Міністерство освіти і науки України

Тернопільський національний технічний університет імені Івана Пулюя

(повне найменування вищого навчального закладу)

Факультет комп'ютерно-інформаційних систем і програмної інженерії

(назва факультету)

Кафедра кібербезпеки

(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр

(освітній рівень)

на тему: *«Оцінка безпеки використання хмарних технологій та розробка методів захисту від кібератак на хмарні сервіси»*

Виконав: студент (ка)

Спеціальності:

125 «Кібербезпека»

(шифр і назва напряму підготовки, спеціальності)

		Мазур В. М.
	підпис	(прізвище та ініціали)
Керівник		*Козак Р. О.*
	підпис	(прізвище та ініціали)
Нормоконтроль		*Лобур Т. Б.*
	підпис	(прізвище та ініціали)
Завідувач кафедри		*Загородна Н. В.*
	підпис	(прізвище та ініціали)
Рецензент		
	підпис	(прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«19» __червня__ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Мазуру Володимиру Михайловичу
(прізвище, ім'я, по батькові)

1. Тема роботи Оцінка безпеки використання хмарних технологій та розробка методів захисту від кібератак на хмарні сервіси

Керівник роботи Козак Руслан Орестович, д.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 03 » 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи 17.06.2023

3. Вихідні дані до роботи публічна хмарна AWS; персональний ноутбук з ОС Windows 10; науково-технічна література, експлуатаційна документація, міжнародні стандарти.

4. Зміст роботи (перелік питань, які потрібно розробити)
Концептуальні основи безпек хмарних технологій
Основні поняття та принципи безпеки в хмарних сервісах
Аналіз загроз та ризиків безпеки хмарних сервісів
Заходи та методи захисту від кібератак в хмарних сервісах
Впровадження методів захисту від кібератак на хмарні сервіси AWS
Вдосконалення ідентифікації та аутентифікації
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пилипець.М.І., проф. кафедри МТ		

7. Дата видачі завдання 16.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.01 – 19.01	*Виконано*
2.	Підбір джерел про принципи побудови та методи забезпечення безпеки в хмарних сервісах	20.01 – 05.02	*Виконано*
3.	Опрацювання джерел в галузі дослідження	06.02 – 22.02	*Виконано*
4.	Розроблення інформаційної інфраструктури	23.02 – 20.03	*Виконано*
5.	Тестування роботи методів захисту та верифікація результатів	21.03-05.04	*Виконано*
6.	Оформлення розділу «Концептуальні основи безпек хмарних технологій»	06.03 – 17.04	*Виконано*
7.	Оформлення розділу «Функціонал і архітектура AWS»	18.04 – 29.04	*Виконано*
8.	Оформлення розділу «Впровадження методів захисту від кібератак на хмарні сервіси AWS»	30.04 – 13.05	*Виконано*
9.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	14.05 – 21.05	*Виконано*
10.	Оформлення кваліфікаційної роботи	22.05 – 05.06	*Виконано*
11.	Нормоконтроль	06.06 – 11.06	*Виконано*
12.	Перевірка на плагіат	12.06 – 14.06	*Виконано*
13.	Попередній захист кваліфікаційної роботи	15.06 – 19.06	*Виконано*
14.	Захист кваліфікаційної роботи	20.06.2023	

Студент _____ *Мазур В. М.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Козак Р. О.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Оцінка безпеки використання хмарних технологій та розробка методів захисту від кібератак на хмарні сервіси // Кваліфікаційна робота ОР «Бакалавр» // Мазур Володимир Михайлович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // с. 58, рис. – 11, табл. – 0, кресл. – 0, додат. – 0.

Ключові слова: АВТЕНТИЧНІСТЬ, КОНФІДЕНЦІЙНІСТЬ, ДОСТУПНІСТЬ, БЕЗПЕКА, КІБЕРЗАГРОЗА, ХМАРНІ СЕРВІСИ, БРАНДМАУЕР, ВИЯВЛЕННЯ, МОНІТОРИНГ.

Кваліфікаційна робота присвячена впровадженню методів захисту від кібератак на хмарні сервіси AWS. Метою дослідження є виявлення, аналіз та розробка ефективних заходів безпеки, спрямованих на забезпечення надійного захисту інфраструктури хмарних сервісів від широкого спектру кіберзагроз. У роботі розглянуті основні види кібератак, їх характеристики та наслідки, а також переваги та обмеження використання хмарних сервісів AWS. Запропоновані методи захисту охоплюють встановлення сучасних фаєрволів, систем виявлення вторгнень та моніторингу, шифрування даних, бекапи та відновлення, аутентифікацію та авторизацію користувачів. Результати дослідження демонструють ефективність запропонованих заходів безпеки, що сприяють підвищенню рівня захищеності хмарної інфраструктури AWS від кібератак. Робота є важливим внеском у розвиток сфери кібербезпеки та допомагає підвищити надійність та безпеку хмарних сервісів.

ABSTRACT

Study of mechanisms for ensuring security in decentralized systems // Thesis of educational level "Bachelor" // Mazur Volodymyr Mykhailovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, СБ-41 group // Ternopil, 2023 // p. 58, fig. - 10, table. - 0, chair. - 0, added. - 0.

Keywords: AUTHENTICITY, CONFIDENTIALITY, AVAILABILITY, SECURITY, CYBERTHREAT, CLOUD SERVICES, FIREWALL, DETECTION, MONITORING.

The qualifying paper focuses on the implementation of cybersecurity methods for protecting cloud services on AWS. The objective of the research is to identify, analyze, and develop effective security measures aimed at ensuring reliable protection of cloud infrastructure from a wide range of cyber threats. The paper examines various types of cyber attacks, their characteristics, and consequences, as well as the advantages and limitations of utilizing AWS cloud services. The proposed security methods include the implementation of state-of-the-art firewalls, intrusion detection and monitoring systems, data encryption, backups and recovery mechanisms, and user authentication and authorization. The research findings demonstrate the effectiveness of the proposed security measures in enhancing the resilience of AWS cloud infrastructure against cyber attacks. This work contributes significantly to the field of cybersecurity and helps improve the reliability and security of cloud services for enterprises and users.

ЗМІСТ

ВСТУП

Перспективи розвитку об'єкту проектування полягають у постійному вдосконаленні та розширенні захисних можливостей хмарних сервісів AWS. З впровадженням штучного інтелекту, аналізу великих обсягів даних та машинного навчання, можливості виявлення та прогнозування кібератак стають ще більш точними та ефективними.

Досягнення мети проектування, а саме впровадження методів захисту від кібератак на хмарні сервіси AWS, сприятиме збереженню конфіденційності, цілісності та доступності даних клієнтів, а також забезпечить безпеку їхніх бізнес-операцій.

Актуальність теми: У сучасному цифровому світі, коли хмарні сервіси набули широкого поширення і стали важливою складовою багатьох організаційних інфраструктур, захист від кібератак на такі сервіси стає надзвичайно важливим завданням. Хмарні сервіси AWS є одними з найпопулярніших на ринку і використовуються мільйонами користувачів по всьому світу. Однак, зростання популярності цих сервісів також приводить до збільшення кількості кібератак, спрямованих на них.

Метою роботи є розробка та впровадження ефективних методів захисту, які дозволять запобігти атакам на хмарні сервіси AWS. Це включає в себе розробку та конфігурацію захисних механізмів, виявлення та моніторинг потенційних загроз, розробку політик безпеки та практик захисту даних.

Досягнення цієї мети дозволить створити надійне та безпечне середовище для хмарних сервісів AWS, що забезпечить захист даних від кібератак та підвищить довіру користувачів до сервісу. Застосування ефективних методів захисту буде мати велике значення для бізнес-сектору, організацій та індивідуальних користувачів, які використовують хмарні сервіси AWS для зберігання своїх даних.

Отже, кваліфікаційна робота має на меті внести вагомий внесок у розвиток безпечних хмарних сервісів та забезпечити захист даних від кібератак, сприяючи підвищенню довіри користувачів до цих сервісів.

Огляд сучасних розробок за темою: На теперішній час існує велика кількість розробок і технологій, спрямованих на захист хмарних сервісів від кібератак. Декілька з них можуть бути наведені нижче:

- firewalls та мережеві механізми: Використання відповідних фаєрволів і мережевих механізмів є одним з найпоширеніших методів захисту. Ці засоби дозволяють контролювати доступ до ресурсів, обмежувати небажану мережеву активність та виявляти аномальні дії;
- шифрування даних: Застосування шифрування даних для зберігання і передачі інформації у хмарних сервісах є важливою складовою безпеки. Використання сучасних алгоритмів шифрування дозволяє забезпечити конфіденційність та цілісність даних;
- моніторинг та аналіз безпеки: Використання спеціалізованих інструментів моніторингу дозволяє виявляти потенційні загрози та атаки на хмарні сервіси AWS. Аналіз ведеться на основі великої кількості лог-файлів та метрик, що дозволяє оперативно реагувати на загрози та уникати інцидентів.
- багатофакторна аутентифікація: Використання багатофакторної аутентифікації, такої як комбінація пароля та одноразового коду, забезпечує додатковий рівень безпеки при використанні хмарних сервісів;
- автоматизація заходів безпеки: Розробка скриптів та автоматизація процесів безпеки можуть значно полегшити впровадження та контроль захисних заходів на хмарних сервісах AWS. Це включає в себе автоматичне масштабування сервісів залежно від потреб, перевірку наявності оновлень та патчів, а також регулярну перевірку на наявність вразливостей.

Ці сучасні розробки є лише деякими прикладами методів захисту від кібератак на хмарні сервіси AWS.

Проблематика даної теми включає в себе наступні аспекти:

- загрози кібербезпеці в хмарних сервісах: Хмарні сервіси AWS зберігають значну кількість конфіденційних даних і ресурсів своїх клієнтів. Вони стають об'єктом атак з боку зловмисників, які можуть спробувати зламати систему, отримати доступ до цих даних і вчинити шкоду;

- недоліки безпеки в хмарних сервісах AWS: Існують різні недоліки безпеки, які можуть вплинути на хмарні сервіси AWS. Це можуть бути недостатні заходи захисту, неправильна конфігурація, слабкі паролі, вразливості в програмному забезпеченні тощо.

У кваліфікаційній роботі ціль розв'язати наступні задачі:

- аналіз загроз безпеці в хмарних сервісах AWS: дослідження типів загроз, з якими можуть стикатися хмарні сервіси AWS, включаючи DDoS-атаки, фішинг, витоки даних та інші;

- вивчення методів захисту: дослідження різних методів та стратегій захисту від кібератак, які можна використовувати на хмарних сервісах AWS. Це може включати мережеві та програмні засоби захисту, шифрування даних, контроль доступу та інші технології;

- впровадження систем захисту: впровадження конкретної системи захисту для хмарних сервісів AWS, використовуючи обрані методи та стратегії. Мета запобігти атакам, виявити порушення безпеки та швидко реагувати на них.

РОЗДІЛ 1 КОНЦЕПТУАЛЬНІ ОСНОВИ БЕЗПЕК ХМАРНИХ ТЕХНОЛОГІЙ

У сучасному світі хмарні технології набувають все більшої популярності у різних сферах діяльності, забезпечуючи широкі можливості для зберігання, обробки та обміну даними. Однак, разом зі зростанням використання хмарних сервісів збільшується ймовірність кібератак та порушень безпеки інформації. Тому вивчення та оцінка безпеки використання хмарних технологій стають надзвичайно важливими завданнями для забезпечення конфіденційності, цілісності та доступності даних.

Даний розділ присвячений концептуальним основам безпеки хмарних технологій. У цьому розділі розглянуто основні поняття та принципи безпеки в хмарних сервісах, проведено аналіз загроз та ризиків безпеки, розглянуто заходи та методи захисту від кібератак, а також проведено огляд безпеки в одному з найпопулярніших хмарних сервісів - AWS.

У першому підрозділі дослідження розглянуто основні поняття та принципи безпеки в хмарних сервісах. Безпека в хмарному середовищі має свої особливості, і для розуміння цих особливостей необхідно ознайомитися з термінологією та базовими концепціями, пов'язаними з безпекою хмарних технологій. Розглянуто такі поняття, як віртуалізація, мультитенантність, шаровість безпеки та інші, а також розглянуто принципи, які лежать в основі безпеки хмарних сервісів.

Другий підрозділ присвячений аналізу загроз та ризиків безпеки хмарних сервісів. Розглянуто потенційні загрози, з якими можуть стикатися організації, що використовують хмарні сервіси, такі як злам аккаунтів, втрата даних, DDoS-атаки та інші. Також проведено оцінку ризиків, пов'язаних з цими загрозами, для кращого розуміння важливості безпеки в хмарному середовищі.

