

$$B = 9 * 2 * 27911{,}92 = 502414{,}56 \text{ грн}$$

де i - число атакованих вузлів, 9 комп'ютерів;

n – середнє число атак на рік, 3 рази.

3.5 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням (В) – загального збитку від атаки; R – очікуваної ймовірності атаки на систему; (С) – щорічних витрат на експлуатацію системи інформаційної безпеки.

Ймовірність R (0…1). Якщо реалізація загроз найймовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25.

Загальний ефект від впровадження політики безпеки:

$$E = B * R - C \tag{3.14}$$

$$E = 502414{,}56 * 0{,}25 - 9921{,}34 = 115682{,}3 \text{ грн}$$

3.6 Визначення та аналіз показників економічної ефективності

Оцінка економічної ефективності системи інформаційної безпеки, розглянутого у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу наступних показників:

– коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій То.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі.

Коефіцієнт ROSI розраховують за допомогою показників:

Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

$$ROSI = \frac{E}{K} \quad (3.15)$$

$$ROSI = \frac{115682,3}{95651,56} = 1,2$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження ПБ.

$$T_o = \frac{K}{E} = \frac{1}{ROSI} \quad (3.16)$$

$$T_o = \frac{1}{1,2} = 0,83 \text{ року} = 10 \text{ місяців}$$

3.7 Висновок

У цьому розділі детально обґрунтовано економічну доцільність впровадження комплексу технічного захисту інформації. Для обґрунтування були проаналізовані такі ключові аспекти:

– загальні витрати на впровадження комплексу технічного захисту інформації на підприємствах;

– можливості збитків у разі успішної інформаційної атаки на підприємство.

Відповідно до отриманих результатів, у разі атаки загальна сума збитків може досягти 502 414,56 грн. Водночас поточні експлуатаційні витрати становлять 9 921,34 грн, а капітальні інвестиції становлять 95 651,56 грн. За підрахунками витрати накопичуються за 10 місяців.

Таким чином, розрахунки, виконані в даному розділі, демонструють, що запропонована модель захисту інформації є економічно вигідною.

ВИСНОВКИ

У процесі виконання цієї кваліфікаційної роботи досягнуто мети, а саме розроблено модель захисту інформації для хмарних інформаційно-комунікаційних систем на основі платформи AWS. Проведені дослідження та впроваджені технічні рішення дозволяють зробити наступні висновки:

1. Сучасні методи захисту інформації, аналіз яких проведено, показали, що застосування хмарних платформ, таких як AWS, потребує всебічного підходу до забезпечення безпеки. До найкращих практик відносяться багатофакторна аутентифікація, управління доступом на основі ролей, шифрування даних у спокої та під час передачі, а також безперервний моніторинг безпеки.

2. Модель загроз і порушника була розроблена з урахуванням можливих внутрішніх і зовнішніх загроз. Це дозволило ретельно оцінити потенційні ризики та розробити відповідні заходи захисту. Особливу увагу було приділено захисту конфіденційних даних, що обробляються та зберігаються у хмарному середовищі.

3. Розробка та впровадження системи безпеки інформації включала організаційні, інженерні та технічні заходи для запобігання несанкціонованому доступу. Важливим елементом було використання інструментів автоматизації, таких як Terraform, для розгортання та управління інфраструктурою як кодом (IaC).

4. Фінансова ефективність запровадження заходів безпеки підтверджена розрахунками. Витрати на впровадження та експлуатацію системи є виправданими з огляду на потенційні збитки від можливих інформаційних атак. Термін окупності капіталовкладень становить приблизно 10 місяців, що свідчить про високу ефективність запропонованих заходів.

5. Практичне значення результатів цієї кваліфікаційної роботи полягає у забезпеченні захисту інформації в хмарному середовищі на платформі AWS. Це сприяє підвищенню рівня безпеки інформаційних ресурсів підприємства та зменшує ризики, пов'язані з можливими інформаційними атаками.

Загальні висновки підтверджують, що розроблена модель захисту інформації є ефективною та економічно доцільною для підприємств, які використовують хмарні платформи. Вона забезпечує необхідний рівень безпеки та дозволяє оперативно реагувати на загрози, зберігаючи конфіденційність, цілісність і доступність даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99 від 15.10.2008р. № 172 (дата звернення: 27.05.2024).

2. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 р. № 1229/99 : станом на 4 трав. 2008 р. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення: 01.06.2024).

3. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 02.06.2024).

4. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99 від 28.04.99р. № 22 (дата звернення: 01.06.2024).

5. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 03.06.2024).

6. Про хмарні послуги : Закон України від 17.02.2022 р. № 2075-IX : станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення: 01.06.2024).

7. Shared Responsibility Model - Amazon Web Services (AWS). *Amazon Web Services, Inc.* URL: https://aws.amazon.com/compliance/shared-responsibility-model/?nc1=h_ls (дата звернення: 08.06.2024).

8. AWS Whitepapers & Guides. *Amazon Web Services, Inc.* URL: https://aws.amazon.com/whitepapers/ (дата звернення: 05.06.2024).

9. Чекушкін Н. Д. «Optimizing DevOps Processes with Single Sign-on (SSO): Benefits, Challenges, and Use Cases.» *Medium*. URL: https://medium.com/@Nick_Chekushkin/optimizing-devops-processes-with-single-

sign-on-sso-benefits-challenges-and-use-cases-04ba2369ef0a (дата звернення: 04.06.2024).

10. Documentation | Terraform | HashiCorp Developer. *Documentation | Terraform | HashiCorp Developer*. URL: https://developer.hashicorp.com/terraform/docs (дата звернення: 24.05.2024).

11. What Are IaaS, PaaS and SaaS? | IBM. *IBM - United States*. URL: https://www.ibm.com/topics/iaas-paas-saas (дата звернення: 04.06.2024).

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	19	
6	А4	2 Розділ	66	
7	А4	3 Розділ	9	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Кваліфікаційна робота_Чекушкін.docx
2. Презентація_Чекушкін.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 94 б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
«Розробка моделі захисту інформації для хмарних
інформаційно-комунікаційних систем на платформі AWS»
студента групи 125-20-3
Чекушкіна Нікіти Дмитровича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 113 сторінках та містить 35 рисунків, 4 таблиці, 11 джерел та 4 додатка.

Метою кваліфікаційної роботи є розробка моделі захисту інформації в хмарному середовищі, що забезпечує підвищення рівня безпеки інформаційних ресурсів на платформі AWS.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: дослідження технічної бази системи ТОВ «ОІК», проведення аудиту та аналізу загроз інформаційної безпеки, розробка коду для модуля автоматизованого розгортання та захисту інформації, визначення витрат на розробку та впровадження захисту інформації та аналіз її економічної ефективності.

У першому розділі кваліфікаційної роботи проведено дослідження технічної бази системи ТОВ «ОІК», проведено аудит та аналіз загроз інформаційної безпеки в хмарі. Розроблено код для модуля автоматизованого розгортання та захисту інформації.

У спеціальній частині виконано розробку моделі захисту інформації, що включає організаційні та технічні заходи щодо захисту інформації від несанкціонованого доступу.

В економічному розділі визначено витрати на розробку та впровадження захисту інформації та проведено аналіз її економічної ефективності.

У процесі виконання роботи студент продемонстрував високий рівень знань у галузі кібербезпеки та здатність використовувати сучасні технології, щоб вирішити завдання з побудови моделі захисту інформації. Студент вивчав особливості хмарних середовищ і проаналізував поточні загрози, побудував модель захисту, яка включає організаційні та технічні заходи. Він продемонстрував здатність працювати з багатьма інструментами AWS, такими як IAM, VPC, CloudTrail, WAF і Secrets Manager, а також ефективно інтегрувати

їх до інфраструктури ТОВ «ОІК», щоб підвищити рівень безпеки інформаційних ресурсів.

Зокрема, студент проаналізував і порівняв кілька моделей хмарних обчислень, досліджуючи їхні переваги та недоліки з точки зору безпеки. Він використав Terraform для розробки та реалізації методології IaC, що дозволило автоматизувати розгортання та налаштування безпеки в хмарному середовищі AWS.

Студент показав достатній рівень володіння теоретичними положеннями й практичними навичками з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою, відповідає вимогам положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка». Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує оцінки «_____».

Керівник кваліфікаційної роботи:
д.т.н. проф. Анна КОРЧЕНКО

Керівник спец. розділу:
ас. Ілля ОЛІШЕВСЬКИЙ