У третьому підрозділі розглянуто заходи та методи захисту від кібератак в хмарних сервісах. Оглянуто різноманітні техніки та інструменти, які можуть

бути використані для підвищення безпеки хмарних сервісів, такі як шифрування даних, контроль доступу, моніторинг та виявлення вторгнень, резервне копіювання та відновлення даних та багато інших. Також проаналізовано ефективність цих заходів та їх можливі обмеження.

У заключному підрозділі розділу проведено огляд безпеки в одному з найпопулярніших хмарних сервісів - Amazon Web Services. AWS є одним з найбільших постачальників хмарних послуг, тому розглянуто його архітектуру та основні механізми безпеки, які надаються користувачам цього сервісу. Розглянуто заходи безпеки, використовувані в AWS, такі як IAM, VPC, AWS CloudTrail та інші.

У цьому розділі надано всебічний огляд концептуальних основ безпеки хмарних технологій. Розглядаючи основні поняття, принципи, загрози та методи захисту, а також оглядаючи безпеку в одному з провідних хмарних сервісів, надано необхідні знання для розуміння та оцінки безпеки використання хмарних технологій. Відповідна розробка методів захисту від кібератак на хмарні сервіси буде розглянута в наступних розділах кваліфікаційної роботи.

1.1 Основні поняття та принципи безпеки в хмарних сервісах

У даному підрозділі розглянуто основні поняття та принципи безпеки в хмарних сервісах. Розуміння цих концепцій є надзвичайно важливим кроком для забезпечення ефективного захисту даних у хмарному середовищі.

Перша ключова концепція - це віртуалізація, яка є основою хмарних сервісів. Вона дозволяє розділити обчислювальні ресурси, мережу та сховище даних між різними користувачами. Завдяки віртуалізації ресурсів, хмарні сервіси можуть надавати гнучкість та ефективне використання обчислювальних потужностей.

У зв'язку з використанням спільної інфраструктури в хмарному середовищі, виникає концепція мультитенантності. Це означає, що різні

організації та користувачі можуть використовувати одну і ту ж хмарну інфраструктуру. При цьому важливо забезпечити ізоляцію та безпеку даних кожного користувача, щоб уникнути несанкціонованого доступу та проникнення між різними "аренами" користувачів.

Для ефективного захисту даних у хмарному середовищі використовується принцип шарування безпеки. Цей принцип передбачає застосування різних рівнів захисту на різних рівнях інфраструктури. Наприклад, на фізичному рівні можуть бути застосовані заходи безпеки, такі як фізичний доступ до серверних приміщень та моніторинг систем. На рівні мережі можуть бути використані механізми захисту мережевого трафіку та перехоплення загроз. На рівні даних можуть застосовуватися шифрування та механізми контролю доступу. Кожен рівень має свої власні механізми безпеки, які взаємодіють з іншими рівнями, створюючи комплексну систему захисту.

Одним з важливих принципів безпеки в хмарних сервісах є принцип доступності, цілісності та конфіденційності (CIA-трикутник). Доступність означає, що дані та ресурси повинні бути доступні для користувачів у потрібний момент. Цілісність гарантує, що дані не будуть незаконно змінені або пошкоджені. Конфіденційність полягає у захисті даних від несанкціонованого доступу, забезпечуючи, що тільки авторизовані особи мають доступ до конфіденційної інформації.

Контроль доступу є ще однією важливою концепцією в безпеці хмарних сервісів. Він включає механізми ідентифікації та автентифікації користувачів, а також контроль доступу до різних ресурсів. Це може включати використання ролей, політик доступу та механізмів аудиту для обмеження прав доступу до даних та функціональності системи.

Шифрування даних є ще одним важливим аспектом безпеки в хмарних сервісах. У зв'язку з тим, що дані можуть бути передані та зберігатися на серверах провайдера, важливо захищати їх шифруванням. Шифрування даних

забезпечує їх конфіденційність та захист навіть у разі несанкціонованого доступу до серверів або злому системи.

1.2 Аналіз загроз та ризиків безпеки хмарних сервісів

Аналіз загроз та ризиків безпеки хмарних сервісів виявляється надзвичайно важливим для організацій та користувачів, які залучають хмарні технології для зберігання та обробки своїх даних. Детальне розуміння цих загроз допомагає ідентифікувати можливі слабкі місця в системі безпеки та прийняти необхідні заходи для їх запобігання.

Однією з основних загроз є несанкціонований доступ до даних. Оскільки хмарні сервіси зберігають дані на віддалених серверах, вони стають привабливою метою для зловмисників, які намагаються отримати несанкціонований доступ до цієї інформації. Несанкціонований доступ може призвести до порушення приватності, розголошення конфіденційної інформації користувачів та компаній. Це підкреслює необхідність міцного шифрування даних та ефективного керування доступом, щоб забезпечити конфіденційність та цілісність даних.

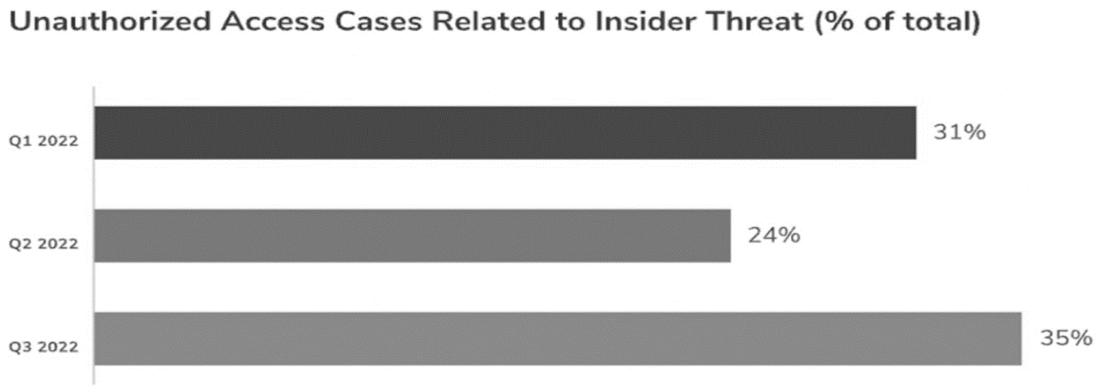

Рисунок 2.1 – Випадки несанкціонованого доступу, пов’язані з внутрішньою загрозою(% від загальної кількості)

Крім того, хмарні сервіси також стикаються з загрозами кібератак. Зловмисники можуть спробувати отримати контроль над хмарною інфраструктурою, використовуючи такі методи, як DDoS-атаки, вторгнення через вразливості програмного забезпечення або соціально-інженерні методи. Такі кібератаки можуть призвести до відмова у наданні обслуговування, втрати даних або порушення цілісності системи. Щоб забезпечити безпеку хмарних сервісів, необхідно впроваджувати системи виявлення та запобігання вторгнень, регулярно оновлювати програмне забезпечення та надавати освіту користувачам щодо використання безпечних паролів та заходів безпеки.

Загрози, пов'язані зі спільною інфраструктурою хмарних сервісів, також не можна ігнорувати. З огляду на те, що різні організації та користувачі використовують одну хмарну інфраструктуру, існує ризик, що один користувач може мати доступ до чужих даних або спотворити нормальну роботу інших користувачів. Це може стати результатом недостатньої ізоляції ресурсів та недосконалостей управління доступом. Необхідно забезпечити ефективну сегрегацію даних та ресурсів між різними користувачами, а також встановити механізми моніторингу та аудиту для виявлення недоречних дій.

Додатковою загрозою є втрата контролю над даними у випадку зупинки або закриття хмарного провайдера. Якщо провайдер припиняє свою діяльність або відмовляється від обслуговування, користувачі можуть стикнутися з втратою доступу до своїх даних або бути змушені швидко мігрувати до іншого провайдера. Це потенційно призводить до проблем з безпекою та недоступності. Для запобігання цим ризикам рекомендується регулярне створення резервних копій даних та встановлення контракту з провайдером щодо умов збереження даних у разі зміни або закриття сервісу.

Враховуючи ці загрози та ризики безпеки хмарних сервісів, необхідно приділяти особливу увагу розробці та впровадженню ефективних стратегій

безпеки. Це включає в себе використання механізмів шифрування для захисту даних, регулярне оновлення та патчінг програмного забезпечення, впровадження мережевих та периметральних заходів безпеки, а також навчання користувачів щодо кращих практик безпеки та використання складних паролів. Важливо також співпрацювати з провайдерами хмарних сервісів для забезпечення високого рівня безпеки та виконання відповідних стандартів безпеки.

Загальний аналіз загроз та ризиків безпеки хмарних сервісів допомагає організаціям та користувачам підготуватися до потенційних небезпек та прийняти необхідні заходи для забезпечення захисту своїх даних. Розгляд методів захисту від кібератак на хмарні сервіси та розробка власних підходів до підвищення безпеки використання хмарних технологій дозволять розглянути конкретні стратегії та методики для забезпечення захисту хмарних сервісів.

1.3 Заходи та методи захисту від кібератак в хмарних сервісах

Зважаючи на постійно зростаючу складність кібератак та загроз кібербезпеці, розробка комплексної стратегії безпеки в хмарних сервісах є критично важливою. Для ефективного захисту від кібератак в хмарних сервісах рекомендується використовувати різноманітні заходи та методи захисту.

Одним з перших кроків у забезпеченні безпеки хмарних сервісів є визначення мережевого периметру. Це включає створення контрольних точок та використання мережевих пристроїв, які можуть виявляти та блокувати шкідливий трафік. Встановлення брандмауерів, систем виявлення вторгнень та інших засобів безпеки допомагає ускладнити доступ для потенційних хакерів.

Шифрування даних є ще одним важливим заходом безпеки. Застосування сильного шифрування дозволяє захистити конфіденційні дані від несанкціонованого доступу, навіть якщо зловмисник отримає фізичний доступ до сховища даних. Шифрування на рівні даних, а також на рівні комунікацій між користувачами та хмарними сервісами, є важливим елементом безпеки.

Моніторинг та аудит безпеки є необхідними практиками для виявлення незвичайної активності, вразливостей та потенційних загроз. Постійний моніторинг системи та аналіз журналів дозволяють оперативно реагувати на випадки порушень безпеки та приймати відповідні заходи для їх усунення.

Регулярні резервні копії даних грають важливу роль у забезпеченні можливості відновлення інформації в разі випадкового видалення, втрати або кібератаки. Резервне копіювання на віддалених серверах або в інших фізичних місцях гарантує надійність та доступність даних.

Регулярне оновлення програмного забезпечення та встановлення оновлень безпеки є необхідними для усунення вразливостей, які можуть бути використані зловмисниками. Встановлення автоматичного оновлення допомагає забезпечити постійну актуальність безпеки системи.

Окрім цих заходів, рекомендується використовувати передові технології, такі як механізми виявлення загроз на основі штучного інтелекту та машинного навчання, а також аналітику безпеки для розпізнавання аномалій та попередження кібератак.

Загальна стратегія безпеки повинна включати розробку і впровадження політик безпеки, постійне навчання персоналу щодо кібербезпеки та співпрацю з провідними постачальниками хмарних сервісів, які надають додаткові заходи безпеки.

1.4 Огляд безпеки в AWS

AWS є одним з провідних постачальників хмарних послуг у світі. Вони пропонують широкий спектр послуг у сфері обчислення, зберігання даних, мереж та інших інфраструктурних рішень. Безпека є невід'ємною частиною всіх цих послуг, оскільки користувачі довіряють AWS для зберігання, обробки та передачі своїх конфіденційних даних.

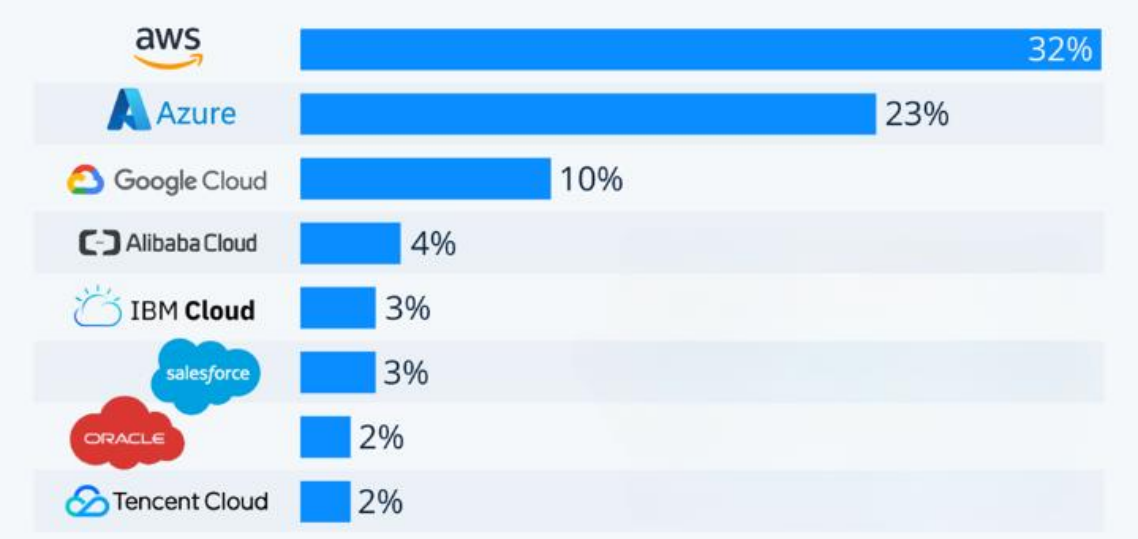

Рисунок 2.2 – Популярність постачальників хмарних послуг

AWS вкладає значні зусилля у забезпечення фізичної безпеки своїх дата-центрів. Вони застосовують високі стандарти фізичного контролю, включаючи системи відеоспостереження та контролю доступу. Також вони приділяють увагу запобіганню пожежам, захисту від води та інших фізичних загроз, щоб забезпечити надійність своїх приміщень.

Щоб захистити дані в хмарному середовищі, AWS надає різноманітні інструменти та сервіси. Пропонують можливість шифрування даних на різних рівнях, від шифрування в спокої до шифрування на рівні об'єктів. AWS забезпечує управління ключами шифрування та контроль доступу до зашифрованих даних, що дозволяє користувачам зберігати дані в безпечному стані.

Автентифікація та авторизація є ще одним важливим аспектом безпеки у AWS. Вони надають різні механізми для контролю доступу до ресурсів та послуг, включаючи управління користувачами, надання ролей з різними рівнями доступу та використання політик доступу. Це дозволяє користувачам ефективно керувати, хто має доступ до їхніх даних та ресурсів, забезпечуючи їх конфіденційність та цілісність.

РОЗДІЛ 2 ФУНКЦІОНАЛ І АРХІТЕКТУРА AWS

Amazon Web Services надає послуги для понад мільйона активних клієнтів у більш ніж 240 країнах і територіях. AWS неперервно розширює свою світову інфраструктуру, щоб забезпечити клієнтам зниження часу затримки та отримання максимальної швидкості передачі даних, а також гарантувати, що їх дані зберігаються тільки у регіоні AWS, який вони обирають. З урахуванням зростання бізнесу своїх клієнтів, AWS продовжуватиме надавати інфраструктуру, що відповідає їхнім глобальним потребам.

Інфраструктура AWS хмарних послуг ґрунтується на концепції регіонів та зон доступності. Регіон AWS - це фізичне місце на Землі, яке складається з кількох зон доступності. Кожна зона доступності включає один або кілька окремих Центрів обробки даних (ЦОД), кожний з яких має власне незалежне підключення, живлення та мережу, що знаходяться у власних приміщеннях. Клієнти мають можливості управляти власними програмами та базами даних за допомогою зон доступності, забезпечуючи більшу доступність, надійність та масштабованість, порівнюючи з ЦОД в якому одним центром.

AWS Cloud охоплює в 80 зонах доступності, розташованих у 25 географічних регіонах по всій планеті. Постійно планується розширення кількості зон доступності та регіонів. Наприклад, кожен регіон в Америці розроблений таким чином, щоб бути незалежними від інших регіонів. Це забезпечує найвищу стійкість до відмов та стабільність. Кожна зона доступності працює автономно та незалежно від інших. Незважаючи на фізичне відокремлення між зонами доступності, вони з'єднані низькозатримковими каналами.

AWS дозволяє розміщувати інстанси та зберігати дані в різних місцезнаходженнях по всьому світу, включаючи різні географічні регіони і кілька зон доступності в кожному з таких регіонів AWS. Кожна зона доступності

має детально розроблену архітектуру з високою надійністю, що дозволяє їй витримувати непередбачувані відмови та зберігати стабільну роботу системи. Це означає, що зони доступності фізично відокремлені всередині одного міського регіону та розташовані на територіях з меншим ризиком, що сприяє забезпеченню вищої безпеки і надійності системи. Крім наявності резервного живлення та генераторів електроживлення на місці, центри обробки даних у різних зонах доступності отримують електроенергію з незалежних підстанцій, що знижує ризик впливу подій у електромережі на більше ніж одну зону доступності.

Рисунок 2.1 – Розміщення центрів обробки даних AWS в Європі та Африці

AWS пропонує широкий спектр сервісів та рішень для підприємств і розробників програмного забезпечення. Для забезпечення кібербезпеки в умовах роботи з цими сервісами, слід враховувати наступні аспекти:

- обчислювальні сервіси: AWS надає різні сервіси для обчислень, включаючи Amazon EC2, Amazon ECS, Amazon EKS та AWS Lambda. Для забезпечення кібербезпеки важливо застосовувати найкращі практики з безпеки віртуальних машин, контейнерів та serverless архітектур;
- сервіси зберігання: AWS пропонує різні сервіси зберігання, такі як Amazon S3, Amazon Elastic Block Store та Amazon Elastic File System. При роботі з цими сервісами слід забезпечити адекватні заходи безпеки для захисту даних, такі як шифрування, контроль доступу та моніторинг активності;
- бази даних та управління даними: AWS надає сервіси для управління реляційними базами даних, такі як Amazon RDS та Amazon Aurora, а також керовані бази даних NoSQL через Amazon DynamoDB. При використанні цих сервісів необхідно дотримуватись засад безпеки баз даних, таких як захист від вторгнень і шифрування даних;
- мережеві сервіси: AWS надає сервіси для керування мережею, такі як Amazon VPC, Elastic Load Balancing та Amazon Route 53. Для забезпечення кібербезпеки слід застосовувати заходи безпеки мережі, такі як налагодження правил файрвола, моніторинг мережевої активності та захист від DDoS-атак;
- інструменти для розробників: AWS надає різні інструменти для розробників, такі як AWS CLI, SDK та сервіси для безперервної інтеграції.

2.1 Модель «Shared security responsibility model» від AWS

Інфраструктура AWS розроблена з урахуванням гнучкості і безпеки, і вона вважається однією з найбезпечніших та найбільш сучасних платформ хмарних обчислень на сьогоднішній день. AWS використовує найкращі практики і стандарти безпеки, враховуючи унікальні потреби хмари. Їх інфраструктура має надлишкові та багаторівневі засоби керування, постійно перевіряється і тестується, а також має значну автоматизацію для неперервного моніторингу та захисту базової інфраструктури. Кожен новий центр обробки даних або сервіс

реплікує ці елементи керування, забезпечуючи стабільну та безпечну інфраструктуру без необхідності великих капітальних та операційних витрат, які часто пов'язані з традиційними центрами обробки даних.

AWS використовує модель "Shared security responsibility model", де вони відповідають за безпеку базової хмарної інфраструктури, а клієнти - за безпеку своїх робочих навантажень, розгорнутих на платформі AWS. Клієнти мають можливість жорстко обмежувати доступ до конфіденційних даних і встановлювати різні рівні контролю для інформації, яку вони хочуть оприлюднити.

AWS пропонує широкий спектр інструментів і функцій для забезпечення захисту, співпрацюючи з довіреними партнерами. Ці інструменти нагадують знайомі елементи керування, які використовуються в локальних середовищах. AWS забезпечує спеціальні інструменти та функції для безпеки мережі, керування конфігурацією, контролю доступу та безпеки даних. Крім того, вони надають інструменти для моніторингу та ведення журналів, які дозволяють отримати повну видимість подій у вашому середовищі.

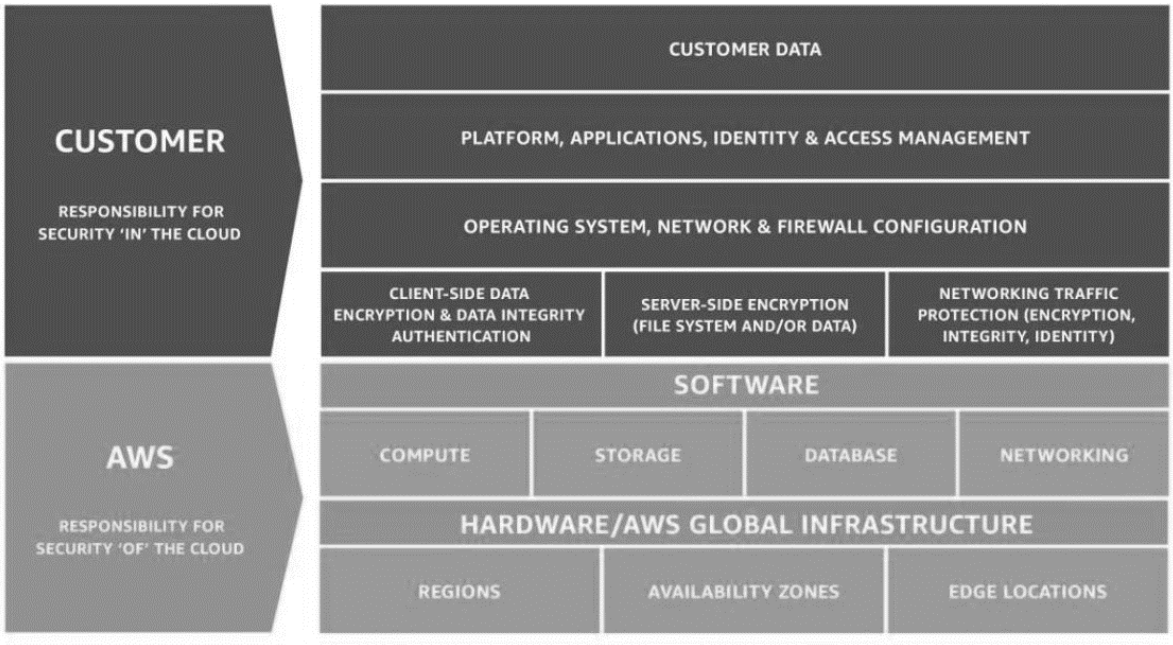

Рисунок 2.2 – Shared security responsibility model від AWS

2.2 Розмежування прав доступу з IAM

AWS світ починається з облікових записів і ресурсів, які містяться в цих облікових записах. Одним із основних інструментів для захисту ресурсів у вашому обліковому записі є IAM (Identity and Access Management). Його головна мета - запобігати проблемам, пов'язаним зі зловмисниками або недбайливими діями користувачів/програм у вашій компанії. Деякі з цих проблем включають спроби викрадення даних з об'єктів S3, випадкове видалення ресурсів або виконання небажаних дій.

AWS рекомендує використовувати багатофакторну аутентифікацію (MFA) для покращення захисту вашого облікового запису. MFA дозволяє забезпечити додатковий захист вашим ресурсам. Ви можете активувати MFA для користувачів IAM або для облікового запису root в AWS. Якщо ви вмикаєте MFA для облікового запису root, це стосується тільки облікових даних самого користувача root. Кожен користувач IAM може налаштувати свою власну конфігурацію MFA.

Для забезпечення вищого рівня безпеки, AWS рекомендує мати кілька облікових записів. Це може бути корисним для розділення середовищ виконання коду для розробників, таких як зони розробки (dev), стейджингу (staging), тестування (test) та продакшну (prod), або для створення облікових записів для різних департаментів, наприклад, розробників (Developers), відділу кадрів (HR), фінансового відділу (Finance) тощо, і їх подальшого об'єднання в AWS Organization. Організація облікових записів в AWS Organization допомагає керувати дозволами між обліковими записами в організації.

В IAM використовуються ресурси, які є постійними об'єктами в обліковому записі. Наприклад, це можуть бути балансувальники навантаження (ELB) або інстанси EC2. Наприклад, для користувача IAM використовується ARN (Amazon Resource Name), який може мати наступний формат: arn:aws:iam::123456789012:user/Development/product_1234/*. У даному ARN

містяться ідентифікатор облікового запису (123456789012) і тип ресурсу, який у даному випадку вказує на користувача в розділі IAM з ім'ям "Development" і ідентифікатором "product_1234".

У службі IAM (Identity and Access Management) існують два основних типи ідентичності: користувачі (IAM Users) та ролі (IAM Roles). Для доступу до консолі AWS або API користувачі використовують ім'я користувача та пароль. Проте, рекомендується використовувати ролі замість користувачів, де це можливо, щоб зменшити ризик втрати довгочасним акаунта та неправомірного доступу до облікового запису AWS. У користувачів також є можливість отримати ключі доступу (access keys), які можуть бути використані для виклику сервісів AWS за допомогою командного рядка (CLI) або розробницького набору інструментів (SDK).

IAM Roles або ролі в AWS є особливим типом ідентичності, подібним до користувачів. Вони використовуються для отримання доступу до ресурсів AWS та API. Ролі використовуються переважно для тимчасового надання облікових даних облікового запису AWS. Можливо передавати ці непостійні облікові дані третім особам або іншим сервісам, що знаходяться на платформі AWS.

Ролі широко використовуються в AWS на прикладі наступних ситуацій:

- EC2 інстанс, якому потрібні права доступу до AWS, використовує EC2 IAM Role для управління іншими сервісами/ресурсами AWS згідно з логікою програми;

- інакші акаунти AWS, які потребують доступу до ресурсів в зовнішньому акаунти AWS, іноді використовують IAM ролі в зовнішньому акаунті, щоб одержувати доступ за допомогою API Assume Role в службі STS (Security Token Service). Для цього акаунт AWS, який надає доступ, повинен надати дозволи на використання конкретної ідентичності в іншому обліковому записі за допомогою політики довіри (IAM trust policy).

Однією з ключових можливостей AWS є можливість виконувати дії від вашого імені. Однак багато служб AWS функціонують як окремі облікові записи, які не мають автоматичного доступу до ресурсів у вашому обліковому записі. Тому вони часто вимагають створення та надання їм доступу до "службової ролі" (Service Role) в вашому акаунту, щоб могли здійснювати дії від вашого імені. Для забезпечення автоматичного масштабування EC2, потрібно мати права на розгортання та видалення EC2 інстансів.

Федерація доступу, відома також як Access Federation, використовує ролі для надання доступу користувачам, які знаходяться поза AWS, до ресурсів AWS. Це дозволяє третім сторонам, таким як сторонні веб-додатки, контролювати доступ до ресурсів AWS через ролі.

Політики або IAM політики визначають, чи має користувач, який використовує певну ідентичність, доступ до запитуваного API AWS. Політики бувають двох типів: політики ідентичності (Identity Policies) та політики ресурсу (Resource Policies). При кожному виклику API AWS, IAM перевіряє одну або кілька політик для визначення допустимості запиту.

Identity Policies.

Політики ідентичності (Identity Policies) визначають список дозволів, які надаються конкретній ідентичності (ролі або користувачу).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:CreateUser"
            ],
            "Resource": [
                "arn:aws:iam::123456789012:role/some-role",
                "arn:aws:iam::123456789012:user/some-user"
            ]
        },
        {
            "Action": [
                "logs:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Рисунок 2.3 – Приклад Identity Policy

Щоб пояснити синтаксис політики IAM, ось кілька важливих роз'яснень:

- дії, які можна викликати за допомогою API, називаються "Action" в політиці IAM. Один API може виконувати декілька дій, але часто дія відповідає одному конкретному API;
- політика вважається білим списком, що означає, що за замовчуванням дії заборонені. Ви явно надаєте дозвіл на дві дії: "CreateRole" і "CreateUser". Для більш детального розуміння того, як політика оцінюється в обліковому записі AWS, варто звернутися до документації;
- більшість викликів API в AWS можна обмежити лише до певних ресурсів, вказаних у політиці. Це досягається тим, що розділ "Resource" не має значення "*", а має конкретний ARN (Amazon Resource Name). Наприклад, ви можете створити роль лише з ARN "arn:aws:iam::012345678912:role/some_role", використовуючи цю політику. Обмеження на окремі ресурси є рекомендованою практикою з метою підвищення безпеки;
- політика ідентичності без політики ресурсу працює лише в межах єдиного акаунту AWS;

- в політиці можна використовувати символи шаблону (wildcard) "*", які підставляються за замовчуванням. Наприклад, другий оператор у цій політиці стосується журналів CloudWatch і надає повний доступ до всіх журналів CloudWatch (для будь-якого API та будь-якого ресурсу).

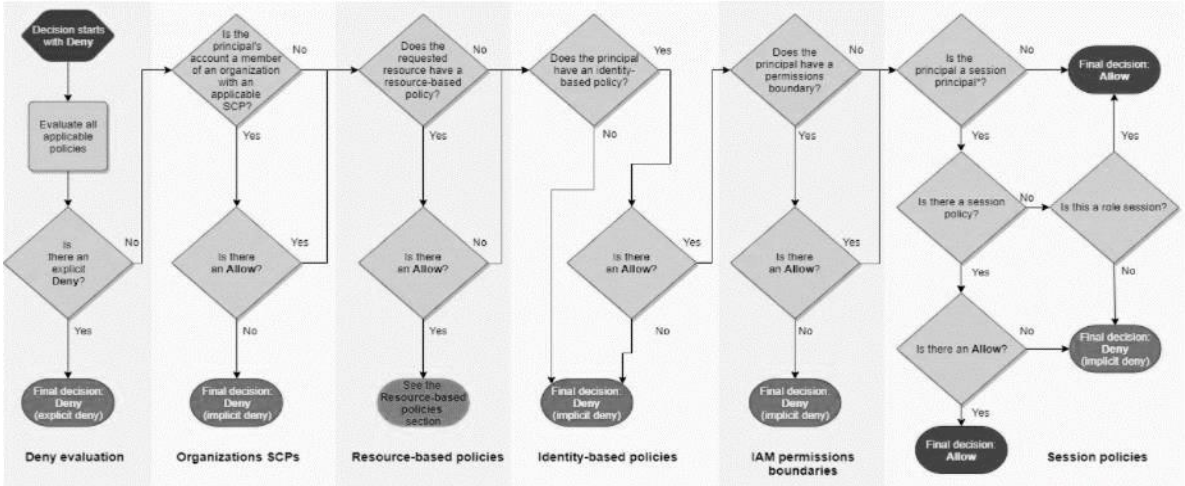

Рисунок 2.4 – Діаграма отримання дозволу на виконання запиту в AWS

2.3 Розгляд мережевої безпеки

Віртуальна приватна хмара (VPC) дозволяє створити ізольоване логічне середовище для розгортання віртуальних мереж. Користувач має повний контроль над своєю віртуальною інфраструктурою і може налаштовувати власний пул IP-адрес, таблицю маршрутизації, створювати підмережі і підключати шлюзи до Інтернету. Крім того, можна налаштувати віртуальну приватну мережу (VPN), щоб підключити її до наявного центру обробки даних та розширити його можливості. Одним з варіантів використання VPC є розміщення веб-серверів у публічній зоні, а внутрішніх систем, наприклад, баз даних і додаткових серверів, у приватній зоні без прямого доступу до Інтернету. Крім того, користувач може налаштовувати взаємодію між компонентами, розгорнутими в кожній зоні. Кожному об'єкту в підмережі надається внутрішній (сірий) IP-адрес, а для підмережі - зовнішній (публічний) IP-адрес для прямого

доступу до Інтернету. Amazon стандартно надає Virtual Private Cloud за замовчуванням для облікових записів, створених після 2013 року.

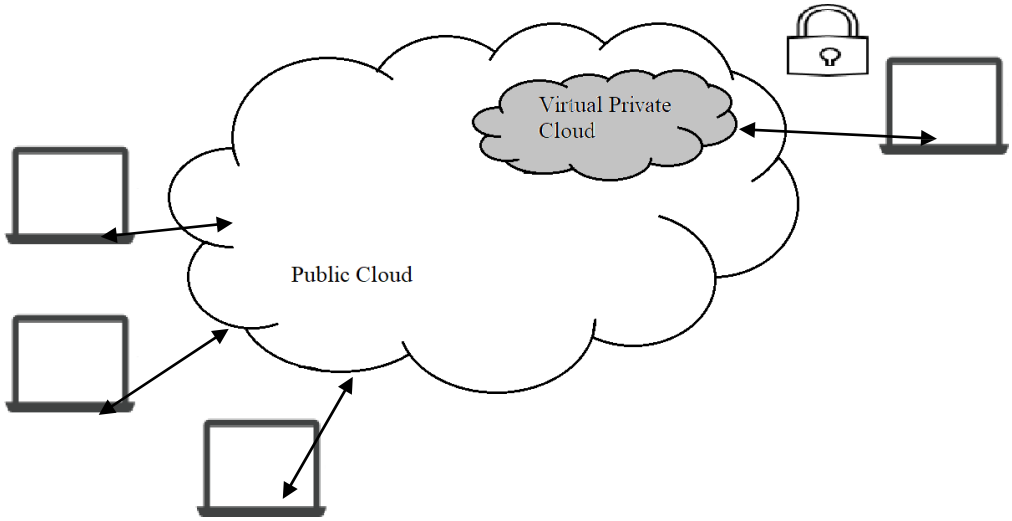

Рисунок 2.5 – Архітектура хмарного середовища із VPC

Virtual Private Cloud в AWS поєднує зручність та масштабованість публічних хмар з приватністю ізольованих мереж. В AWS VPC використовуються основні концепції, такі як:

- VPC - віртуальна приватна мережа, призначена для користувача в AWS;
- підмережа - IP-діапазон в межах віртуальної приватної хмари (Virtual Private Cloud);
- gateway - шлюз, який забезпечує з'єднання між VPC та Інтернетом;
- блок CIDR - метод виділення та маршрутизації IP-адрес;
- таблиця маршрутизації - містить правила (маршрути), які визначають, куди спрямовується трафік з VPC.

В AWS VPC ви маєте можливість контролювати спосіб доступу екземплярів, які запускаються в межах VPC, до ресурсів поза ним. За замовчуванням, VPC має встановлений інтернет-шлюз, а кожна підмережа за замовчуванням є публічно

доступною. Екземпляри, що вводяться в дію в підмережі за замовчуванням, мають приватні IPv4-адреси та загальнодоступні IPv4-адреси. Ці екземпляри можуть отримувати доступ до Інтернету через інтернет-шлюз, який дозволяє їм підключатися до Інтернету через мережі Amazon EC2.

2.4 Аналіз безпеки даних

Amazon S3 (Simple Storage Service) є одним з найпопулярніших хмарних сервісів для зберігання і управління об'єктами даних. Він розроблений компанією Amazon Web Services (AWS) і надає простий, масштабований та дуже надійний спосіб зберігання різних типів даних в хмарі.

S3 пропонує безліч можливостей для зберігання, організації та управління вашими данними. Основні риси Amazon S3 включають:

- масштабованість: S3 дозволяє зберігати великі обсяги даних, починаючи від кількох байт із обмеженням в 5 терабайт на об'єкт. Ви можете зберігати нескінченну кількість об'єктів в хмарному сховищі S3;
- доступність: S3 забезпечує високу доступність ваших даних. Він реплікує ваші об'єкти автоматично на кількох серверах та доступний для використання з будь-якого місця в Інтернеті. S3 гарантує 99,999999999% (11 дев'яток) дурнійності (durability) для збережених об'єктів;
- безпека: S3 надає високий рівень безпеки для ваших даних. Ви можете використовувати політики управління доступом, щоб контролювати, хто має доступ до вашого сховища та об'єктів. Ви також можете використовувати шифрування для захисту вашої інформації під час передачі та зберігання;
- універсальність: S3 підтримує різноманітні типи даних, включаючи тексти, зображення, відео, аудіо, документи тощо. Ви можете зберігати будь-які файли будь-якого розміру в S3;

- легкість використання: S3 має простий інтерфейс управління, що дозволяє легко створювати, видаляти та керувати вашими сховищами та об'єктами через консоль керування AWS або за допомогою API;
- інтеграція: S3 інтегрується з іншими сервісами AWS, що дозволяє використовувати його в якості основного сховища для резервних копій, аналітики даних, статичного хостингу веб-сайтів, масштабування зображень.

2.5 Огляд сервісу AWS CloudTrail

AWS CloudTrail - це сервіс, наданий AWS, який дозволяє увімкнути для облікового запису AWS функціональні можливості, що забезпечують:

- управління;
- дотримання вимог щодо відповідності;
- аудит операційної діяльності та ризиків.

Всі дії, виконані користувачем, роллю або сервісом AWS, записуються як події в CloudTrail. Ці події включають дії, виконані в консолі керування AWS, командному рядку AWS, а також за допомогою SDK та API AWS. CloudTrail включений в обліковому записі AWS за замовчуванням при створенні, але зберігається лише протягом 90 днів. Кожна активність, яка відбувається в обліковому записі AWS, записується як подія CloudTrail. Останні події можна легко переглянути на консолі CloudTrail, перейшовши до "Історії подій". Для зберігання постійного журналу активності та подій в обліковому записі AWS рекомендується створити "слід" (trail).

Перегляд активності в обліковому записі AWS є важливим елементом забезпечення безпеки та дотримання найкращих практик. CloudTrail надає можливість переглядати, шукати, завантажувати, архівувати, аналізувати та реагувати на активність в обліковому записі AWS, що стосується хмарної інфраструктури. За допомогою CloudTrail можна встановити, хто виконував певні дії, які ресурси були задіяні, коли сталися певні події та інші деталі, які

дозволяють аналізувати та реагувати на дії, що відбуваються в обліковому записі AWS. Крім того, на бажання можна ввімкнути AWS CloudTrail Insights для трейлу, що допоможе виявити незвичайну активність та забезпечити відповідну реакцію.

CloudTrail надає можливість інтегрувати його в програми за допомогою API, що дозволяє автоматизувати процес створення трейлу для AWS Organization. Також API CloudTrail дозволяє перевіряти статус створених трейлів і контролювати налаштування, що стосуються способу перегляду подій CloudTrail користувачами. Це дає можливість програмно керувати CloudTrail і забезпечити потрібні налаштування та контроль над процесом перегляду активності в обліковому записі AWS.

2.6 Ефективне виявлення загроз за допомогою Amazon GuardDuty

Amazon GuardDuty - це сервіс постійного моніторингу безпеки, який аналізує та обробляє різні джерела даних, такі як журнали VPC Flow Logs, журнали подій керування AWS CloudTrail, журнали подій CloudTrail S3 і DNS-журнали. GuardDuty використовує дані розвідки загроз (Threat Intelligence, TI), такі як списки шкідливих IP-адрес і доменів, а також машинне навчання, щоб встановлювати непередбачувані та потенційно несанкціоновані та шкідливі дії у вашому оточенні AWS. Це можуть бути проблеми, такі як підвищення привілеїв, використання витіклих облікових даних або зв'язок з шкідливими IP-адресами або доменами.

Наприклад, GuardDuty може виявляти скомпрометовані екземпляри EC2, що обслуговують шкідливе програмне забезпечення або займаються майнінгом біткоїну. Він також відстежує поведінку доступу до акаунту AWS на наявність ознак компрометації, таких як несанкціоноване розгортання інфраструктури, наприклад, екземпляри, запущені в регіоні, який ніколи не застосовувся, або

незвичайні виклики API, наприклад, зміна політики паролів для погіршення надійності паролю.

GuardDuty, як інструмент Threat Intelligence, тісно пов'язаний з іншими процесами інформаційної безпеки, такими як реагування на інциденти, управління ризиками, управління вразливостями, виявлення шахрайства та операційна діяльність підрозділу ІБ. Посилення ефективності цих процесів, підвищення якості та швидкості прийняття рішень в рамках них, є основним завданням роботи з TI. Ефективне використання Threat Intelligence дозволяє покращити якість та швидкість реагування на кіберзагрози. Інформація про нові загрози надає змогу оперативно моніторити їх і одночасно блокувати потенційно компрометовані ресурси.

Аналізуючи контекст, розуміючи можливі сценарії кібератак та шляхи їх проникнення, можна вчасно виявляти загрози, реагувати на них та розробляти відповідні стратегії. Управління вразливостями значно полегшується завдяки інформації про загрози, яка допомагає встановити пріоритети та оцінити критичність вразливостей. Threat Intelligence надає необхідну базу для аналізу та оцінки ризиків на тактичному та стратегічному рівнях. Це дозволяє побудувати ефективний процес управління ризиками, планувати та реалізовувати захисні заходи, відповідаючи актуальному ландшафту загроз. Інтеграція Threat Intelligence у роботу підрозділу IT-безпеки дозволяє діяти проактивно та забезпечувати захист на основі відомостей про поточні загрози, не покладаючись на випадковість.

Хоча процес кіберрозвідки може бути викликом для організацій, він є необхідним для ефективного управління кібербезпекою. Одним з основних викликів у кіберрозвідці є складність отримання даних. Існує велика кількість джерел інформації, і кожен постачальник або канал надає дані у власному форматі, відсутній єдиний стандарт. Частина даних надходить у машинночитабельному форматі, а інша - у вигляді звітів, призначених для

читання аналітиками. Перед початком аналізу даних, навіть якщо використовуються всього 2-3 джерела, їх потрібно привести до єдиної моделі розуміння і нормалізувати. Для зрозумілого тлумачення даних та прийняття обґрунтованих рішень необхідно не лише мати сирі дані, але й збагачувати їх контекстом та додатковою інформацією, що допомагає визначити найкращу тактику дій у відповідь. Однак, коли джерел даних стає занадто багато, виникає проблема їх практичного використання. Тому важливо здійснювати фільтрацію та відбір, щоб не бути перенавантаженим потоком інформації. Ці проблеми вирішує GuardDuty.

GuardDuty є важливим інструментом для прийняття рішень в галузі кібербезпеки. Він надає розуміння ландшафту загроз, що дозволяє прогнозувати можливі атаки та вживати відповідних заходів захисту. Використання цього інструменту також сприяє поліпшенню якості та швидкості реагування на інциденти, допомагаючи зменшити можливі збитки. Інформація про поточні загрози дозволяє більш точно оцінювати ризики в сфері кібербезпеки та планувати необхідні заходи для їх запровадження. GuardDuty надає звіти про стан середовища AWS, які можна переглянути на консолі GuardDuty або за допомогою подій CloudWatch.

2.7 Переваги використання AWS Security Hub

AWS Security Hub забезпечує повну інформацію про безпеку в AWS та допомагає перевірити відповідність середовища вимогам безпеки та найкращим практикам. Він здійснює збір інформації про безпеку з усіх акаунтів AWS, сервісів та підтримуваних продуктів сторонніх партнерів, а також надає можливість аналізувати тенденції безпеки та виявляти проблеми безпеки.

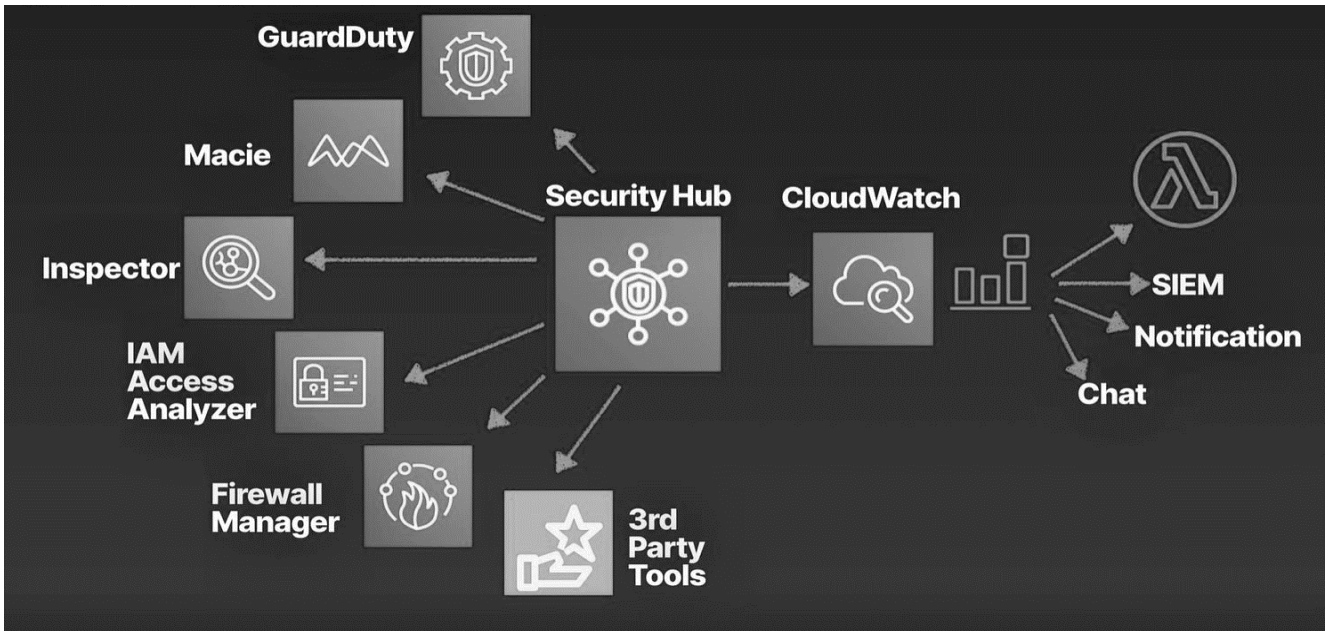

Рисунок 2.6 – Інтеграція Security Hub з інструментами безпеки та моніторингу

Основні переваги використання Security Hub такі:

- спрощення процесу збору та пріоритезації знахідок;
- Security Hub опрацьовує дані пошуку у стандартному форматі, що усуває потребу в управлінні даними пошуку з різних форматів. Потім він порівнює результати між постачальниками даних, щоб визначити найважливіші пріоритети;
- автоматична перевірка відповідності безпеці передового досвіду та стандартам;
- Security Hub автоматично виконує постійну конфігурацію на рівні акаунту та проводить перевірку безпеки згідно найкращих практик AWS та галузевих стандартів, таких як PCI DSS. Він ідентифікує конкретні облікові записи та ресурси, які вимагають уваги;
- підсумковий огляд результатів для облікових записів та постачальників даних;
- Security Hub агрегує та надає зведену інформацію про безпеку в облікових записах і продуктах постачальників даних та відображає результати

на консолі Security Hub. Це дозволяє переглядати загальний поточний стан безпеки, щоб виявити тенденції, виявити потенційні проблеми та вжити необхідні заходи для їх вирішення;

- можливість автоматизованого виправлення виявлених проблем;
- Security Hub дозволяє інтегруватися з EventBridge. Це дає змогу автоматично вирішувати окремі проблеми, встановивши певні дії, які будуть виконуватися при виявленні неприйнятних результатів. Наприклад, можна настроювати відправку результатів до автоматизованої системи відновлення або до команди підтримки хмарної інфраструктури компанії.

Security Hub - це потужний інструмент для керування безпекою в середовищі Amazon Web Services (AWS). Використання Security Hub має декілька вагомих переваг. По-перше, він спрощує процес збору та пріоритезації знахідок, дозволяючи швидко виявляти та реагувати на потенційні проблеми безпеки. Друга перевага полягає в тому, що Security Hub обробляє дані пошуку у стандартному форматі, сприяючи усуненню потреби в управлінні даними різних форматів і порівнює результати між постачальниками даних для визначення пріоритетів. Третя перевага полягає в автоматичній перевірці відповідності безпеці передового досвіду та стандартам.

РОЗДІЛ 3 ВПРОВАДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВІД КІБЕРАТАК НА ХМАРНІ СЕРВІСИ AWS

У даному розділі кваліфікаційної роботи акцентовано увагу на практичній роботі, яка має на меті впровадження методів захисту від кібератак у контексті інфраструктури машинного навчання в хмарній платформі AWS.

Проєкт спрямований на створення безпечного середовища для проєкту розпізнавання фруктів і овочів за допомогою AWS. Розглянуто ключові аспекти безпеки інфраструктури машинного навчання в AWS та впроваджено найкращі практики та правила безпеки, щоб забезпечити надійність та стійкість сервісу перед кібератаками.

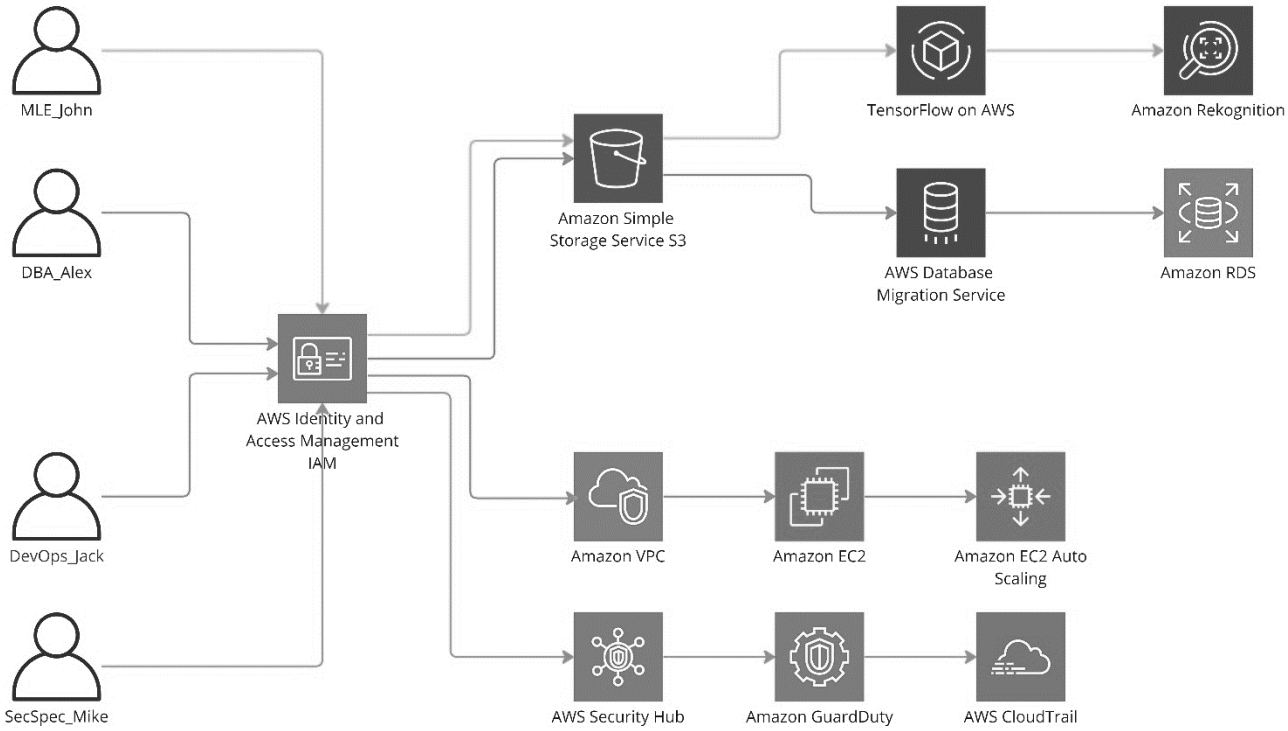

Рисунок 3.1 – Схема інфраструктури проєкту розпізнавання фруктів і овочів в AWS

Основна мета роботи полягає в створенні безпечного середовища, яке забезпечує захист даних та гарантує довіру користувачів до сервісу

розпізнавання фруктів і овочів. Розглянуто різні техніки та стратегії безпеки, щоб побудувати захищену інфраструктуру, яка забезпечує конфіденційність, цілісність та доступність наших даних.

У цьому розділі представлено практичні застосування, описуючи важливі кроки та прийняті заходи щодо безпеки, а також надано розгорнуту аналітику та обґрунтування використання конкретних методів захисту від кібератак. Також виконано оцінку ефективності наших заходів безпеки та їхній вплив на процес розпізнавання фруктів і овочів за допомогою машинного навчання.

Цей розділ є важливим кроком у кваліфікаційній роботі, оскільки допоможе створити надійну та безпечну систему, забезпечуючи високий рівень захисту від кібератак та збереження довіри користувачів.

3.1 Вдосконалення ідентифікації та аутентифікації

Впровадження та вдосконалення систем ідентифікації та аутентифікації стають все більш критичними завданнями в сучасному цифровому світі. З постійним зростанням обсягів даних та збільшенням кількості злочинів, пов'язаних з кібербезпекою, організації стикаються з викликами, пов'язаними з захистом своїх ресурсів та конфіденційності даних.

У цьому контексті ідентифікація і аутентифікація відіграють ключову роль в управлінні доступом до систем, послуг і ресурсів. У цьому підрозділі розглянуто, як системи управління доступом, зокрема IAM в публічних хмарних платформах, таких як AWS, допомагають організаціям забезпечувати безпеку, ефективність та контроль над доступом до своїх обчислювальних ресурсів.

IAM в AWS надає механізми для створення та керування користувачами, групами, ролями та політиками доступу. Вони дозволяють організаціям налаштовувати точний контроль над тим, які ресурси можуть використовувати користувачі, і які операції вони можуть виконувати. Це дозволяє забезпечити

принцип найменшого привілею та обмежити доступ лише до необхідних ресурсів.

Вдосконалення систем ідентифікації та аутентифікації включає в себе використання сучасних технологій, таких як двофакторна аутентифікація, мультифакторна аутентифікація та біометричні методи, для забезпечення більш високого рівня безпеки. При цьому важливо забезпечити зручність використання для користувачів, уникнути зайвих перешкод і запровадити міцні механізми перевірки та захисту ідентифікаторів.

У даному підрозділі розглянуто основні принципи та методики, що використовуються в IAM в AWS, а також будуть представлені приклади практичного застосування для забезпечення безпеки обчислювальних ресурсів. Також будуть проаналізовані переваги та обмеження використання цих систем управління доступом і запропоновані практичні рекомендації для досягнення оптимального рівня безпеки та зручності використання.

За допомогою вдосконалених систем ідентифікації та аутентифікації, організації можуть забезпечити надійний захист своїх ресурсів, запобігти несанкціонованому доступу та зберегти цінні дані в безпеці. Продовжуючи розвивати та вдосконалювати ці системи, створено надійний фундамент для довіри та безпеки в цифровому середовищі.

У цій частині описуються кроки для створення груп, акаунтів та налаштування безпеки першої авторизації та MFA в AWS. Перш за все, розглянуто процес створення груп, які дозволяють згрупувати користувачів з подібними правами доступу. Далі створення акаунтів, налаштовано їх паролі та прив'язано до відповідних груп. Нарешті, розглянуто важливий аспект безпеки - налаштування вимоги зміни паролю при першій авторизації та активування двофакторної аутентифікації для кожного акаунту. Виконання цих кроків забезпечить надійний доступ та захист даних в середовищі AWS:

1. створення груп:

- увійдено до консолі AWS та перейдено до служби Identity and Access Management (IAM);

- у розділі "User groups" обрано "Create group".

- введено назву групи, наприклад, "Database_Administrator", та натиснено "Створити групу";

- повторено ці кроки для створення груп "Machine_Learning_Engineer", "Security_Specialist" та "DevOps".

2. створення акаунтів:

- у розділі "Users" оберіть "Add user";

- введено ім'я користувача, наприклад "MLE_John", та встановлено прапорець "Provide user access to the AWS Management Console";

- обрано "Autogenerated password" та встановлено прапорець "Users must create a new password at next sign-in";

- встановлено вимоги до пароля: мінімальна довжина (8+ символів), наявність спеціальних символів, верхнього і нижнього регістру;

- перейдено до наступного кроку та обрано необхідні групи для користувача;

- натиснено "Create user" і повторено ці кроки для створення акаунтів для інших груп;

- повторено ці кроки для створення користувачів "DBA_Alex", "SecSpec_Mike" та "DevOps_Jack".

3. налаштування безпеки першої авторизації та MFA:

- у розділі "Users" обрано створеного користувача та перейдено до вкладки "Security credentials";

- у розділі "Multi-factor authentication (MFA)" обрано "Assign MFA device" та вибрано метод аутентифікації;
- дотримано інструкцій для завершення налаштування MFA для користувача;
- повторено ці кроки для кожного створеного акаунту.

Після виконання цих кроків створено групи та акаунти з відповідними правами, а також забезпечено безпеку першої авторизації шляхом вимоги нового пароля та налаштування MFA для кожного користувача.

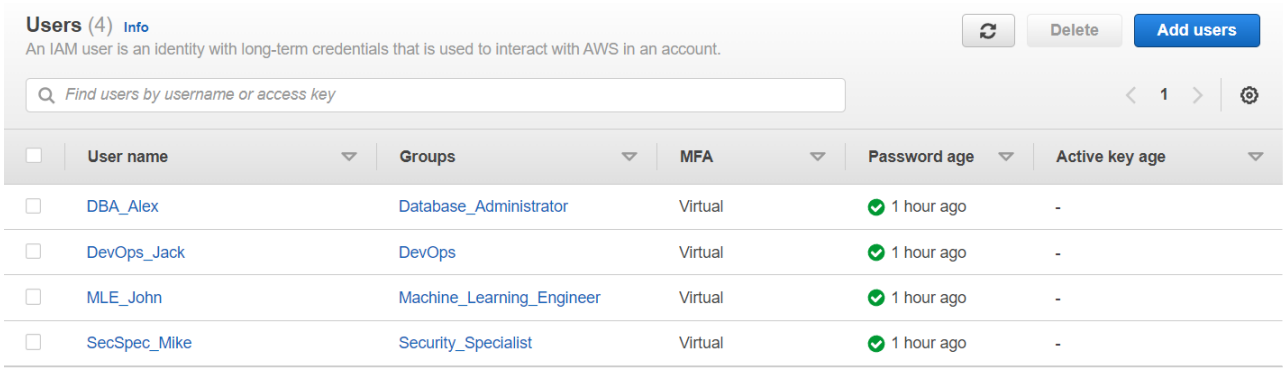

Рисунок 3.2 – Демонстрація успішного створення користувачів та налаштування MFA

3.2 Зміцнення контролю доступу та авторизації

В сучасному цифровому світі безпека та контроль доступу є невід'ємною частиною будь-якої організації. Вдосконалення системи контролю доступу та авторизації відіграє критичну роль у захисті цінної інформації та ресурсів. Шляхом ефективного використання сервісів IAM, можливо зміцнити інфраструктуру, обмежити доступ до ресурсів лише для авторизованих користувачів та забезпечити більший контроль над діями та привілеями. В даній роботі досліджено і реалізовано кращі практики в сфері контролю доступу та авторизації, забезпечуючи надійну захист від потенційних загроз.

Для зміцнення контролю доступу та авторизації, перший крок - налаштування сервісу IAM. Створено користувачів з обмеженими привілеями та визначено політики безпеки. Використано множину факторів аутентифікації. Переглянуто та оновлено політики та права доступу. Проведено навчання користувачів щодо використання IAM та безпеки даних. Виконання нижче наведених кроків забезпечило зміцнення контролю доступу та авторизації:

1) створено політики доступу:

- у консолі IAM вибрано "Policies" у лівому меню та натиснено "Create policy";
- на вкладці "Policy editor" та обрано "Visual";
- вибрано потрібні сервіси AWS, з якими пов'язані ці групи, наприклад, RDS для групи "Database Administrator" або S3 для групи "Machine Learning Engineer";
- визначено дозволи, які надано цим групам для кожного вибраного сервісу. Наприклад, для групи "Database Administrator" надано дозвіл на створення, зчитування, оновлення та видалення баз даних RDS;
- натиснено "Next" для перевірки синтаксису та потім натиснено "Create policy".

2) налаштовано політики доступу для груп:

- у консолі IAM вибрано "User Groups" у лівому меню та вибрано потрібну групу, наприклад, "Database Administrator";
- у вкладці "Permissions" натиснено "Add permissions";
- вибрано політику, яку створено на попередньому кроці, та натиснено "Add permissions".

Тепер користувачі будуть мати відповідні права доступу залежно від групи, до якої вони належать. Рекомендується також регулярно переглядати та

оновлювати політики доступу для забезпечення потрібного рівня безпеки та доступу до ресурсів в AWS.

3.3 Посилення мережевої безпеки

У сучасному цифровому середовищі забезпечення безпеки мережевих інфраструктур є надзвичайно важливим завданням. При використанні хмарних рішень AWS існує кілька кроків, які можна вжити для зміцнення мережевої безпеки та захисту вашої інфраструктури. В цьому розділі розглянуто рекомендації та практичні вказівки, щоб ефективно вдосконалити безпеку мережі в AWS.

Використано сервіс VPC для створення приватної ізольованої мережі у середовищі AWS. Встановлено правила безпеки мережі, маршрутизацію та налаштування доступу до ресурсів.

1) створено VPC:
   - у консолі керування AWS перейдено до сервісу VPC;
   - вибрано опцію "Create VPC" і вказано необхідні налаштування, такі як ім'я, діапазон IP-адрес та інші параметри мережі;
   - після створення VPC зроблено нотатку про його ідентифікатор (VPC ID), оскільки він буде використовуватись для подальших кроків.
2) налаштування правил безпеки мережі (Network Security Groups):
   - у розділі "Security" у консолі керування VPC вибрано "Security Groups";
   - створено потрібну групу безпеки (Security Group);
   - налаштовано вхідні та вихідні правила для контролю доступу до різних рівнів мережі;
   - встановлено правила фільтрації трафіку, забороняючи небезпечні або небажані з'єднання.

3) налаштування маршрутизації:

- у розділі "Route Tables" вибрано маршрутну таблицю (Route Table), пов'язану з VPC;

- додано потрібні записи маршрутизації, вказуючи наступний хід для трафіку до різних мереж та підмереж;

- налаштовано інші параметри маршрутизації за необхідністю, такі як VPN-з'єднання та приватні з'єднання з іншими AWS-регіонами.

4) налаштування доступу до ресурсів:

- використано Subnets, щоб призначити IP-адреси конкретним зонам доступу;

- налаштовано NACL для контролю доступу на рівні subnets та встановлення правил фільтрації трафіку;

- використано Elastic IP-адреси для надання статичних IP-адрес ресурсам і контролю доступу до них.

Рисунок 4.3 – Демонстрація створеної приватної мережі

3.4Захист даних в AWS: рекомендації та методи

Забезпечення високого рівня безпеки даних є одним з найважливіших аспектів роботи з хмарним середовищем AWS. У цьому розділі досліджено рекомендації та методи забезпечення захисту даних в AWS, зосереджено увагу

на використанні сервісів S3 та RDS. Розглянуто кроки, які можна вжити для налаштування належного контролю доступу до сховищ S3 та баз даних RDS, а також методи шифрування та резервного копіювання даних.

3.4.1 Збереження та керування даними з використанням S3

Використання правильних методів та рекомендацій для безпеки даних у S3 відіграє важливу роль у забезпеченні конфіденційності, цілісності та доступності даних. У цьому розділі розглянуто практичні вказівки для ефективного захисту даних у сервісі S3, включаючи контроль доступу, шифрування та механізми резервного копіювання.

- налаштовано політики контролю доступу до об'єктів (S3 Bucket Policies): Використано політики контролю доступу до сховищ S3 для точного контролю над тим, які користувачі та ресурси можуть отримувати доступ до вашого сховища даних. Встановлюйте обмеження на основі принципу найменшого доступу, надано доступ тільки необхідним користувачам та заборонено загальнодоступний доступ до конфіденційних даних;
- використання дозволів на рівні об'єкту (S3 ACLs): Встановлено права доступу до кожного об'єкта окремо за допомогою дозволів на рівні об'єкту. Це дозволяє точно контролювати доступ до кожного об'єкта в сховищі S3;
- шифрування даних в S3: Для забезпечення безпеки даних використано SSL/TLS для шифрування даних під час передачі до та з S3. Крім того, AWS надає сервіс KMS, який дозволяє керувати ключами шифрування та забезпечувати шифрування даних під час зберігання в S3;
- резервне копіювання даних: Використано механізми резервного копіювання, які надає S3, такі як S3 Object Versioning, для забезпечення захисту від втрати даних. Object Versioning дозволяє зберігати різні версії об'єктів і відновлювати дані до попередніх станів;

- аудит та моніторинг: Важливо регулярно аудитувати та моніторити ресурси S3 для виявлення можливих загроз та невідповідностей. Для цього використовуються сервіси CloudTrail, CloudWatch та Config, які дозволяють відстежувати та аналізувати події в середовищі AWS.

3.4.2 Забезпечення конфіденційності даних в RDS

В цьому розділі розглянуто практичні вказівки та рекомендації, які допомогли забезпечити інфраструктури баз даних в RDS, включаючи використання захищених з'єднань, керування правами доступу та аудит доступу:

- використання захищених з'єднань (SSL/TLS): налаштовано бази даних RDS для використання захищених з'єднань з використанням SSL/TLS протоколу. Це забезпечило шифрування даних під час їх передачі між додатком і базою даних;
- встановлено політики безпеки: використано політики безпеки, доступні в RDS, для обмеження доступу до баз даних. Встановлено точні правила доступу до різних об'єктів бази даних, таких як таблиці і процедури;
- резервне копіювання та відновлення: використано автоматичні резервні копії, надані RDS, для забезпечення захисту даних в разі втрати або пошкодження. Періодично перевірено процес відновлення з резервних копій, щоб переконатися в його ефективності;
- поновлення паролів та доступу: регулярно оновлено паролі користувачів баз даних та інших облікових записів, що мають доступ до RDS. Використано міцні паролі та встановлено політики паролів для запобігання несанкціонованому доступу;
- використання патчей та оновлень: слідковано за патчами та оновленнями, які надаються AWS для RDS. Регулярно оновлено бази даних до останньої версії, щоб усунути вразливості та забезпечити безпеку даних;

- використання аудиту доступу: використано можливості аудиту доступу, що надаються RDS, для відстеження та аналізу активності користувачів в базі даних. Це допомогло виявити незвичайні або підозрілі дії, які можуть свідчити про потенційні загрози безпеці даних.

3.5 Моніторинг та реагування на загрози безпеки

Моніторинг та реагування на загрози безпеки є критично важливими аспектами в забезпеченні безпеки даних в середовищі AWS. Здатність швидко виявляти та реагувати на потенційні атаки, вразливості та несправності дозволяє попередити серйозні наслідки та зменшити вплив на систему. У цьому пункті розглянуто практичні вказівки щодо моніторингу безпеки та ефективного реагування на загрози у середовищі AWS:

- використано сервіс AWS CloudTrail для моніторингу та журналювання подій у AWS-середовищі. Налаштовано моніторинг на підозрілі активності, невдачні спроби аутентифікації та інші підозрілі події;
- встановлено систему моніторингу безпеки, таку як Amazon GuardDuty або AWS Security Hub, для виявлення аномальних активностей та потенційних загроз в реальному часі. Налаштовано сповіщення та автоматизовані реакції на виявлені загрози;
- використано сервіс Amazon CloudWatch для моніторингу метрик, логів та подій вашого AWS-середовища. Створено метрики та сповіщення для моніторингу системних параметрів, активності мережі та інших важливих аспектів безпеки;
- налаштовано систему реагування на інциденти безпеки. Створено процедури реагування на виявлені загрози та проникнення, включаючи ізоляцію компрометованих ресурсів, аналіз впливу і відновлення системи;

- проведено регулярні аудити системи безпеки та виявлення загроз. Аналізовано журнали подій, логи моніторингу та звіти моніторингових сервісів для виявлення вразливостей, неправильних конфігурацій та потенційних загроз.

Забезпечення безпеки даних та ресурсів у середовищі AWS має вирішальне значення для проєктів, спрямованих на розпізнавання овочів і фруктів на основі зображень. Розглянуті в цій кваліфікаційній роботі рекомендації та методи надають надійну основу для забезпечення конфіденційності даних та високого рівня безпеки.

Використання сервісу IAM та багатофакторної аутентифікації дозволяє забезпечити безпеку доступу до ресурсів, що використовуються для розпізнавання овочів і фруктів. Це дозволяє контролювати, які користувачі мають доступ до системи та обмежувати їхні привілеї.

Мережеві заходи безпеки, такі як використання VPC, Security Groups та NACL, забезпечують захист системи від небажаних атак та забезпечують безпечний обмін даними. Використання S3 для зберігання зображень та RDS з належним шифруванням даних допомагає захистити конфіденційну інформацію про овочі і фрукти від несанкціонованого доступу та забезпечує їхню цілісність.

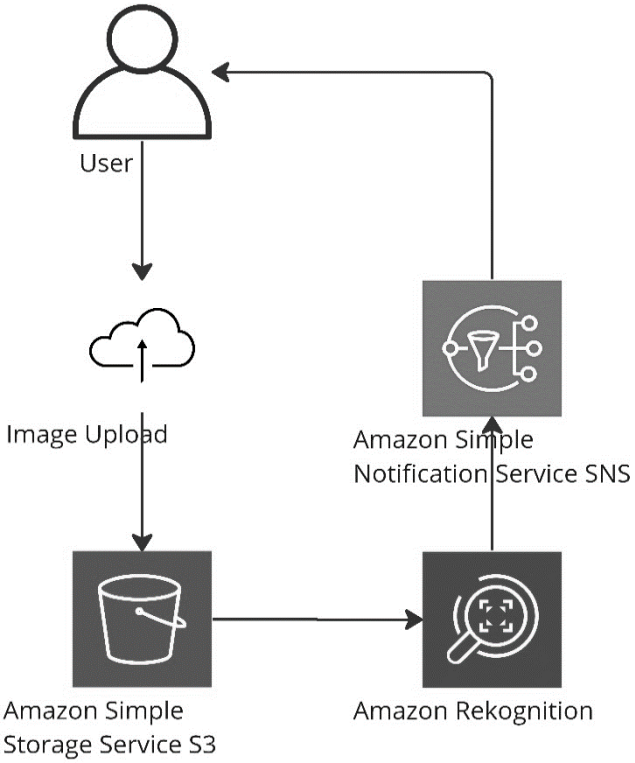

Рисунок 4.4 – Приклад використання проєкту користувачем

Ця діаграма проєкту відображає основні компоненти та їх взаємозв'язки. Вона демонструє, як користувач завантажує зображення фрукта або овоча, яке потім зберігається в Amazon S3. Після цього, з використанням сервісу Amazon Rekognition, проводиться розпізнавання фрукта або овоча, і отримані результати будуть повідомлені користувачеві за допомогою SNS.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Вплив діяльності людини на довкілля

Діяльність людини має значний вплив на довкілля, і цей вплив набуває все більшої актуальності в контексті швидкого розвитку інформаційних технологій. Інформаційні технології, такі як комп'ютери, мобільні пристрої, інтернет та програмне забезпечення, відіграють важливу роль у нашому сучасному житті, але разом зі своїми перевагами вони також створюють низку негативних наслідків для довкілля.

Одним з основних аспектів негативного впливу інформаційних технологій на довкілля є проблема відходів електронного сміття. За останні роки кількість використаних та викинутих пристроїв зросла експоненційно. Багато з цих пристроїв містять небезпечні речовини, такі як ртуть, свинець та кадмій, які можуть негативно впливати на здоров'я людей і природу, якщо вони потрапляють до навколишнього середовища. Правильне утилізування електронного сміття стає важливим завданням, щоб зменшити негативний вплив.

Крім того, зростаюче використання електроенергії для живлення інформаційних технологій призводить до збільшення споживання природних ресурсів і викиду парникових газів у атмосферу. Це може призвести до зміни клімату та глобального потепління. Щоб зменшити енергетичний слід інформаційних технологій, можна застосовувати енергоефективні компоненти, покращувати енергетичну ефективність дата-центрів, використовувати відновлювальні джерела енергії та сприяти раціональному використанню електронних пристроїв.

Також інформаційні технології мають вплив на використання природних ресурсів. Велика кількість ресурсів використовується для виробництва комп'ютерів, смартфонів та інших електронних пристроїв. Видобуток деяких матеріалів, таких як рідкі кристали та дорогоцінні метали, може

супроводжуватися деструкцією екосистем, забрудненням водних джерел та викликати соціальні конфлікти. Важливо здійснювати раціональне використання ресурсів, працювати над розробкою екологічно чистих матеріалів та промоутувати рециклінг. З іншого боку, інформаційні технології можуть також мати позитивний вплив на довкілля. Вони можуть допомагати в ефективному керуванні енергією, зменшенні втрат, оптимізації транспортних потоків та забезпеченні ефективного використання ресурсів. Також інформаційні технології дозволяють розвивати нові екологічно чисті методи виробництва, такі як 3D-друкування, віртуальна реальність та інші інновації, які можуть зменшити використання матеріалів і енергії.

Узагалі, вплив діяльності людини на довкілля у контексті інформаційних технологій є складним і має як позитивні, так і негативні аспекти. Важливо постійно працювати над зменшенням негативного впливу, впроваджувати екологічно чисті технології, розробляти енергоефективні рішення та стимулювати відповідальну поведінку в сфері використання інф. технологій.

4.2 Безпека умов праці при використанні персональних комп’ютерів

На користувачів ПК діє ряд шкідливих та небезпечних чинників, які враховуються при використанні персональних комп’ютерів у виробничій діяльності. Значна роль у профілактиці захворювань користувачів ПК відводиться медицині. Існує перелік профілактичних заходів для користувачів ПК, що включає як складові первинної профілактики здоров’я (професійний відбір), так і вторинної, яка направлена на зниження ймовірності розвитку перевтоми та перенапруження. Ці комплексні заходи спрямовані на відновлення функціонального стану зорового та опорно-рухового апарату.

Відповідні робочі місця заборонено облаштовувати у підвальних або цокольних приміщеннях будинків. В обладнанні приміщень забороняється

використання полімерних матеріалів, що виділяють шкідливі хімічні речовини. Також приділяється увага забезпеченню достатнім для здійснення роботи рівнем освітлення (природного та штучного – у темну пору доби) та звукоізоляції. Для регуляції рівня освітлення природним світлом бажано застосовувати жалюзі. У приміщеннях, де здійснюється робота з комп'ютерами, щодня здійснюється вологе прибирання з метою недопущення запиленості підлоги та меблів.

Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця операторів (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), мають бути надійно захищені діелектричними щитками або сітками з метою недопущення потрапляння людини під напругу.

Враховуються заходи дотримання протипожежної безпеки. Так, у всьому офісі лінії електромережі забезпечені від виникнення короткого замикання, а також від перепадів мережевої напруги, що може спричинити збої в роботі електронно-обчислювальної техніки. Приміщення (окрім тих, де розташовуються сервери) оснащуються системою автоматичної пожежної сигналізації та вогнегасниками. Під час монтажу та експлуатації ліній електромережі необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією і, за можливості, застосовувати негорючу ізоляцію.

Найбільш повним нормативним документом щодо забезпечення охорони праці користувачів ПК є «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами (ВДТ) електронно-обчислювальних машин» ДСанПіН 3.3.2.007-98.

Значне місце у профілактиці розладів здоров'я належить психології праці. Тому заходи, пов'язані з формуванням раціональних виробничих колективів, у яких відсутня психологічна несумісність, сприяють зменшенню нервово-психічного перенапруження, підвищенню працездатності та ефективності праці.

Особливої значущості у користувачів відеодисплейних терміналів набуває психоемоційний стрес, який більшою або меншою мірою проявляється у кожного з них. Тому заходи щодо охорони праці користувачів ПК спрямовані на усунення та попередження наслідків синдрому комп'ютерного стресу.

Площа, відведена на одне робоче місце має становити не менше 6 $м^2$, а об'єм – не менше 20 $м^3$. Конструкція робочого місця повинна забезпечувати підтримання оптимальної робочої пози (тобто такої, яка дозволяє працівникові виконувати роботу з мінімальним напруженням тіла, і яка дозволяє уникнути перевтоми в ході і після закінчення робочого процесу). Раціональна робоча поза має важливе значення для збереження здоров'я працівника, оскільки тривале перебування його в незручній і напруженій позі може призвести до таких захворювань, як сколіоз (викривлення хребта), варикозне розширення вен, плоскостопість тощо. Установлено, що робота в зігнутому положенні збільшує затрати енергії на 20%, а при значному нахиленні − на 45% порівняно з прямим положенням корпуса.

За потреби особливої концентрації уваги під час робіт суміжні робочі місця операторів відділяти одне від одного перегородками висотою 1,5-2 м.

Для виключення впливу підвищених рівнів електромагнітних випромінювань відстань між екраном монітора і працівником облаштовуємо не менше 500 мм (оптимально - 600 - 700 мм).

При роботі з ПК забезпечуємо доступ працівників до первинних засобів пожежогасіння, аптечки першої медичної допомоги. Тривалість безперервної роботи з ПК без регламентованого перерви не повинна перевищувати 2 годин.

При 8-годинній робочій зміні і роботі з ПК регламентовані перерви встановлюємо:

- для I категорії робіт через 2 години від початку робочої зміни і через 2 години після обідньої перерви тривалістю 15 хвилин кожен;

- для II категорії робіт через 2 години від початку робочої зміни і через 1,5 - 2 години після обідньої перерви тривалістю 15 хвилин кожен або тривалістю 10 хвилин через кожну годину роботи;

- для III категорії робіт через 1,5 - 2 години від початку робочої зміни і через 1,5 - 2 години після обідньої перерви.

Під час регламентованих перерв для зниження нервово-емоційного напруження, стомлення зорового аналізатора, поліпшення функціонального стану нервової, серцево-судинної, дихальної систем, а також м'язів плечового пояса, рук, спини, шиї і ніг доцільно виконувати комплекси вправ.

Працівникам з високим рівнем напруженості праці під час регламентованих перерв і наприкінці робочого дня показано психологічне розвантаження у спеціально обладнаних кімнатах психологічного розвантаження. З метою зменшення негативного впливу монотонності необхідно застосовувати чергування операцій. Робочий стіл з урахуванням характеру виконуваної роботи повинен мати достатній розмір для раціонального розміщення монітора (дисплея), клавіатури, іншого використовуваного обладнання та документів, поверхню, що володіє низькою відображає. Щоб забезпечувалося зручність зорового спостереження, швидке і точне зчитування інформації, площину екрана монітора розташовуємо нижче рівня очей працівника переважно перпендикулярно до нормальної лінії погляду працівника (нормальна лінія погляду – 15% вниз від горизонталі).

ВИСНОВКИ

Кваліфікаційна робота націлена на впровадження ефективних методів захисту від кібератак на хмарні сервіси AWS. Одним із головних аспектів роботи є впровадження та конфігурація захисних механізмів, які будуть забезпечувати безпеку та захищати дані клієнтів, що зберігаються в хмарних сервісах.

Одним з можливих методів захисту є використання фаєрволів та мережевих механізмів. Фаєрволи дозволяють контролювати трафік, який виходить та входить до хмарних сервісів, тим самим забезпечуючи фільтрацію та блокування небажаного трафіку. Додатково, можна налаштувати правила доступу, що дозволяють обмежити комунікацію до конкретних ресурсів або сервісів в межах хмарного сервісу.

Шифрування даних є ще одним важливим аспектом захисту від кібератак. Використання шифрування дозволяє захистити дані в хмарних сервісах, навіть якщо зловмисники отримають несанкціонований доступ до цих даних. AWS пропонує різні можливості для шифрування даних на різних рівнях, включаючи транзитне шифрування та шифрування даних в спокої. Впровадження та налагодження правильної стратегії шифрування є важливим кроком у забезпеченні безпеки даних в хмарному середовищі.

Моніторинг та аналіз безпеки є необхідними для ефективного виявлення потенційних загроз та кібератак. AWS пропонує різні інструменти та служби для моніторингу та аналізу безпеки, такі як AWS CloudTrail, AWS CloudWatch та Amazon GuardDuty. Ці інструменти дозволяють виявляти підозрілу активність, реагувати на загрози в реальному часі та вживати необхідні заходи для захисту від кібератак.

Крім того, важливо розглянути питання фізичної безпеки та доступу до хмарних сервісів. AWS забезпечує фізичну безпеку своїх дата-центрів та

інфраструктури, забезпечуючи контрольований доступ та захист фізичного середовища, де знаходяться сервери та обладнання.

У роботі також будуть розглянуті методи та практики резервного копіювання та відновлення даних, аутентифікації та авторизації, а також інші аспекти безпеки, які варто враховувати при використанні хмарних сервісів AWS.

В результаті дослідження та розробки ефективних методів захисту від кібератак на хмарні сервіси AWS, ця кваліфікаційна робота сприятиме покращенню безпеки використання хмарних ресурсів та допоможе організаціям захистити свої дані від потенційних загроз.

Окрім вищезазначених аспектів безпеки, важливим кроком у захисті від кібератак на хмарні сервіси AWS є регулярне оновлення та патчінг програмного забезпечення. AWS забезпечує оновлення своїх сервісів та інфраструктури для усунення вразливостей та виправлення помилок. Важливо встановлювати оновлення та патчі якомога швидше, щоб уникнути використання вразливостей зловмисниками.

При впровадженні захисних механізмів важливо також враховувати принцип найменшого привілею (principle of least privilege). Цей принцип передбачає надання користувачам лише тих привілеїв та доступу, які є необхідними для виконання їхніх обов'язків. Це допоможе уникнути надлишкових привілеїв та зменшить можливість зловживання користувачами або зловмисниками.

Для підвищення безпеки використання хмарних сервісів AWS рекомендується також використовувати механізми багатофакторної аутентифікації. Це дозволяє додатково перевірити ідентифічність користувача шляхом використання додаткових методів, таких як одноразові паролі, біометричні дані або фізичні пристрої. Такий підхід ускладнює процес несанкціонованого доступу до облікових записів та знижує ризик компрометації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Побудова iaas з amazon web servises – BC solutions LLC. BC Solutions LLC – Business Continuity and Disaster Recovery Solutions. URL: https://bcsolutions.com.ua/services/aws/. (Дата звернення: 20.04.2023)

2. Принципи проектування інфраструктури на amazon web services. На головну. URL: https://naukam.triada.in.ua/index.php/konferentsiji/52-dvadtsyat-druga-vseukrajinska-praktichno-piznavalna-internet-konferentsiya/524-printsipi-proektuvannya-infrastrukturi-na-amazon-web-services. (Дата звернення: 20.04.2023)

3. Хмарна платформа Amazon Web Services. Apix-Drive. URL: https://apix-drive.com/ua/blog/reviews/amazon-web-services. (Дата звернення: 20.04.2023)

4. Amazon elastic compute cloud (EC2). ESKA. URL: https://eska.global/products/amazon-ec2. (Дата звернення: 20.04.2023)

5. Anthony A. Mastering AWS Security: Create and maintain a secure cloud ecosystem. Packt Publishing, 2017.

6. AWS DevOps: як це працює і яку користь може принести вашому ПЗ. Створення та розробка сайтів на Drupal та WordPress– Internetdevels. URL: https://internetdevels.ua/blog/introduction-to-devops-on-aws. (Дата звернення: 20.04.2023)

7. AWS for solutions architects / A. Shrivastava et al. 2nd ed. Packt Publishing, 2013.

8. AWS: VPC flow logs – знайомство та аналітика з cloudwatch logs insights. RTFM: Linux, DevOps та системне адміністрування | DevOps-інжиніринг та системне адміністрування. Випадки з практики. URL: https://rtfm.co.ua/aws-vpc-flow-logs-znajomstvo-ta-priklad-analitiki-z-cloudwatch-logs-insights/. (Дата звернення: 20.04.2023)

9. Bacon M. What is AWS CloudTrail? | Definition from TechTarget. Security. URL: https://www.techtarget.com/searchsecurity/definition/AWS-CloudTrail. (Дата звернення: 20.04.2023)

10. Culkin J., Zazon M. AWS cookbook. O'Reilly Media, Incorporated, 2021.

11. Felsen N. Effective DevOps with AWS: ship faster, scale better, and deliver incredible productivity. Packt Publishing, 2017.

12. Global infrastructure. Amazon Web Services, Inc. URL: https://aws.amazon.com/about-aws/global-infrastructure/.

13. King T. H. Aws: the ultimate guide from beginners to advanced for the amazon web services. Independently Published, 2019.

14. Koston M. Aws: amazon web services, the ultimate guide for beginners to advanced. Independently Published, 2020.

15. Lakhera P. AWS for System Administrators: Build, automate, and manage your infrastructure on the most popular cloud platform – AWS. Packt Publishing, 2021.

16. Mishra A. Machine learning in the AWS cloud: add intelligence to applications with AWS sagemaker and AWS rekognition. Wiley & Sons, Incorporated, John, 2019.

17. Raje G. Security and microservice architecture on AWS. O'Reilly Media, Incorporated, 2021.

18. Shields D. AWS security. Manning Publications Co. LLC, 2022.

19. Simplilearn. AWS full course 2022 | AWS tutorial for beginners 2022 | AWS training for beginners | simplilearn, 2022. YouTube. URL: https://www.youtube.com/watch?v=ZB5ONbD_SMY. (Дата звернення: 20.04.2023)

20. Swaraj N. Accelerating devsecops on AWS: create secure CI/CD pipelines using chaos and aiops. Packt Publishing, Limited, 2022.

21. What is AWS. Amazon Web Services, Inc. URL: https://aws.amazon.com/what-is-aws/?nc1=h_ls. (Дата звернення: 20.04.2023)

22. What is AWS RDS?. W3Schools Online Web Tutorials. URL: https://www.w3schools.com/whatis/whatis_aws_rds.asp. (Дата звернення: 20.04.2023)

23. Why your organization needs AWS security hub. Infopulse. URL: https://www.infopulse.com/blog/why-use-aws-security-hub. (Дата звернення: 20.04.2023)

24. Wilkins M. AWS certified solutions architect - associate (SAA-C02) cert guide. Pearson Education, Limited, 2021.

25. Young M. Implementing cloud design patterns for AWS. Packt Publishing, Limited, 2015.